SecureTrack

User's Guide

R21-3 HF6

TufinOS 3.100

tufin

The Security Policy Company.

Table of Contents

SecureTrack Overview

The Tufin Orchestration Suite™ intelligently analyzes the network, automates configuration changes and proactively maintains security and compliance across the entire enterprise network. By improving network security processes, organizations using the Tufin Orchestration Suite will have a positive impact on the entire business by reducing the time and cost to implement changes by 80 percent. An essential component of the Tufin Orchestration Suite, SecureTrack provides central management across a wide variety of devices along with the network intelligence and security analysis technologies that are the foundation for network security change automation.

SecureTrack is the foundation of the Tufin Orchestration Suite which accelerates service delivery, improves efficiency and ensures security – while facilitating communication throughout the organization. SecureTrack makes it possible to manage all of your network-layer, next-generation and IPv6 firewalls as well as network security infrastructure - including routers, switches, load balancers and more - from a central platform.

In addition to SecureTrack, TOS includes:

- **SecureApp™** - An automated solution that enables organizations to easily define, update, monitor and remove applications and services from the network. By providing detailed insight into an application’s connectivity needs and status, SecureApp helps to accelerate service deployment, assure business continuity and simplify network operations.
- **SecureChange**® - A comprehensive solution for automating network configuration changes to firewalls and routers. SecureChange enables organizations to dramatically improve their network change process with an automated solution for designing, provisioning and verifying security configuration changes, so you can make accurate changes up to five times faster.

This chapter provides an overview of SecureTrack's capabilities and user structure.

SecureTrack Capabilities

SecureTrack™ is a comprehensive management solution for firewalls and additional network devices. Today’s enterprise networks are complex and diverse, including thousands of firewalls, routers, switches and load-balancers from multiple vendors. Because of frequent changes required by networked enterprise applications, device configurations need to be constantly modified, and have grown increasingly large and complex.

SecureTrack provides security and network engineers the visibility and insight to ensure that security policies are optimized to enable business while meeting the most stringent security and compliance requirements. It enables you to track and analyze network device configurations, optimize and recertify firewall rules, design changes, and ensure continuous compliance across the network. Thanks to powerful automation capabilities, customers report that SecureTrack cuts the cost of firewall operations in half.

SecureChange Basic

SecureTrack also includes SecureChange Basic. **SecureChange Basic** is the version of SecureChange that is included when you purchase SecureTrack. SecureChange Basic lets you use the pre-defined workflows to manage network requests for your organization with all of the SecureChange features, except workflow customization. All other workflows and the SecureChange provisioning capabilities are only available for fully licensed SecureChange users.

When you purchase **SecureChange** and install the license, you can customize the workflows to match the processes that your organization uses to handle network requests, including conditional workflows and automatic actions.

Device Monitoring

TOS Classic monitors the various components of your network and security infrastructure, and provides tracking, analysis, and reporting tools for the received policy revisions for any monitored device. You can manage TOS Classic from any PC that has HTTPS access to TOS Classic's web interface.

For increased scalability, TOS Classic's Distributed Architecture enables multiple TOS Classic servers to perform device monitoring and processing. Each distributed component can receive revisions and traffic logs. All management, revision viewing, and reporting is done on the TOS Classic central server.

TOS Classic uses a few different technologies to monitor each vendor's devices:

- **Cisco, Fortinet, and Juniper**: By default, TOS Classic uses periodic polling where TOS Classic connects to each firewall or network device using SSH according to a configurable frequency (by default, 5 minutes) and retrieves its configuration. In addition, TOS Classic can be configured as a Syslog server for the monitored devices to provide real-time monitoring.
- **Palo Alto Networks**: TOS Classic connects to each firewall or network device via the REST API, according to a configurable frequency (by default, 5 minutes) and retrieves its configuration.
- **Check Point**: TOS Classic uses Check Point OPSEC™ (Open Platform for Security) to track all the changes made by administrators to Check Point management servers (CMAs, Provider-1 MDSs, and SmartCenters). Whenever an administrator saves or installs a policy, TOS Classic is immediately notified of the change. A secure OPSEC connection is then used to retrieve the new security policy. When a Check Point management server contains multiple Policy Packages, TOS Classic records all packages with each revision.

- **Check Point Security Gateway OS**: For Security Gateway OS Monitoring, TOS Classic also directly monitors the operating system of Check Point gateways. TOS Classic polls each gateway with SNMP according to a configurable frequency and retrieves configuration and performance data. OS monitoring requires a separate license.

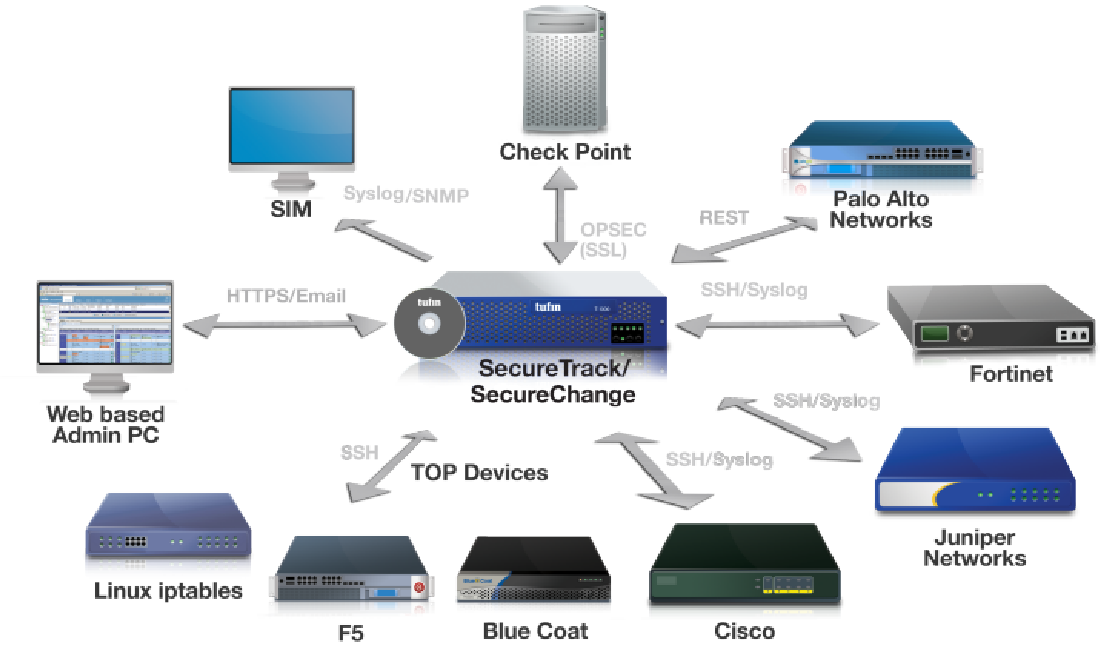
Automatic Revisions: For devices monitored in real-time, if no revisions for a monitored device are received within a configurable frequency, TOS Classic also performs automatic, scheduled fetches of the device's database. If any changes are found, TOS Classic records a new revision, defined as an Automatic Revision. This enables policy change coverage for changes that were implemented when TOS Classic was not monitoring devices (for example, before device monitoring was set up), and for direct changes such as via cpconfig for Check Point management servers. The default automatic fetch frequency is 60 minutes.

Device monitoring occurs seamlessly and automatically, without user intervention. Whenever TOS Classic discovers changes made to the policy, TOS Classic records a new revision of the policy. The configuration is parsed, analyzed and stored in TOS Classic's database. TOS Classic uses this information to generate scheduled and on-event reports, and several types of real-time change notifications:

- Email reports with configurable levels of detail, to registered TOS Classic administrators
- Syslog messages to a Syslog server, with details about the changes made
- SNMP traps to registered applications, with details about the changes made

TOS Classic's policy change notifications supply real-time policy change tracking and integration with external security management frameworks (for example: SIM and SOC).

TOS Classic includes a watchdog mechanism, which ensures that the TOS Classic processes are up and running at all times. This diagram illustrates the interactions between the TOS Classic server and other devices in the security policy management process.



Working with SecureTrack

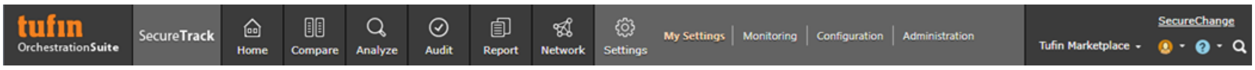
Before you log in, make sure you have:

- **Operating System:** Microsoft Windows 10 or higher
- **Screen resolution:** 1280x800 or higher

- **Browser:** Microsoft Edge, Mozilla Firefox, Google Chrome

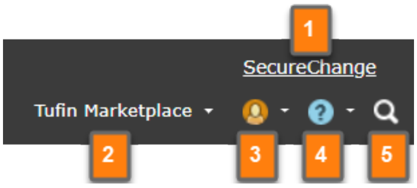
> Microsoft Internet Explorer (IE) is no longer supported by this TOS release

SecureTrack contains a number of views, accessed from the main tabs at the top of the SecureTrack screen:



When you first login, you see the **Home** or Dashboard view. You can configure the initial view and other personal preferences in **Settings** > **My Settings** > **Display Options**.

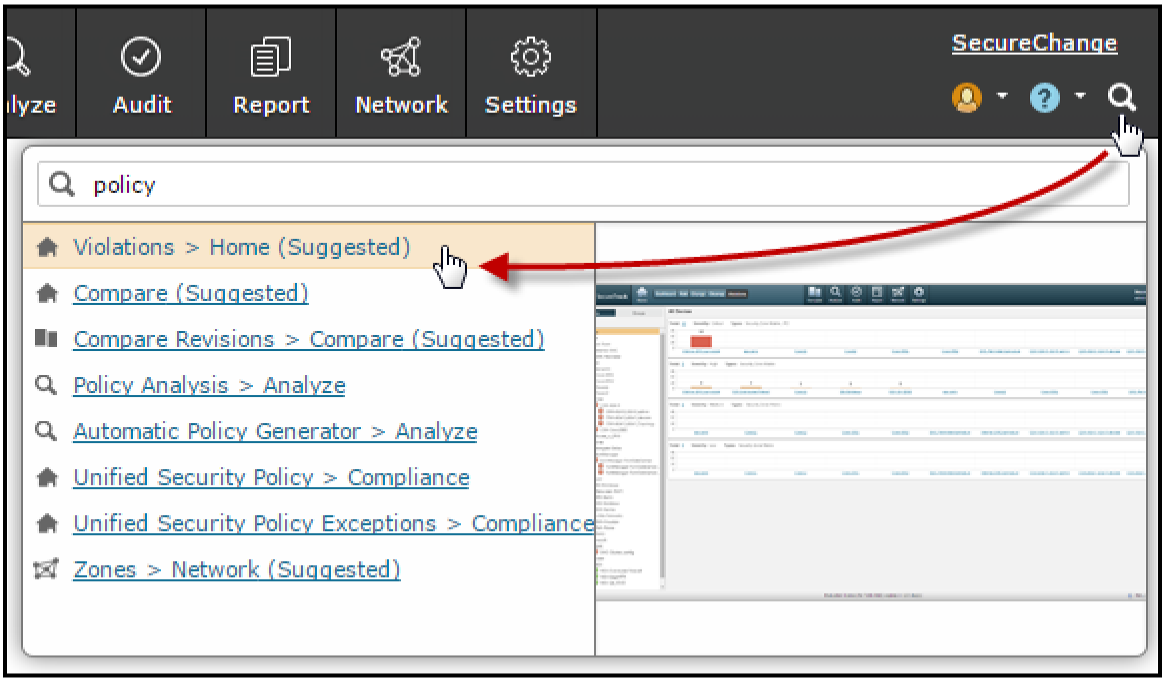
In the top-right corner of SecureTrack you can:



1. Go to the SecureChange login screen.
2. Go to:
   - The Tufin Marketplace
   - The SecureTrack Reporting Essentials login page
   - The Vulnerability Mitigation App login page
   - If the apps are not installed, you will be redirected to the Tufin Marketplace
3. **Logout** from SecureTrack.
4. View the following:
   - **What can I do on this page?** - Opens context-sensitive help from the Tufin Knowledge Center. From the Knowledge Center you can view and search additional TOS topics, including API documentation and technical notes.

     If you do not have an internet connection, the link opens context-sensitive help from the local server. The local help files contain the same content as the User Guide.
   - **API Documentation** - Opens the REST API documentation.
   - **Tufin Academy Online Training** - Opens the Tufin Academy, where you can take online courses based on your role and expertise.
   - **Version** number and **Build** number
5. Search for features in SecureTrack - You can enter text in the search box and press Enter to get suggestions of SecureTrack features that are related to the text. For example, a search for "policy" returns results with the word "policy" (for example, Policy Analysis) and results that are related to policies (for example, Home > Violations).

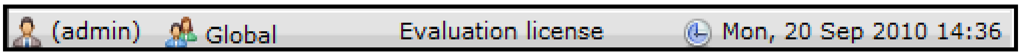
You can see a thumbnail of the feature and click on the feature to go to it in SecureTrack.



policy

Violations > Home (Suggested)
Compare (Suggested)
Compare Revisions > Compare (Suggested)
Policy Analysis > Analyze
Automatic Policy Generator > Analyze
Unified Security Policy > Compliance
Unified Security Policy Exceptions > Compliance
Zones > Network (Suggested)

At the bottom of SecureTrack is a status bar that shows:



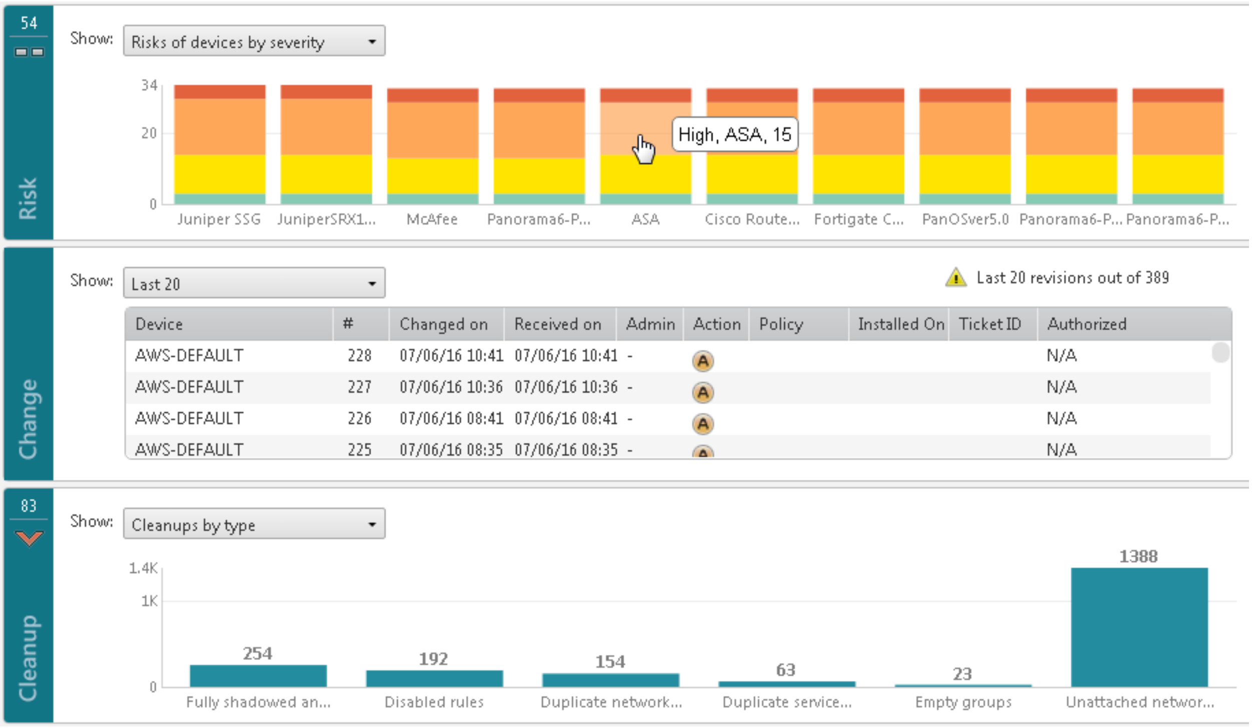
(admin) Global Evaluation license Mon, 20 Sep 2010 14:36

- The name of the user that is logged-in
- In a Multi-Domain environment, the active context
- License status
- The current date and time on the SecureTrack server host

Dashboard View

The Dashboard view provides an overview of all security risks, configuration changes, and optimization opportunities in your network security devices.

SecureTrack analyzes common security risks in the network and misconfigurations in complex rulebases in order to prevent security breaches. SecureTrack enables the administrator to optimize device configurations and improve the visibility of network changes to support business continuity.



Device	#	Changed on	Received on	Admin	Action	Policy	Installed On	Ticket ID	Authorized
AWS-DEFAULT	228	07/06/16 10:41	07/06/16 10:41	-	A				N/A
AWS-DEFAULT	227	07/06/16 10:36	07/06/16 10:36	-	A				N/A
AWS-DEFAULT	226	07/06/16 08:41	07/06/16 08:41	-	A				N/A
AWS-DEFAULT	225	07/06/16 08:35	07/06/16 08:35	-	A				N/A

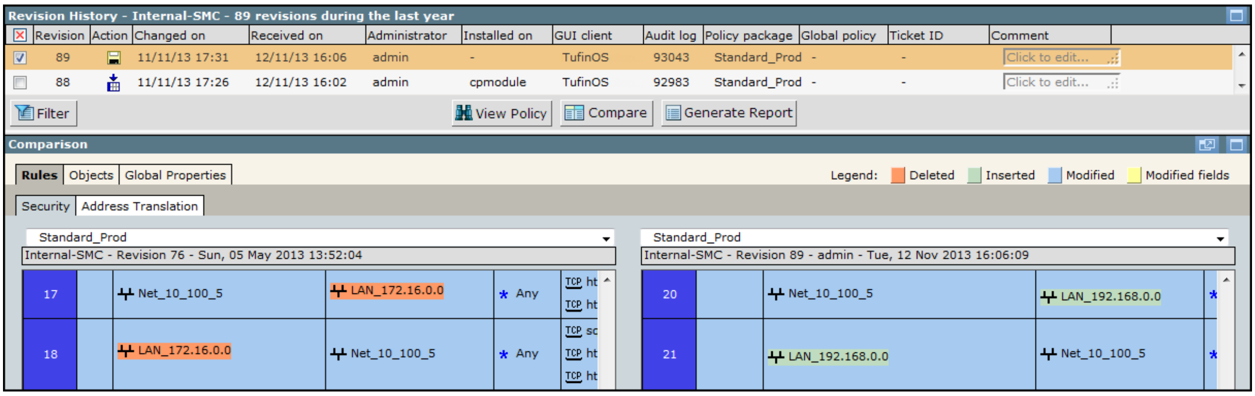
Here you can identify the actions you can take to improve security posture of your organization, including:

- Remediation of security risks in device policies
- Correlating policy changes with authorized change requests
- Reducing the number of unnecessary rules and objects in device policies

Compare View

In the Compare view, SecureTrack monitors device configuration changes and maintains an audit trail showing you who changed what, when, and how, across the entire network.

SecureTrack's change tracking is event-driven to assure complete accuracy and accountability. By comparing policy revisions, you can identify device configuration changes and get an up-to-date picture of your security posture.


Revision History - Internal-SMC - 89 revisions during the last year

☒	Revision	Action	Changed on	Received on	Administrator	Installed on	GUI client	Audit log	Policy package	Global policy	Ticket ID	Comment
☑	89		11/11/13 17:31	12/11/13 16:06	admin	-	TufinOS	93043	Standard_Prod	-	-	Click to edit...
□	88		11/11/13 17:26	12/11/13 16:02	admin	cpmodule	TufinOS	92983	Standard_Prod	-	-	Click to edit...

Internal-SMC - Revision 76 - Sun, 05 May 2013 13:52:04

17		Net_10_100_5	LAN_172.16.0.0	Any	TCP ht TCP ht
18		LAN_172.16.0.0	Net_10_100_5	Any	TCP sc TCP ht TCP ht

Internal-SMC - Revision 89 - admin - Tue, 12 Nov 2013 16:06:09

20		Net_10_100_5	LAN_192.168.0.0	*
21		LAN_192.168.0.0	Net_10_100_5	*

Here you can track the changes to your firewall policies, including:

- Status of the connection between SecureTrack and the relevant device
- Who changed the policy and when they made the change
- View the rules in the policy in graphical or textual format
- Compare all rules and objects in the policy between two policy revisions
- Export of a revision or comparison as a PDF file

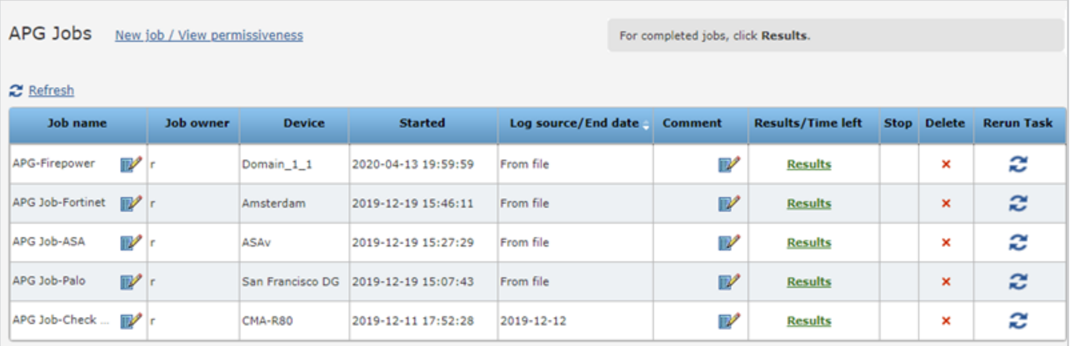
Analyze View

In the Analyze view, you can leverage the data collected from your policy revisions to better understand how traffic actually traverses the network. You can also find network and service objects in use throughout your network security infrastructure and see the objects that do not meet your organizational standards.

Based on the actual traffic passing through the devices, SecureTrack can simplify your policies to match the permissiveness level that you need. You can even install a clean firewall device and create a policy from scratch based on real network traffic.

Here you can analyze firewall policies, including:

- Troubleshoot connectivity problems and simulating planned network changes
- Instant rule and object lookup across large networks and multiple device vendors
- Analyze rules and assign a permissiveness score to define a more granular set of rules that tightens up your security policy while ensuring business continuity.



APG Jobs New job / View permissiveness

For completed jobs, click **Results**.

⟳ Refresh

Job name	Job owner	Device	Started	Log source/End date	Comment	Results/Time left	Stop	Delete	Rerun Task
APG-Firepower	r	Domain_1_1	2020-04-13 19:59:59	From file		Results		×	⟳
APG Job-Fortinet	r	Amsterdam	2019-12-19 15:46:11	From file		Results		×	⟳
APG Job-ASA	r	ASAv	2019-12-19 15:27:29	From file		Results		×	⟳
APG Job-Palo	r	San Francisco DG	2019-12-19 15:07:43	From file		Results		×	⟳
APG Job-Check ...	r	CMA-R80	2019-12-11 17:52:28	2019-12-12		Results		×	⟳

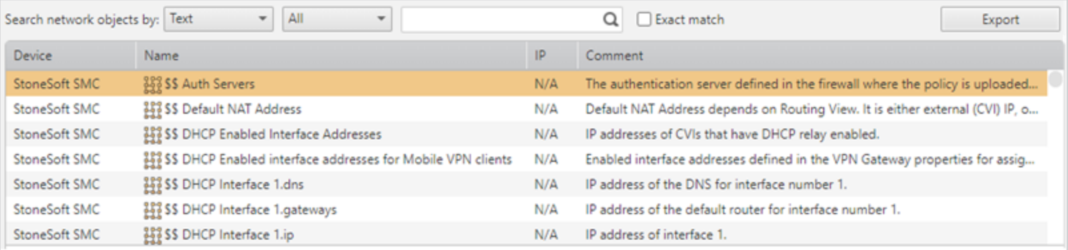
APG Jobs tab in Analyze View

Audit View

In the Audit view, SecureTrack enables Continuous Compliance with real-time monitoring, assessment and alerts about security and compliance risks. SecureTrack rapidly generates a variety of configurable audit reports that support compliance with standards such as PCI DSS, SOX, ISO 17799, NERC and Basel II. It also features industry and vendor best practice audits such as the Cisco Device Configuration Report which is based on CIS guidelines.

Here you can see the areas of your device policies that cause violations of your enterprise standards or external regulations, including:

- Common industry best practices
- PCI-DSS and SOX governmental regulations
- Documentation of all rules in your policies



Search network objects by: Text ▾ All ▾ □ Exact match

Device	Name	IP	Comment
StoneSoft SMC	$$ Auth Servers	N/A	The authentication server defined in the firewall where the policy is uploaded...
StoneSoft SMC	$$ Default NAT Address	N/A	Default NAT Address depends on Routing View. It is either external (CVI) IP, o...
StoneSoft SMC	$$ DHCP Enabled Interface Addresses	N/A	IP addresses of CVIs that have DHCP relay enabled.
StoneSoft SMC	$$ DHCP Enabled interface addresses for Mobile VPN clients	N/A	Enabled interface addresses defined in the VPN Gateway properties for assig...
StoneSoft SMC	$$ DHCP Interface 1.dns	N/A	IP address of the DNS for interface number 1.
StoneSoft SMC	$$ DHCP Interface 1.gateways	N/A	IP address of the default router for interface number 1.
StoneSoft SMC	$$ DHCP Interface 1.ip	N/A	IP address of interface 1.

USP Security Policy Tab in Audit View

Report View

In the Report view, you can leverage all of the data collected by SecureTrack to present the activities that impact your network infrastructure to any interested party. Reports are created on-demand, on a schedule or on-event and can be saved in the repository or sent by email. This helps you make sure that the right information gets to the right people at the right time.

Reports available include:

- Policy change reports on new revisions and specific rule or object changes
- Rule recertification reports on rule expiration

- Rule or object usage showing you the most unused rules and objects
- Security risk reports on specific configuration aspects that you define as risky or cirtical to your business processes
- Compliance reports on compliance with best practices or governmental regulations and documentation of the purpose of each rule
- Traffic simulation reports that analyze the way specific traffic is handled by your security infrastructure

Network View

In the Network view, SecureTrack uses Topology Intelligence to automatically build a map of all of the devices, subnets and zones on the network. This map provides comprehensive visibility into access paths between any source and destination, and provides security teams the visibility required to rapidly understand and manage configuration changes.

The network zones and topology intelligence is used by other components in the TOS, including:

- SecureTrack policy analysis, compliance policies, and PCI DSS reporting
- SecureChange risk analysis and policy change designer
- SecureApp connection status and analysis

Settings View

In the Settings view, you can control all of the SecureTrack system configuration. The **My Settings** tab contains user-specific interface preferences. The other tabs control other functions of SecureTrack, including:

- Device monitoring - Adding devices to monitor and organizing the devices into groups and domains
- Feature configuration - Settings that govern:
  - Local or external authentication of SecureTrack users
  - Methods for sending notifications from SecureTrack
  - Correlation of policy changes to requests made in a ticketing system
  - Handling of risk, cleanup and regulation results
- System administration - License management and auditing of all actions taken in SecureTrack

Secure Track Features by Vendor

These TOS Classic features are supported for monitorable devices:

- Amazon
- Check Point
- Cisco
- F5
- Forcepoint (formerly McAfee Stonesoft SMC)
- Fortinet
- Juniper
- Microsoft Azure
- Open Stack
- Palo Alto Networks
- VMware NSX

Amazon

AWS

Dashboard and Browsers	**Change Tracking** **Policy Analysis** **Risk** **Dashboard** **Violations** **Cleanup**
Change Management	**Change Management** **Graphical Policy** **Real-time Monitoring** **Create SecureChange ticket from Policy Browser for:** **• Rule Decommission** **• Rule Recertification**
Policy Analysis	**Policy Analysis** **Object Lookup**
Auditing and Reporting	**Auditing and Reporting**
Topology	**Static Topology** **VPC Peering** **Transit Gateway**

Notes for Amazon devices:

- Real-time monitoring uses device polling.
  - PCI results do not include these tests: 1.1.5, 1.1.7, 1.3.4, 2.2.4.
    To pass PCI DSS tests that require rule comments or ticket IDs, add the comments and ticket IDs in Policy Browser (formerly Rule Documentation).
  - Dashboard support does not include Risk and Cleanup.
  - Auditing support does not include Compliance Policies and Unified Security Policy.

- Topology path calculation simulates traffic if there is no more than one dynamic connection, but as many static connections as necessary.
  Supported configurations are internal VPC connectivity and connectivity between VPC and the data center.
- In Compare, nested SGs of peered VPCs are shown as empty groups in rule source and destination. Also, no calculations are made for those rules.
  Users may look at the SG origin VPC for more details.

Check Point

Firewalls (Gateways, VE, VSX, Edge)

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Cleanup Violations
Change Management	Rule and Object Usage Report Change Management Full Accountability Display IPv6 objects Graphical Policy Real-time Monitoring Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Modification • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Policy Analysis Object Lookup
Auditing and Reporting	Expired Rules Report Auditing and Reporting
Topology	Calculate impact of NAT rules Static Topology Dynamic Topology Calculate impact of VPN policies

Notes for Edge and Gateways:

- Supports change management and rule usage when managed by a SmartCenter/Provider-1, but supports only change management when managed by LSM.

VSX notes:

- Supports all features except OS-level monitoring for VSX hosts or VSX gateways.
- Supports Vsys WARP interfaces in topology calculations.

Management Devices (CMA, Smart Center)

Dashboard and Browsers	Policy Analysis Risk Changes Dashboard Cleanup Violations

Change Management	Rule and Object Usage Report Change Management Full Accountability Display IPv6 objects Graphical Policy Change Window Real-time Monitoring Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Modification
Policy Analysis	Automatic Policy Generation (APG) Policy Analysis Object Lookup
Auditing and Reporting	Expired Rules Report Auditing and Reporting
Topology	Static Topology Dynamic Topology Calculate impact of NAT rules Calculate impact of VPN policies IPv6 routes Path analysis with IPv6 addresses in source and destination

Notes for CMA and R80:

- The Baseline Settings Compliance report is deprecated for Check Point R80.
- R80 unattached network object does not recognized host in opsec.
- Inline layers are supported for R80 gateways.
- Partial support of Check Point CloudGuard integration with Azure (Supporting Check Point R80 and above)
- After an upgrade, the revision may appear as modified in Compare Revisions:
  - Section headers may be shown as deleted and added
  - The revision shows legacy user access as a modified field on the revision although no change was done
  - Generate Report changes are not accurate
- Supports the Last Hit field for both security rules and NAT rules.

Management Devices (MDS)

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Cleanup Violations
Change Management	Rule and Object Usage Report Change Management Full Accountability Display IPv6 objects Graphical Policy Real-time Monitoring Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Modification • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Policy Analysis Object Lookup
Auditing and Reporting	Auditing and Reporting

	Expired Rules Report
Topology	**Static Topology** **Dynamic Topology** **Calculate impact of VPN policies**

Notes for MDS:

- Partial support of Check Point CloudGuard integration with Azure (Supporting Check Point R80 and above)
- Supports the Last Hit field for both security rules and NAT rules.

Cisco

ACI

Change Management	**Graphical Policy**
Policy Analysis	**Object Lookup**
Topology	**Static Topology** **Dynamic Topology**

Notes for ACI:

- For each Tenant, supports tracking, comparing, and generating reports on the changes to the following: Application profiles, contracts, consumers, providers, filters, EPGs, subnets.
- Supports Policy Browser, Object Lookup, comparing rules on ACI Tenant.
- Static Topology and Dynamic Topology is supported for East/West and North/South connectivity.
- Interactive map supports path queries to external IP addresses that travel via specific EPGs. In the query, the source and destination can include an IP address AND an EPG, and the query results will return paths that include both. For example: 1.1.1.1@EPG1
- OSPF and BGP routing is supported for Cisco ACI devices
- uEPG and Contract Master visibility is supported for revisions and topology retrieved from Cisco ACI Devices
- Limited support for IPv6 Objects

ASA

Dashboard and Browsers	**Change Tracking** **Policy Analysis** **Risk** **Dashboard** **Violations** **Cleanup**
Change Management	**Rule and Object Usage Report** **Change Management** **Graphical Policy** **Real-time Monitoring** **Full Accountability** **Display IPv6 objects** **Create SecureChange ticket from Policy Browser for:** **• Rule Decommission** **• Rule Modification** **• Rule Recertification**

Policy Analysis	**Automatic Policy Generation (APG)** **Policy Analysis** **Object Lookup**
Auditing and Reporting	**Auditing and Reporting**
Topology	**Static Topology** **Dynamic Topology** **Calculate impact of NAT rules** **Calculate impact of VPN policies**

Notes for ASA:

- ASA 9.5 support does not include SCTP.
- NAT rules are supported by ASA 8.3 or higher
- IPv6 Objects are supported by ASA 8.x or higher

Firepower Management Center

Dashboard and Browsers	**Change Tracking** **Policy Analysis** **Risk** **Dashboard** **Cleanup** **Violations**
Change Management	**Change Management** **Graphical Policy** **Real-time Monitoring** **Full Accountability** **Create SecureChange ticket from Policy Browser for:** **• Rule Decommission** **• Rule Modification** **• Rule Recertification**
Policy Analysis	**Object Lookup**
Auditing and Reporting	**Auditing and Reporting**
Topology	**Static Topology** **Dynamic Topology**

Notes for Firepower Management Center:

- Dashboard support includes Cleanup, however it does not support the cleanup of “Unused network objects".
- In the Interactive Map, Path Analysis calculations take Cisco Network Zones into account
- When dynamic topology is enabled for FMC devices:
  - Both static and dynamic routes are displayed in the Interactive Map.
  - Static routes are not shown as part of the revisions.
- When the Usage Tracking options are selected in the configuration of devices managed by the FMC:
  - Policy Browser displays the last time specific rules were hit
  - Automatic Policy Generation (APG) is supported
  - Rule and Object Usage Report is supported
  - Policies need to have unique names. If there are multiple policies that share the same name, rule hits will not be mapped correctly to these policies

IOS L3 Switch (IOS or IOS XE)

Dashboard and Browsers	**Change Tracking**

	Policy Analysis Risk Dashboard Violations Cleanup
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Full Accountability Display IPv6 objects Create SecureChange ticket from Policy Browser for: Rule Decommission Rule Recertification
Policy Analysis	Policy Analysis Object Lookup
Auditing and Reporting	Auditing and Reporting
Topology	Static Topology Dynamic Topology Calculate impact of VPN policies

IOS-XR

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Create SecureChange ticket from Policy Browser for: Rule Decommission Rule Recertification
Policy Analysis	Policy Analysis Object Lookup
Auditing and Reporting	Auditing and Reporting
Topology	Static Topology Dynamic Topology Display IPv6 objects Path analysis with IPv6 addresses in source and destination

Notes for IOS-XR:

- Change Management includes visibility on MPLS option B

Nexus

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup

Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Full Accountability Create SecureChange ticket from Policy Browser for: Rule Decommission Rule Recertification
Policy Analysis	Policy Analysis Object Lookup
Auditing and Reporting	Auditing and Reporting
Topology	Static Topology Dynamic Topology

Routers (IOS or IOS XE)

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Cleanup Violations
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Full Accountability Display IPv6 objects Create SecureChange ticket from Policy Browser for: Rule Decommission Rule Recertification
Policy Analysis	Policy Analysis Object Lookup
Auditing and Reporting	Auditing and Reporting Expired Rules Report
Topology	Static Topology Dynamic Topology Calculate impact of VPN policies Calculate impact of policy-based routing and related ACL rules

Notes for Routers

- Tufin supports policy-based routing (PBR) for Cisco IOS routers for the following configuration types, when the next hop in the route map is to a monitored device in the Tufin Orchestration Suite topology:
  - `set interface <interface name>`
  - `set ip next-hop <ip address>`
  - `set vrf <vrf name>`

Zone-based firewalls

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup

Change Management	Change Management Graphical Policy Real-time Monitoring Create SecureChange ticket from Policy Browser for: Rule Decommission Rule Recertification
Policy Analysis	Object Lookup
Auditing and Reporting	Auditing and Reporting
Topology	Static Topology Dynamic Topology

Notes for all Cisco devices

- Cisco Security Manager (CSM):
    - Supports change tracking in textual policy view only for ASA 8.x-9.x, Catalyst switch 3560, IOS router 2801 devices.

F5

BIG-IP

Change Management	Change Management Graphical Policy
Topology	Static Topology Calculate impact of NAT rules

Notes for BIG-IP

- Real-time monitoring uses device polling.
- Graphical policy shows virtual servers.
- Policy analysis queries show translation between virtual IP addresses and IP addresses of member servers.

Forcepoint (formerly Stonesoft)

Sidewinder (formerly Firewall Enterprise):

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup
Change Management	Change Management Graphical Policy Real-time Monitoring Display IPv6 objects

	•
Policy Analysis	**Policy Analysis** **Object Lookup**
Auditing and Reporting	**Auditing and Reporting**
Topology	**Static Topology** **Calculate impact of NAT rules**

Notes for Sidewinder

- Sidewinder devices and objects are not shown in SecureApp connection analysis or in SecureChange.

  8.3

SMC

Dashboard and Browsers	**Change Tracking** **Policy Analysis** **Risk** **Dashboard** **Violations** **Cleanup**
Change Management	
	Policy Analysis **Object Lookup**
Auditing and Reporting	**Auditing and Reporting**
Topology	**Calculate impact of NAT rules** **Static Topology** **Dynamic Topology**

Notes for SMC:

- These features are not supported: APG, dynamic topology information and NAT rule impact on topology.
- Dynamic topology only supports BGP protocol. Stonesoft 5.10 uses the 5.9 APIs

Notes for all Forcepoint devices:

- Real-time monitoring uses device polling.

Fortinet

FortiGate (standalone)

Dashboard and Browsers	**Change Tracking** **Policy Analysis** **Risk** **Dashboard** **Cleanup** **Violations**
Change Management	**Rule and Object Usage Report** **Change Management**

	Graphical Policy Real-time Monitoring Full Accountability Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Policy Analysis Object Lookup
Auditing and Reporting	Auditing and Reporting
Topology	Static Topology Dynamic Topology

FortiManager Advanced (managing FortiGate)

Advanced means device management mode in SecureTrack is **Advanced management**

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Cleanup Violations
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Full Accountability Display IPv6 objects, routes, and interfaces Change Window Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Modification • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Global configuration visibility Object Lookup
Auditing and Reporting	Auditing and Reporting
Topology	Static Topology Dynamic Topology IPv6 routes Path analysis with IPv6 addresses in source and destination Calculate impact of NAT (Policy NAT and Central NAT) rules

Notes for FortiManager Advanced (5.4 or higher):

- API for fetching dynamic topology is not supported for ADOM 5.2 and below.
- These features are not supported: Regulations report, Risks, Policy Analysis, dynamic objects (treated as static object with the "default" as its value)
- Support for “Collect dynamic topology information” feature, when dynamic addressing (DHCP) or routing protocols (OSPF and BGP) are in use.
- Support for Fortinet FortiManager Web Filters.
- For Fortinet FortiManager Global Rules that are assigned to ADOM policies, the following features are not supported:

  - Automatic Policy Generator (APG)
  - Last hit for rules in Policy Browser
  - Rule and object usage
- If you have IPv6 policies and upgrade to FortiManager 6.4 from an earlier version, all IPv6 policies will be deleted and recreated. In SecureTrack, it will appear as a diff in the Change Report.
- Destination NAT using Services as optional filters is not supported yet
- Source NAT is not supported for Fortimanagers 6.4 and below with Policy-based Policies that do not have the Central NAT Check box selected.
- Calculating the impact of Central NAT rules is supported for FortiManager 6.0.5 and above.
- Virtual routing and forwarding information is part of the firewall revision and is supported in the Topology Map.

FortiManager Basic (managing FortiGate)

Basic means device management mode in SecureTrack is **Basic firewalll management**.

Dashboard and Browsers	**Change Tracking** **Policy Analysis** **Risk** **Dashboard** **Cleanup** **Violations**
Change Management	**Change Management** **Graphical Policy** **Real-time Monitoring** **Full Accountability** **Display IPv6 objects** **Create SecureChange ticket from Policy Browser for:** **• Rule Decommission** **• Rule Recertification**
Policy Analysis	**Policy Analysis**
Auditing and Reporting	**Auditing and Reporting**
Topology	**Static Topology** **Calculate impact of NAT rules**

Notes for FortiManager Basic:

As of R19-3, creating new Fortinet FortiManager - Basic Mode devices is not supported. As of R22-1, retrieving new revisions is not supported. For details see Deprecated Devices

If you use FortiManager devices, we recommend using Advanced mode, which is still supported by Tufin

- Real-time monitoring uses device polling.
- For the policy packages on FortiManager: view and compare policies in graphical format, view the global object database, create New Revision and Advanced Change reports.
- To get full support for a device that is connected to FortiManager, add the managed device to SecureTrack monitoring directly.
- IPv6 objects are not supported.
- VIP, IP pool, and destination interface NAT are supported on Fortigate devices that are managed by FortiManager.
- Fortinet FortiManager workflow mode is not supported.

Juniper

JunOS M/MX

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Cleanup Violations
Change Management	Change Management Graphical Policy Real-time Monitoring Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Recertification
Policy Analysis	Policy Analysis Object Lookup
Auditing and Reporting	Auditing and Reporting Expired Rules Report
Topology	Static Topology Dynamic Topology Calculate impact of NAT rules Calculate impact of VPN policies

Notes for JunOS M/MX

- Accountability, Rule and Object Usage, IPv6 objects logical systems are not supported.
- Topology and dynamic topology (with MPLS L3 VPNs) are supported on standalone MX routers.

JunOS SRX

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Cleanup Violations
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Full Accountability Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Modification • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Policy Analysis Object Lookup
Auditing and Reporting	Expired Rules Report Auditing and Reporting
Topology	Static Topology Dynamic Topology Calculate impact of NAT rules Calculate impact of VPN policies Path analysis with IPv6 addresses in source and destination

Notes for JunOS SRX

- NAT rules and display of IPv6 objects are supported for directly-monitored SRX firewalls only.
- Topology supports routes with a VR as the next hop.

NetScreen

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Cleanup Violations
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Full Accountability Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Policy Analysis Object Lookup
Auditing and Reporting	Expired Rules Report Auditing and Reporting
Topology	Static Topology Dynamic Topology Calculate impact of NAT rules Calculate impact of VPN policies

NSM

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Cleanup Violations
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Full Accountability Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Policy Analysis Object Lookup
Auditing and Reporting	Expired Rules Report Auditing and Reporting
Topology	Static Topology Dynamic Topology Calculate impact of NAT rules Calculate impact of VPN policies

Notes for NSM

- Real-time monitoring uses device polling.
- Only these reports are supported for managed devices: Best Practices, Compliance Policies, Policy Analysis, Rule Documentation and Recertification, Rule and Object Usage, and Firewall Module Change.
- The Firewall Module Change report can only be used to report on Juniper devices connected to a monitored NSM Central Manager. To get full support for a device that is connected to NSM, add the managed device to SecureTrack monitoring directly.

Notes for all Juniper devices

- IPv6 objects display is not supported.
- Routing information is not collected from virtual routers; Support the Expired Rules report.
- ISG series:
  - Vsys devices when managed by Juniper NSM can be included in rule usage report, APG, and unused objects cleanup.
  - Rule usage is supported only when syslogs are sent from NSM.

Microsoft Azure

Azure Resource Manager

Dashboard and Browsers	**Change Tracking** **Policy Analysis** **Risk** **Dashboard** **Cleanup** **Violations**
Change Management	**Change Management** **Graphical Policy** **Create SecureChange ticket from Policy Browser for:** **• Rule Decommission** **• Rule Recertification**
Policy Analysis	**Object Lookup**
Auditing and Reporting	**Auditing and Reporting**
Topology	**Dynamic Topology** **Calculate impact of NSGs** **Connectivity between VNets** **ExpressRoute** **VNet peering**

Supported Devices

The following devices are supported on Microsoft Azure:

Fortinet

FortiManager
FortiGate

Check Point

Management Devices (MDS) CloudGuard Network Security - Firewall & Threat Prevention
Checkpoint Gateway with dynamic routes

Palo Alto

Panorama

Notes for Azure Resource Manager

- Azure Resource Manager is the supported device type.
- PCI DSS compliance is not currently supported.
- Azure Classic (Azure Service Management API): Support for this device has reached its "end of life" (EOL).
- Partial support of Check Point CloudGuard integration with Azure (Supporting Check Point R80 and above)

Open Stack

Open Stack

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup
Change Management	Change Management Graphical Policy Real-time Monitoring Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Recertification
Policy Analysis	Object Lookup
Auditing and Reporting	Auditing and Reporting

Notes for Open Stack:

- Real-time monitoring uses device polling.
- Only these reports are supported: Advanced Change, Object Change, Rule Change, Policy Browser (formerly Rule Documentation).
- Policy Browser does not include data for the violation, shadowing status, action and last hit columns.
- For Object Lookup, to see the objects in a VM instance in the search results you must show results for "Objects and Related Groups".
- Dashboard support does not include Risk and Cleanup.
- Auditing support does not include PCI DSS, Compliance Policies and Unified Security Policy.

Palo Alto Networks

Panorama Advanced (managing PanOS)

Advanced means device management mode in SecureTrack is **Advanced management**

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Accountability - Saved Revisions Display IPv6 objects Change Window Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Modification • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Object Lookup
Auditing and Reporting	Expired Rules Report Auditing and Reporting
Topology	Static Topology Dynamic Topology Calculate impact of NAT rules Calculate impact of VPN policies

Notes for Panorama Advanced:

- Visibility for Dynamic Address Groups (DAGs) and Panorama Tags in View Policy, Policy Browser, Topology, and Violations
- Panorama 8 and earlier is no longer supported.

Panorama Basic (managing PanOS)

Basic means device management mode in SecureTrack is **Basic firewall management**

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Accountability - Saved Revisions Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Recertification
Policy Analysis	Policy Analysis Object Lookup
Auditing and Reporting	Expired Rules Report Auditing and Reporting
Topology	Static Topology

Notes for Panorama Basic:

As of R19-3, creating new Panorama - Basic Mode devices is not supported. As of R22-1, retrieving new revisions is not supported. For details see Deprecated Devices

If you use Panorama devices, we recommend using Advanced mode, which is still supported by Tufin

PanOS firewalls

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup
Change Management	Rule and Object Usage Report Change Management Graphical Policy Real-time Monitoring Accountability - Saved Revisions Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Recertification
Policy Analysis	Automatic Policy Generation (APG) Object Lookup
Auditing and Reporting	Auditing and Reporting
Topology	Static Topology

Notes for PanOS firewalls:

- Real-time monitoring uses syslogs.
- APG does not recognize Palo Alto users and applications.
- Accountability is supported when changes are made directly to a firewall.

VMware NSX

VMware NSX

Dashboard and Browsers	Change Tracking Policy Analysis Risk Dashboard Violations Cleanup
Change Management	Change Management Graphical Policy Real-time Monitoring Accountability - Installed Revisions Display IPv6 objects Create SecureChange ticket from Policy Browser for: • Rule Decommission • Rule Recertification
Policy Analysis	Policy Analysis

	Object Lookup
Auditing and Reporting	**Auditing and Reporting**
Topology	**Static Topology** **BGP Dynamic Routes**

Notes for VMware NSX:

- Real-time monitoring uses device polling.
- These features are not supported: unused objects cleanup, offline analysis.
- "Applied to" criteria in Policy Analysis is only supported in view mode.
- Topology support only includes North-South connectivity and, in topology diagrams, traffic inside a logical switch will be seen as passing logical router.
- For Auditing and Reporting, these features are supported: Regulations browser, Policy Browser (formerly Rule Documentation), New Revision report.
- Dynamic Topology (BGP dynamic routing) is supported for NSX-T
- To conform with recommendations from VMWare, in TOS R21-1 and later, new NSX-T devices are automatically configured with Declarative (Policy) APIs. Devices that were previously added using Imperative APIs will continue to work. In the Device Manager, the name of a device indicates whether the device is configured with a Declarative or Impertitive API.

  To convert a device that was previously added using Imperative APIs to Declarative APIs you need to add the device as a new device, and remove or disable the old instance of the device.
- In NSX-T Devices, support for dynamic Security Groups based on tags set in the device.

Getting Started with SecureTrack

After you install TOS, you can use SecureTrack to connect to your network devices and retrieve the policies from the devices.

Let's get started.

Logging into SecureTrack

Before you log in, make sure you have:

- **Operating System:** Microsoft Windows 10 or higher
- **Screen resolution:** 1280x800 or higher
- **Browser:** Microsoft Edge, Mozilla Firefox, Google Chrome

> Microsoft Internet Explorer (IE) is no longer supported by this TOS release

- **Local storage:** Local storage must be enabled in your browser settings for the session expiration functionality to work. For most browsers, the default is **enabled**.

  Before you browse to SecureTrack for the first time, make sure your networking configuration on the server is correct.

SecureTrack local users are required to set a new password the first time they log in to SecureTrack after any of the following actions performed by an administrator:

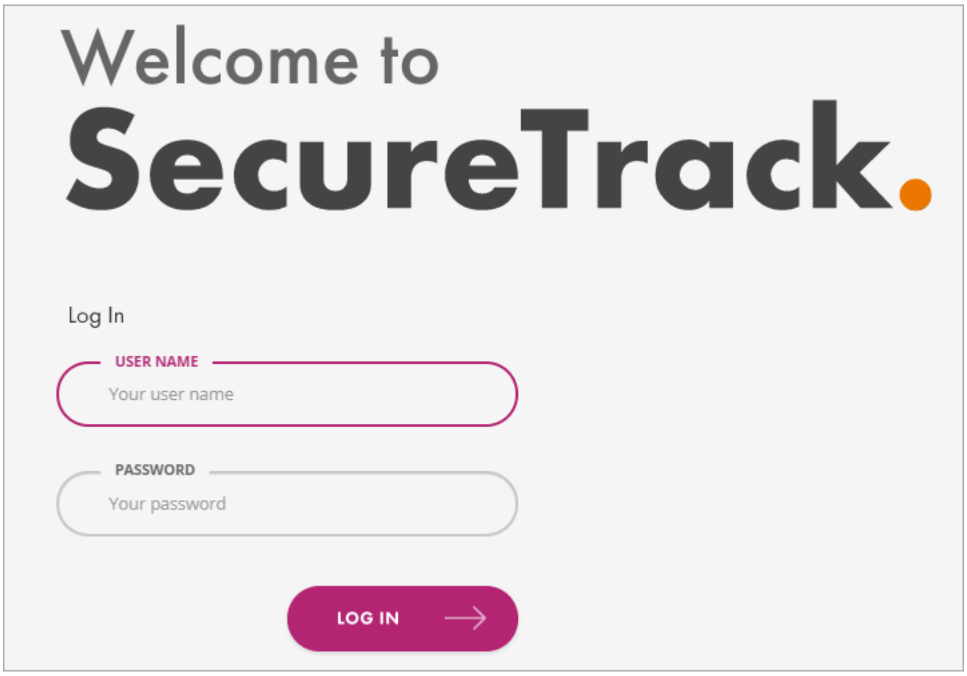
- Being added as a new user
- Password reset

To log into SecureTrack for the first time:

1. Browse to SecureTrack at: `https://<server>`

   <server> is the IP address or DNS name of the SecureTrack server. Make sure port 443 (HTTPS) is open between your host and the server.

   The initial login screen appears:



2. Enter the default user name (`admin`) and password (`admin`) and click **Log in**.

   After you log in for the first time, you can change the password and add users. LDAP users login in the format: **username@domain**

3. Select the options that you want from the SecureTrack setup wizard and click **Continue**.

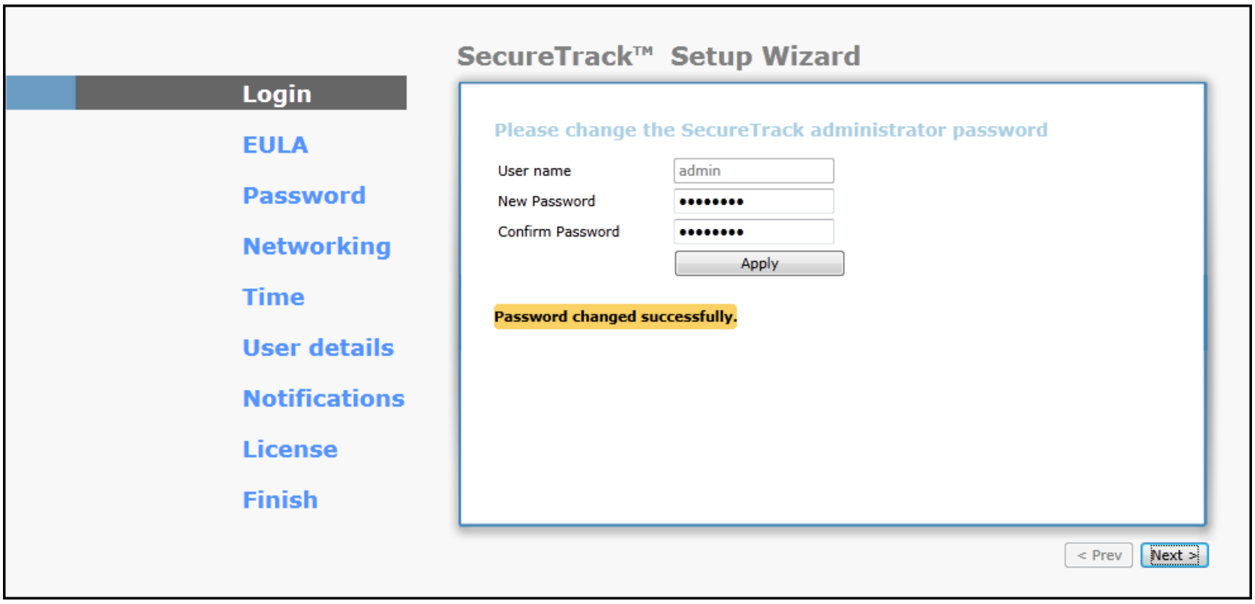
The SecureTrack Setup Wizard

When you login for the first time, you see the SecureTrack Setup wizard.

Follow the instructions in the wizard to get started:

Some pages (indicated below) appear only when SecureTrack is running on TufinOS.

1. Change the password for the **admin** user:



SecureTrack™ Setup Wizard

Please change the SecureTrack administrator password

User name: admin

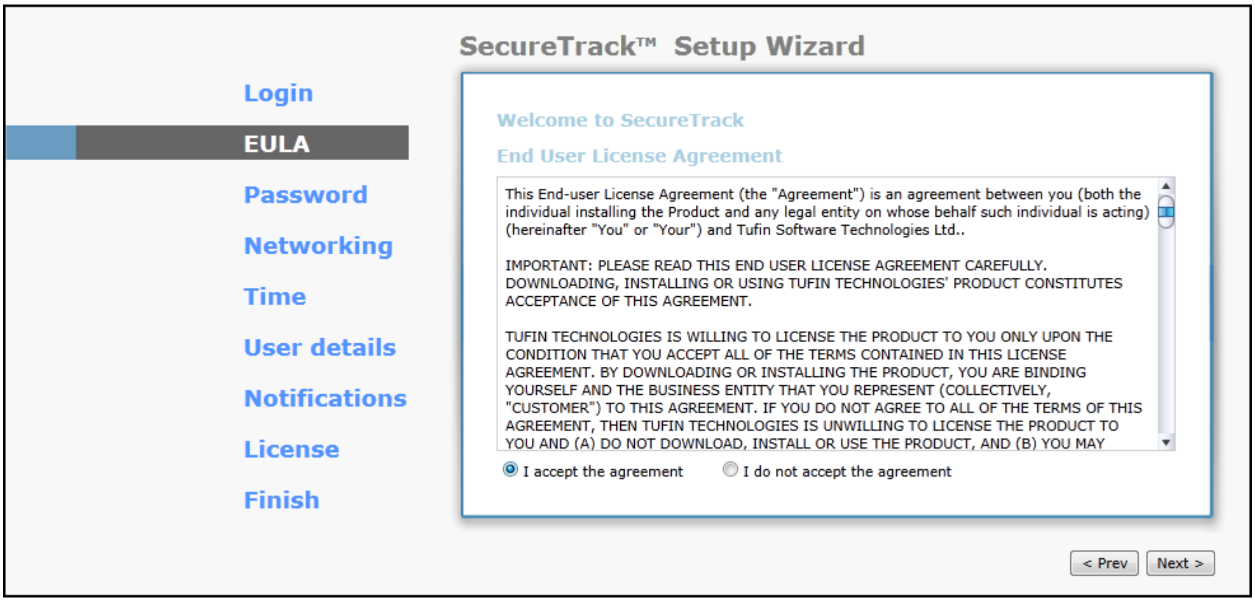
New Password: ••••••••

Confirm Password: ••••••••

Password changed successfully.

Click **Apply**, and **Next**.

2. Read and accept the SecureTrack End-User License Agreement:



SecureTrack™ Setup Wizard

Welcome to SecureTrack

End User License Agreement

This End-user License Agreement (the "Agreement") is an agreement between you (both the individual installing the Product and any legal entity on whose behalf such individual is acting) (hereinafter "You" or "Your") and Tufin Software Technologies Ltd..

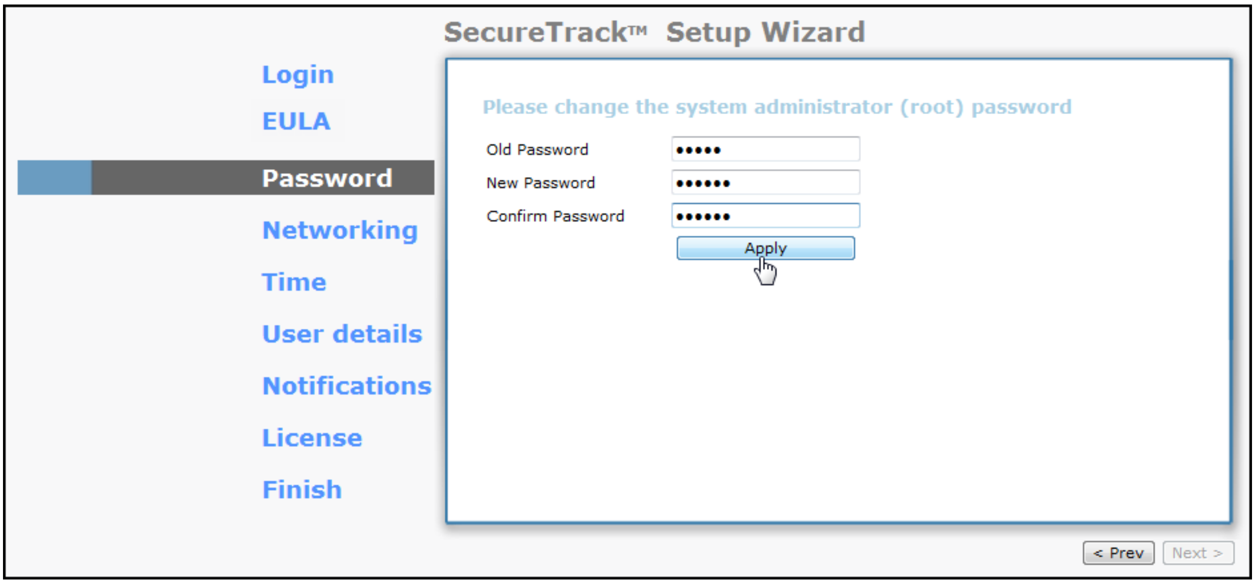
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING TUFIN TECHNOLOGIES' PRODUCT CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

TUFIN TECHNOLOGIES IS WILLING TO LICENSE THE PRODUCT TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE PRODUCT, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN TUFIN TECHNOLOGIES IS UNWILLING TO LICENSE THE PRODUCT TO YOU AND (A) DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT, AND (B) YOU MAY

● I accept the agreement ○ I do not accept the agreement

Click **Next**.

3. (TufinOS only) For the **Old Password** of the TufinOS root user, type: **system** , and change the password:



Please change the system administrator (root) password

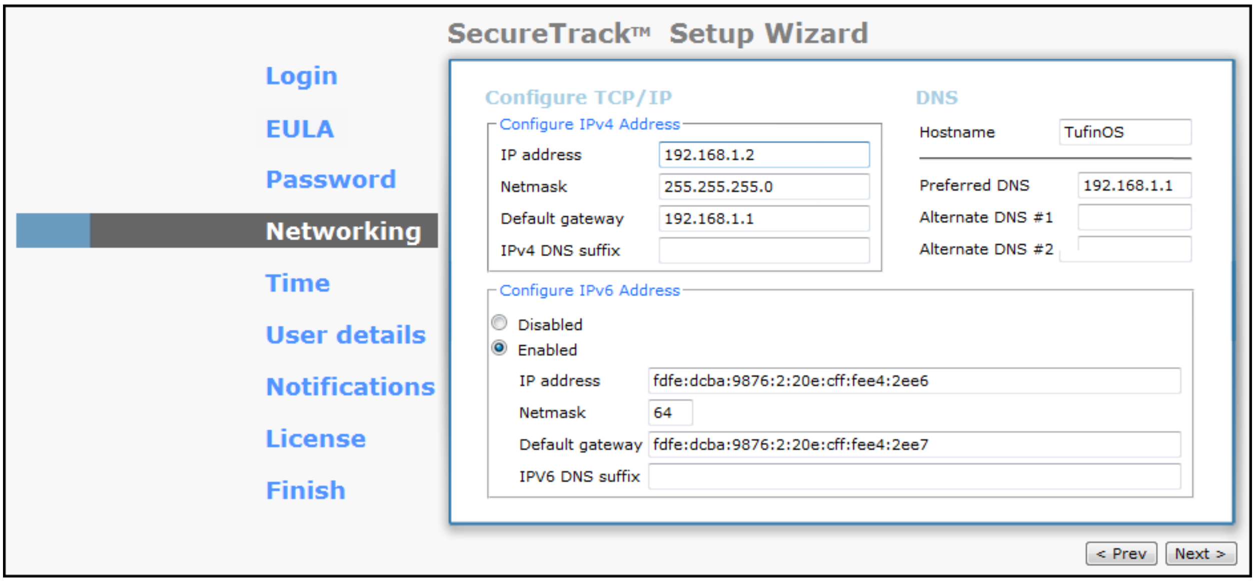
Old Password •••••

New Password ••••••

Confirm Password ••••••

Click **Apply**, and **Next**.

4. (TufinOS only) Configure networking (DNS settings can also be configured later on from SecureTrack's web interface):



Configure TCP/IP

Configure IPv4 Address

IP address 192.168.1.2

Netmask 255.255.255.0

Default gateway 192.168.1.1

IPv4 DNS suffix

DNS

Hostname TufinOS

Preferred DNS 192.168.1.1

Alternate DNS #1

Alternate DNS #2

Configure IPv6 Address

○ Disabled

● Enabled

IP address fdfe:dcba:9876:2:20e:cff:fee4:2ee6

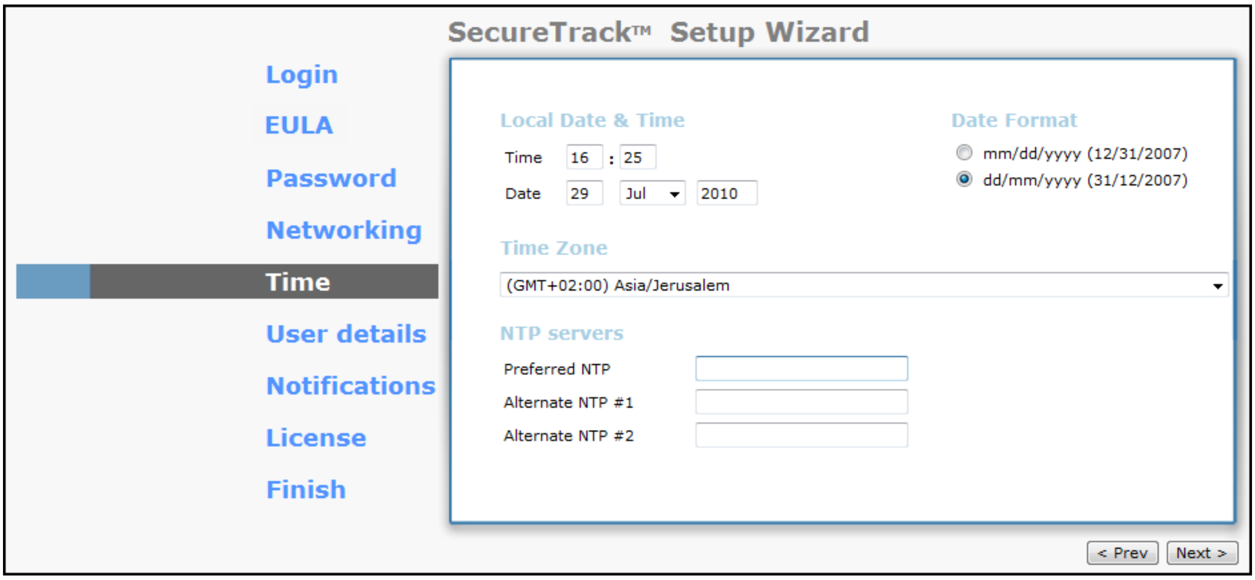
Netmask 64

Default gateway fdfe:dcba:9876:2:20e:cff:fee4:2ee7

IPV6 DNS suffix

Click **Next**.

5. (TufinOS only) Configure date and time settings:



Local Date & Time

Time 16 : 25

Date 29 Jul 2010

Date Format

○ mm/dd/yyyy (12/31/2007)

● dd/mm/yyyy (31/12/2007)

Time Zone

(GMT+02:00) Asia/Jerusalem

NTP servers

Preferred NTP

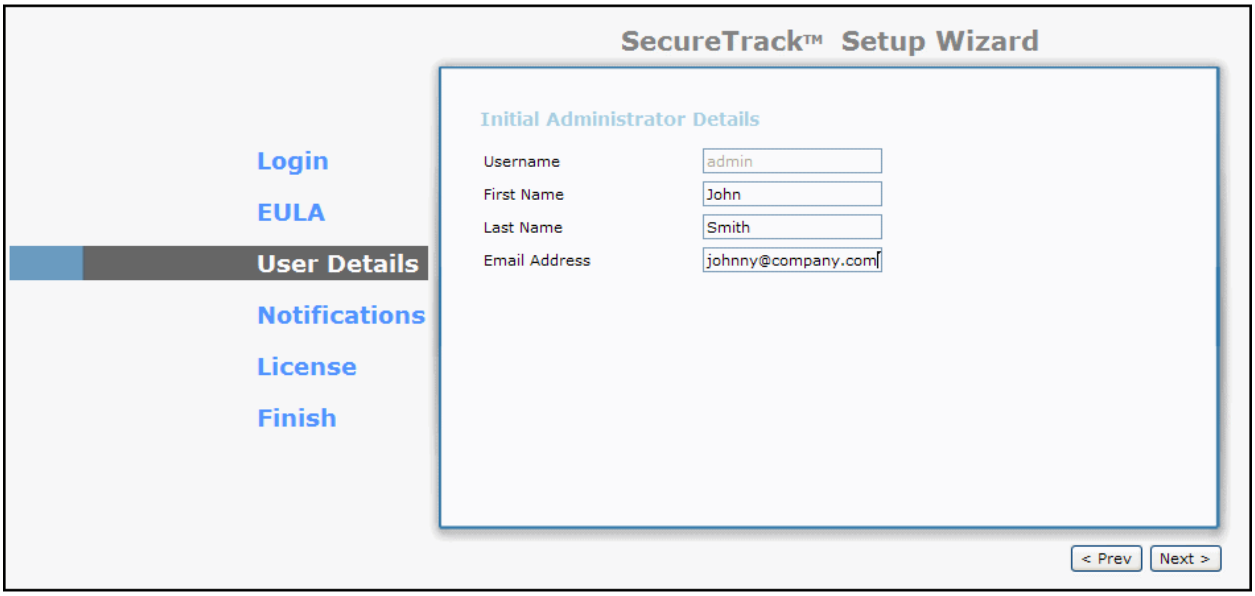
Alternate NTP #1

Alternate NTP #2

Click **Next**.

The following steps can be performed here in the wizard, or later on from SecureTrack's web interface.

6. Configure the administrator's user details:

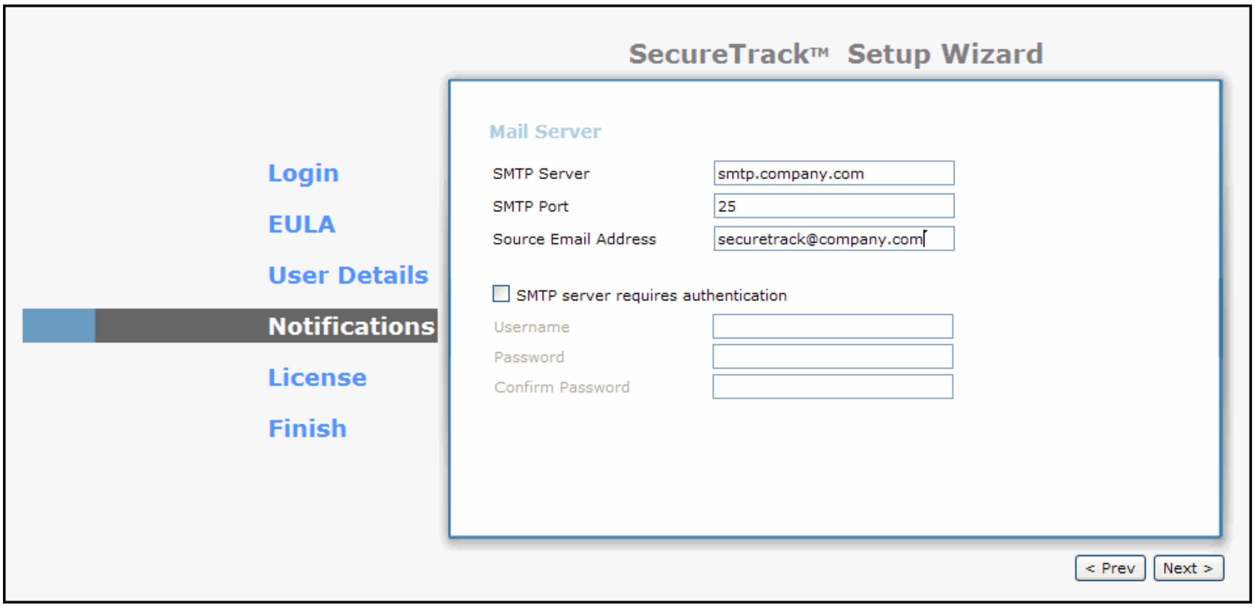


Initial Administrator Details

Username	admin
First Name	John
Last Name	Smith
Email Address	johnny@company.com

Click **Next**.

7. Configure SecureTrack's emailing capability:



SMTP Server: smtp.company.com

SMTP Port: 25

Source Email Address: securetrack@company.com

□ SMTP server requires authentication

Username

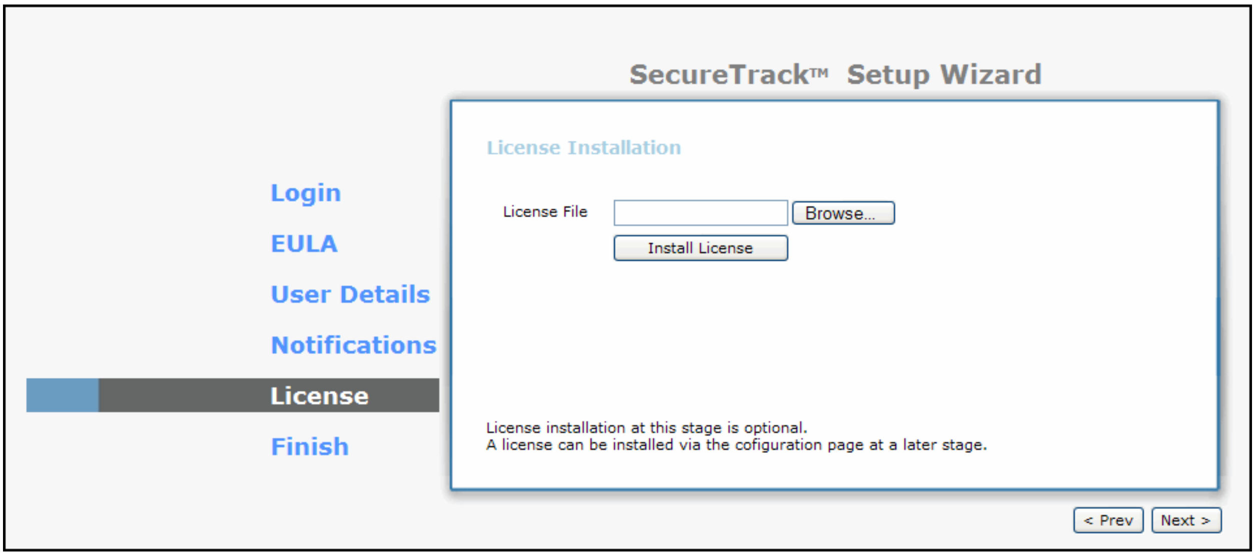
Password

Confirm Password

The emailing capability of SecureTrack enables reports to be sent to specified users when the reports are generated. Without email support, users need to view saved reports in SecureTrack's web interface.

Click **Next**.

8. You should have an evaluation or production license file provided to you by your Tufin representative or partner. Install the License file:



License installation at this stage is optional.
A license can be installed via the cofiguration page at a later stage.

After navigating to or typing the path of the license file, click **Install License**, and **Next**.

9. In the **Finish** page, click **Save**.

Additional Initial Configuration

For SecureTrack to send email and syslog notifications, you must configure the server information in SecureTrack in **Settings** > **Configuration** > **Notifications**.

1. Enter SMTP information for:
   - **SMTP Server**: SecureTrack can send email notifications and alerts directly (using its SMTP engine), or act as an email client, and send emails to an organizational SMTP server. In order to send emails to an SMTP server, configure its IP address in this option. The default setting for the SMTP Mail Server is localhost, which sends emails directly.
   - **SMTP Port**: The port used by your SMTP server.

- **Source Email Address**: The email address chosen by SecureTrack in the SMTP email messages sent (for example: securetrack@yourcompany.com). This can be used for easy identifications of email messages coming from SecureTrack.
- **SMTP server requires authentication**: Select this if your SMTP server requires authentication for sending email, and type the username and password that will be used by SecureTrack to communicate with the SMTP server.

2. You can also configure:
    - External user authentication
    - SecureTrack users and administrators
    - Notifications
    - Integrating with ticketing systems
    - Other configuration options

Managing Device Connections

All of the features of Tufin Orchestration Suite are based on the security and network configurations that SecureTrack retrieves from your physical, virtual or cloud network platforms, also known as devices.

To retrieve security configurations, you can:

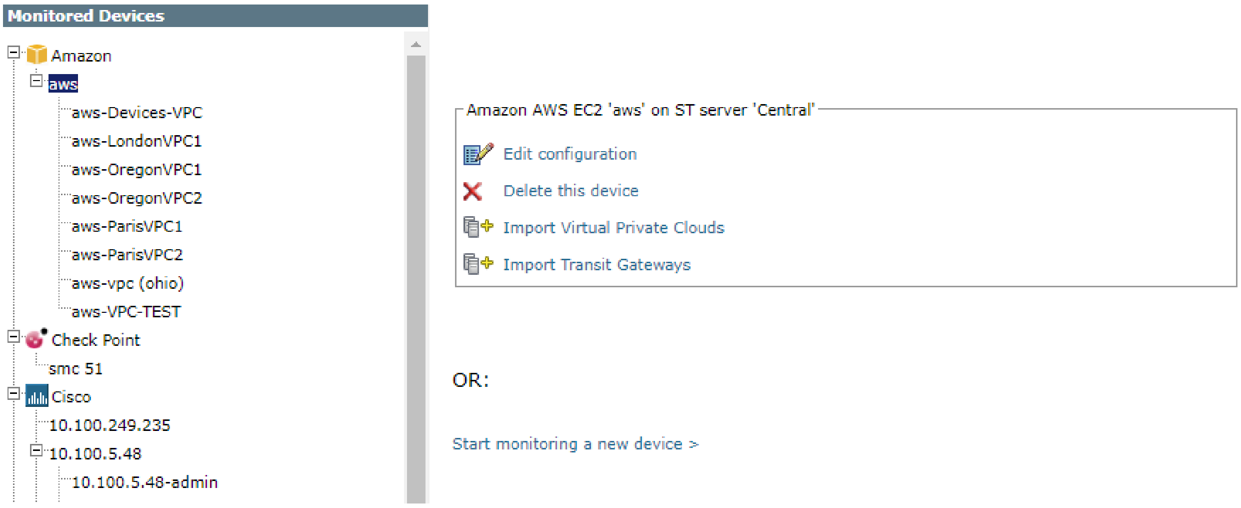
- Add devices to SecureTrack so that SecureTrack gets new policy revisions from the devices
- Configuring Devices to Send Logs to SecureTrack with policy change and traffic flow information
- Upload a device configuration file to SecureTrack so that you can analyze the configuration without actually connecting SecureTrack to the device

You can also organize your devices to take advantage of:

- Easy administration with logical groups
- Data segmentation with domains
- Scalable performance with distributed TOS servers

Managing Monitored Devices

You can add devices to be monitored and manage monitored devices in **Settings** > **Monitoring** > **Manage Devices**. You can also arrange the devices into groups.



Select a device from the device tree on the left. You can **Edit** the device configuration or **Delete** the device from SecureChange. Some other options are specific to Check Point management servers.

You can also:

Migrate (ST servers): In a Distributed environment, you can migrate the device to change the monitoring SecureTrack server.

Migrate (Domains): In a Multi-Domain environment, a Super Administrator in the Global context can migrate the device from one domain to another.

Multi-domain Deployments

You can migrate devices to different environments. This feature is available only if you have configured your system for multi-domains. After migrating a device to another domain, the device is automatically removed from reports, queries, audits and alerts that were configured in the source domain. After migration, administrators of the target domain have permissions for the device, but users do not.

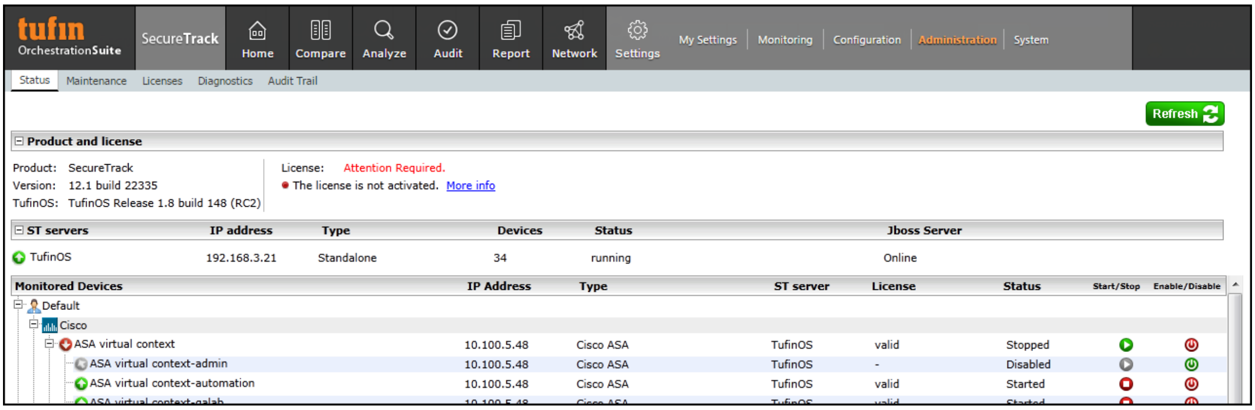
Migrate (move) a Device to Another Domain

1. Click on a device.
2. Click **Migrate (Domains)**.
3. Select a domain.
4. Click **Migrate**.

The device now appears in the device tree under the new domain.

Managing Devices in a Distributed Deployment

In a distributed deployment, each device is monitored by only one SecureTrack server (Central, Distribution, or Remote Collector). Monitoring servers can be viewed in Status:



⊟ Product and license

Product: SecureTrack
Version: 12.1 build 22335
TufinOS: TufinOS Release 1.8 build 148 (RC2)

License: Attention Required.
● The license is not activated. More info

ST servers	IP address	Type	Devices	Status	Jboss Server
TufinOS	192.168.3.21	Standalone	34	running	Online

Monitored Devices	IP Address	Type	ST server	License	Status	Start/Stop	Enable/Disable
Default							
Cisco							
ASA virtual context	10.100.5.48	Cisco ASA	TufinOS	valid	Stopped	▶	⏻
ASA virtual context-admin	10.100.5.48	Cisco ASA	TufinOS	-	Disabled	▶	⏻
ASA virtual context-automation	10.100.5.48	Cisco ASA	TufinOS	valid	Started	■	⏻
ASA virtual context-galab	10.100.5.48	Cisco ASA	TufinOS	valid	Started	■	⏻

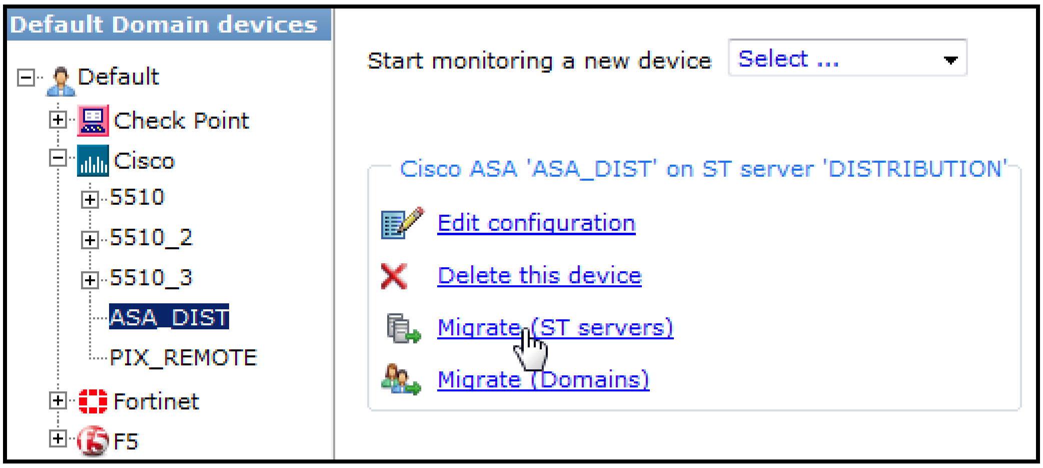
For each SecureTrack server, the number of monitored devices is shown. For each monitored device, the name of the monitoring SecureTrack server is shown.

To change which server monitors a device, first migrate the device to the Central SecureTrack server, and then migrate to the target server. For example, when migrating a device from one remote collector to another, you must first migrate to the Central server and then from the Central server to the required remote collector.

In a Multi-Domain environment, virtual system host devices can be migrated between monitoring servers only by a Super Administrator in the Global context.

To change the monitoring SecureTrack server of a monitored device:

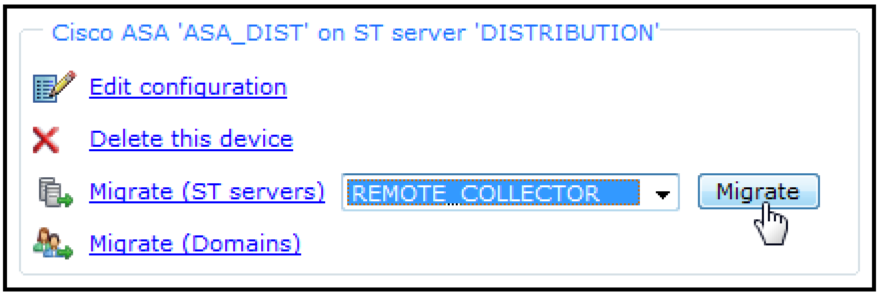
1. In **Settings** > **Monitoring**, select **Devices**.
2. Under Device Configuration, select the monitored device.
3. Click **Migrate (ST servers)**:



Start monitoring a new device: Select ...

Cisco ASA 'ASA_DIST' on ST server 'DISTRIBUTION'

4. Select the desired SecureTrack server, and click **Migrate**:



Cisco ASA 'ASA_DIST' on ST server 'DISTRIBUTION'

Migrate (ST servers): REMOTE_COLLECTOR

5. If the device is configured to send syslogs to SecureTrack, change the syslog configuration on the device to send syslogs to the IP address of the SecureTrack server, remote collector or distribution server that is managing the device.

Adding Devices to TOS Classic

Adding a physical or virtual firewall device to TOS Classic adds the device to the list of Monitored Devices and gives you visibility to the device policy and revisions.

Devices can be added and managed only by SecureTrack Administrators. If you have configured your system for multi-domain management, devices can be added by Multi-Domain Administrators in a selected domain or Super Administrators in a selected domain or when All Domains is selected.

SecureTrack automatically attaches new devices to an available license component (SKU), the one with the longest duration. If there is an available perpetual license, SecureTrack will attach the device to that license. If not, SecureTrack will choose the subscription license with the latest expiration date. If there is no available license, the device will be considered **Plug and Play**, and you will have 30 days to contact Tufin and purchase a license for your device. When disabling the devices, the attached SKUs become available and you can use them with other devices.

You can install devices from the manufacturers listed below using a simple wizard. The wizard will prompt you for required device information such as the device type, IP address, user name, and password. The required information is different for each device type.

All devices need to use TLS 1.2. SecureTrack will not retrieve revisions from devices that use TLS 1.0 or 1.1

For a list of supported devices, see Supported Devices and Platforms.

Adding Amazon AWS Cloud Platform

Overview

TOS Classic monitors the Amazon AWS cloud platform for policy revision changes. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Prerequisites

Before you begin, make sure that you have an AWS user that has a policy that has all the permissions you require for the TOS features you will be using.

Feature	AWS Permissions
Visibility and Change Tracking Read-Only access to EC2, VPC, and Direct Connect, which lets you Retrieve information about instances, Security Groups, VPCs and all relevant networking data, such as subnets, interfaces, routes and table.	AmazonEC2ReadOnlyAccess, AmazonVPCReadOnlyAccess, AWSDirectConnectReadOnlyAccess
Application Discovery	CloudWatchLogsReadOnlyAccess
Routes for Transit Gateways	SearchTransitGatewayRoutes
Provisioning	User must have either: • AmazonVPCFullAccess or create a custom IAM policy with the following permissions: • AuthorizeSecurityGroupEgress • AuthorizeSecurityGroupIngress • RevokeSecurityGroupEgress • RevokeSecurityGroupIngress
Cross-Account Access	To use the `AssumeRole` option, you must have an Amazon Resource Name (ARN) identifier. For more information, see Amazon AWS AssumeRole Support.

You can assign the policy to the user directly or through a role that it is assigned to. For more about AWS policies or creating a custom IAM policy, see the Amazon AWS documentation. This following is a sample custom IAM policy:

```
{
  "Version": "2012-10-17",
  "Statement":[
  {
    "Effect":"Allow",
    "Action":[
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress"
    ],
      "Resource": [
        "arn:aws:ec2:*"
      ]
    }
  ]
}
```

Automatic Import of VPCs

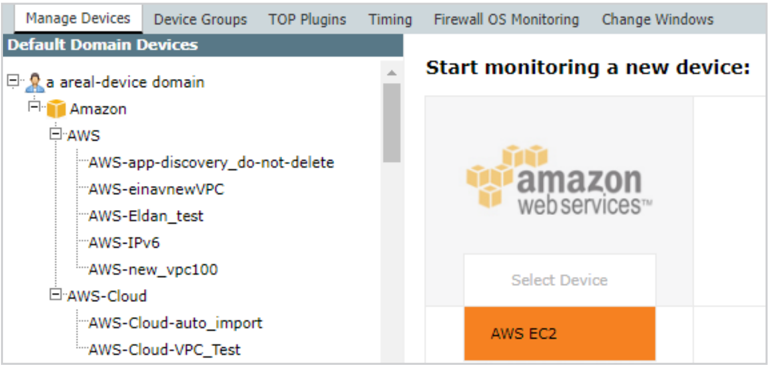
When you select **Automatic Import** of VPCs, SecureTrack automatically detects changes to the AWS environment (adding, deleting, and editing VPCs) and reflects them in the device list and revision history. Changes to the VPCs will be reflected in the Interactive Map when a scheduled sync occurs or when you click **Sync** in the Interactive Map.

With **Automatic Import** enabled, devices that have been deleted from the AWS are automatically deleted from the list of devices in SecureTrack and their history will no longer be available. Therefore, if your continuous integration/continuous deployment (CICD) pipeline regenerates VPCs, the history of the deleted VPC will not be available in the new replacement VPC. To retain revision data in SecureTrack for devices that have been deleted from your Amazon account, use manual import.

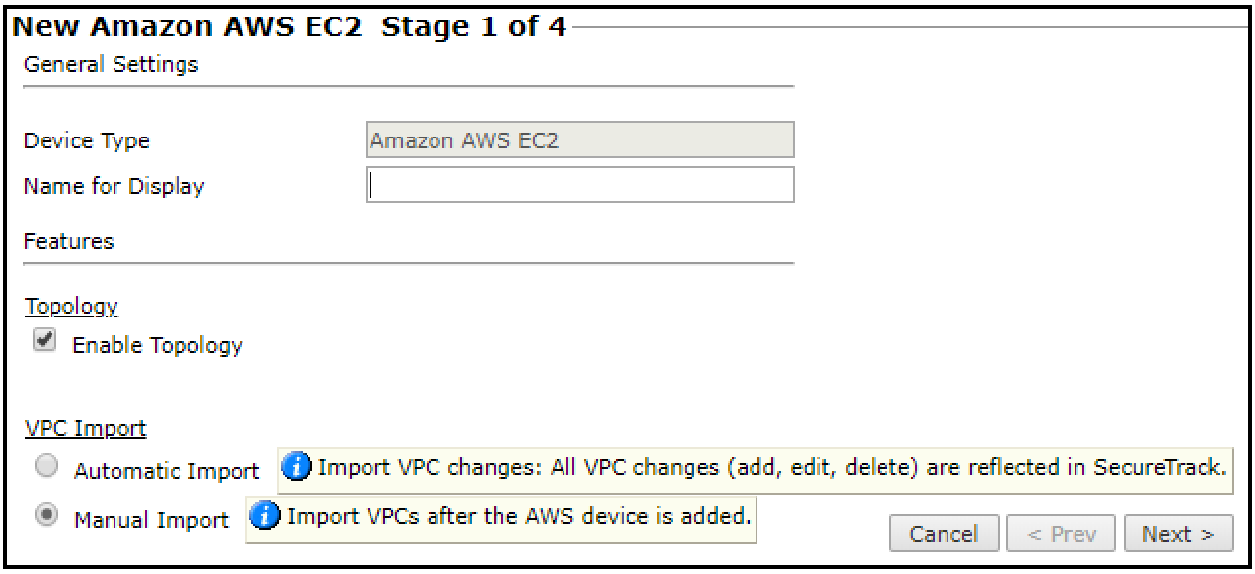
There is a limit to the number of VPCs that can be supported for **Automatic Import**, depending on your TOS deployment. For more information, contact Tufin Customer Support.

Adding an AWS Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Amazon AWS EC2 Stage 1 of 4

General Settings

Device Type: Amazon AWS EC2

Name for Display:

Features

Topology

☑ Enable Topology

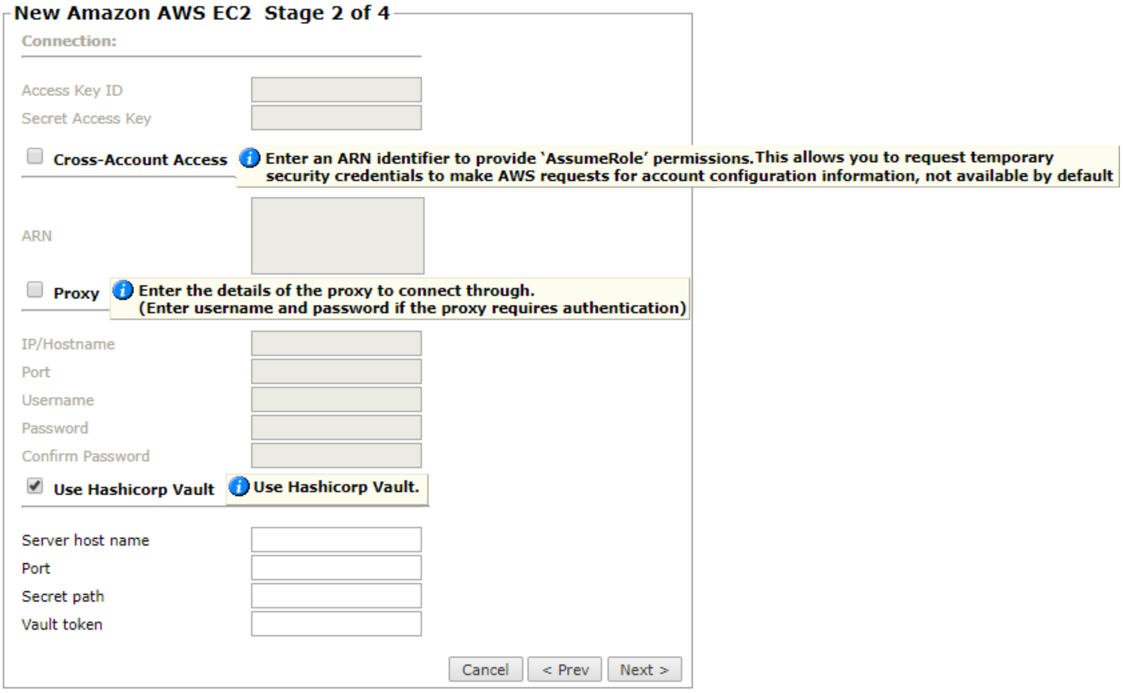
VPC Import

○ Automatic Import — Import VPC changes: All VPC changes (add, edit, delete) are reflected in SecureTrack.

● Manual Import — Import VPCs after the AWS device is added.

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **ST server**: In a distributed deployment, the AWS parent device and its VPCs must be monitored by the same server (Not shown in image).
- **Features >Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- **Features > VPC Import**:
  - **Automatic Import**: For a given AWS account, automatically detect deleted VPCs and add new VPCs in SecureTrack.
  - **Manual Import**: Import VPCs after the AWS device is added.

4. Click **Next**.
5. Configure the SecureTrack connection to the Amazon AWS device, according to the parameters required by the device:



New Amazon AWS EC2 Stage 2 of 4

Connection:

Access Key ID

Secret Access Key

□ Cross-Account Access — Enter an ARN identifier to provide 'AssumeRole' permissions.This allows you to request temporary security credentials to make AWS requests for account configuration information, not available by default

ARN

□ Proxy — Enter the details of the proxy to connect through. (Enter username and password if the proxy requires authentication)

IP/Hostname

Port

Username

Password

Confirm Password

☑ Use Hashicorp Vault — Use Hashicorp Vault.

Server host name

Port

Secret path

Vault token

a. Enter the **Access Key ID** and the **Secret Access Key**.

   You can get the access keys from the AWS Identity and Access Management (IAM) console.

b. For **Cross-Account Access**, enter an Amazon Resource Name (ARN) identifier to use the `AssumeRole` permissions.

   This allows you to request temporary security credentials to make AWS requests for the account configuration information that is not available by default, and to access VPCs that are not part of your Account configuration.
   For more information, see Amazon AWS AssumeRole Support.

c. **Proxy**: Select this option if you connect to AWS through a proxy which requires authentication and enter the proxy details:

   - **IP** address or **Hostname** of the proxy
   - **Port** that you connect to on the proxy
   - **Username** to use for authentication
   - **Password** (and password confirmation) to use for authentication

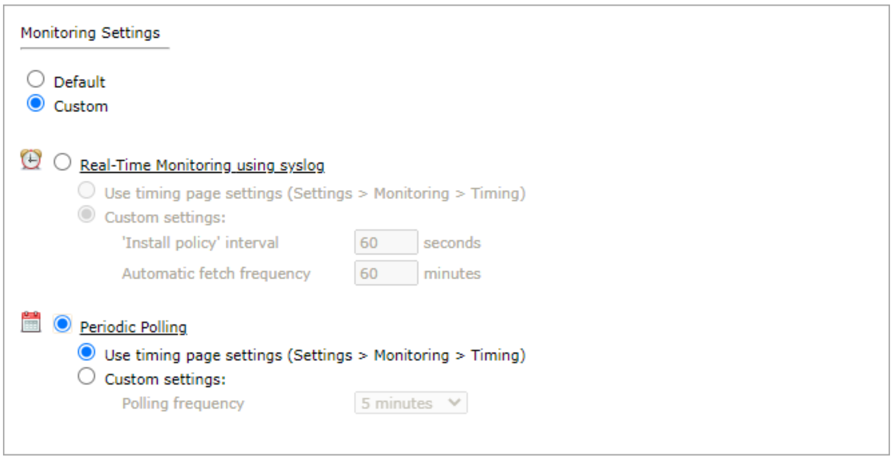
   If SSL decryption is enabled on the Proxy server and applied to the traffic from SecureTrack to AWS, you must configure a white list on the proxy server. The white list allows the traffic from SecureTrack to bypass SSL decryption and authentication.

d. **Use Hashicorp Vault:** Select this option if you use Hashicorp Vault to store your AWS authentication credentials

   - **Server host name:** The name of the server used to host the Hashicorp Vault
   - **Port:** The TCP / UDP port that SecureTrack uses to communicate with the Hashicorp Vault
   - **Secret path:** The path to the AWS authentication details within the Hashicorp Vault
   - **Vault token:** The token required for SecureTrack to authenticate AWS via the Hashicorp Vault

e. Click **Next**.

6. The Monitoring Settings page appears:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

   - **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often SecureTrack fetches the configuration from each device.

     If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

7. Click **Next**.

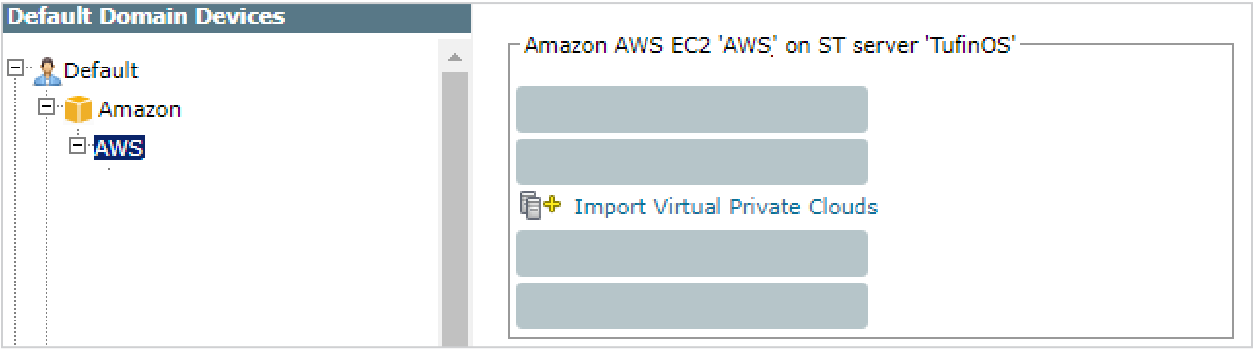
8. **Save** the configuration.

   The Amazon AWS device now appears in the **Monitored Devices** tree.

9. To manually add Virtual Private Clouds to your device, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the Virtual Private Clouds:

   a. In the **Monitored Devices** tree, select the device.

   b. Click **Import Virtual Private Clouds** (only enabled for **Manual Import**):



Default Domain Devices

- Default
  - Amazon
    - AWS

Amazon AWS EC2 'AWS' on ST server 'TufinOS'

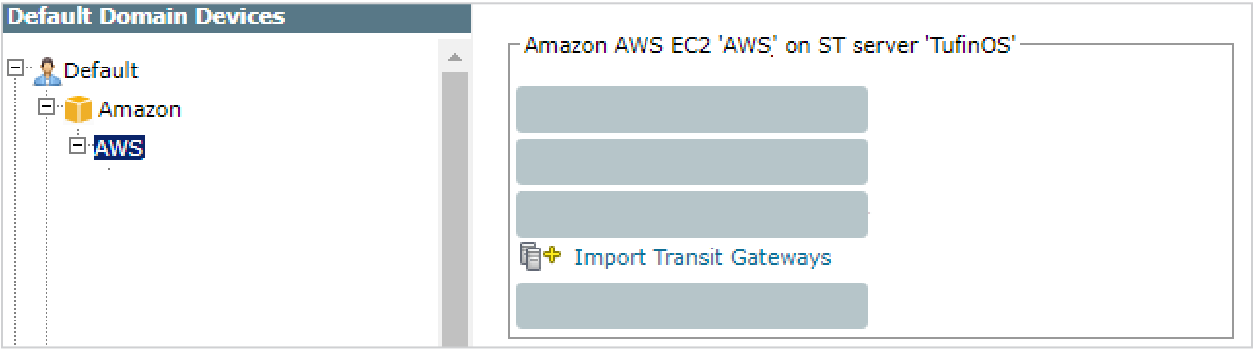
Import Virtual Private Clouds

c. Select all the Virtual Private Clouds to be added.

10. To add Transit Gateways (supported for Topology only):

    a. In the **Monitored Devices** tree, select the device.

    b. Click **Import Transit Gateway**:



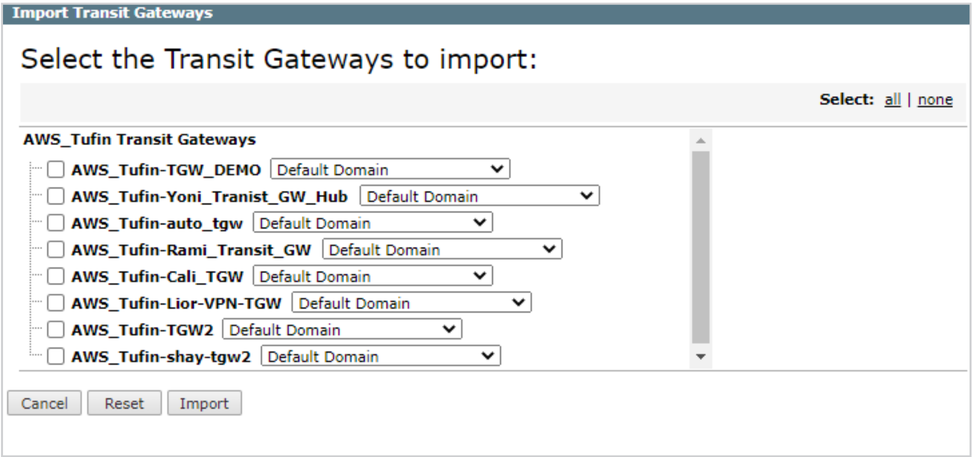
Default Domain Devices

- Default
  - Amazon
    - AWS

Amazon AWS EC2 'AWS' on ST server 'TufinOS'

Import Transit Gateways

c. Select the Transit gateways to import and the domain for each Transit Gateway



Import Transit Gateways

Select the Transit Gateways to import:

Select: all | none

AWS_Tufin Transit Gateways

- □ AWS_Tufin-TGW_DEMO Default Domain
- □ AWS_Tufin-Yoni_Tranist_GW_Hub Default Domain
- □ AWS_Tufin-auto_tgw Default Domain
- □ AWS_Tufin-Rami_Transit_GW Default Domain
- □ AWS_Tufin-Cali_TGW Default Domain
- □ AWS_Tufin-Lior-VPN-TGW Default Domain
- □ AWS_Tufin-TGW2 Default Domain
- □ AWS_Tufin-shay-tgw2 Default Domain

d. Click **Import**.

11. Click **Save**.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**.

Amazon AWS AssumeRole Support

AWS Accounts and Role Trust Policy

To assume a role, your AWS account must be trusted by the role. The trust relationship is defined in the role's trust policy when the role is created. That trust policy states which accounts are allowed to delegate access to this account's role.

The user who wants to access the role must also have permissions delegated from the role's administrator. If the user is in a different account than the role, then the user's administrator must attach a policy that allows the user to call `AssumeRole` on the Amazon Resource Name (ARN) of the role in the other account. If the user is in the same account as the role, then you can either attach a policy to the user (identical to the previous different account user), or you can add the user as a principal directly in the role's trust policy.

AWS `AssumeRole` API

The Amazon AWS `AssumeRole` API returns a set of temporary security credentials that you can use for cross-account access to AWS resources you might not normally have access to. To configure Cross-Account Access for Amazon AWS Cloud devices in SecureTrack, see Adding Amazon AWS Cloud Platform. For more information about the AWS `AssumeRole` API, see http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html (**AWS Documentation » AWS Security Token Service » API Reference » Actions » AssumeRole**).

The following required and optional parameters are used for SecureTrack Cross-Account Access, via the `AssumeRole` API:

Parameter	Description	Status
RoleArn	The Amazon Resource Name (ARN) of the role to assume. Example: `arn:aws:iam::006751140943:role/AssumRoleAdmin`	required
RoleSessionName	An identifier for the assumed role session. Use the role session name to uniquely identify a session when the same role is assumed by different principals or for different reasons. In cross-account scenarios, the role session name is visible to, and can be logged by the account that owns the role	required
DurationSeconds	Duration of the role session. in seconds: 900 s - 3600 s (15 minutes - 1 hour). Default: 3600 s	optional
ExternalID	A unique identifier that is used by third parties when assuming roles in their customers' accounts. For each role that the third party can assume, they should instruct their customers to ensure the role's trust policy checks for the external ID that the third party generated. Each time the third party assumes the role, they should pass the customer's external ID. http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html	optional
SerialNumber	The identification number of the MFA device that is associated with the user who is making the `AssumeRole` call. Specify this value if the trust policy of the role being assumed includes a condition that requires MFA authentication. The value is either the serial number for a hardware device (such as `GAHT12345678)` or an Amazon Resource Name (ARN) for a virtual device (such as `arn:aws:iam::123456789012:mfa/user)`.	optional
TokenCode	The value provided by the MFA device, if the trust policy of the role being assumed requires MFA (that is, if the policy includes a condition that tests for MFA). If the role being assumed requires MFA and if the TokenCode value is missing or expired, the `AssumeRole` call returns an **"access denied"** error.	optional

AWS Temporary Security Credentials

- The temporary security credentials are valid for the duration that you specify when you call `AssumeRole`.
- You must use credentials for an AWS Identity and an Access Management (IAM) user or an IAM role to call `AssumeRole`.

  If you call `AssumeRole` using the AWS root account credentials, you will receive an **access is denied** message.
- Optionally, you can pass an IAM access policy to this operation.

  If you choose not to pass a policy, the temporary security credentials that are returned by the operation have the permissions that are defined in the access policy of the role that is being assumed.
- It is possible to activate/deactivate the AWS security token service (STS) in an aws region, as follows:

```
AWSSecurityTokenServiceClient stsClient = new AWSSecurityTokenServiceClient();
stsClient.setEndpoint("sts.eu-west-1.amazonaws.com");
```

- Do not use the `setRegion` method to set a regional endpoint for AWS STS: For backward compatibility, that method continues to resolve to the original single global endpoint of **sts.amazonaws.com**.

For more information, see http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_enable-regions.html

Additional Links:

- AWS official description of the `AssumeRole` procedure: https://aws.amazon.com/blogs/aws/delegating-api-access-to-aws-services-using-iam-roles/ (**Delegating API Access to AWS Services Using IAM Roles**)
- `AssumeRole` API parameters details: http://docs.aws.amazon.com/STS/latest/APIReference/API_AssumeRole.html (**AWS Documentation » AWS Security Token Service » API Reference » Actions » AssumeRole**)
- Scenarios for Temporary Security Credentials http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html#sts-

introduction (AWS Documentation » AWS Identity and Access Management » User Guide » Identities (Users, Groups, and Roles) » Temporary Security Credentials » Common Scenarios for Temporary Credentials)

Adding Blue Coat Devices

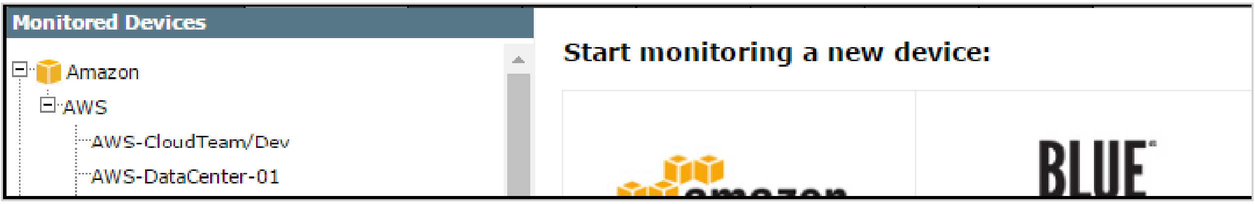
TOS Classic can monitor Blue Coat devices with pre-installed TOP plugins. To help you organize the information for your devices, you can use the device information worksheet.

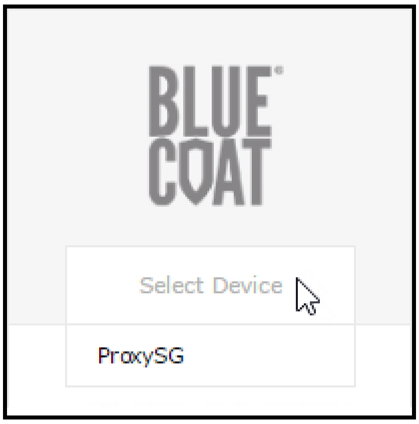
> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Monitor a Blue Coat Device

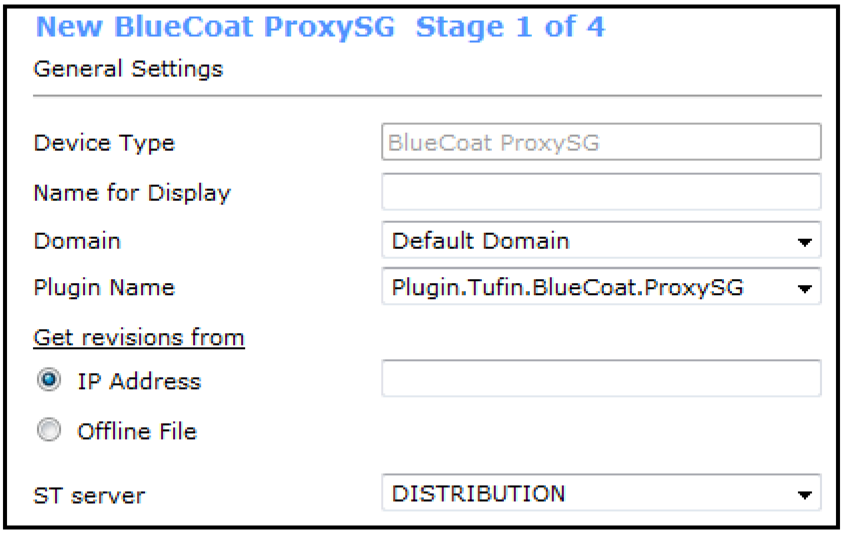
To configure TOS Classic to monitor the policy revisions of a Blue Coat device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:





3. Configure the device settings:



New BlueCoat ProxySG Stage 1 of 4

General Settings

Device Type	BlueCoat ProxySG
Name for Display	
Domain	Default Domain
Plugin Name	Plugin.Tufin.BlueCoat.ProxySG

Get revisions from

● IP Address

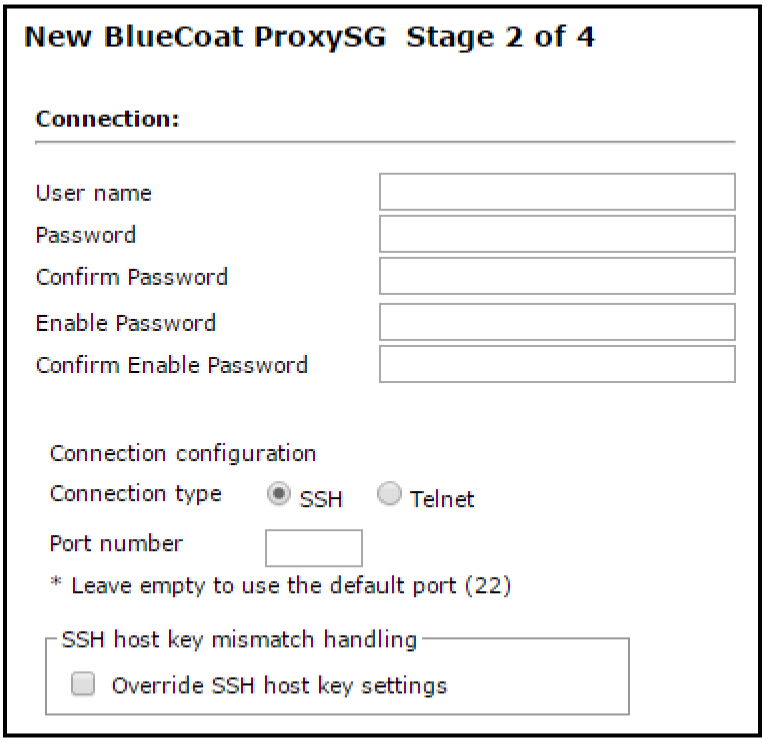
○ Offline File

ST server	DISTRIBUTION

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Plugin name**: If there are multiple plugins installed for the same device type, select the plugin for your device.
- **Get revisions from**: One of the following:
    - **IP Address**: Revisions are retrieved automatically
    - **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis
- **ST server**: In a distributed deployment, select which SecureTrack server monitors this device (Not shown in image) TOP devices monitored via preinstalled TOP plugins can be monitored by any SecureTrack server (Central, Distribution, or Remote Collector).

Click **Next**.

4. Configure the SecureTrack connection to the Blue Coat device, according to the parameters required by the device:



New BlueCoat ProxySG Stage 2 of 4

Connection:

User name

Password

Confirm Password

Enable Password

Confirm Enable Password

Connection configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

- Depending on the device type, Enter the authentication details needed to connect to the Blue Coat device.
    - **Username and password**: Enter the device username and password
    - **Enable password**: Enter the password to give SecureTrack elevated privileges on the device
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
  The device must be configured to use SSH version 2.

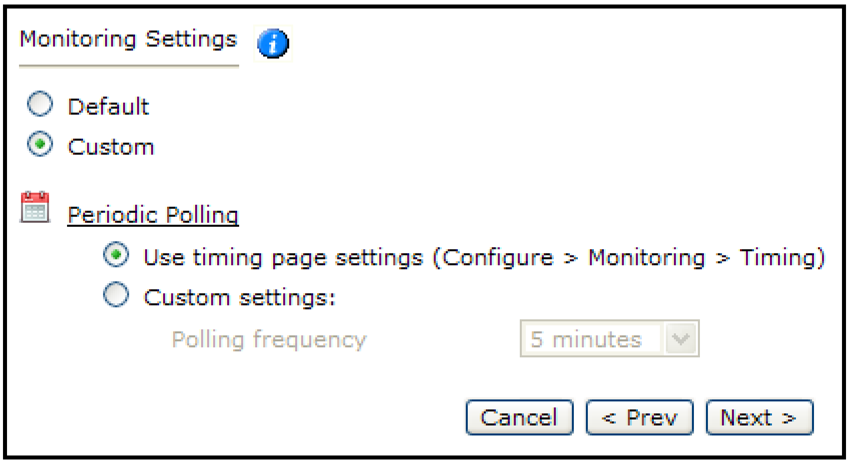
  Special characters in the password are not supported for some plugins.

  Depending on your device configuration, SecureTrack web interface may include more fields than are necessary for logging into the device. Make sure not to fill in these fields, as this may cause monitoring to fail.

  Make sure to use a username representing a user account that has Read (Read Only, or Read/Write) permissions for all information on the Blue Coat device. For **ProxySG**, the user must have an enabled privileged mode.

Click **Next**.

5. The Monitoring Settings page appears:



Monitoring Settings

○ Default

● Custom

Periodic Polling

● Use timing page settings (Configure > Monitoring > Timing)

○ Custom settings:

Polling frequency 5 minutes

To use timing settings from the Timing page for this device, select **Default**.

- To define specific timing settings for this device, select **Custom**, then select **Custom settings**, and configure the **Polling frequency**: How often SecureTrack fetches the configuration from each device.

If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

6. **Save** the configuration.

The Blue Coat device now appears in the Device Configuration list.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Check Point Devices

For Check Point deployments, TOS Classic monitors the management servers (SmartCenters, CMAs, and MDSs) for revision changes, and retrieves logs from Log servers and CLMs. For monitoring and usage analysis of all of your Check Point policies, add all management and log servers to TOS Classic.

TOS Classic uses Check Point OPSEC™ protocols and SNMP to monitor Check Point servers in real-time. At startup, TOS Classic establishes a LEA session to the management server and monitors the LEA connection. By default, SNMP traffic is authenticated with MD5, and you can change it to SHA authentication.

Before you add a Check Point server to TOS Classic, you must:

- Configure the Check Point server to communicate with TOS Classic using OPSEC
- In a Provider-1 environment, define TOS Classic as a GUI client for the MDSs

Record the details of all of your Check Point devices to make it easier for you to add all of them. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

After you upgrade a monitored Check Point CMA device to R80.x, you must upgrade the device in TOS Classic to use Check Point R80.x support.

Configure monitoring of Check Point servers in this order:

1. Provider-1 MDS
2. SmartCenter servers and Provider-1 CMAs
3. Log Servers and CLMs

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

To monitor the system configuration and performance of a gateway, enable Firewall OS Monitoring.

To monitor a Standby Check Point Management Server, see the Technical Note Monitoring a Standby Check Point Management Server.

To monitor a Check Point Management Server with Non-Standard LEA Authentication, see the Technical Note Monitoring a Check Point Management Server with Non-Standard LEA Authentication.

Notes for Check Point topology:

- In Check Point environments, if Firewall OS Monitoring is enabled, TOS Classic can use it to collect routing information from the gateway. If not, TOS Classic collects routing information from the management server.
- VSX WARP interface connections are shown with the WARP label.
- To obtain topology information for a VSX and its managed devices, TOS Classic must monitor the management server (SMC or CMA) that manages the physical VSX box.

Adding Check Point R7x Management and MDS Devices

For Check Point deployments, TOS Classic monitors the management servers (SmartCenters, CMAs, and MDSs) for revision changes, and retrieves logs from Log servers and CLMs. For monitoring and usage analysis of all of your Check Point policies, add all managements and log servers to TOS Classic.

After you upgrade a monitored Check Point CMA device to R80.x, you must upgrade the device in TOS Classic to use Check Point R80.x support.

Configure monitoring of Check Point servers in this order:

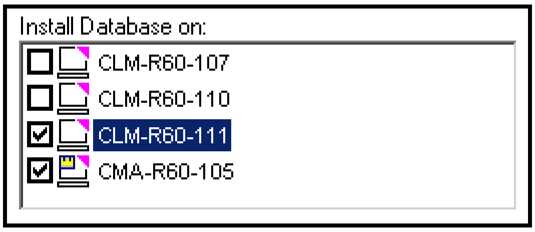
1. Provider-1 MDS
2. SmartCenter servers and Provider-1 CMAs
3. Log Servers and CLMs

To monitor the system configuration and performance of a gateway, enable Firewall OS Monitoring.

Prerequisites

To prepare a Check Point server (SmartCenter, CMA, MDS, Log Server, or CLM) for monitoring:

1. Configure the Check Point server for OPSEC communication with TOS Classic.
2. Apply the changes to the server:
   - **For a Provider-1 MDS**:
     1. From the **File** menu, select **Save**.
     2. Right-click on the Global Policy and select **Assign/Install Global Policy**.
   - **For a CMA**: If the CMA has one or more associated CLMs, select the relevant CLMs.



Install Database on:

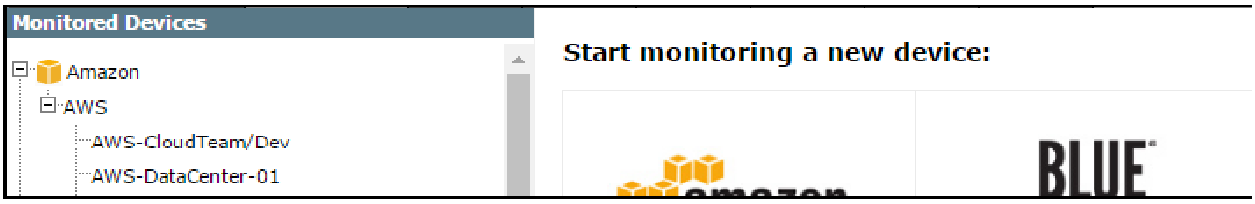
☐ CLM-R60-107
☐ CLM-R60-110
☑ CLM-R60-111
☑ CMA-R60-105

   - **For all others**: From the **Policy** menu, select **Install Database**.
3. Wait for confirmation that the database was saved.

Monitor a Check Point Device

To configure TOS Classic to monitor the policy revisions of a Check Point device:

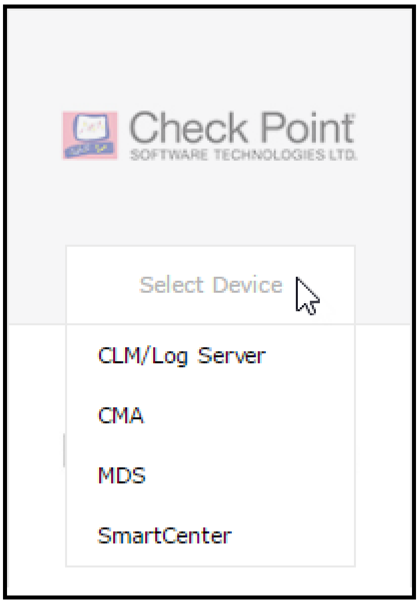
1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type e.g.:



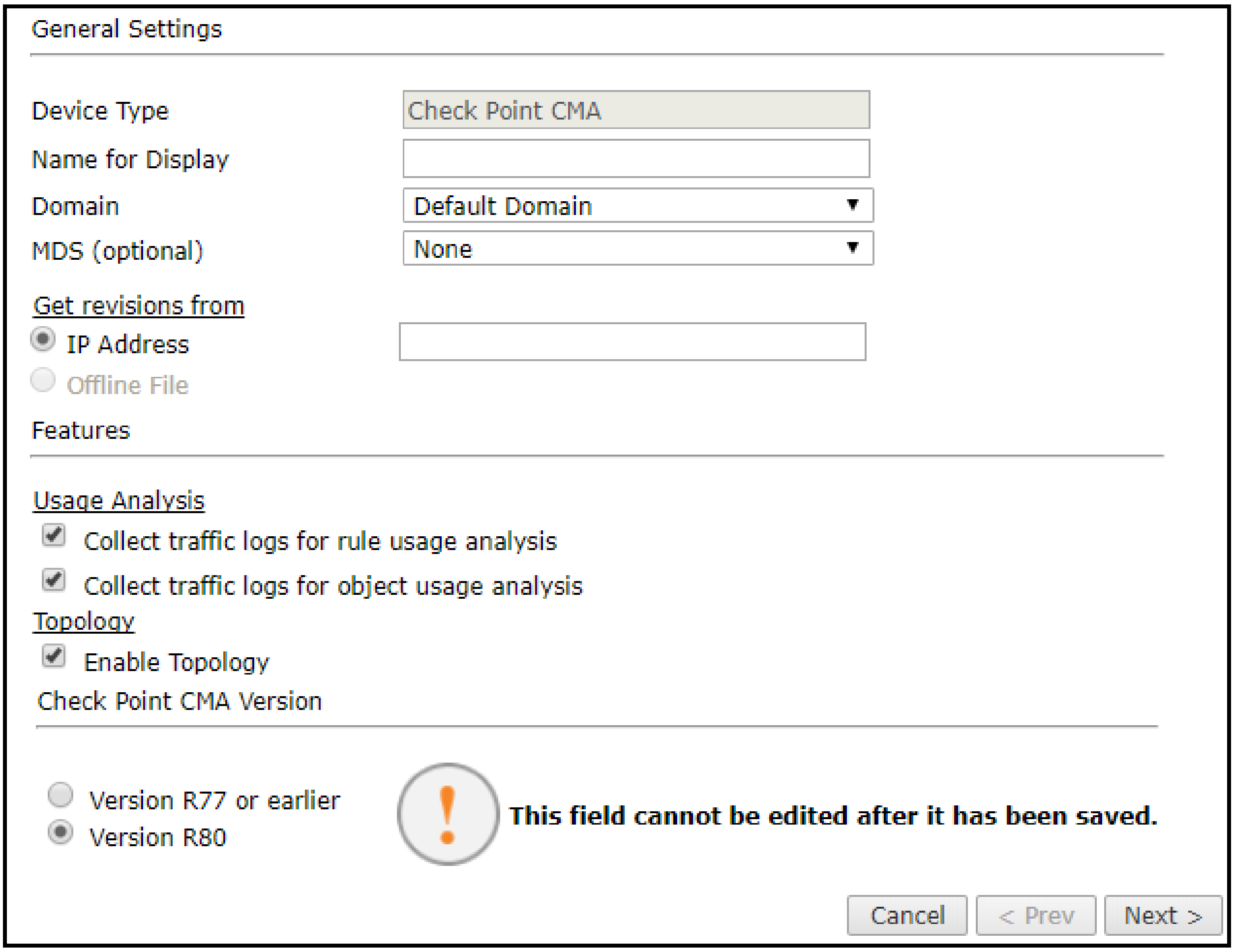
Monitored Devices

- Amazon
  - AWS
    - AWS-CloudTeam/Dev
    - AWS-DataCenter-01

Start monitoring a new device:



3. Configure the device settings:



General Settings

Device Type	Check Point CMA
Name for Display	
Domain	Default Domain ▼
MDS (optional)	None ▼

Get revisions from

● IP Address

○ Offline File

Features

Usage Analysis

☑ Collect traffic logs for rule usage analysis

☑ Collect traffic logs for object usage analysis

Topology

☑ Enable Topology

Check Point CMA Version

○ Version R77 or earlier

● Version R80

This field cannot be edited after it has been saved.

Depending on the Check Point server type, some or all of the following options will appear:

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you

must migrate the device.

- Device Specific Settings:
  - CMA only - **MDS**: the MDS that manages the CMA.
  - Log Server/CLM only - **Associated Management**: the SmartCenter sending logs to the Log Server, or the CMA sending the logs to the CLM.
  - MDS only - **MDS version**: Select the Check Point version installed on the MDS (R77 and below). After you save the device configuration, you cannot change this setting.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)

> For a Log Server/CLM, make sure the monitoring TOS Classic server is the same as for the Log Server/CLM's associated Check Point management server (SmartCenter/CMA).

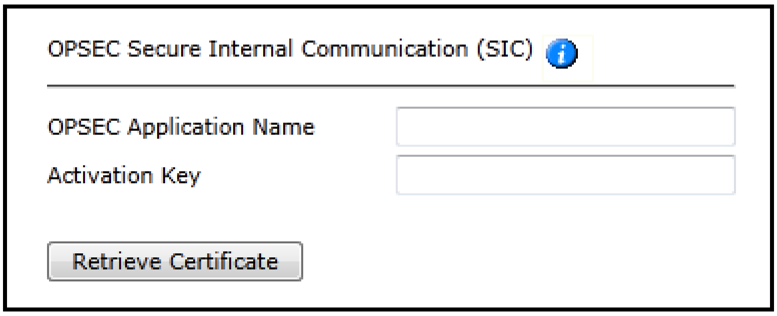
- **Collect traffic logs for rule usage analysis** is necessary for Rule Usage reports.
  - **Collect traffic logs for object usage analysis** is necessary for reporting on unused objects and services in Rule Usage Reports.

> Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure TOS Classic to limit the number of days that data is kept.

> We recommend that you enable TOS Classic administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, TOS Classic sends an alert.

- **Enable Topology**: Collects routing information for building the Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- **Check Point Software Version** (for CMAs only): Select the version of Check Point software installed on the device: (R77 and below)

4. Click **Next**.
5. Configure OPSEC communication in **OPSEC Secure Internal Communication (SIC)** (except for CLM/Log Server):



- Enter TOS Classic's **OPSEC Application Name** as you defined it for this Check Point server (case sensitive).
- Enter the **Activation Key** as defined when the OPSEC object was created.

> Before retrieving the certificate you must create an OPSEC Application in SmartDashboard

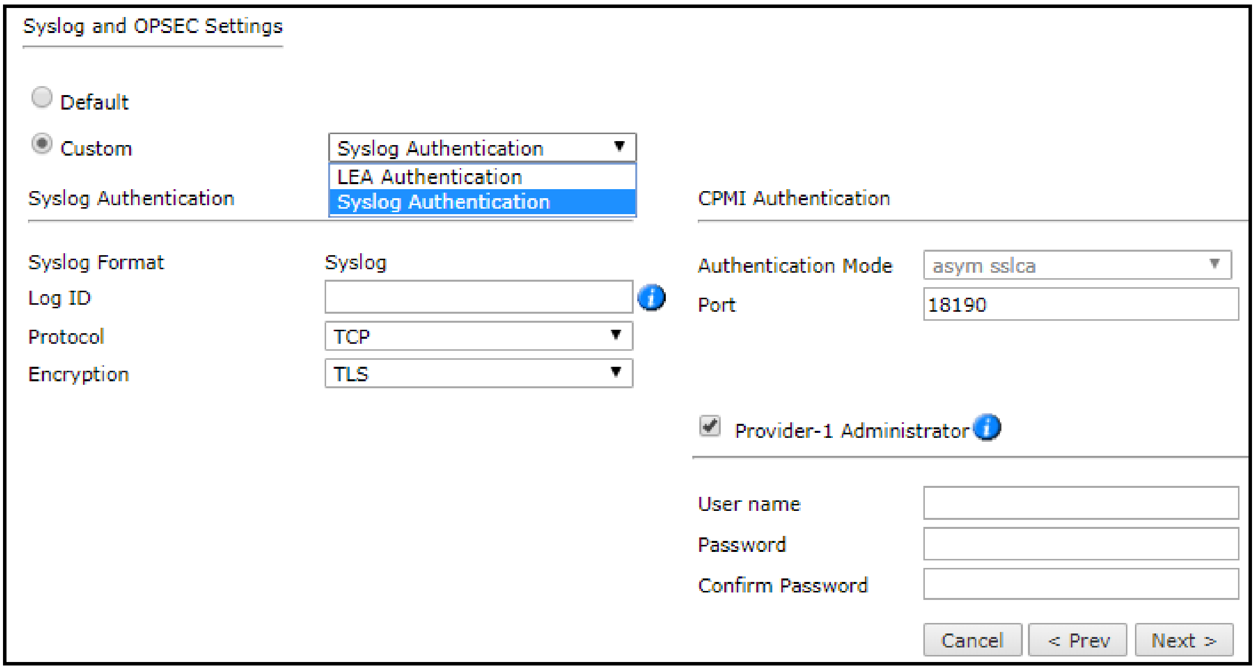
> - The OPSEC Application must have the LEA and CPMI client entities selected
> - You need to initialize Secure Internal Communications
> - You need to select Permissions Profile in the CPMI tab and create a Read-Only All permission
> - After creating the OPSEC Application you must run Install Database from the Policy menu (or just Save Policy for an MDS)

- Click **Retrieve Certificate** to setup encrypted communication between TOS Classic and the Check Point device.

  The certificate appears, and the following message is displayed:

  The certificate was retrieved successfully.

6. Click **Next**.
7. In **Syslog and OPSEC Settings**:



Syslog and OPSEC Settings

○ Default

● Custom [Syslog Authentication ▼]

Syslog Authentication

Syslog Format	Syslog
Log ID	
Protocol	TCP ▼
Encryption	TLS ▼

CPMI Authentication

Authentication Mode	asym sslca ▼
Port	18190

☑ Provider-1 Administrator

User name	
Password	
Confirm Password	

- **For MDS or CMA syslog or LEA logging:** To configure the log type, select **Custom** and the relevant option: **Syslog Authentication** or **LEA Authentication**.

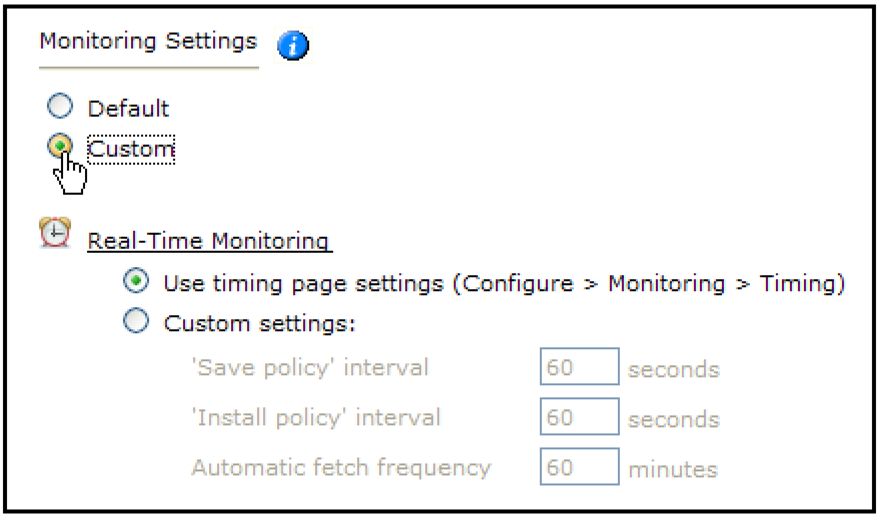
  For additional information on Check Point R7x syslog configuration, see Configuring Check Point Syslogs.

- **For a Provider-1 MDS**: To include monitoring of the Global Database, select **Custom** and **Provider-1 Administrator**. Enter Multi-Domain Super user credentials.

  > For Global Database monitoring, TOS Classic must also be set as a valid GUI client for the MDS. This enables monitoring of Provider-1 Customers, Administrators, GUI clients, and other global settings.

- **For a CMA version FP3**:
  a. Select **Custom**.
  b. Select **Backward compatibility for Provider-1 FP3**.
  c. Enter credentials of a Provider-1 Administrator.
  d. Enter the DN of the MDS.
- **For all others**: If you are not certain, select **Default**.

8. Click **Next**.
9. In the monitoring settings:



Monitoring Settings

○ Default

● Custom

Real-Time Monitoring

● Use timing page settings (Configure > Monitoring > Timing)

○ Custom settings:

'Save policy' interval 60 seconds

'Install policy' interval 60 seconds

Automatic fetch frequency 60 minutes

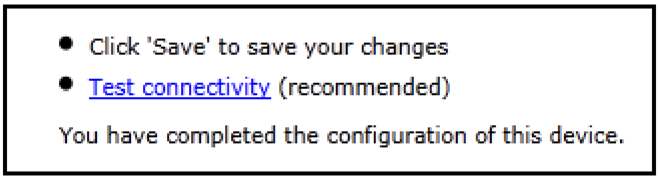
To use timing settings from the Timing configuration for this device, select **Default**.

To define specific timing settings for this device, select Custom, then select **Custom settings**, and configure:

- **'Save policy' interval**: When a Save Policy event is followed within this time interval by an Install Policy event for the same policy, TOS Classic tries to combine the two events into a single revision. The default value is 60 seconds.
    - **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch

Click **Next**.

10. You can test the communication with the Check Point server by clicking **Test Connectivity**:



- Click 'Save' to save your changes
- Test connectivity (recommended)

You have completed the configuration of this device.

11. Click **Save**.

    The Check Point device is shown in the **Device Configuration** list.

    If you use non-standard LEA authentication, see this technical note.

12. If you have a secondary Check Point management server, configure TOS Classic to communicate with the secondary server in the event of a failover.

To customize the device object that represents the Internet, see Define Internet Object.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Check Point R8x Management Devices

See the following topics to add Check Point R8x Management devices to TOS Classic:

- Adding Check Point R8x MDS Devices
- Adding Check Point R8x CMA Devices
- Adding Check Point R8x SmartCenter Server Devices

Adding Check Point R8x MDS Devices

After you upgrade a monitored Check Point MDS device to R8x, you must upgrade the device in SecureTrack to use Check Point R8x support. A CMA can be assigned to an MDS after the initial configuration is complete.

Prerequisites

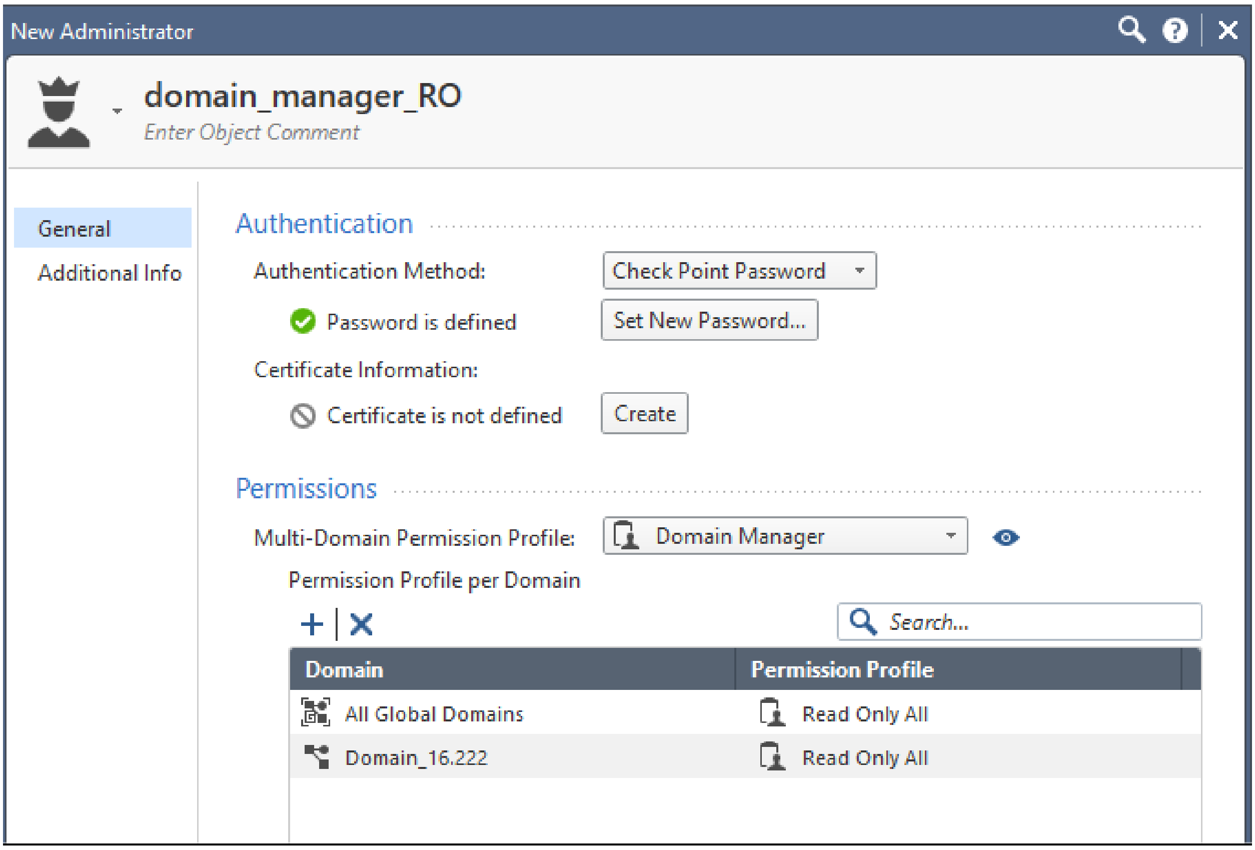
You will need to complete the following prerequisite steps to add Check Point Multi-Domain Security (MDS) devices to SecureTrack:

1. Configure the Check Point server for OPSEC communication with SecureTrack.
2. Configure the Check Point device to use your SecureTrack server as a GUI client.

   The SecureTrack server is displayed in a revision in the GUI client column.
3. Enable the API software blade.
4. Create a Check Point user with Rest API Access to retrieve revisions:
   a. SecureTrack uses Check Point APIs to connect to (and monitor) Check Point R8x devices. A user with the **Domain Manager** profile who has the **Read Only All** Permission Profile configured for **All Global Domains** with the required collection access via the Check Point APIs can retrieve revisions for the device.

   > To allow the SecureChange Designer tool to provision changes to Check Point devices, the API user must have a **Read/Write All** permission profile or a customized profile with API and change permissions for all policies and objects.

   On an MDS:



New Administrator

domain_manager_RO

Enter Object Comment

Authentication

Authentication Method: Check Point Password

✓ Password is defined

Certificate Information:

Certificate is not defined

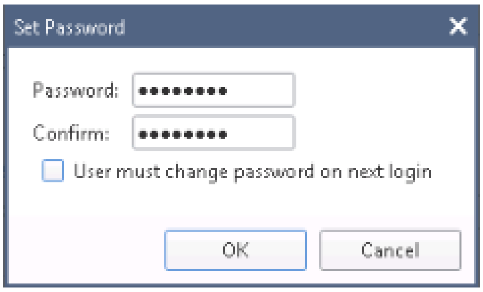
Permissions

Multi-Domain Permission Profile: Domain Manager

Permission Profile per Domain

Domain	Permission Profile
All Global Domains	Read Only All
Domain_16.222	Read Only All

   b. To maintain the password you defined for the Check Point user with REST API access, **in Set Password**, uncheck **User must change password on next login**.



Set Password

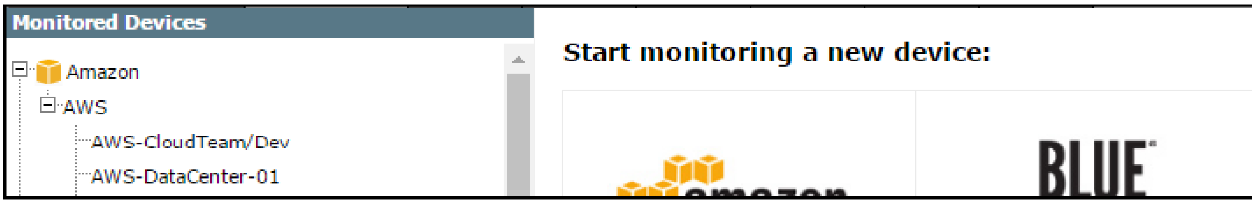
Password: ●●●●●●●●●

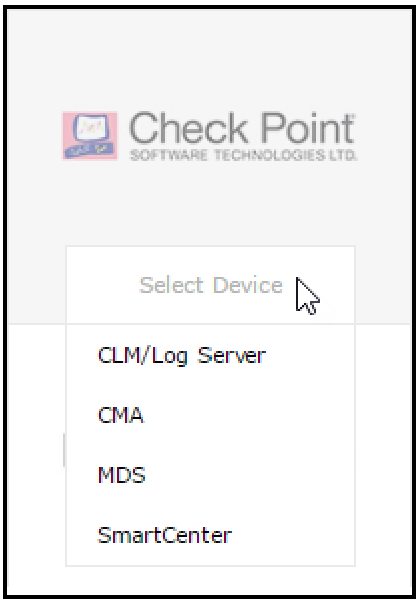
Confirm: ●●●●●●●●●

□ User must change password on next login

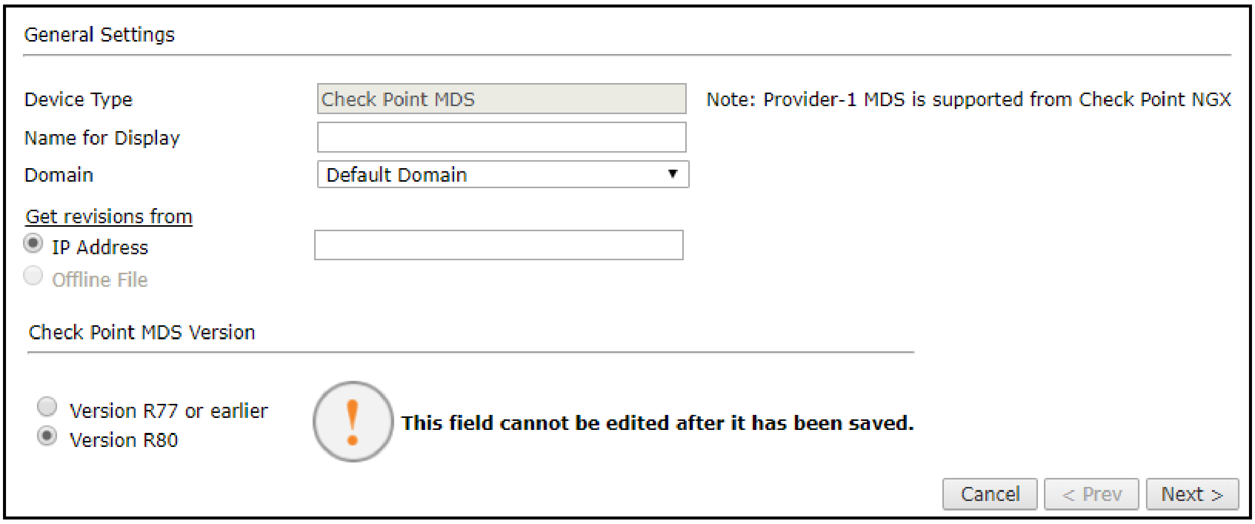
Monitoring a Check Point Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type.





3. Configure the device settings:



General Settings

Device Type: Check Point MDS — Note: Provider-1 MDS is supported from Check Point NGX

Name for Display:

Domain: Default Domain ▼

Get revisions from

● IP Address

○ Offline File

Check Point MDS Version

○ Version R77 or earlier

● Version R80

This field cannot be edited after it has been saved.

Depending on the Check Point server type, some or all of the following options will appear:

- **Device Type: Check Point MDS** (filled automatically)
- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:

- **IP Address**: Revisions are retrieved automatically
- **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis

  This option is not available for R80.x MDS devices

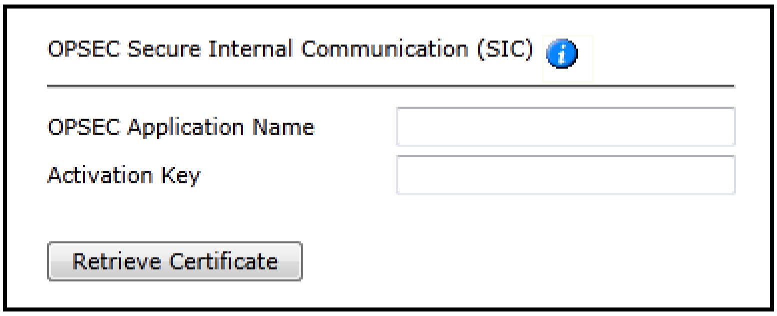
- **Check Point MDS version**: Select the Check Point version installed on the MDS:
  - Version R77 and below
  - Version R8x

  After you save the device configuration, you cannot change this setting.

4. Click **Next**.
5. Configure OPSEC Secure Internal Communication (SIC):
   - Enter TOS Classic's **OPSEC Application Name** as you defined it for this Check Point server (case sensitive).
   - Enter the **Activation Key** as defined when the OPSEC object was created.
   - Click **Retrieve Certificate** to setup encrypted communication between SecureTrack and the Check Point device.

     The certificate appears, and the following message is displayed:

     The certificate was retrieved successfully.

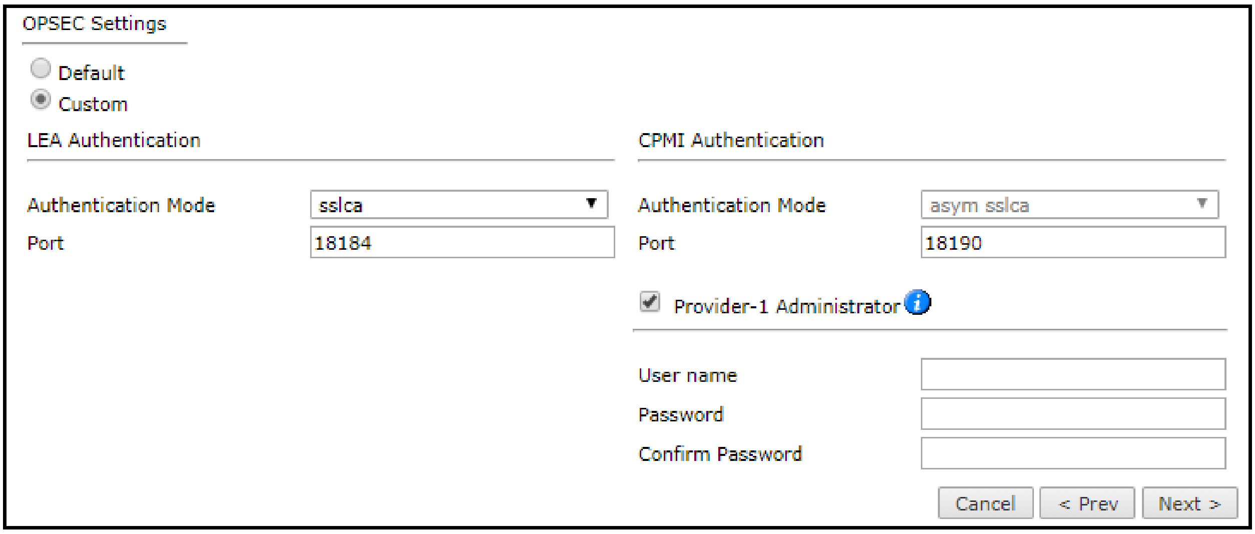


OPSEC Secure Internal Communication (SIC)

OPSEC Application Name

Activation Key

6. Click **Next**.
7. In the **OPSEC Settings**:



OPSEC Settings

○ Default

● Custom

LEA Authentication

Authentication Mode: sslca

Port: 18184

CPMI Authentication

Authentication Mode: asym sslca

Port: 18190

☑ Provider-1 Administrator

User name

Password

Confirm Password

   a. Select **Custom**.

   b. Configure the **LEA Authentication** fields:

   - **Authentication Mode** - Some options require you to enter an **SL** or **FWN1 Secret Key** in the **Authentication Keys**section and **Establish Authentication Key**.
   - **Port**

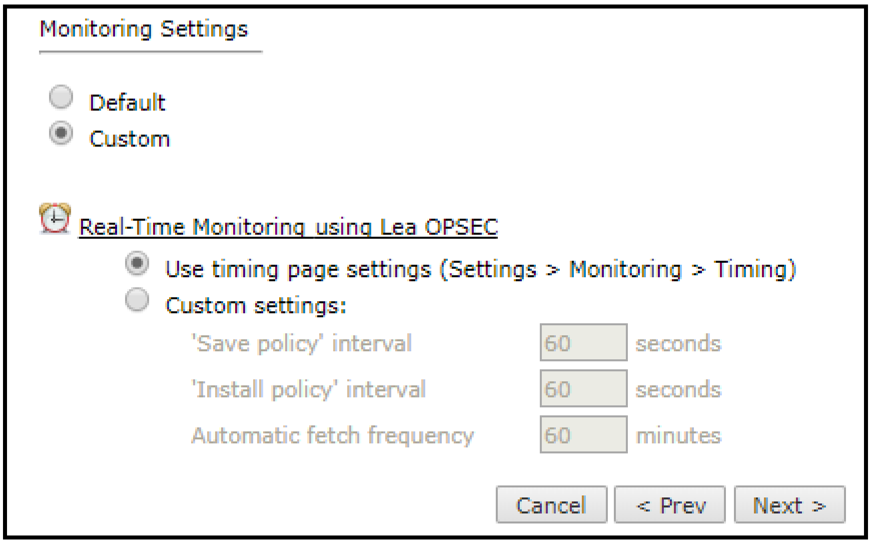
   c. Configure the **CPMI Authentication** fields:

        - **Authentication Mode - asym sslca** (filled automatically)
        - **Port**

    d. To include monitoring of the Global Database for a Provider-1 MDS, select **Provider-1 Administrator** and configure the Provider-1 Superuser credentials.

    For Global Database monitoring, TOS Classic must also be set as a valid GUI client for the MDS.

8. Click **Next**.
9. For a Check Point MDS R8x device, configure the Management API.
10. In the monitoring settings, do one of the following:



Monitoring Settings

○ Default
● Custom

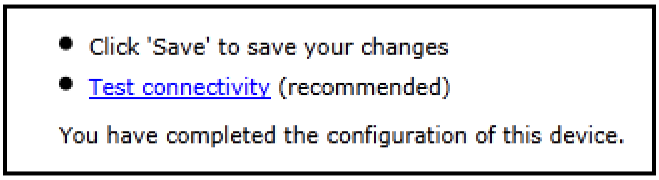
Real-Time Monitoring using Lea OPSEC

● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:

'Save policy' interval 60 seconds
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

    - To use timing settings from the Timing configuration for this device, select **Default**.
    - To define specific timing settings for this device, select **Custom**, then select **Custom settings**, and configure:
        - **'Save policy' interval**: When a Save Policy event is followed within this time interval by an Install Policy event for the same policy, SecureTrack tries to combine the two events into a single revision. The default value is 60 seconds.
        - **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, SecureTrack combines the events into a single Install Policy revision (Default: 60 seconds)
        - **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch

11. Click **Next**.
12. You can test the communication with the Check Point server by clicking **Test Connectivity**:



- Click 'Save' to save your changes
- Test connectivity (recommended)

You have completed the configuration of this device.

13. Click **Save**.

    The Check Point device is shown in the **Device Configuration** list.

    If you use non-standard LEA authentication, see this technical note.

14. If you have a secondary Check Point management server, configure SecureTrack to communicate with the secondary server in the event of a failover.

Define an Internet Object

To customize the device object that represents the Internet, see Define Internet Object.

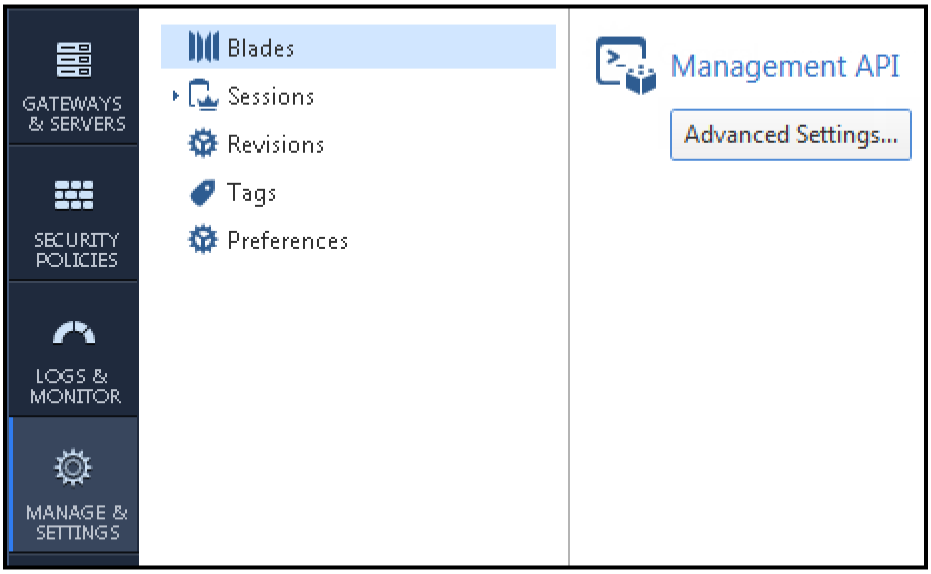
How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**.

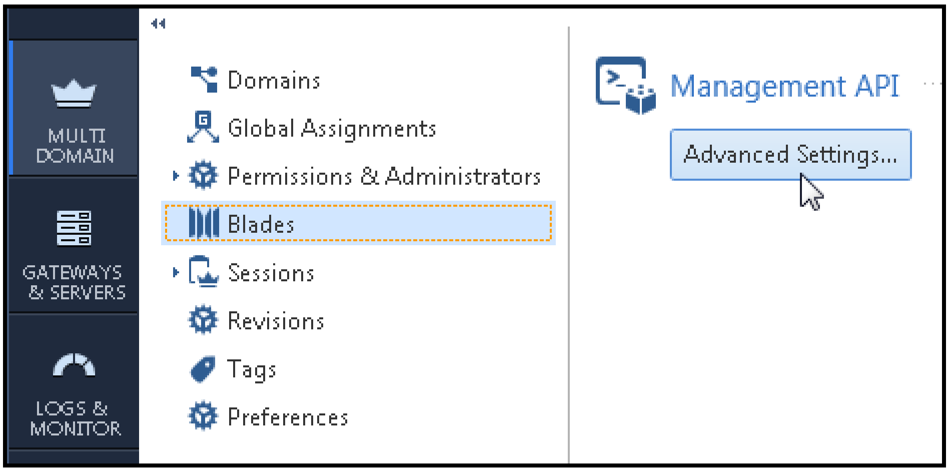
Enabling the API Software Blade

To enable the API software blade

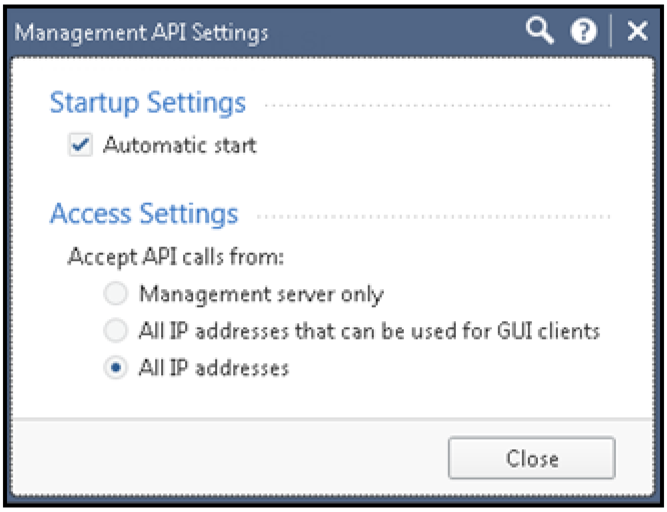
1. Go to Management API **Advanced Settings**.
    - On an SMC or a CMA: **Manage & Settings** > **Blades**



    - On an MDS: **Multi-Domain** > **Blades**



2. Select **Automatic start** and select whether to accept API calls from one of the following options:
    - **All IP addresses that can be used for GUI clients** - More secure, but you must define your SecureTrack server as a GUI client. (See the Check Point documentation.)
    - **All IP addresses** - Less secure because the Check Point MDS accepts API connections from any IP address.



Management API Settings

Startup Settings

☑ Automatic start

Access Settings

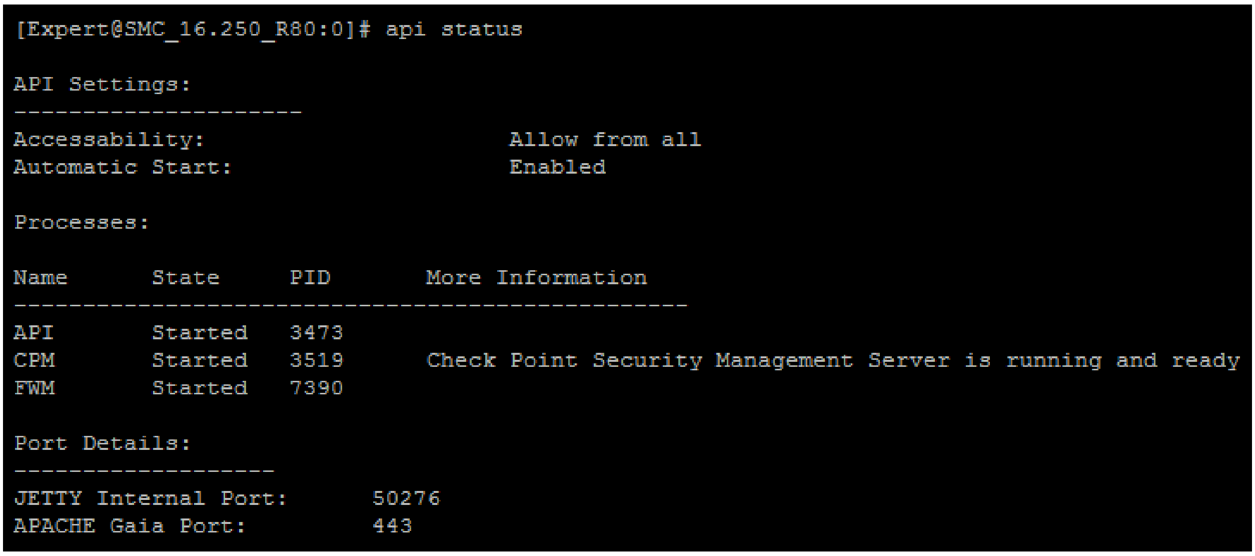
Accept API calls from:

○ Management server only

○ All IP addresses that can be used for GUI clients

● All IP addresses

3. The default API port is 443.
    1. To verify the API port configuration, open the GAIA command line in expert mode and run: `api status`

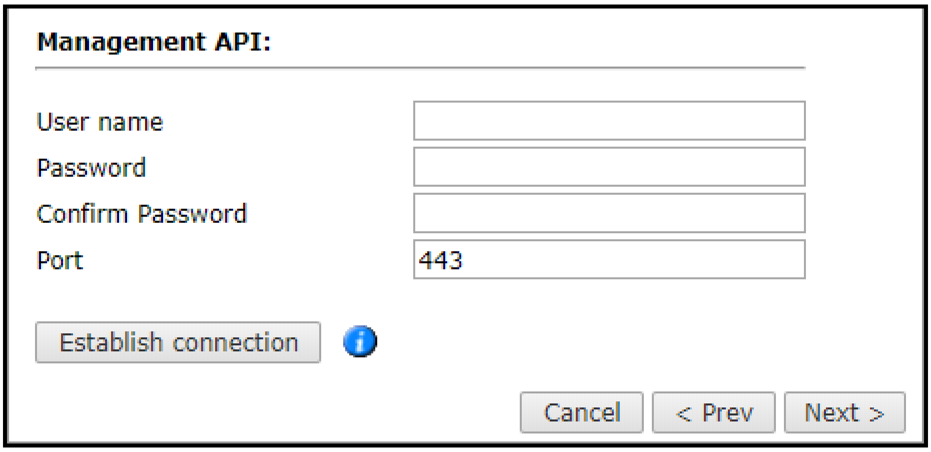


```
[Expert@SMC_16.250_R80:0]# api status

API Settings:
---------------------
Accessability:                      Allow from all
Automatic Start:                    Enabled

Processes:

Name      State     PID       More Information
-------------------------------------------------
API       Started   3473
CPM       Started   3519      Check Point Security Management Server is running and ready
FWM       Started   7390

Port Details:
-------------------
JETTY Internal Port:      50276
APACHE Gaia Port:         443
```

    2. To change the APACHE Gaia port from the default value, refer to the relevant Check Point documentation for port configuration.

CP Management API

1. For R80 devices, in the **Management API** settings:
    1. Enter the credentials for an administrator on the Check Point device.
    2. Enter the port that the Check Point device uses for REST API connections.

    Management API:

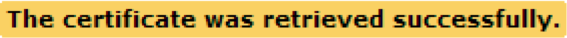
    User name

    Password

    Confirm Password

    Port: 443

    3. Click **Establish Connection** to setup encrypted communication between SecureTrack and the Check Point device. The certificate appears, and the following message appears:

    The certificate was retrieved successfully.

2. Click **Next**.

Adding Check Point R8x CMA Devices

After you upgrade a monitored Check Point CMA device to R8x, you must upgrade the device in SecureTrack to use Check Point R8x support. A CMA can be assigned to an MDS after the initial configuration is complete.

To manage a CMA device in SecureTrack, enable the API software blade for your MDS device.

Prerequisites

To enable a CMA device to monitor the system configuration and performance of a gateway, enable Firewall OS Monitoring.

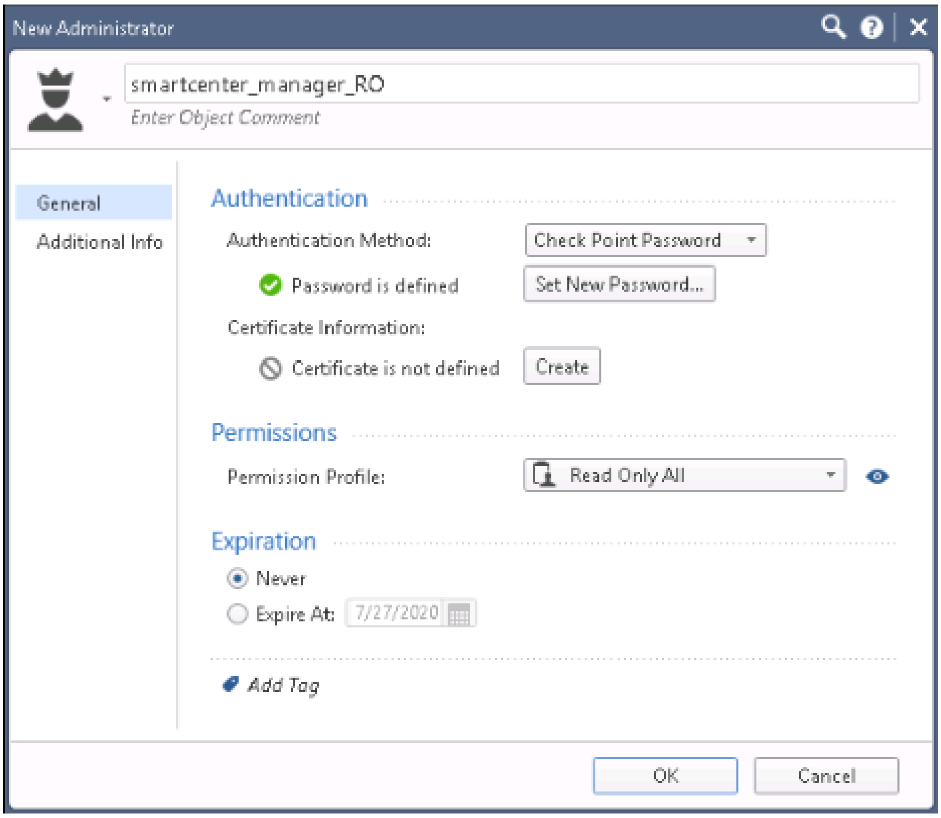
You will need to complete the following prerequisite steps to add Check Point CMA devices to SecureTrack:

1. Configure the Check Point server for OPSEC communication with SecureTrack.
2. Configure the Check Point device to use your SecureTrack server as a GUI client.

    The SecureTrack server is displayed in a revision in the GUI client column.
3. Create a Check Point user with Rest API Access to retrieve revisions:
    a. SecureTrack uses Check Point APIs to connect to (and monitor) Check Point R80.x devices. A user with the **SmartCenter Manager** or **Domain Manager** profile who has the **Read Only All** Permission Profile configured for **All Global Domains** with the required collection access via the Check Point APIs can retrieve revisions for the device.

    > To allow the SecureChange Designer tool to provision changes to Check Point devices, the API user must have a **Read/Write All** permission profile or a customized profile with API and change permissions for all policies and objects.

    On an SMC or a CMA :



New Administrator

smartcenter_manager_RO

Enter Object Comment

General

Additional Info

Authentication

Authentication Method: Check Point Password

✓ Password is defined — Set New Password...

Certificate Information:

Certificate is not defined — Create

Permissions

Permission Profile: Read Only All

Expiration

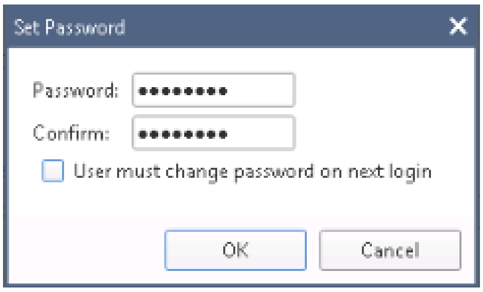
● Never

○ Expire At: 7/27/2020

Add Tag

OK Cancel

b. To maintain the password you defined for the Check Point user with REST API access, in **Set Password**, uncheck **User must change password on next login**.



Set Password

Password: ●●●●●●●●●

Confirm: ●●●●●●●●●

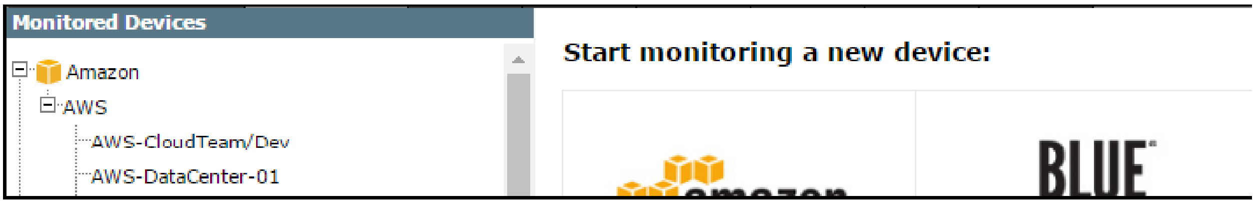
□ User must change password on next login

OK Cancel

Monitor a Check Point Device

To configure SecureTrack to monitor the policy revisions of a Check Point device:

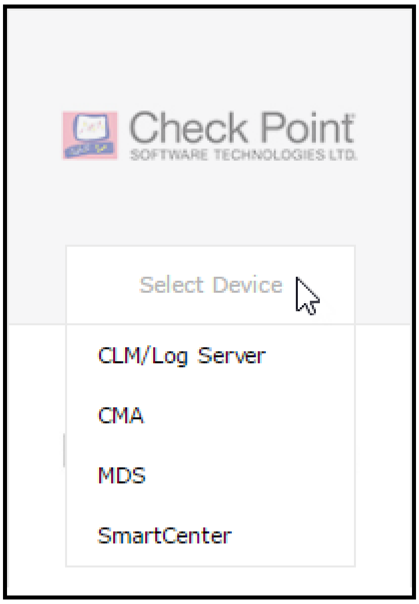
1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type e.g.:



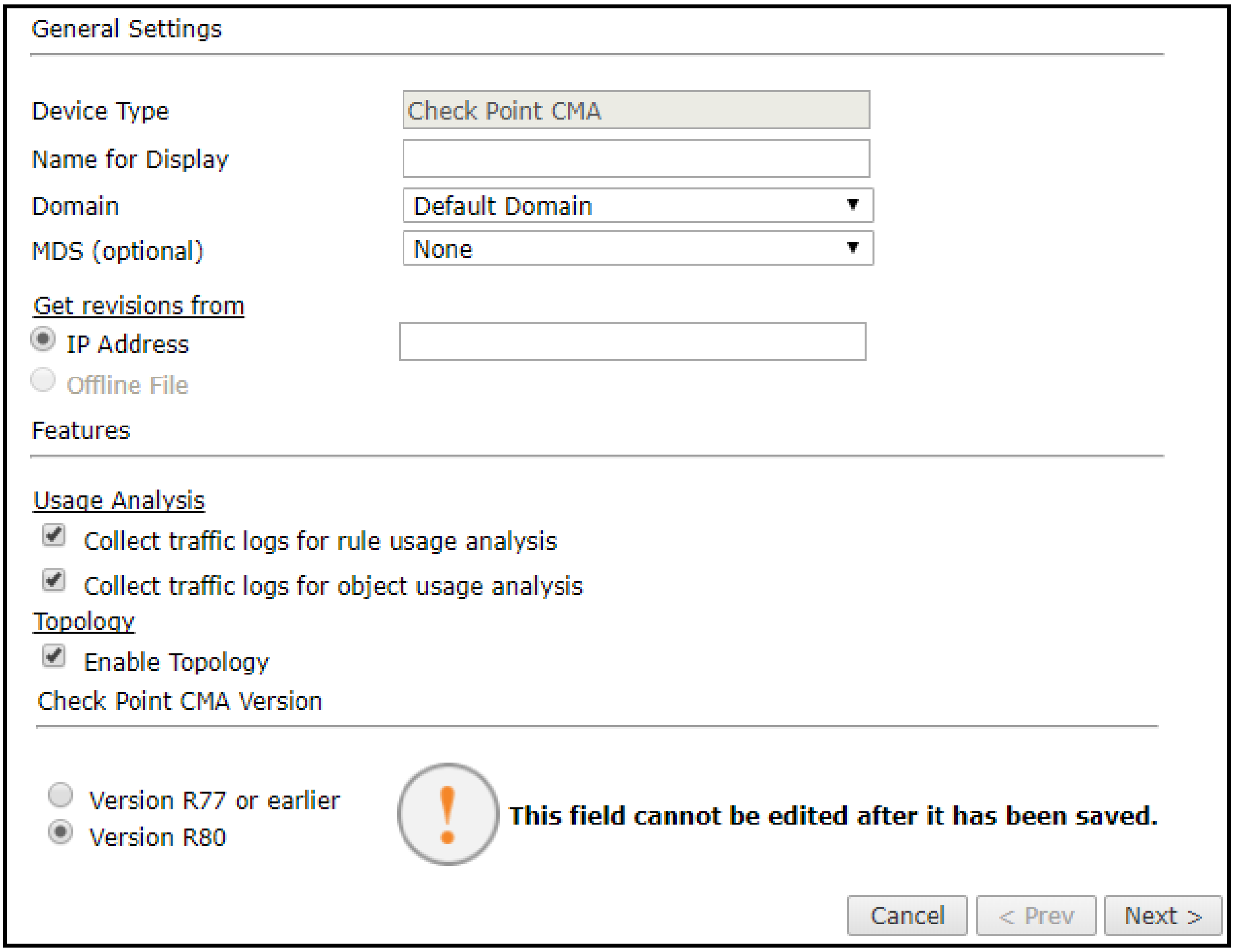
Monitored Devices

Amazon
- AWS
  - AWS-CloudTeam/Dev
  - AWS-DataCenter-01

Start monitoring a new device:



3. Configure the device settings:



General Settings

Device Type	Check Point CMA
Name for Display	
Domain	Default Domain ▼
MDS (optional)	None ▼

Get revisions from

● IP Address

○ Offline File

Features

Usage Analysis

☑ Collect traffic logs for rule usage analysis

☑ Collect traffic logs for object usage analysis

Topology

☑ Enable Topology

Check Point CMA Version

○ Version R77 or earlier

● Version R80

This field cannot be edited after it has been saved.

Depending on the Check Point server type, some or all of the following options will appear:

- Device Type: **Check Point CMA** (filled automatically)
- **Name for Display**

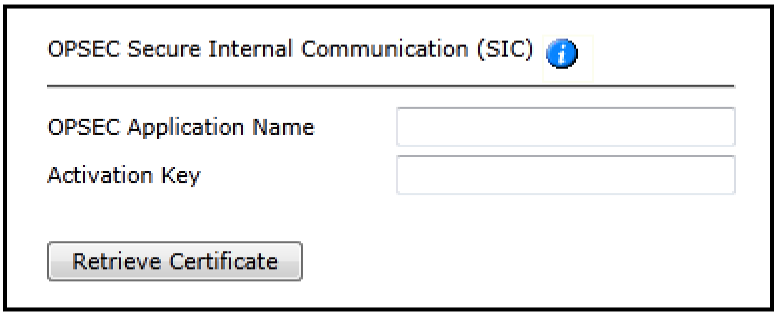
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **MDS** (optional for CMA devices): The MDS that manages the CMA.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis
    This option is not available for R80.x CMA devices
- **Usage Analysis** - select the relevant options:
  - **Collect traffic logs for rule usage analysis** is necessary for Rule Usage reports.
  - **Collect traffic logs for object usage analysis** is necessary for reporting on unused objects and services in Rule Usage Reports.

  Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure SecureTrack to limit the number of days that data is kept.

  We recommend that you enable SecureTrack administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, SecureTrack sends an alert.
- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- **Check Point CMA Version**: Select the Check Point version installed on the SMC/CMA:
  - Version R77 or earlier
  - Version R80.x

  After you save the device configuration, you cannot change this setting.

4. Click **Next**.
5. Configure OPSEC Secure Internal Communication (SIC):



OPSEC Secure Internal Communication (SIC)

OPSEC Application Name

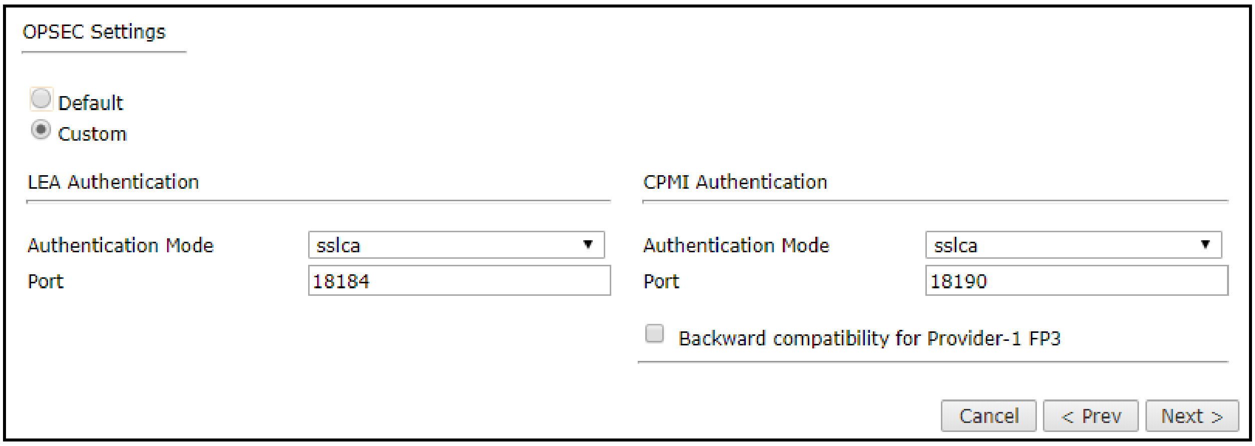
Activation Key

- Enter **SecureTrack's OPSEC Application Name** as you defined it for this Check Point server (case sensitive).
- Enter the **Activation Key** as defined when the OPSEC object was created.
- Click **Retrieve Certificate** to setup encrypted communication between SecureTrack and the Check Point device.

  The certificate appears, and the following message is displayed:

The certificate was retrieved successfully.

6. Click **Next**.
7. In the **OPSEC Settings**:



OPSEC Settings

○ Default
● Custom

LEA Authentication

Authentication Mode	sslca
Port	18184

CPMI Authentication

Authentication Mode	sslca
Port	18190

□ Backward compatibility for Provider-1 FP3

a. Select **Custom**.

b. Configure the **LEA Authentication** fields:

  - **Authentication Mode** - Some options require you to enter an **SL** or **FWN1 Secret Key** in the **Authentication Keys** section and **Establish Authentication Key**.
  - **Port**

c. Configure the **CPMI Authentication** fields:

  - **Authentication Mode** - (For CMA devices **asym sslca**)
  - **Port**

d. **For a CMA version FP3** device, select **Backward compatibility for Provider-1 FP3**.

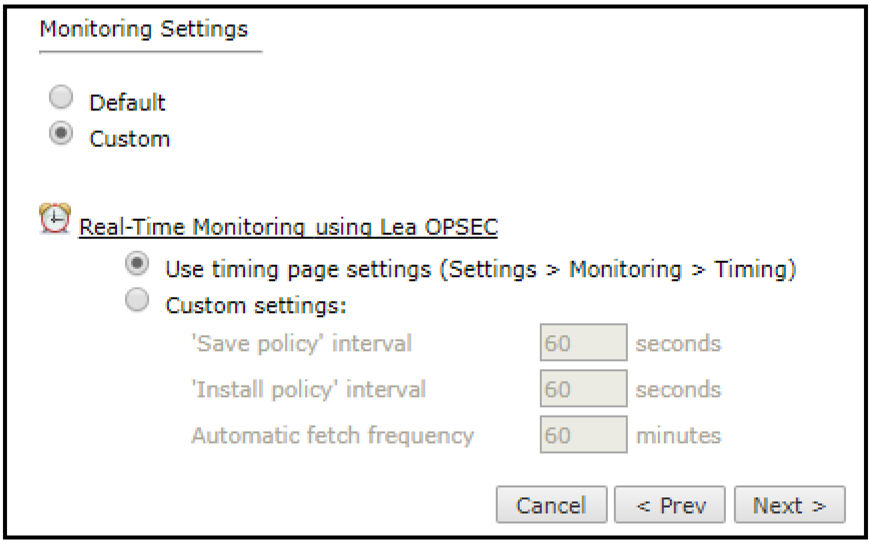
  i. Enter the credentials of a Provider-1 Administrator.

  ii. Enter the DN of the MDS.

8. Click **Next**.

9. For a Check Point CMA R80.x device, configure the Management API.

10. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

Real-Time Monitoring using Lea OPSEC

● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:

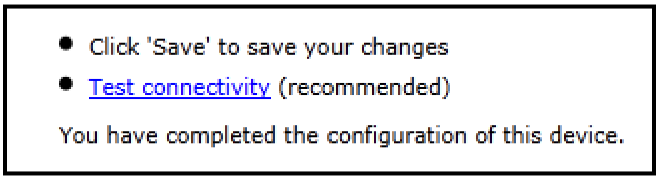
'Save policy' interval	60	seconds
'Install policy' interval	60	seconds
Automatic fetch frequency	60	minutes

- To use timing settings from the Timing configuration for this device, select **Default**.
- To define specific timing settings for this device, select **Custom**, then select **Custom settings**, and configure:
  - **'Save policy' interval**: When a Save Policy event is followed within this time interval by an Install Policy event for the same policy, SecureTrack tries to combine the two events into a single revision. The default value is 60 seconds.
  - **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval,

SecureTrack combines the events into a single Install Policy revision (Default: 60 seconds)

- Automatic fetch frequency: Frequency (in minutes) for automatic fetch

11. Click **Next**.
12. You can test the communication with the Check Point server by clicking **Test Connectivity**:



- Click 'Save' to save your changes
- Test connectivity (recommended)

You have completed the configuration of this device.

13. Click **Save**.

    The Check Point device is shown in the **Device Configuration** list.

    If you use non-standard LEA authentication, see this technical note.

14. If you have a secondary Check Point management server, configure SecureTrack to communicate with the secondary server in the event of a failover.

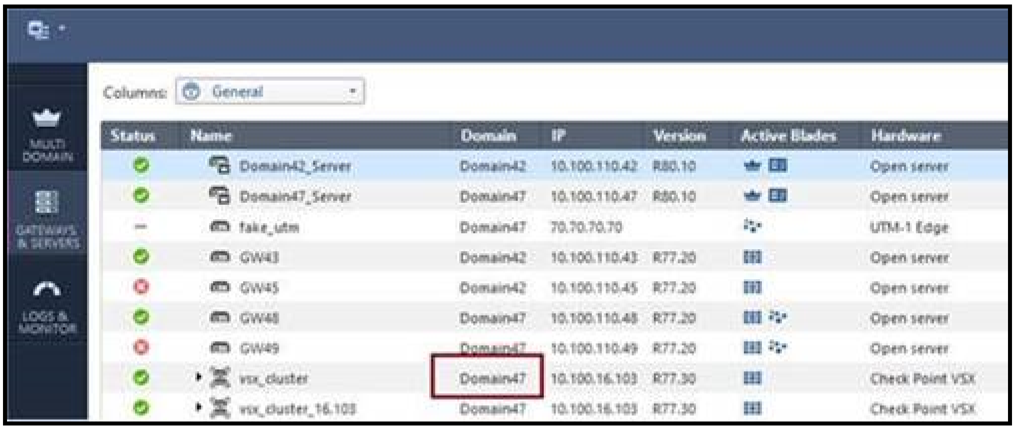
Define an Internet Object

To customize the device object that represents the Internet, see Define Internet Object.

Enabling Check Point CMA Devices for Topology

To obtain topology information for VSX virtual devices, SecureTrack must also monitor the CMA management server that manages the physical VSX box. To ensure that topology information is being retrieved, verify that the relevant CMA is monitored by SecureTrack.

In the following example, the **vsx_cluster** is managed by the **Domain47** CMA. To properly monitor this cluster and retrieve its topology information, you must verify that **Domain47** has also been added to SecureTrack.



Columns: General

Status	Name	Domain	IP	Version	Active Blades	Hardware
✓	Domain42_Server	Domain42	10.100.110.42	R80.10		Open server
✓	Domain47_Server	Domain47	10.100.110.47	R80.10		Open server
—	fake_utm	Domain47	70.70.70.70			UTM-1 Edge
✓	GW43	Domain42	10.100.110.43	R77.20		Open server
✕	GW45	Domain42	10.100.110.45	R77.20		Open server
✓	GW48	Domain47	10.100.110.48	R77.20		Open server
✕	GW49	Domain47	10.100.110.49	R77.20		Open server
✓	vsx_cluster	Domain47	10.100.16.103	R77.30		Check Point VSX
✓	vsx_cluster_16.103	Domain47	10.100.16.103	R77.30		Check Point VSX

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Check Point R8x SmartCenter Server Devices

Overview

You must configure the Check Point servers in the following order: Provider-1 MDS, Provider-1 CMAs, SmartCenter servers (SMCs), and Log Servers (CLMs).

After you upgrade a monitored Check Point SmartCenter device to R80.x, you must upgrade the device in TOS Classic to use Check Point R8x support.

Prerequisites

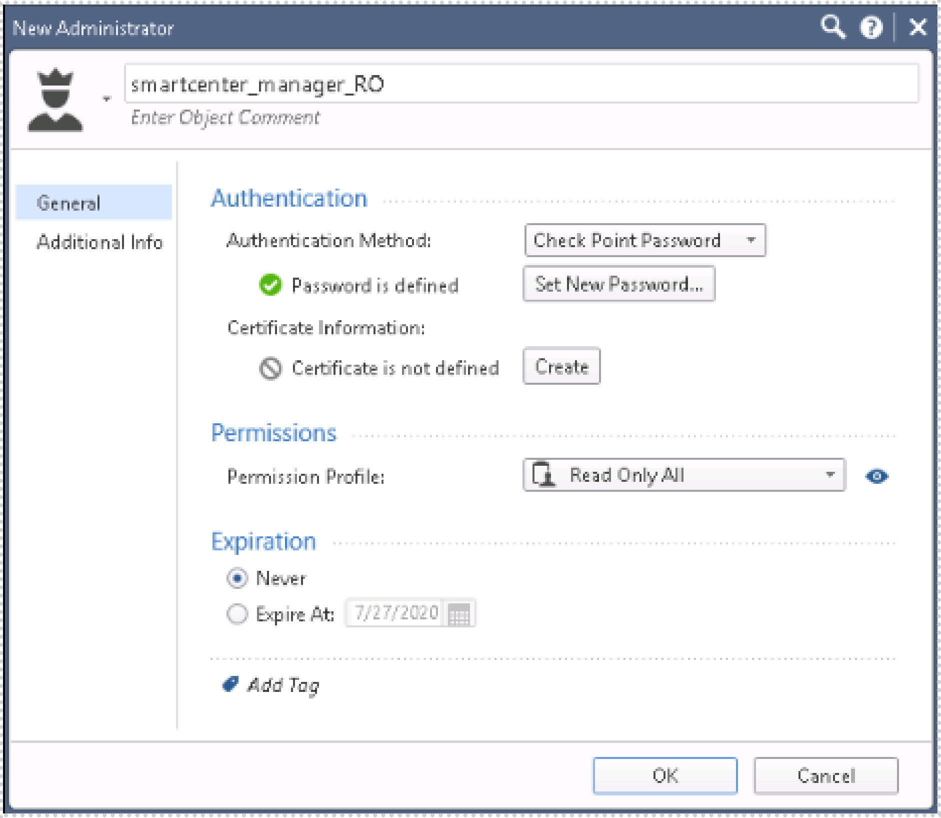
Enable a SmartCenter (SMC) Device

Enable a SmartCenter (SMC) device to monitor the system configuration and Performance of a Gateway, enable Firewall OS Monitoring.

You will need to complete the following prerequisite steps to add Check Point SmartCenter devices to TOS Classic:

1. Configure the Check Point server for OPSEC communication with TOS Classic.
2. Configure the Check Point device to use your TOS Classic server as a GUI client.

   The TOS Classic server is displayed in a revision in the GUI client column.
3. For SMC devices, enable the API software blade.
4. Create a Check Point user with Rest API Access to retrieve revisions:
   a. TOS Classic uses Check Point APIs to connect to (and monitor) Check Point R80.x devices. A user with the **SmartCenter Manager or Domain Manager** profile who has the **Read Only All** Permission Profile configured for **All Global Domains** with the required collection access via the Check Point APIs can retrieve revisions for the device. On an SMC or a CMA:



New Administrator

smartcenter_manager_RO

Enter Object Comment

General | Additional Info

Authentication

Authentication Method: Check Point Password

✓ Password is defined — Set New Password...

Certificate Information:

Certificate is not defined — Create

Permissions

Permission Profile: Read Only All

Expiration

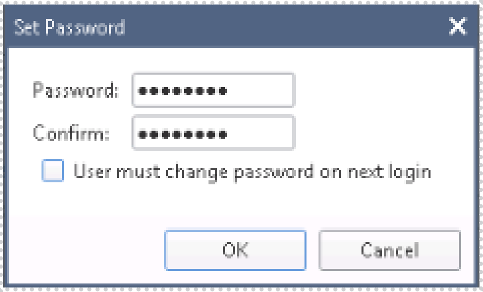
● Never

○ Expire At: 7/27/2020

Add Tag

OK | Cancel

   b. To maintain the password you defined for the Check Point user with REST API access, in **Set Password**, uncheck **User must change password on next login**.



Set Password

Password: ●●●●●●●●

Confirm: ●●●●●●●●

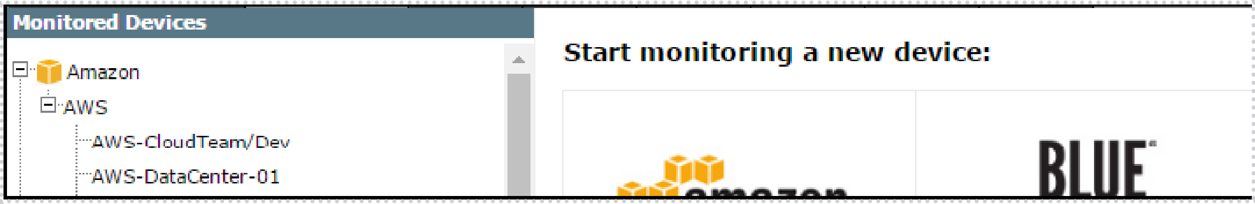
□ User must change password on next login

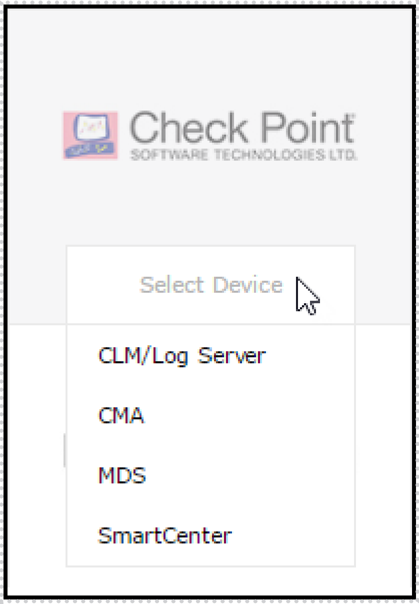
OK | Cancel

What Can I Do Here?

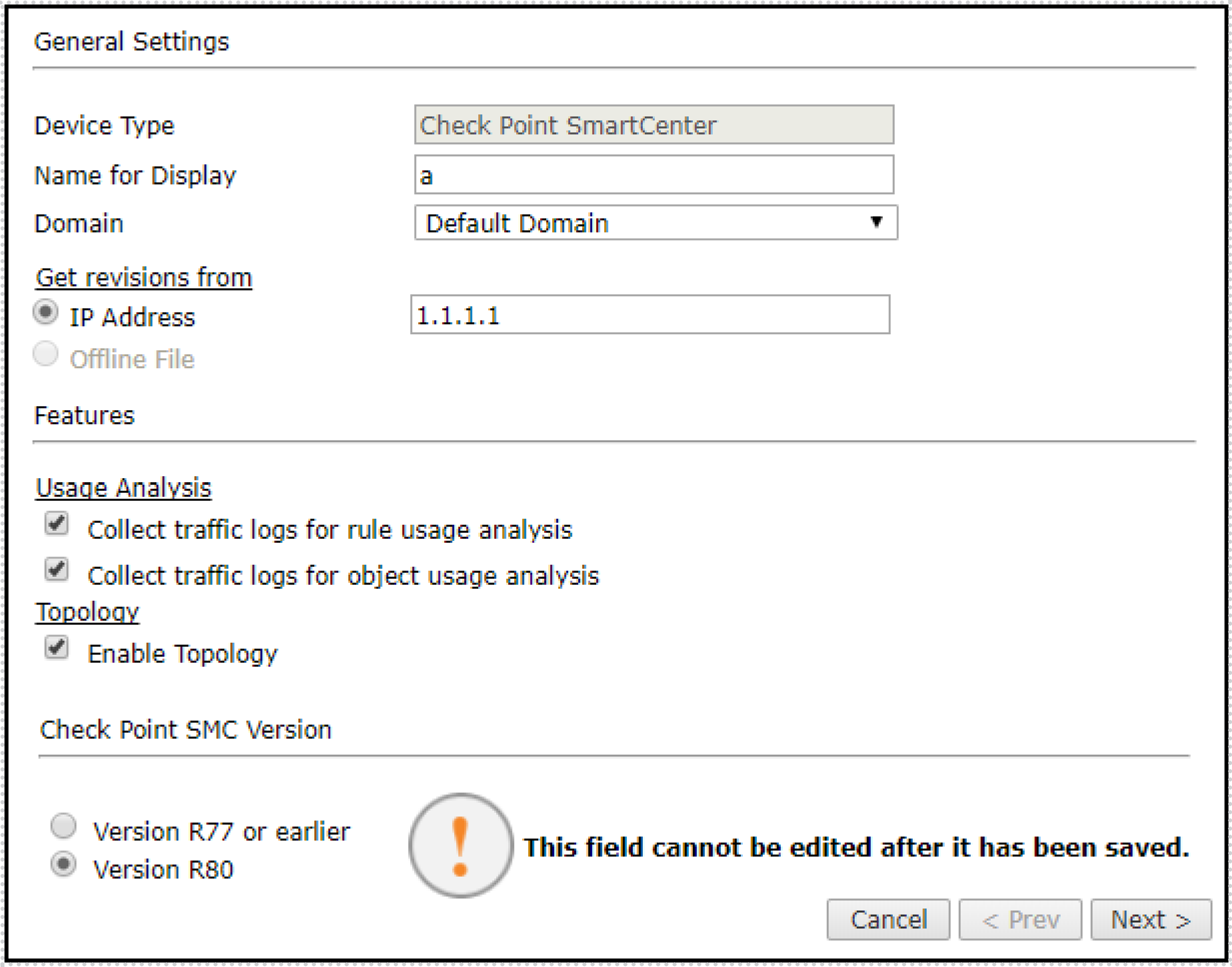
Configuring TOS Classic to Monitor the Policy Revisions of a Check Point Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type.





3. Configure the device settings:



General Settings

Device Type: Check Point SmartCenter

Name for Display: a

Domain: Default Domain ▼

Get revisions from

● IP Address 1.1.1.1

○ Offline File

Features

Usage Analysis

☑ Collect traffic logs for rule usage analysis

☑ Collect traffic logs for object usage analysis

Topology

☑ Enable Topology

Check Point SMC Version

○ Version R77 or earlier

● Version R80

This field cannot be edited after it has been saved.

Depending on the Check Point server type, some or all of the following options will appear:

- **Device Type**: **Check Point SmartCenter**
- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address:** Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
    This option is not available for R80.x SMC devices
- **Usage Analysis**: Select the relevant options:
  - **Collect traffic logs for rule usage analysis**: Necessary for Rule Usage reports.
  - **Collect traffic logs for object usage analysis** : Necessary for reporting on unused objects and services in Rule Usage Reports.

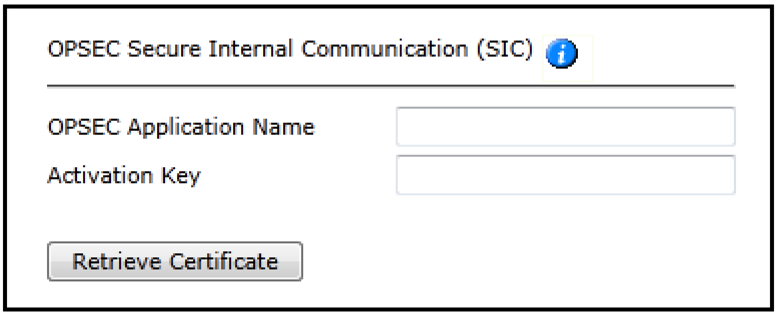
> Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure TOS Classic to limit the number of days that data is kept.

> We recommend that you enable TOS Classic administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, TOS Classic sends an alert.

- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- **Check Point SMC Version**: Select the Check Point version installed on the SMC:
  - Version R77 or earlier
  - Version R80.x

  After you save the device configuration, you cannot change this setting.

4. Click **Next**.
5. Configure OPSEC Secure Internal Communication (SIC):



OPSEC Secure Internal Communication (SIC)

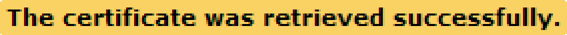
OPSEC Application Name

Activation Key

Retrieve Certificate

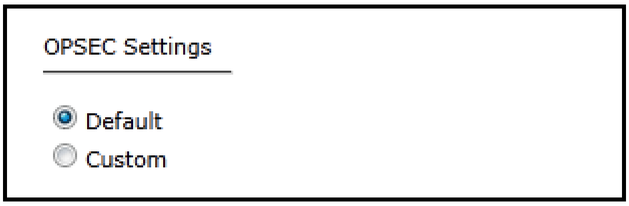
- Enter TOS Classic's **OPSEC Application Name** as you defined it for this Check Point server (case sensitive).
- Enter the **Activation Key** as defined when the OPSEC object was created.
- Click **Retrieve Certificate** to setup encrypted communication between TOS Classic and the Check Point device.

  The certificate appears, and the following message is displayed:



The certificate was retrieved successfully.

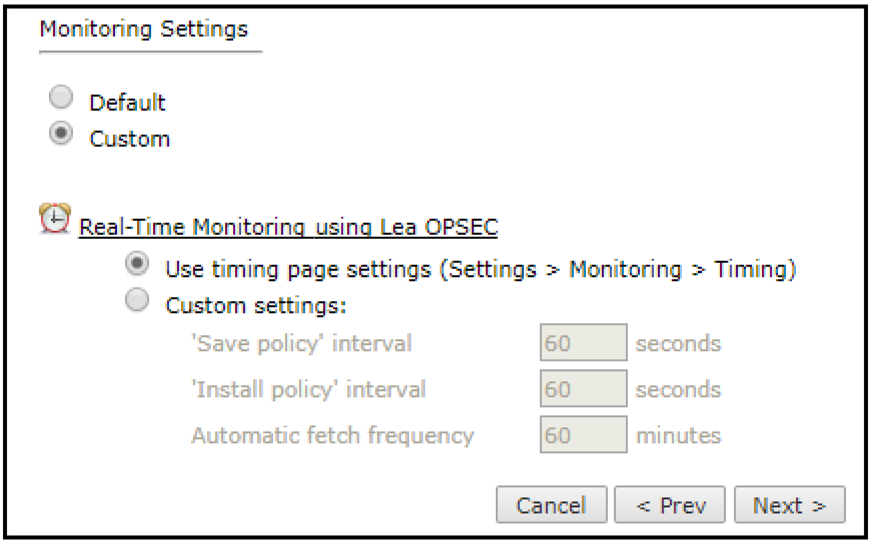
6. Click **Next**.
7. In the **OPSEC Settings**:



OPSEC Settings

● Default
○ Custom

   a. Select **Custom**.
   b. Configure the **LEA Authentication** fields:
      - **Authentication Mode**: Some options require you to enter an SL or FWN1 Secret Key in the Authentication Keys section and Establish Authentication Key.
      - **Port**
   c. Configure the **CPMI Authentication** fields:
      - **Authentication Mode**
      - **Port**
8. Click **Next**.
9. For a Check Point SmartCenter Server R80.x device, configure the Management API.
10. In the **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

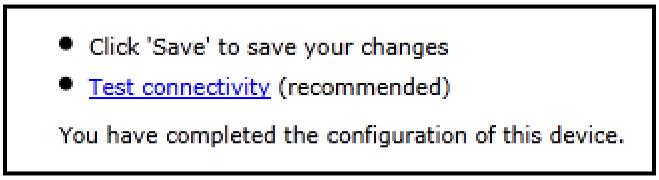
Real-Time Monitoring using Lea OPSEC

● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:

'Save policy' interval 60 seconds
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

- To use timing settings from the Timing configuration for this device, select Default.
- To define specific timing settings for this device, select **Custom**, then select **Custom settings**, and configure:
  - **'Save policy' interval**: When a Save Policy event is followed within this time interval by an Install Policy event for the same policy, TOS Classic tries to combine the two events into a single revision. The default value is 60 seconds.
  - **'Install policy' interval:** When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
  - **Automatic fetch frequency:** Frequency (in minutes) for automatic fetch

11. Click **Next**.
12. You can test the communication with the Check Point server by clicking **Test Connectivity**:



- Click 'Save' to save your changes
- Test connectivity (recommended)

You have completed the configuration of this device.

13. Click **Save**.

    The Check Point device is shown in the **Device Configuration** list.

    If you use non-standard LEA authentication, see this technical note.
14. If you have a secondary Check Point management server, configure TOS Classic to communicate with the secondary server in the event of a failover.

Define an Internet Object

To customize the device object that represents the Internet, see Define Internet Object.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Check Point CLM/Log Server Devices

You must configure the Check Point servers in the following order: Provider-1 MDS, Provider-1 CMAs, SmartCenter servers (SMCs), and Log Servers (CLMs).

Prerequisites

You will need to complete the following prerequisite steps to add Check Point CLM/Log Server devices to SecureTrack:

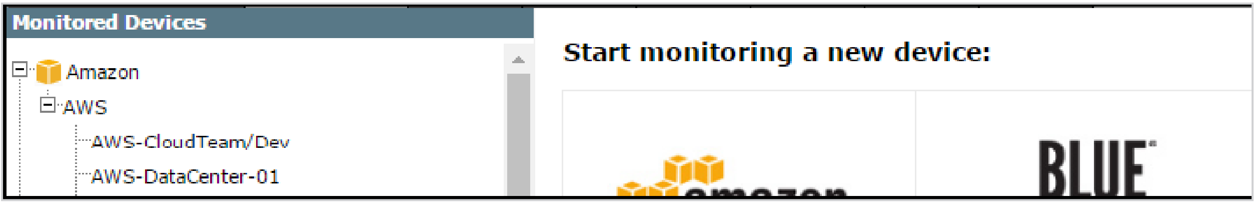
- Configure the Check Point Management server for OPSEC communication with SecureTrack.

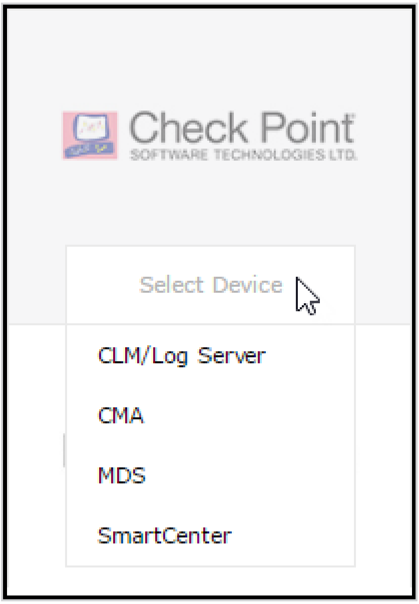
To allow the SecureChange Designer tool to provision changes to Check Point devices, the API user must have a **Read/Write All** permission profile or a customized profile with API and change permissions for all policies and objects.

Monitor a Check Point Device

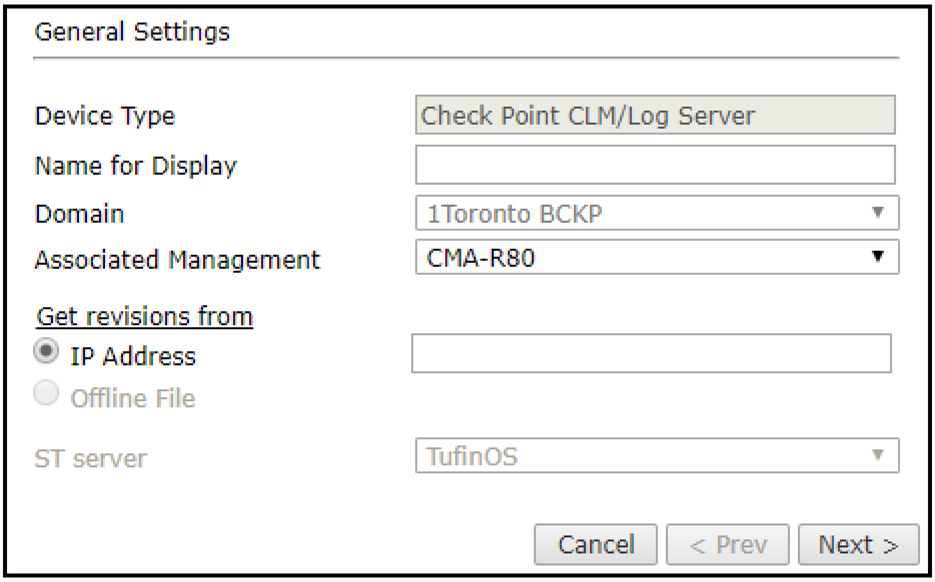
To configure TOS Classic to monitor Check Point LEA logs:

1. Select the appropriate device type e.g.:





2. Configure the device settings:



General Settings

Device Type	Check Point CLM/Log Server
Name for Display	
Domain	1Toronto BCKP
Associated Management	CMA-R80

Get revisions from

● IP Address

○ Offline File

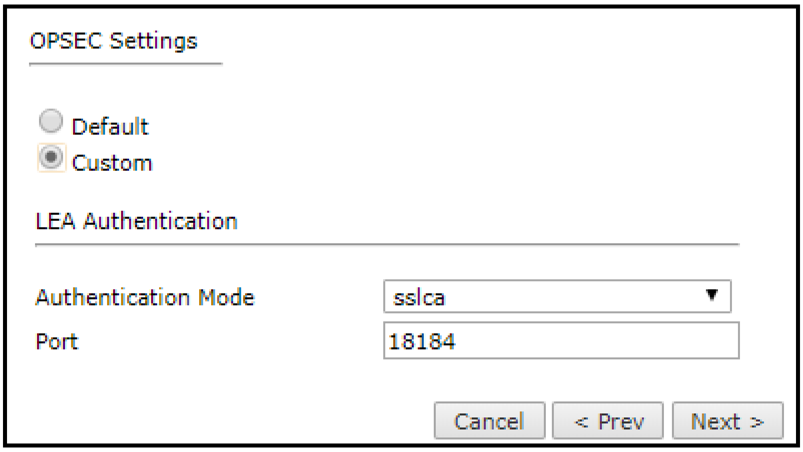
ST server: TufinOS

Depending on the Check Point server type, some or all of the following options will appear:

- **Device Type: Check Point CLM/Log Server**
- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Associated Management**: The SmartCenter sending logs to the Log Server, or the CMA sending the logs to the CLM.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis
    This option is not available for Check Point CLM/Log Server devices.
- **ST server**: In a distributed deployment, select which SecureTrack server monitors this device (Not shown in image)
  This option is not available for CLM/Log Server devices.

  For a Log Server/CLM, make sure the monitoring SecureTrack server is the same as for the Log Server/CLM's associated Check Point management server (SmartCenter/CMA).

3. Click **Next**.
4. Configure the OPSEC communication settings:
   - **Default**
   - **Custom** - Configure the **LEA Authentication** fields:
     - **Authentication Mode** - Some options require you to enter an **SL** or **FWN1 Secret Key** in the **Authentication Keys** section and **Establish Authentication Key**.
     - **Port**



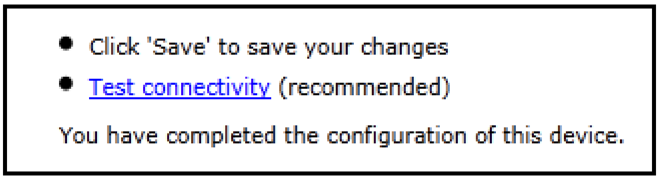
OPSEC Settings

○ Default
● Custom

LEA Authentication

Authentication Mode: sslca
Port: 18184

5. Click **Next**.
6. You can test the communication with the Check Point server by clicking **Test Connectivity**:



- Click 'Save' to save your changes
- Test connectivity (recommended)

You have completed the configuration of this device.

7. Click **Save**.

   The Check Point device is shown in the **Device Configuration** list.

   If you use non-standard LEA authentication, see this technical note.
8. If you have a secondary Check Point management server, configure SecureTrack to communicate with the secondary server in the event of a failover.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Upgrading to Check Point R80 Support

Check Point R80 devices use CPMI and REST API protocols to integrate with SecureTrack. After you upgrade your Check Point devices, some SecureTrack features stop working until you upgrade the device in SecureTrack to R80 support.

During the upgrade, you connect to the host Check Point MDS for the CMA. SecureTrack shows a list of all CMAs on the MDS and on any other MDSs that are configured for High Availability. All CMAs that are shown are upgraded to R80 support at the same time.

SecureTrack gives the same feature support for R80 devices as for versions lower than R80, except for the Baseline Settings Compliance Report. If you have a Baseline Settings Compliance Report configured, you must delete it before you can upgrade to R80 support.

Prerequisites

Before you upgrade to R80 support, you must have:

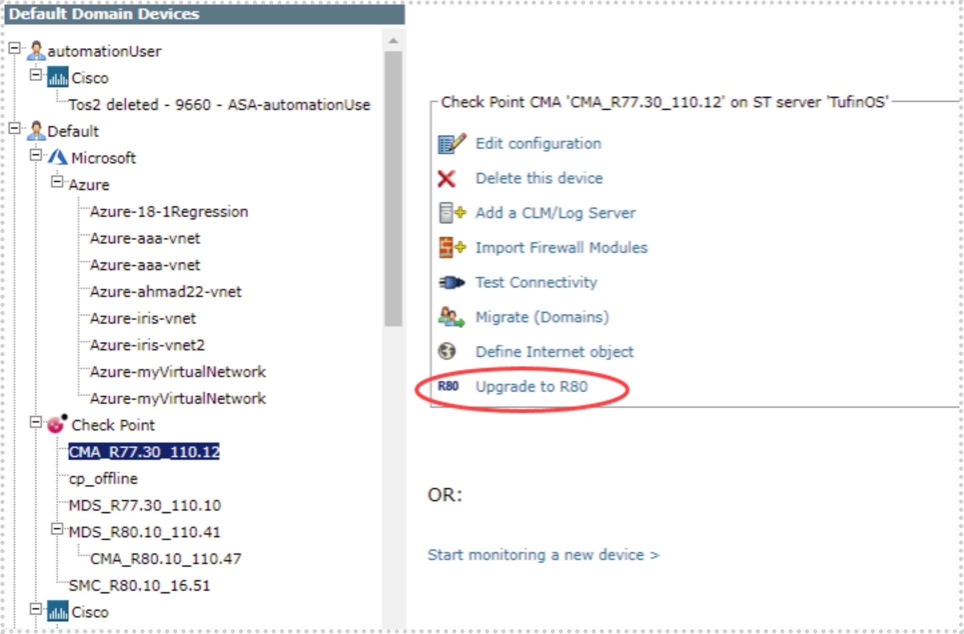
- A SecureTrack user with administrator permissions. (In Multi-Domain mode, the user must have Multi-Domain superuser permissions.)
- A Check Point MDS user with multi-domain superuser permissions.
- The port that the Check Point MDS uses for REST API connections.

To ensure that you the SecureTrack server has been granted access to the Check Point API server, follow the resolution steps in Troubleshooting: Check Point R80 - "CheckPoint API client error".

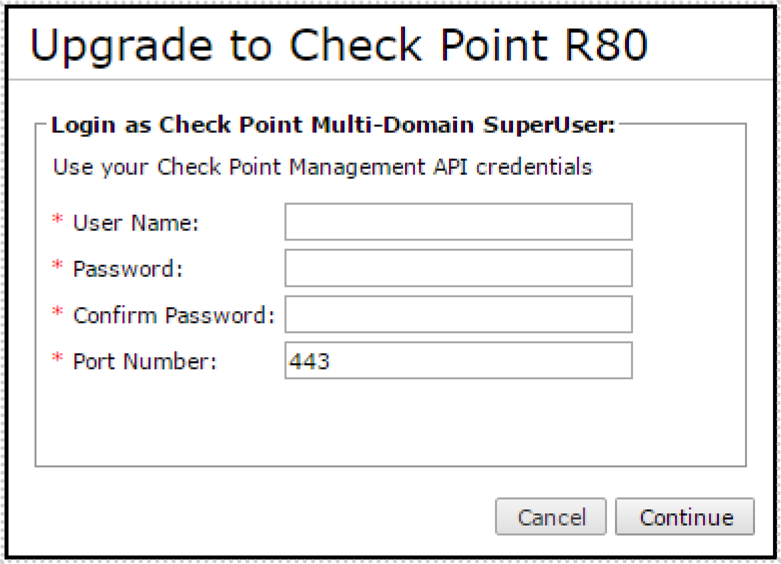
Procedure

To upgrade a CMA to R80 support:

1. Select a Check Point CMA device from the list of monitored devices, example below.
2. Click **Upgrade to R80**.



3. Enter:
   - The credentials for a multi-domain superuser on the MDS
   - The port that the Check Point MDS uses for REST API connections (Default port is 443)



Upgrade to Check Point R80

Login as Check Point Multi-Domain SuperUser:

Use your Check Point Management API credentials

* User Name:

* Password:

* Confirm Password:

* Port Number: 443

4. Click **Continue**.
5. Review the list of devices to upgrade to R80 support.
6. Click **Upgrade**.

   The upgrade process may take a few minutes to complete. Do not leave the page of the upgrade process until the upgrade process is complete.
7. When the upgrade process is complete, click **Done**.

Troubleshooting: Check Point R80 - "CheckPoint API client error"

Symptom

TOS returns a **Checkpoint API client error** even though a status check on the Check Point R80 API server shows that it running.

Check the Status of the Check Point API server

- Run the following commands to display the status of the API server:

```
[[[Undefined variable Local.admin-hash-prompt]]]expert
                    [[[Undefined variable Local.admin-hash-prompt]]]api
status
```

The output displays the following:

```
-------------------------------------------
                    Overall API Status: Started
                    -------------------------------------------
                    Test SUCCESSFUL. The server is up and ready to
receive connections

```

Cause

You do not have permission to access `/web_api/login` on this server. You can verify the cause by looking at the following log files on the Tufin server:

- `/var/log/st/securetrack.client.*_id`

```
--> 42299 20220531 22:36:23.031  ::err_exception
                        FAULT: 42299 20220531
22:36:23.031  Checkpoint API client error at: static std::string
CCheckpointR80PlusApiClient::Expect(const string&, const
TStringBoolPairVector&, const CCheckpointR80PlusApiClientArgs&,
const TStringVector&)
                        FAULT: 25335 20220531 22:10:31.492  File:
/root/jenkins/workspace/tss/securetrack/checkpoint/libcheckpoint/Che
ckpointR80PlusApiClient.cc:232

```

- `/var/log/st/checkpoint.get_checkpoint_conf_<IP>`

```
Checkpoint error code: http_forbidden API: CPApi#loginToMds
(CPObjectParamLogin), Status Code: 403, Error Code: http_forbidden
on Domain:
                        ERROR 2017-04-03 11:06:44,838
[main::c.t.s.c.AbstractClient.retrieveConf] [user:] Failed to
retrieve device configuration [ ]
                        com.tufin.securetrack.javatool_
util.ClientException: Cannot init Checkpoint SDK
                        Caused by:
com.tufin.checkpoint.entities.CPException: <!DOCTYPE HTML PUBLIC "-
//IETF//DTD HTML 2.0//EN">
                        <html><head>
                        <title>403 Forbidden</title>
                        </head><body>
                        <h1>Forbidden</h1>
                        <p>You don't have permission to access /web_
api/v1/login
                        on this server.</p>
                    </body></html>
```

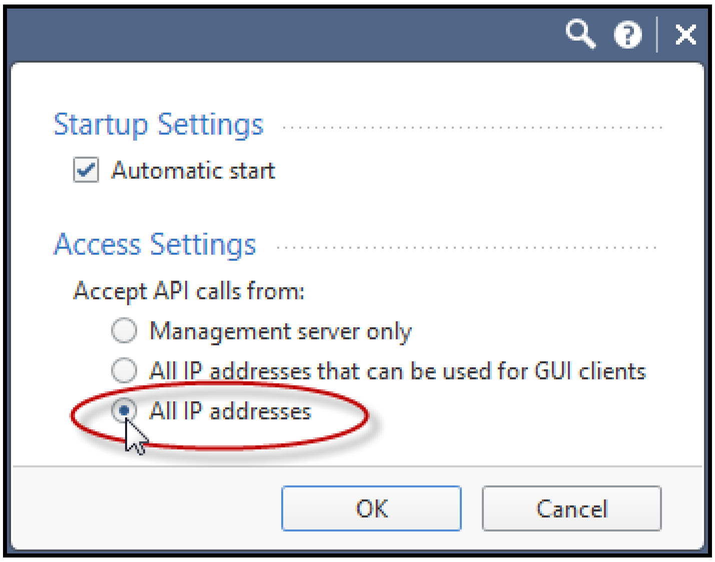
Resolution

1. Open SmartConsole and log in to the management server.

   If you have a multi-domain environment, log in to the MDS domain.

2. Click the **Manage and Settings** button.
3. Select **Blades**.

4. In the **Management API** section, click **Advanced Settings**.
5. Select **All IP addresses** to grant the SecureTrack server access to the API server.



Startup Settings

☑ Automatic start

Access Settings

Accept API calls from:

○ Management server only

○ All IP addresses that can be used for GUI clients

● All IP addresses

6. Click **Publish**.
7. Connect to the Check Point management server via SSH and and restart the API:

```
[[[Undefined variable Local.admin-hash-prompt]]]expert
```

```
                [[[Undefined variable Local.admin-hash-prompt]]]api
restart
```

Firewall OS Monitoring

This is a Legacy Feature. This feature will not be available in future releases of TOS Classic.

Firewall OS Monitoring extends SecureTrack's capabilities into the realm of actual device configuration changes, as well as monitoring the devices' performance and health. Firewall OS Monitoring is supported for Check Point gateways on supported operating systems using SNMPv3, and requires a separate license in SecureTrack.

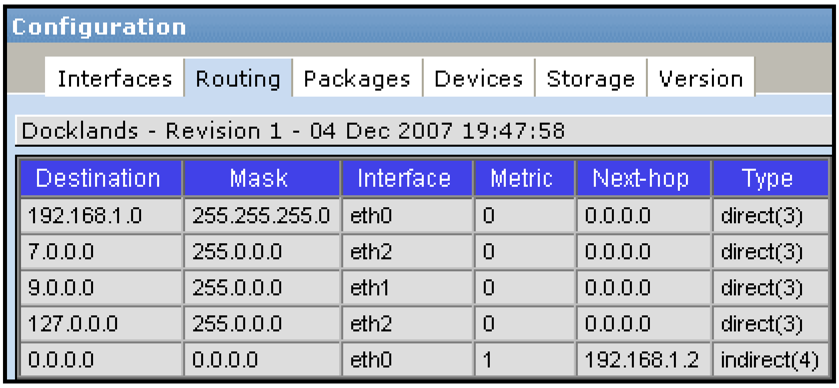
The combination of SecureTrack's policy revision information and Firewall OS monitoring gives administrators and auditors a complete picture of any change that occurred on the firewall.

SecureTrack periodically connects to monitored firewall devices via SNMPv3, and retrieves different types of data:

- OS-level configuration data, such as interfaces, routing tables, file system partitions, etc.
- Real-time performance data, such as CPU and disk utilization

This information is obtained from periodic SNMPv3 connections to monitored Check Point gateways. Whenever a configuration change is made, SecureTrack records a new OS-level revision, and sends out detailed change reports to designated SecureTrack users. In addition, users can view performance graphs for each monitored firewall, and configure real-time alerts based on OS-related thresholds.

The Firewall OS Monitoring information is arranged in a number of tabs:



Configuration

Docklands - Revision 1 - 04 Dec 2007 19:47:58

Destination	Mask	Interface	Metric	Next-hop	Type
192.168.1.0	255.255.255.0	eth0	0	0.0.0.0	direct(3)
7.0.0.0	255.0.0.0	eth2	0	0.0.0.0	direct(3)
9.0.0.0	255.0.0.0	eth1	0	0.0.0.0	direct(3)
127.0.0.0	255.0.0.0	eth2	0	0.0.0.0	direct(3)
0.0.0.0	0.0.0.0	eth0	1	192.168.1.2	indirect(4)

Using Firewall OS Monitoring

After you set up Firewall OS Monitoring, to view a revision of OS-level configuration data:

1. In **Compare** view, in the left-hand pane, select the relevant Check Point gateway.
2. In the revisions list, select a revision.
3. Click **Configuration**.

The configuration data is displayed.

To compare two revisions:

1. In **Compare** view, select the Check Point gateway.
2. In the revisions list, select two revisions.
3. Click **Compare**.

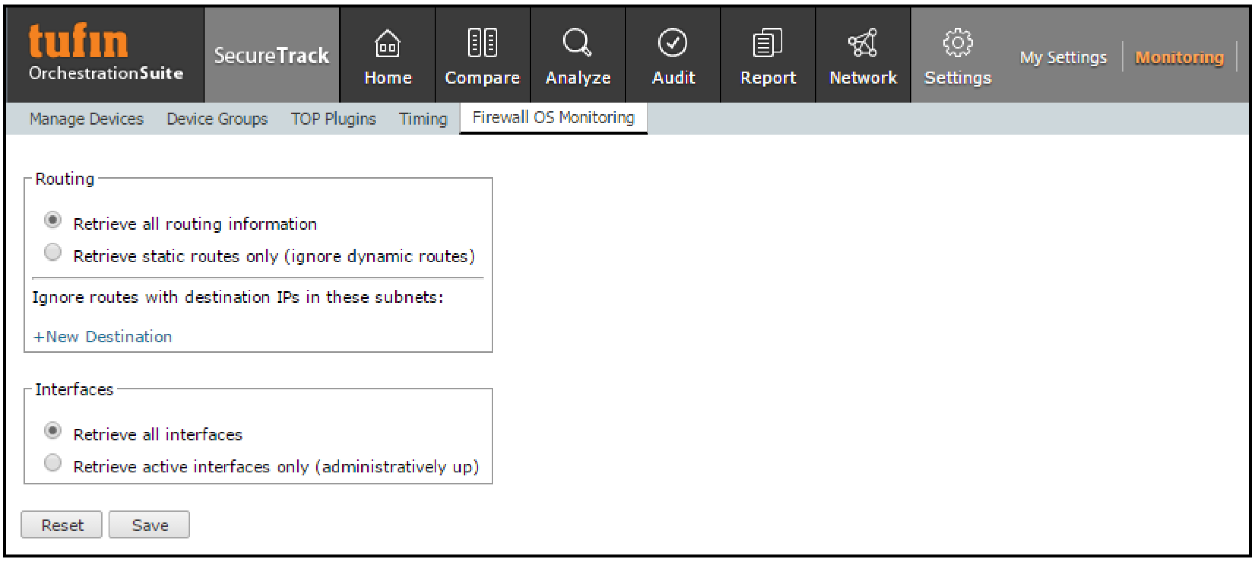
   When a change is detected, a "New Revision Report" is sent to SecureTrack users who are configured to receive them.

You can configure the extent of interface and routing information that is retrieved and displayed.

To configure interface and routing retrieval:

In **Settings** > **Monitoring**, select **Firewall OS Monitoring**.

The Firewall OS Monitoring tab contains the following settings:



Routing

● Retrieve all routing information

○ Retrieve static routes only (ignore dynamic routes)

Ignore routes with destination IPs in these subnets:

+New Destination

Interfaces

● Retrieve all interfaces

○ Retrieve active interfaces only (administratively up)

- Routing
  - **Retrieve all routing information**: SecureTrack collects and analyzes all routing information, including dynamic routes. Dynamic routes are displayed in the routing tab of Check Point firewall modules. Firewall OS Monitoring is performance-intensive and causes SecureTrack to collect many revisions.
  - **Retrieve static routes only (ignore dynamic routes)**: SecureTrack does not fetch dynamic routes.
  - **Ignore routes with destination IPs in these subnets**: Click **new destination** to configure destination subnets to be ignored by SecureTrack.

- Interfaces
  - **Retrieve all interfaces**: SecureTrack fetches and analyzes information on all interfaces, including stopped interfaces.
  - **Retrieve active interfaces only (administratively up)**: SecureTrack fetches information only on interfaces that are configured as up (regardless of hardware state).

Performance Monitoring

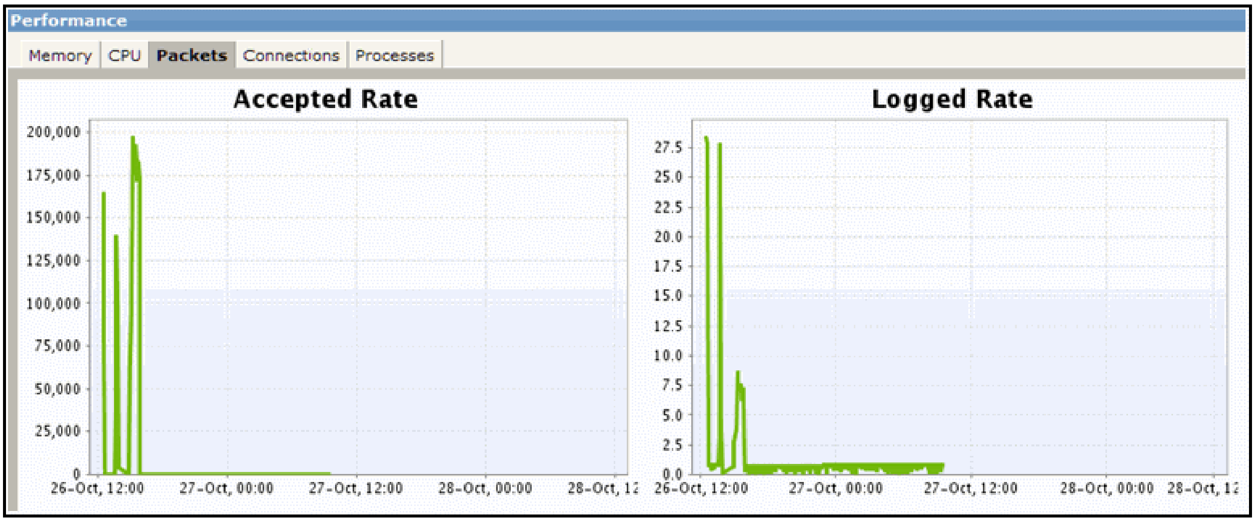
As part of the Firewall OS Monitoring feature, SecureTrack uses SNMP to keep a record of various performance statistics for each device over time.

Historic performance statistics can be useful for:

- Identifying busy periods
- Identifying traffic anomalies
- Planning when to increase hardware capacity

To view performance data, click **Performance** (there is no need to select any revision).

You can view memory and CPU utilization, and can see the packet rates and number of connections on each device.



Real time performance information can be used to create alerts that are triggered when specified criteria are met.

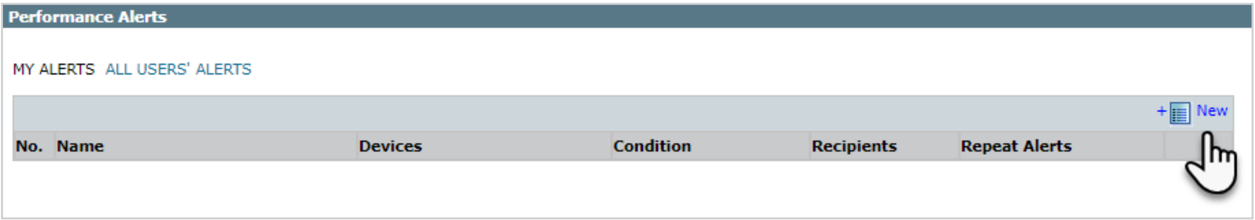
Performance Alerts

Performance alerts can be created after firewall OS monitoring has been enabled. Such alerts are used to notify SecureTrack users when certain thresholds are met, not met, or exceeded. The following system parameters can be monitored:

- CPU Utilization
- System Processes
- Concurrent firewall connections
- Memory utilization

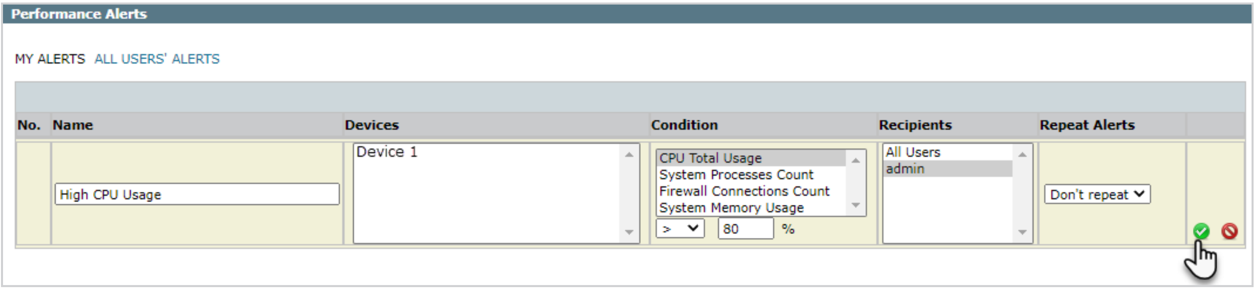
Creating a New Performance Alert

1. Go to **Audit** > **Performance**.
2. Click **New**.



No.	Name	Devices	Condition	Recipients	Repeat Alerts

3. Configure the alert. The following example would cause an alert to be sent to Admin when the CPU utilization of Device 1 exceeds 80%:



Performance Alerts

MY ALERTS ALL USERS' ALERTS

No.	Name	Devices	Condition	Recipients	Repeat Alerts
	High CPU Usage	Device 1	CPU Total Usage System Processes Count Firewall Connections Count System Memory Usage > 80 %	All Users admin	Don't repeat

4. Click ✓ to save the alert.

Once an alert has been triggered it will not be sent again before a Reload occurs. Reload is relevant to alerts with "Greater Than" or "Less Than" conditions. For example, an alert for >=80% CPU utilization will only be triggered again once CPU utilization has gone down to 64% and then up again to 80%.

Configuring Check Point Firewall OS Monitoring

For Firewall OS Monitoring, add all Check Point gateways to SecureTrack.

Configuring SecurePlatform and Crossbeam OS Monitoring

To configure Firewall OS Monitoring for a SecurePlatform or Crossbeam gateway:

1. Make sure SecureTrack has received at least one policy revision from the relevant Check Point management server (SmartCenter or CMA).
2. On each gateway to be monitored, log in in Expert mode, and do the following:
   a. Configure SNMP as explained in Check Point SecureKnowledge article sk34511.
   b. Run the following commands:

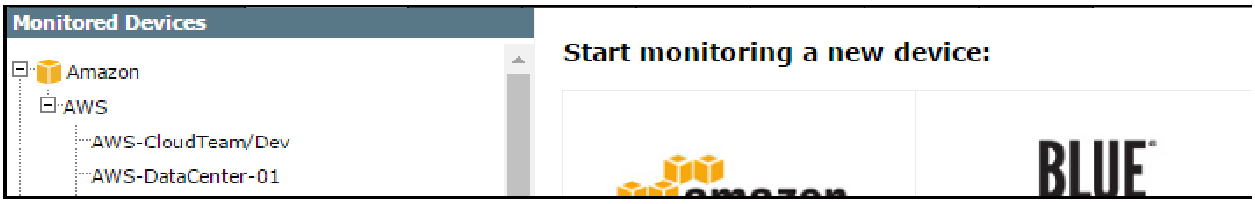
```
snmp service disable
snmp user add authuser <username> pass <passphrase>
snmp service enable
```

   The passphrase must be at least 8 characters. Record the username and password for subsequent use.

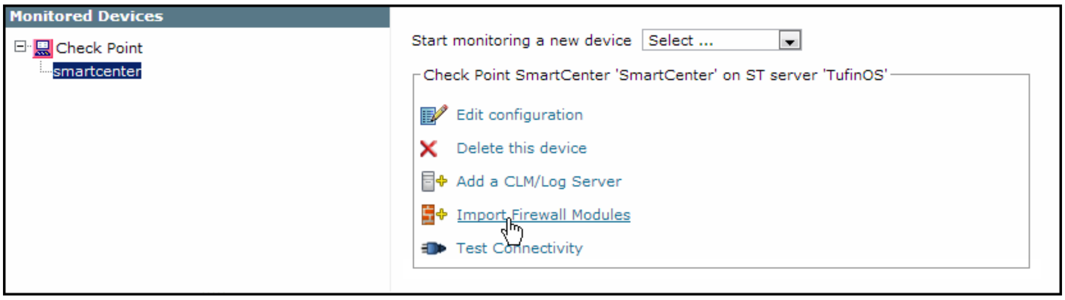
   To simplify importing the gateways to SecureTrack in the following steps, use the same authentication information for as many gateways as possible.

   For assistance in configuring SNMP on Crossbeam, please contact support.

3. In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**:



4. Select the managing SmartCenter or CMA, and click **Import Firewall Modules**:



5. From the device list, select the gateways to be imported, and supply the SNMP **username** and **passphrase** that you configured on the gateways.

   All gateways imported at one time must use the same SNMP authentication username and passphrase. Gateways which use different SNMP credentials must be separately imported. It is also possible to later edit the information for each gateway separately.

   Click **Next**.

6. For gateways with multiple interfaces, select an interface routable from SecureTrack.
7. Click **Save**.

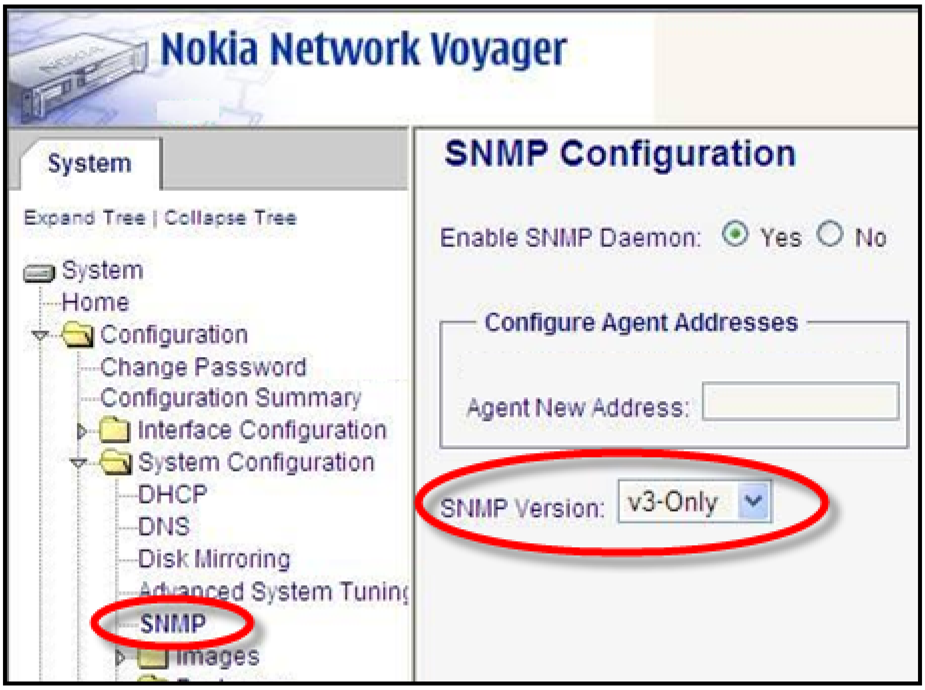
The gateways now appear in the **Device Configuration** list.

The SNMP polling frequency is 5 minutes. You can change this setting.

Configuring Nokia IPSO OS Monitoring

To configure Firewall OS Monitoring for a Nokia IPSO gateway:

1. Make sure SecureTrack has received at least one policy revision from the relevant Check Point management server (SmartCenter or CMA).
2. Log into the IPSO gateway with Voyager, and go to: **Configuration** > **System Configuration** > **SNMP**.
3. Enable **SNMP Versionv3**:



SNMP Configuration

Enable SNMP Daemon: ● Yes ○ No

Configure Agent Addresses

Agent New Address:

SNMP Version: v3-Only

4. Add a user, configured with authentication but **no privacy**. Record the username and password for subsequent use.

   To simplify importing the gateways to SecureTrack in the following steps, use the same authentication information for as many gateways as possible.

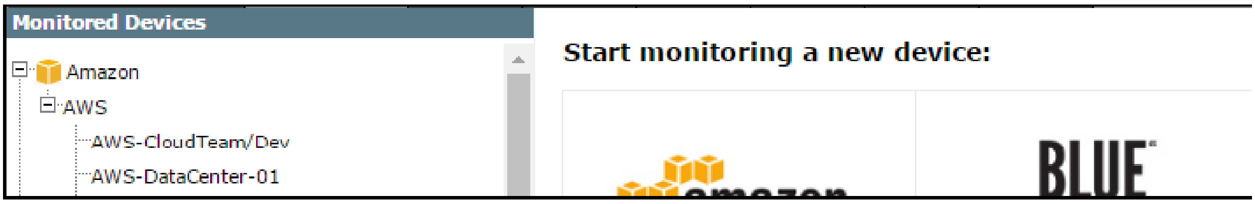
5. Apply the changes.
6. Open a command line to the gateway, and run:

   cpconfig

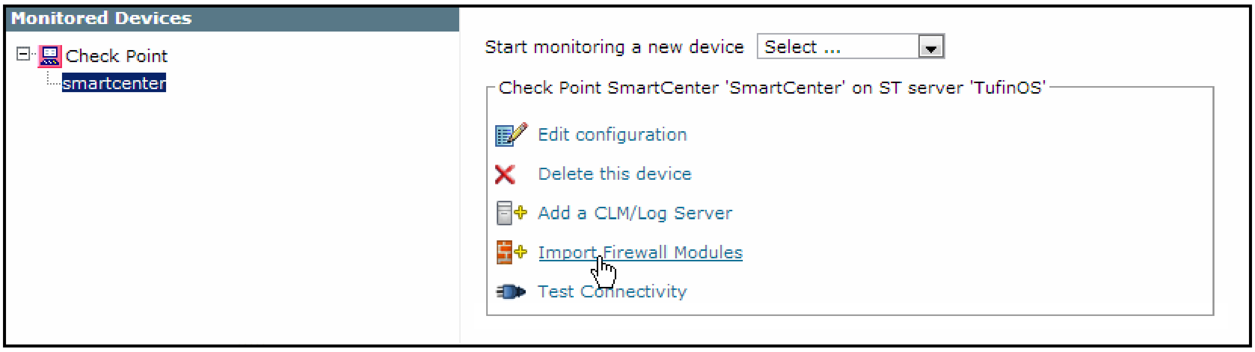
7. Select option `4) SNMP Extension`

   Confirm enabling the Check Point SNMP daemon. Select to exit cpconfig, and make sure the change is activated. If there are any problems, see Check Point sk38470.

8. In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**:



9. Select the managing SmartCenter or CMA, and click **Import Firewall Modules**:



10. From the device list, select the gateways to be imported, and supply the SNMP **username** and **passphrase** that you configured on the gateways.

    All gateways imported at one time must use the same SNMP authentication username and passphrase. Gateways which use different SNMP credentials must be separately imported. It is also possible to later edit the information for each gateway separately.

    Click **Next**.
11. For gateways with multiple interfaces, select an interface routable from SecureTrack.
12. Click **Save**.

The gateways now appear in the **Device Configuration** list.

The SNMP polling frequency is 5 minutes. You can change this setting.

Configuring GAiA and Gateway OS Monitoring

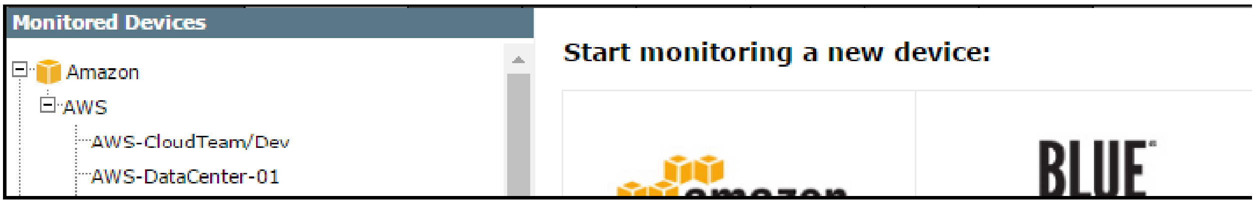
> This feature is not available for Check Point R81 devices as these devices cannot be configured with SNMP in SecureTrack.

To configure Firewall OS Monitoring for a GAiA gateway:

1. Make sure SecureTrack has received at least one policy revision from the relevant Check Point management server (SmartCenter or CMA).
2. Log into the Gaia Portal of the gateway , and go to: **System Management** > **SNMP**.
3. In SNMP General Settings, select **Enable SNMP Agent**:
4. Add a user account for authentication:
    a. In V3 - User-Based Security Model (USM), click **Add**.
    b. Enter a name for the user.
    c. For the Security Level, select: **authNoPriv**
    d. For the User Permissions, select: **read-write**
    e. Enter a passphrase. Remember the username and password for later use.

       To simplify importing the gateways to SecureTrack in the following steps, use the same authentication information for as many gateways as possible.
    f. Click **Save**.
5. Click to save the configuration changes.
6. To verify that the changes are saved, open a command line to the gateway and run:

    ```
    show snmp usm user
    ```
7. In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**:

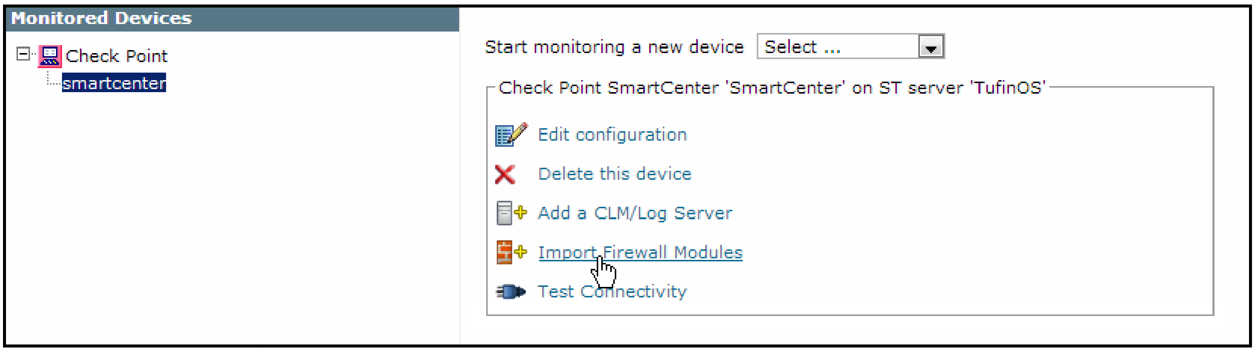


Monitored Devices

- Amazon
  - AWS
    - AWS-CloudTeam/Dev
    - AWS-DataCenter-01

Start monitoring a new device:

8. Select the managing SmartCenter or CMA, and click **Import Firewall Modules**:



Monitored Devices

- Check Point
  - smartcenter

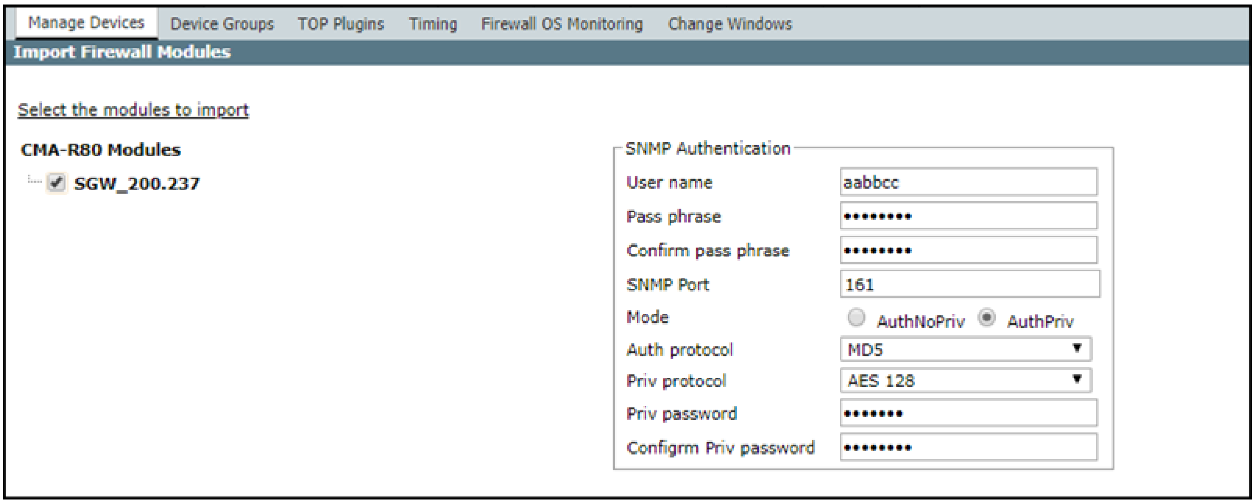
Start monitoring a new device Select ...

Check Point SmartCenter 'SmartCenter' on ST server 'TufinOS'

9. From the device list, select the gateways to be imported, and supply the SNMP **username** and **passphrase** that you configured on the gateways.

   All gateways imported at one time must use the same SNMP authentication username and passphrase. Gateways which use different SNMP credentials must be separately imported. It is also possible to later edit the information for each gateway separately.

10. To include SNMP encryption select AuthPriv from the **Mode** field and complete the fields as required.



Import Firewall Modules

Select the modules to import

CMA-R80 Modules

☑ SGW_200.237

SNMP Authentication

User name	aabbcc
Pass phrase	••••••••
Confirm pass phrase	••••••••
SNMP Port	161
Mode	○ AuthNoPriv ● AuthPriv
Auth protocol	MD5
Priv protocol	AES 128
Priv password	•••••••
Configrm Priv password	••••••••

11. Click **Next**.
12. For gateways with multiple interfaces, select an interface routable from SecureTrack.
13. Click **Save**.

The gateways now appear in the **Device Configuration** list.

The SNMP polling frequency is 5 minutes. You can change this setting.

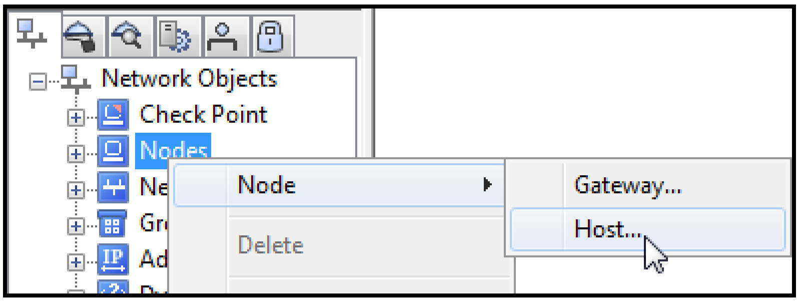
Configuring Check Point Server for OPSEC Communication

Configuring the Check Point server for OPSEC communication with TOS Classic

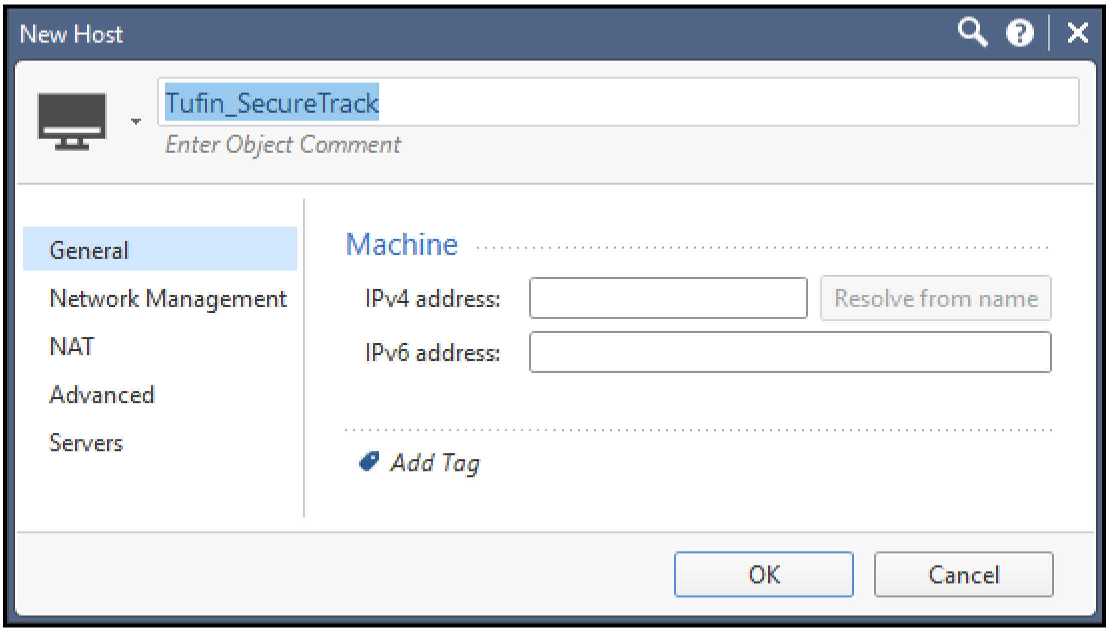
1. Open the management application:
   - **For a Provider-1 MDS**: Open the MDG for the MDS and, in **Global Policies**, right-click a Global Policy and select **Open selected global policy**.
   - **For a CMA, SmartCenter or Log Server**: Open SmartDashboard.
2. Create a SecureTrack Host:

> **For a CMA**: If you already configured monitoring for the MDS, use the global host object that you configured and skip this step.

a. In the **Objects** menu, select **More > Network Object > Host...**:



b. In the **Host Node - General Properties** window, enter a **Name** and the **IP Address** of SecureTrack:


New Host

Tufin_SecureTrack

Enter Object Comment

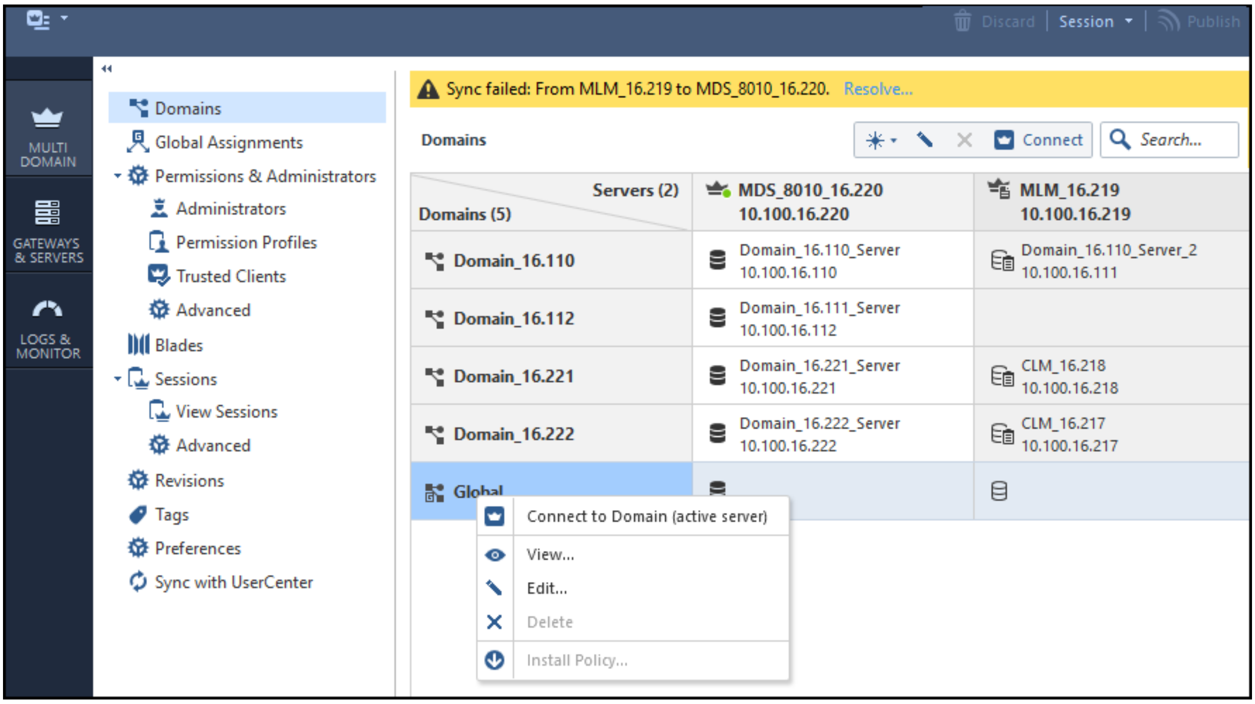
IPv4 address:

IPv6 address:

c. Click **OK**.

3. Create an OPSEC Application for SecureTrack for Check Point R80:

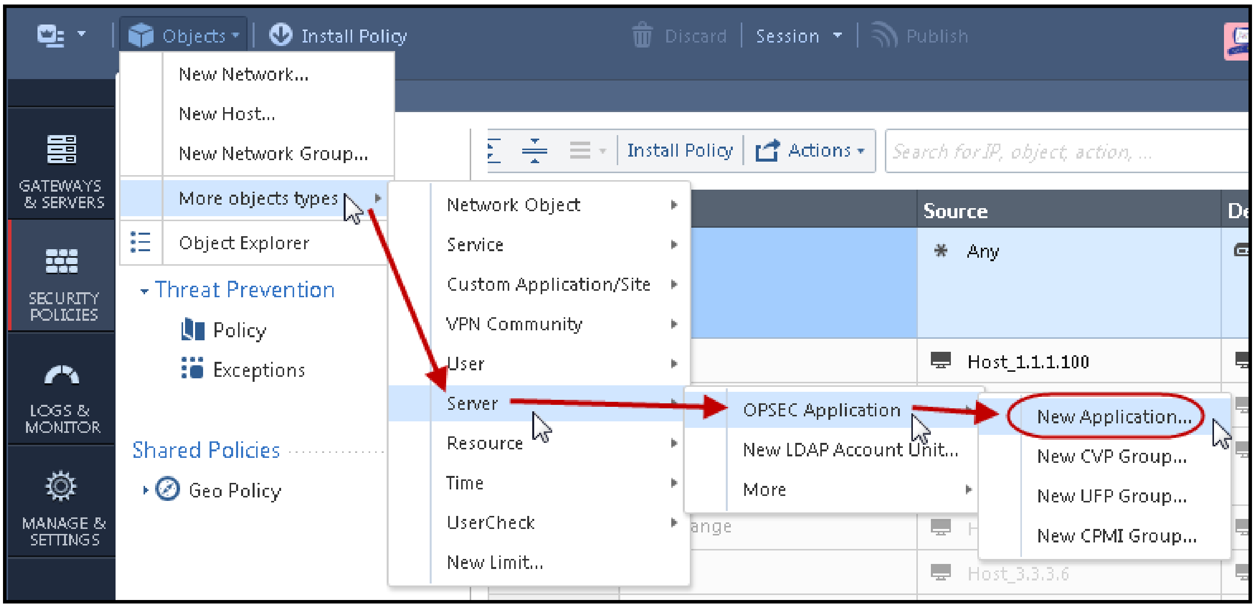
a. In the Global Domain Manager GDM, connect to a Domain server.

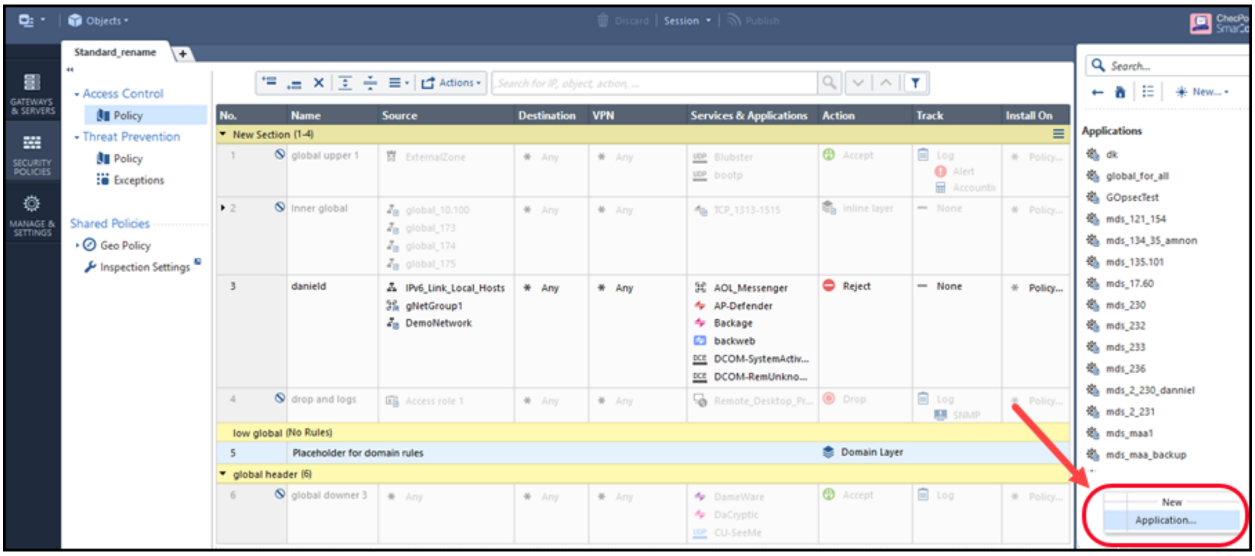


Sync failed: From MLM_16.219 to MDS_8010_16.220. Resolve...

Domains (5) / Servers (2)	MDS_8010_16.220 10.100.16.220	MLM_16.219 10.100.16.219
Domain_16.110	Domain_16.110_Server 10.100.16.110	Domain_16.110_Server_2 10.100.16.111
Domain_16.112	Domain_16.111_Server 10.100.16.112	
Domain_16.221	Domain_16.221_Server 10.100.16.221	CLM_16.218 10.100.16.218
Domain_16.222	Domain_16.222_Server 10.100.16.222	CLM_16.217 10.100.16.217
Global		

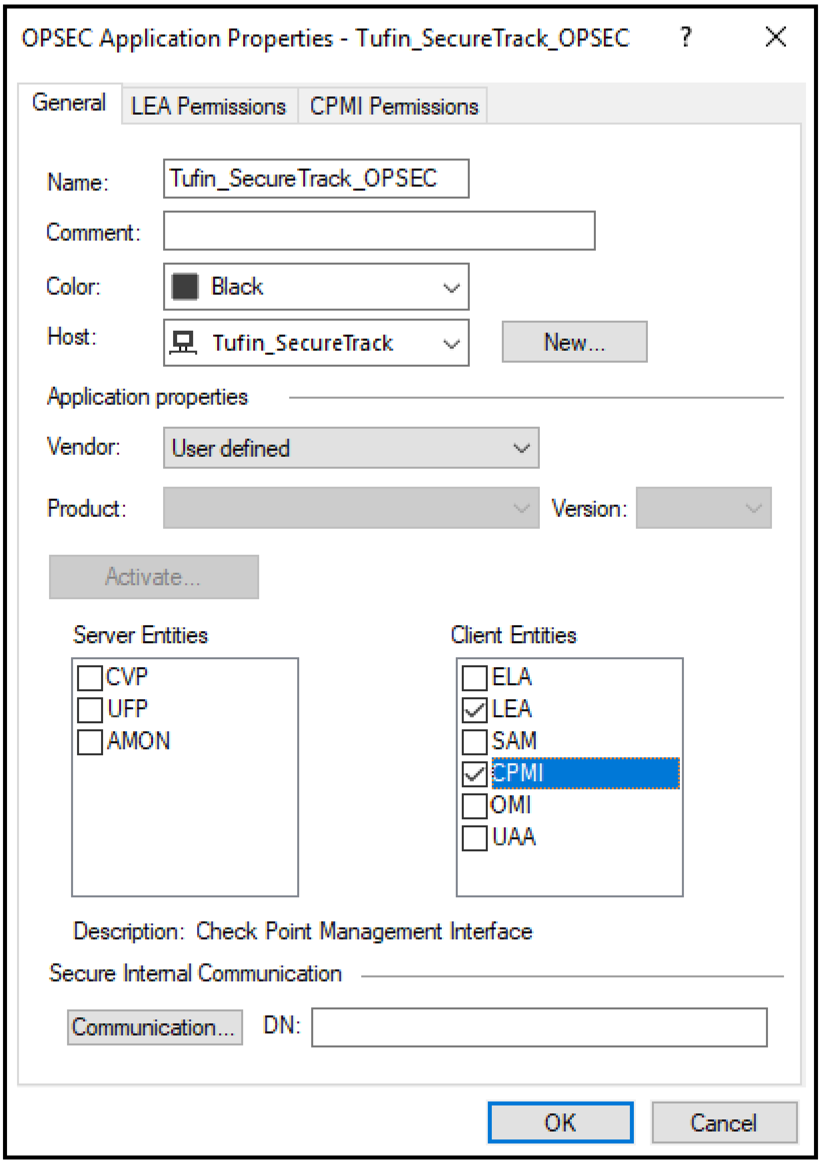
b. In the **Objects** menu, select: **More object types** > **Server** > **OPSEC Application** > **New Application**





No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
New Section (1-4)								
1	global upper 1	ExternalZone	Any	Any	Blubster bootp	Accept	Log Alert Accounti	Policy...
2	inner global	global_10.100 global_173 global_174 global_175	Any	Any	TCP_1313-1515	inline layer	None	Policy...
3	danield	IPv6_Link_Local_Hosts gNetGroup1 DemoNetwork	Any	Any	AOL_Messenger AP-Defender Backage backweb DCOM-SystemActiv... DCOM-RemUnkno...	Reject	None	Policy...
4	drop and logs	Access role 1	Any	Any	Remote_Desktop_Pr...	Drop	Log SNMP	Policy...
low global (No Rules)								
5	Placeholder for domain rules					Domain Layer		
global header (6)								
6	global downer 3	Any	Any	Any	DameWare DaCryptic CU-SeeMe	Accept	Log	Policy...

The **OPSEC Application Properties** window opens.



OPSEC Application Properties - Tufin_SecureTrack_OPSEC

Name: Tufin_SecureTrack_OPSEC

Comment:

Color: Black

Host: Tufin_SecureTrack

Application properties

Vendor: User defined

Product:

Version:

Server Entities

- □ CVP
- □ UFP
- □ AMON

Client Entities

- □ ELA
- ☑ LEA
- □ SAM
- ☑ CPMI
- □ OMI
- □ UAA

Description: Check Point Management Interface

Secure Internal Communication

DN:

c. Enter a **Name** for the OPSEC Application.

   For a CMA: Do not use the same name as the OPSEC Application in the MDS.

d. Select the SecureTrack Host object:

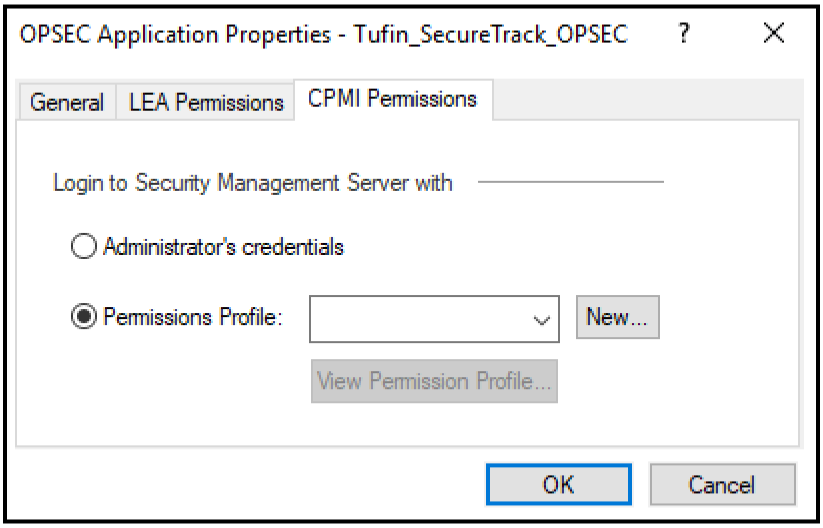
   - **For a CMA**: You can use the SecureTrack host global object that you created on the MDS.
   - **For all others**: Select the Host object that you created for SecureTrack.

   For **Vendor**, do not select **Tufin**. This will not work, due to a known Check Point issue.

e. In **Client Entities**, select **LEA** and **CPMI**, but do not click OK.

4. Set the CPMI Permissions:

   a. In the **CPMI Permissions** tab, select **Permissions Profile**.



OPSEC Application Properties - Tufin_SecureTrack_OPSEC

General | LEA Permissions | CPMI Permissions

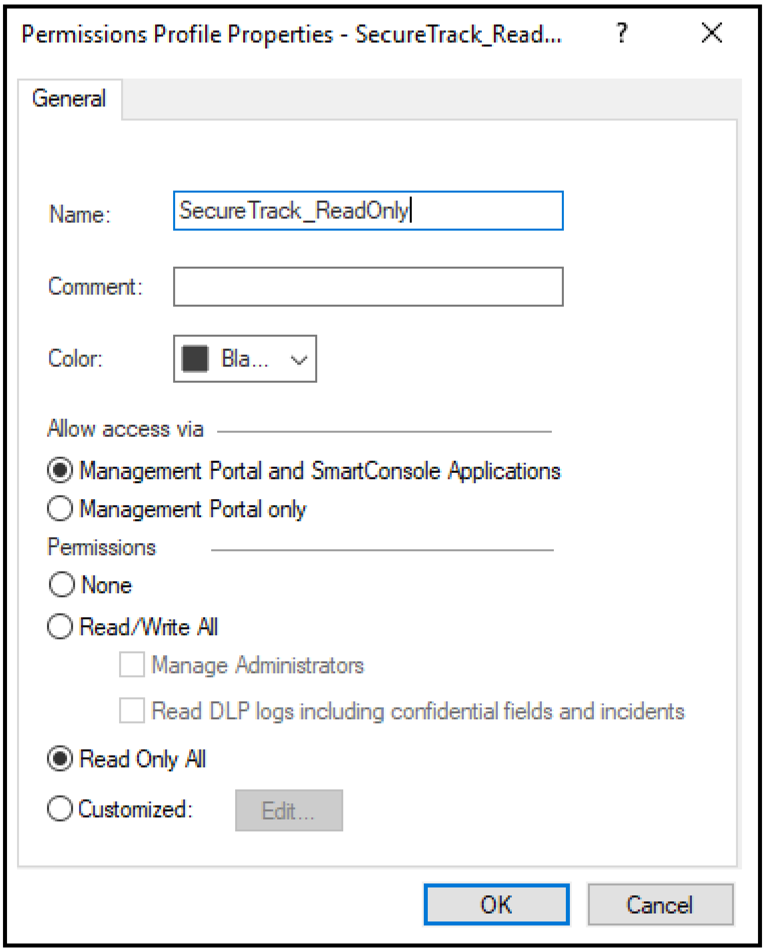
Login to Security Management Server with

○ Administrator's credentials

● Permissions Profile:

b. Select a Permissions Profile:

- **For a CMA**: Select from the list the Permissions Profile global object that you created for the MDS, and click **OK**.
- **For all others**: Click **New**, enter a name for the profile, and make sure that **Read Only All** is selected.



Permissions Profile Properties - SecureTrack_Read...

General

Name: SecureTrack_ReadOnly

Comment:

Color: Bla...

Allow access via

● Management Portal and SmartConsole Applications

○ Management Portal only

Permissions

○ None

○ Read/Write All

□ Manage Administrators

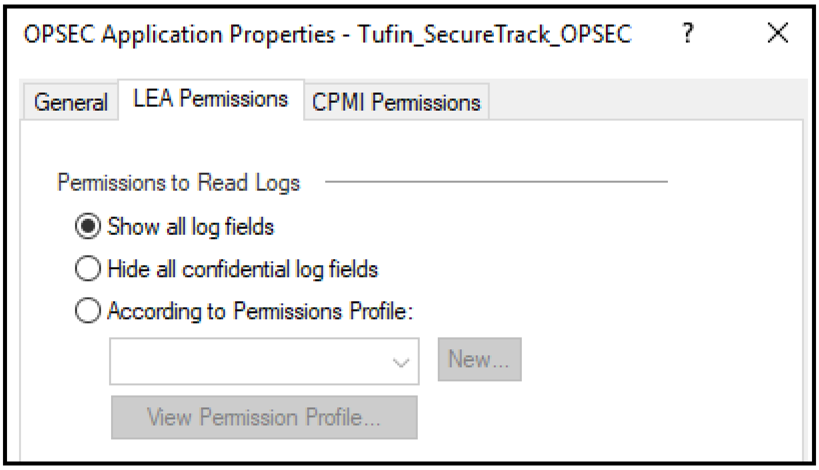
□ Read DLP logs including confidential fields and incidents

● Read Only All

○ Customized:

Note: For the SecureChange Designer to apply changes directly to Check Point policies, you must configure TOS Classic to use an OPSEC object that has **Read/Write All** permissions. (Do not select **Manage Administrators**.)

5. If you are using SmartDashboard R76 or higher, set the LEA permissions:
   - In the **LEA Permissions** tab, select **Show all log fields**.



OPSEC Application Properties - Tufin_SecureTrack_OPSEC

General | LEA Permissions | CPMI Permissions

Permissions to Read Logs

● Show all log fields

○ Hide all confidential log fields

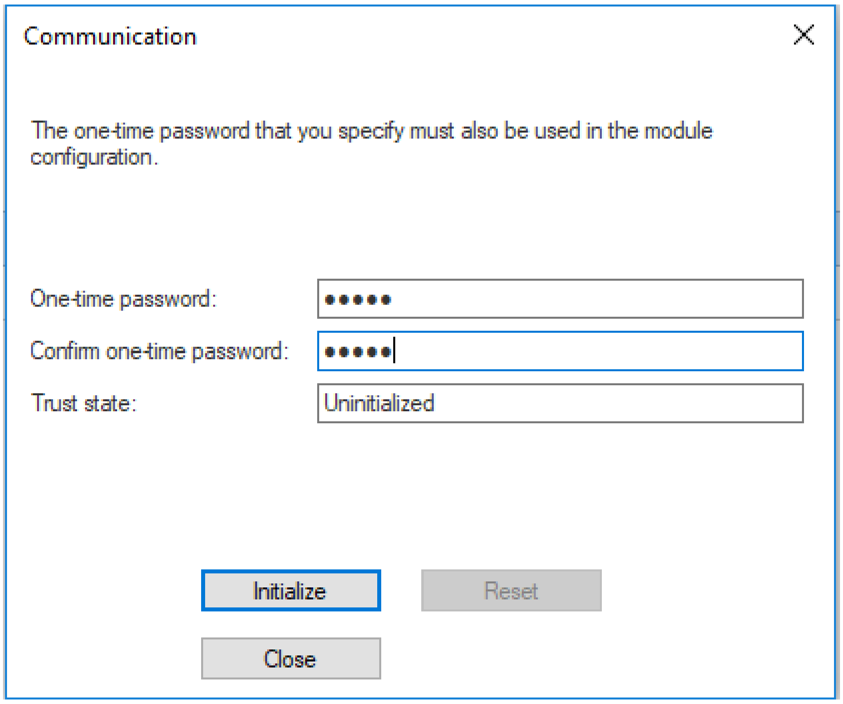
○ According to Permissions Profile:

6. Initialize trust with TOS Classic:

a. In the OPSEC Application Properties window, click **Communication**.

b. In the **Communication** window, enter and confirm an **Activation Key** and click **Initialize**:

You will need to enter the same Activation Key when you add the server to SecureTrack.



Communication

The one-time password that you specify must also be used in the module configuration.

One-time password: ●●●●●

Confirm one-time password: ●●●●●

Trust state: Uninitialized

The **Trust state** changes to: **Initialized but trust not established**.

c. **Close** the Communication window.

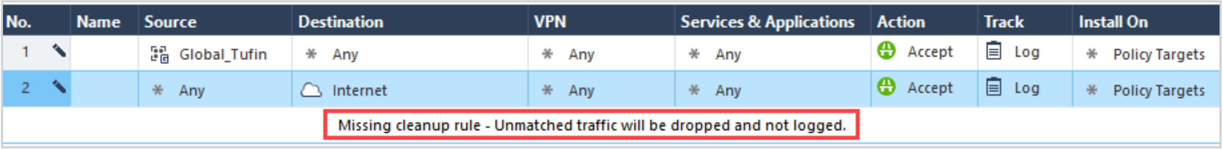
7. Click **OK**.

8. If you have an Application Control Policy layer, create a Cleanup rule that will send rule UIDs to SecureTrack.

If you already have an existing cleanup rule, skip to step 8c.

a. Go to **Access Control** > **Policy**, and select the Application Control Policy Layer.

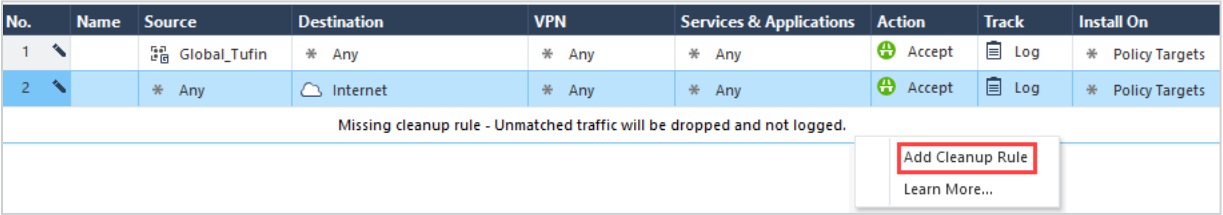
If you are missing a cleanup rule, a message will be displayed.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Global_Tufin	Any	Any	Any	Accept	Log	Policy Targets
2		Any	Internet	Any	Any	Accept	Log	Policy Targets

Missing cleanup rule - Unmatched traffic will be dropped and not logged.

b. Click on the message, and select **Add Cleanup Rule**.

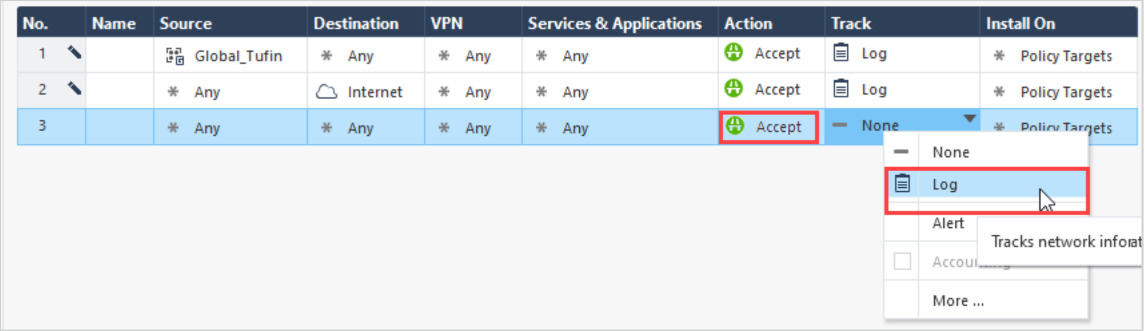


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Global_Tufin	Any	Any	Any	Accept	Log	Policy Targets
2		Any	Internet	Any	Any	Accept	Log	Policy Targets

Missing cleanup rule - Unmatched traffic will be dropped and not logged.

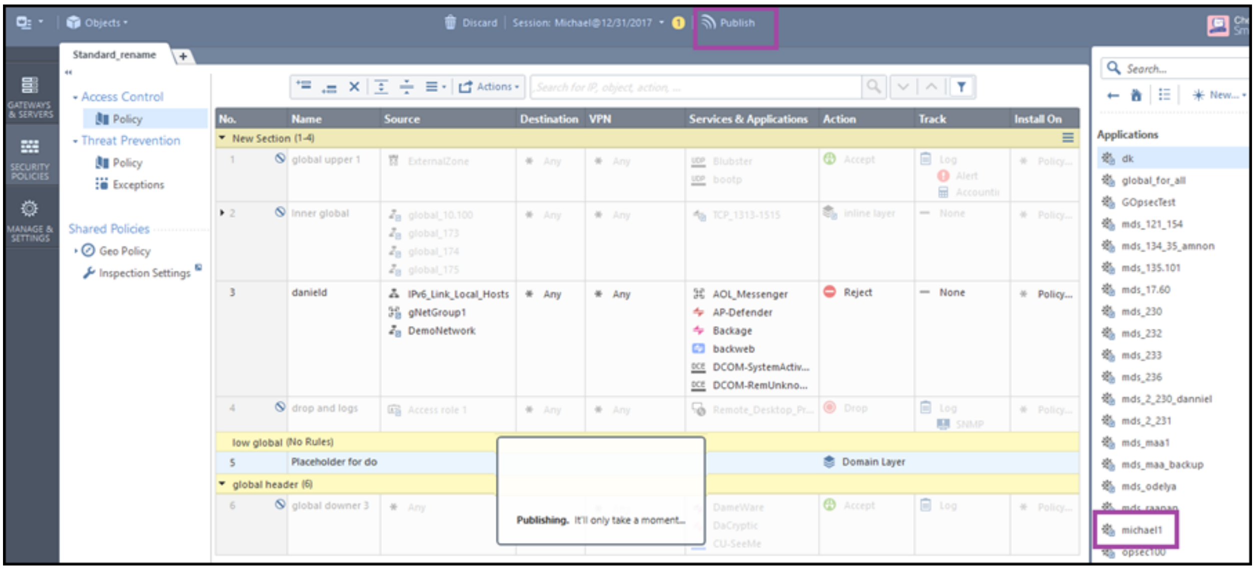
c. Edit the following settings:

- **Action:** Change to **Accept**
- **Track:** Change to **Log**



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Global_Tufin	Any	Any	Any	Accept	Log	Policy Targets
2		Any	Internet	Any	Any	Accept	Log	Policy Targets
3		Any	Any	Any	Any	Accept	None	Policy Targets

9. To save the changes for an MDS device, click **Publish** in the Global Domain Manager.

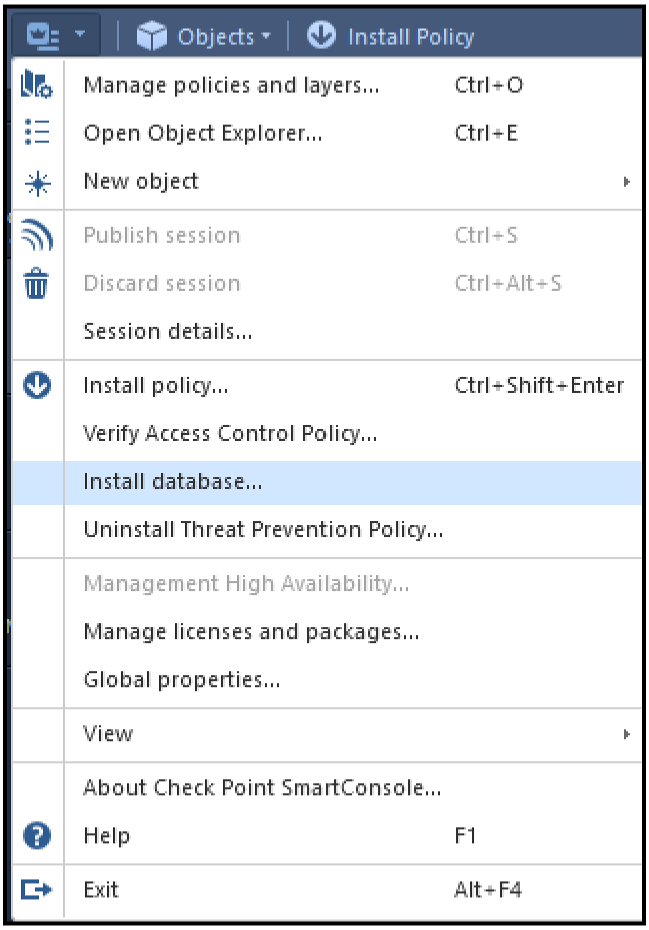


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
New Section (1-4)								
1	global upper 1	ExternalZone	Any	Any	Blubster bootp	Accept	Log Alert Accounti	Policy...
2	Inner global	global_10.100 global_173 global_174 global_175	Any	Any	TCP_1313-1515	inline layer	None	Policy...
3	danield	IPv6_Link_Local_Hosts gNetGroup1 DemoNetwork	Any	Any	AOL_Messenger AP-Defender Backage backweb DCOM-SystemActiv... DCOM-RemUnkno...	Reject	None	Policy...
4	drop and logs	Access role 1	Any	Any	Remote_Desktop_Pr...	Drop	Log SNMP	Policy...
low global (No Rules)								
5	Placeholder for do					Domain Layer		
global header (6)								
6	global downer 3	Any			DameWare DaCryptic CU-SeeMe	Accept	Log	Policy...

Publishing. It'll only take a moment...

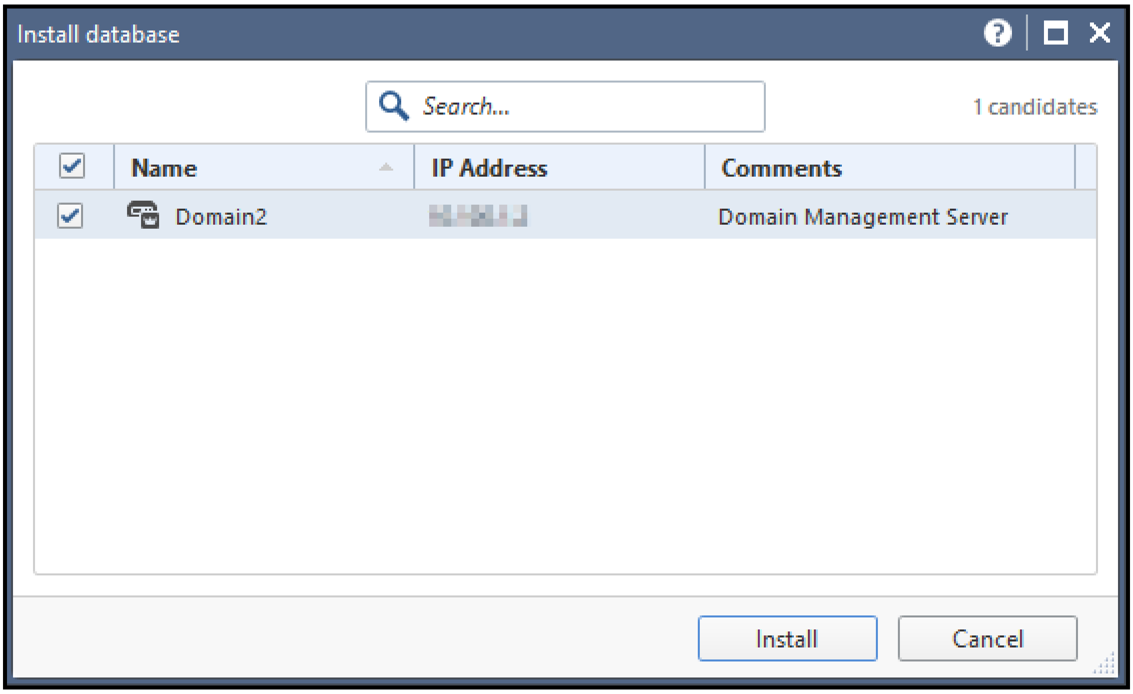
10. For SMC and CMA devices:

a. Select **Install database...**.


Objects
Install Policy
Manage policies and layers... Ctrl+O
Open Object Explorer... Ctrl+E
New object
Publish session Ctrl+S
Discard session Ctrl+Alt+S
Session details...
Install policy... Ctrl+Shift+Enter
Verify Access Control Policy...
Install database...
Uninstall Threat Prevention Policy...
Management High Availability...
Manage licenses and packages...
Global properties...
View
About Check Point SmartConsole...
Help F1
Exit Alt+F4

b. In the **Install database** dialog, select the relevant options and click **Install**.

If there is a CLM/Log Server device, select the relevant option.



☑	Name	IP Address	Comments
☑	Domain2	[redacted]	Domain Management Server

Adding Check Point Devices Configured for High Availability

To add Check Point devices that are configured for High Availability (HA):

1. Add the active member of the HA configuration.
2. Get the server DN of the secondary HA member.
    a. Login to SmartCenter.
    b. Locate the management object (SmartCenter or CMA).
    c. Right-click on the object and click **View**.
    d. In the General Properties tab of the object, click Test SIC status.

    The DN is displayed.
3. Go to `https://<SecureTrack_IP>/tools`, select **Add Standby Check Point Management Server** , and enter the configuration information:
    a. **Primary management server ID** - Enter the first HA member management_id from SecureTrack.
    b. **Standby Management Server Details** – information for the secondary HA member from step 2 above.
    c. **Show result in html format** – Select the checkbox to display the result in a browser (optional).
    d. Click **submit**.

    After completing these steps, SecureTrack should start connecting to the secondary server as well, and after that both members should be "Connected" (green icon).

    For more information on this SecureTrack tool, see Monitoring a Standy Check Point Management Server.

The primary server will receive all LEA change messages (Install\Save\Automatic) and the secondary member will get automatic revisions only.

Managing Failover

On failover (from inside the Check Point Policy > Management High Availability Server):

* For this example, server 1 is the primary server, server 2 is the standby, and we are now committing failover from server 1 to server 2.

1. Edit server 1 (Primary) , and clear these options topology option:
    - **Collect traffic logs for rule usage analysis**
    - **Collect traffic logs for object usage analysis**
    - **Enable Topology**
2. Edit server 2 (Secondary) and select the options that you cleared for server 1.
3. Install a new revision on the server 2 from the Check Point dashboard, and wait for SecureTrack to receive this change as "Install".

    Do not change the LEA configurations. They are configured automatically.

LEA Monitoring

To keep the LEA connection alive, TOS Classic:

- Attempts to re-establish the connection until it succeeds. This resolves disconnections when the management server is restarted.
- Sends keep-alive messages on the LEA session to avoid TCP timeouts.
- Refreshes the LEA connection when no logs are received for 15 minutes. This resolves unexpected disconnections without a TCP FIN message.

If TOS Classic cannot retrieve the logs for 2 days, TOS Classic sends an administrative alert at midnight with the st_monitor process every day until the logs are successfully retrieved. You can change the default delay for this administrative alert in the Rule_Usage_Not_Being_Collected_Alert_Period field in the stconf table. TOS Classic also has a command line utility to manually retrieve historical logs in case a gap was created.

Configuring SNMP to Use SHA Authentication

SNMP authentication is determined by the Check Point devices settings. Unless specified by the device, SNMP is authenticated with MD5.

We recommend that you backup the stconf table prior to making any changes.

To configure the SNMP communication with Check Point devices to use SHA authentication:

1. Go to: `https://<SecureTrack_IP>/stcgitest.htm`
2. Click **Edit StConf**.
3. Click **Fetch StConf**.
4. Add this line to the StConf file:

    ```
    <snmp_auth_method>SHA</snmp_auth_method>
    ```
5. Click **Submit New Conf**.

6. From the CLI of the SecureTrack server:

```
# st restart <check_point_mgmt_id>
```

Adding Cisco Devices

Adding Cisco ASA Firewall Devices

Overview

TOS Classic monitors ASA firewall devices for policy revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Prerequisites

TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Before you start, make sure that the device user account that you use for TOS Classic monitoring has permission to run these commands:

- Retrieve revision:

```
show running-config
show access-list
show ipv6 access-list
show clock
show version
terminal pager 512
show cluster info
```

> ℹ `show cluster info` is only required for R21-3 HF2 and later.

- Retrieve dynamic topology:

```
show version
show name
show route
show route management-only
show interface
```

- Virtual context:

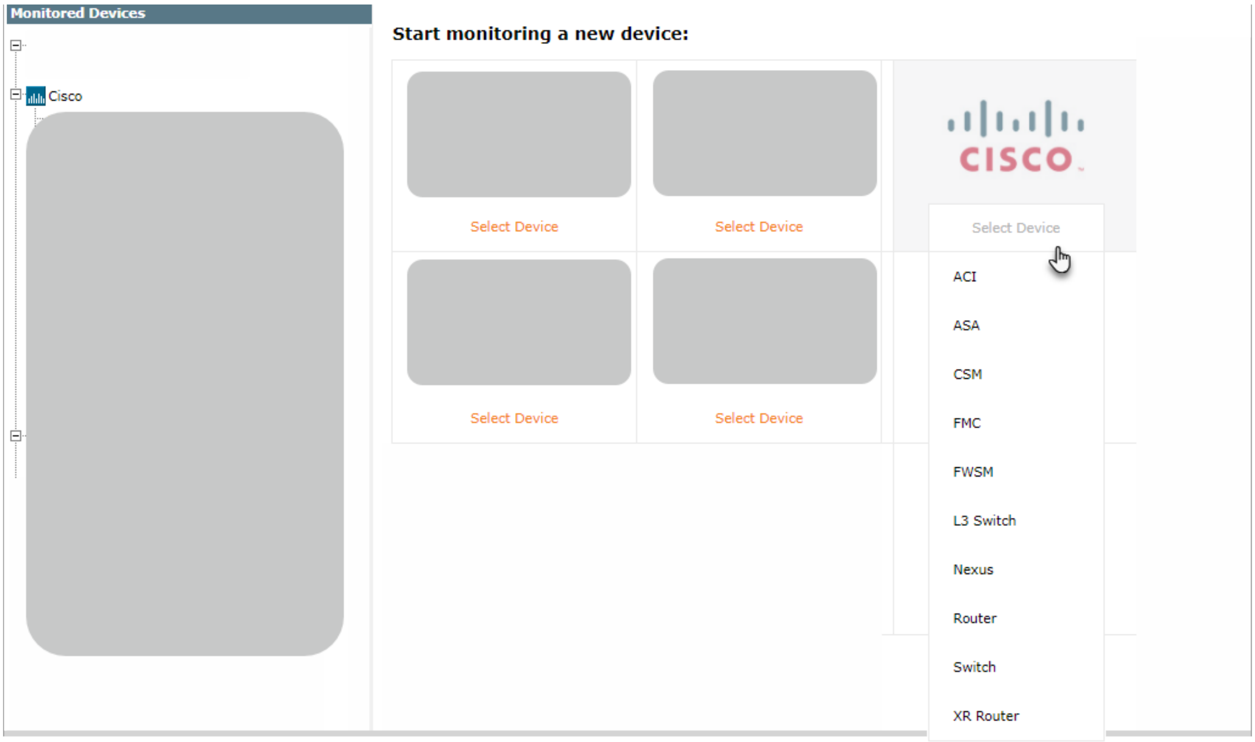
```
changeto context <context_name>
```

- Provisioning:

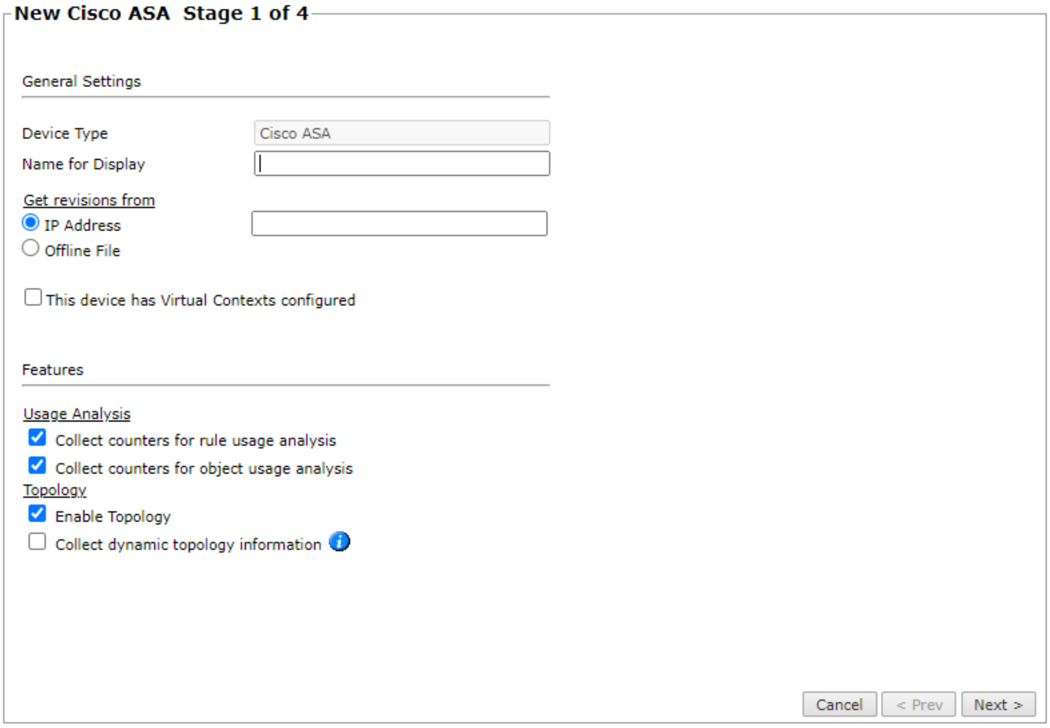
```
changeto system
show context
```

Adding a Cisco ASA Firewall Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Cisco ASA Stage 1 of 4

General Settings

Device Type	Cisco ASA
Name for Display	

Get revisions from

● IP Address
○ Offline File

□ This device has Virtual Contexts configured

Features

Usage Analysis

☑ Collect counters for rule usage analysis
☑ Collect counters for object usage analysis

Topology

☑ Enable Topology
□ Collect dynamic topology information

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:

    - **IP Address**: Revisions are retrieved automatically
    - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- To enable adding and monitoring Virtual Contexts, select **This device has Virtual Contexts configured**.
- **Collect counters for rule usage analysis** is necessary for Rule Usage reports.
- **Collect counters for object usage analysis** enables Rule Usage reports to include per-object usage information.

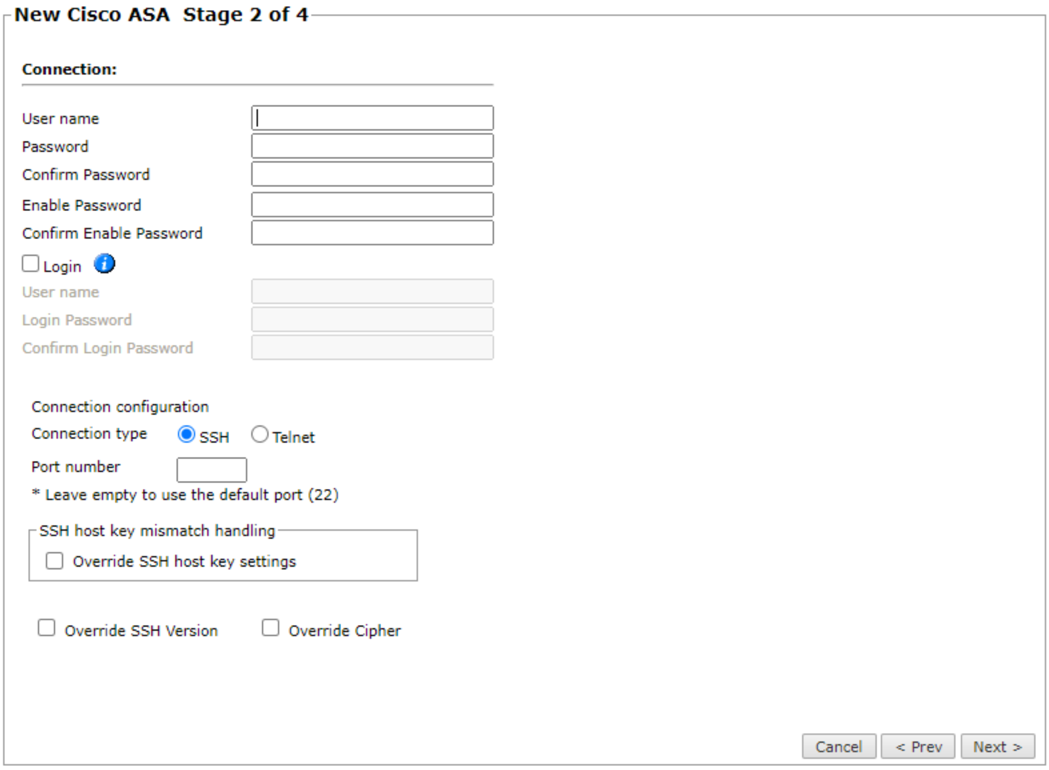
> Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure TOS Classic to limit the number of days that data is kept.

> We recommend that you enable TOS Classic administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, TOS Classic sends an alert.

- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- If the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), also select **Collect dynamic topology information**. To collect dynamic topology information from Cisco routers using SNMP v2 or v3, select **SNMP** in the next stage and specify the protocol details for your device.

Click **Next**.

4. Configure the TOS Classic connection to the Cisco ASA Firewall device, according to the parameters required by the device:



New Cisco ASA Stage 2 of 4

Connection:

User name
Password
Confirm Password
Enable Password
Confirm Enable Password
□ Login
User name
Login Password
Confirm Login Password

Connection configuration
Connection type ● SSH ○ Telnet
Port number
* Leave empty to use the default port (22)

SSH host key mismatch handling
□ Override SSH host key settings

□ Override SSH Version □ Override Cipher

- Enter the authentication details needed to connect to the Cisco ASA Firewall device.
    - **Username and password**: Enter the device username and password
    - **Enable password**: Enter the password to give TOS Classic elevated privileges on the device

- **Login**: If your device requires the Login password, select this option and enter the username and password that is required for the login command

- Select whether to use **SSH** (preferred) or **Telnet**.

  You can configure the connection to use either SSH version 1 or 2 with the **Override SSH version** option.

- To use default settings (recommended in most cases), leave the **Port number** and both **Override** options clear.

- If TOS Classic is configured to automatically replace the SSH host key when a new SSH host key is detected for a device, you can **Override SSH host key settings** to prevent the host key from being replaced for this device.

  You can then set TOS Classic to **Replace SSH host key automatically** for this specific device.

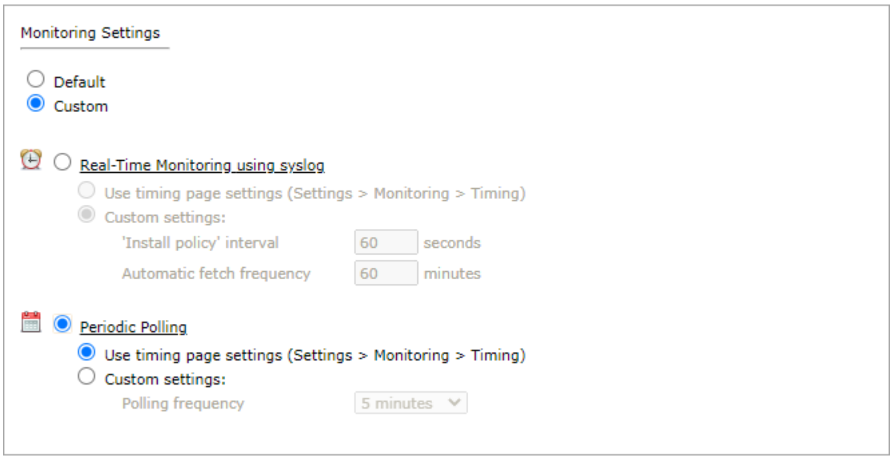
  Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.

- **Override SSH Version**: Select this option to force the device to use SSH-1 or SSH-2

- **Override Cipher**: Select this option to force the device to use DES or 3DES encryption

Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

- **Real-Time Monitoring**: Applies only if syslogs (Configuring Devices to Send Logs) are configured. Select **Custom settings** and configure:
  - **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
  - **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

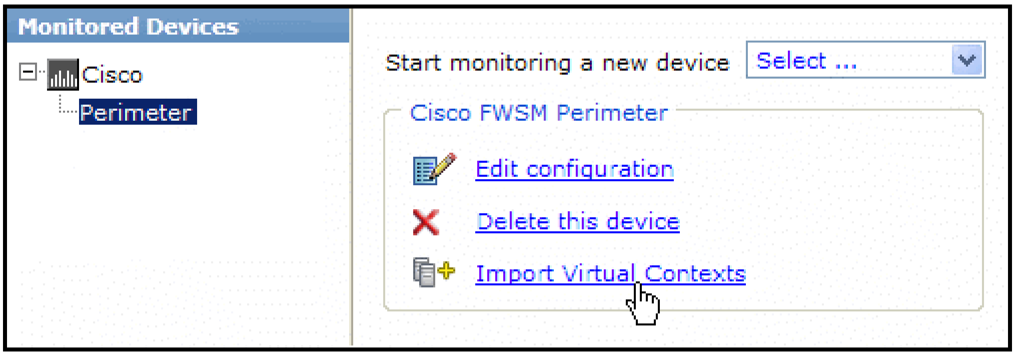
6. Click **Next**.
7. **Save** the configuration.

   The Cisco ASA Firewall device now appears in the **Monitored Devices** tree.

8. To manually add Virtual Contexts to your device, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the Virtual Contexts:

a. In the **Monitored Devices** tree, select the device.

b. Click **Import Virtual Contexts** (only enabled for **Manual Import**):



c. Select all the Virtual Contexts to be added.

If the option to collect rule and object usage statistics for virtual contexts is available, it is enabled.

If you do not want to collect these statistics, clear the options before you import the virtual contexts.

d. Click **Save**.

For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Cisco FWSM Firewall Devices

TOS Classic monitors FWSM firewall devices for policy revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Prerequisites

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Before you start, make sure that the device user account that you use for TOS Classic monitoring has permission to run these commands:

- Retrieve revision:

  ```
  show running-config
  show access-list
  show ipv6 access-list
  show clock
  show version
  ```

- Retrieve dynamic topology:

  ```
  show version
  show name
  show route
  show route management-only
  show interface
  ```

- Virtual context:

  ```
  changeto context <context_name>
  ```

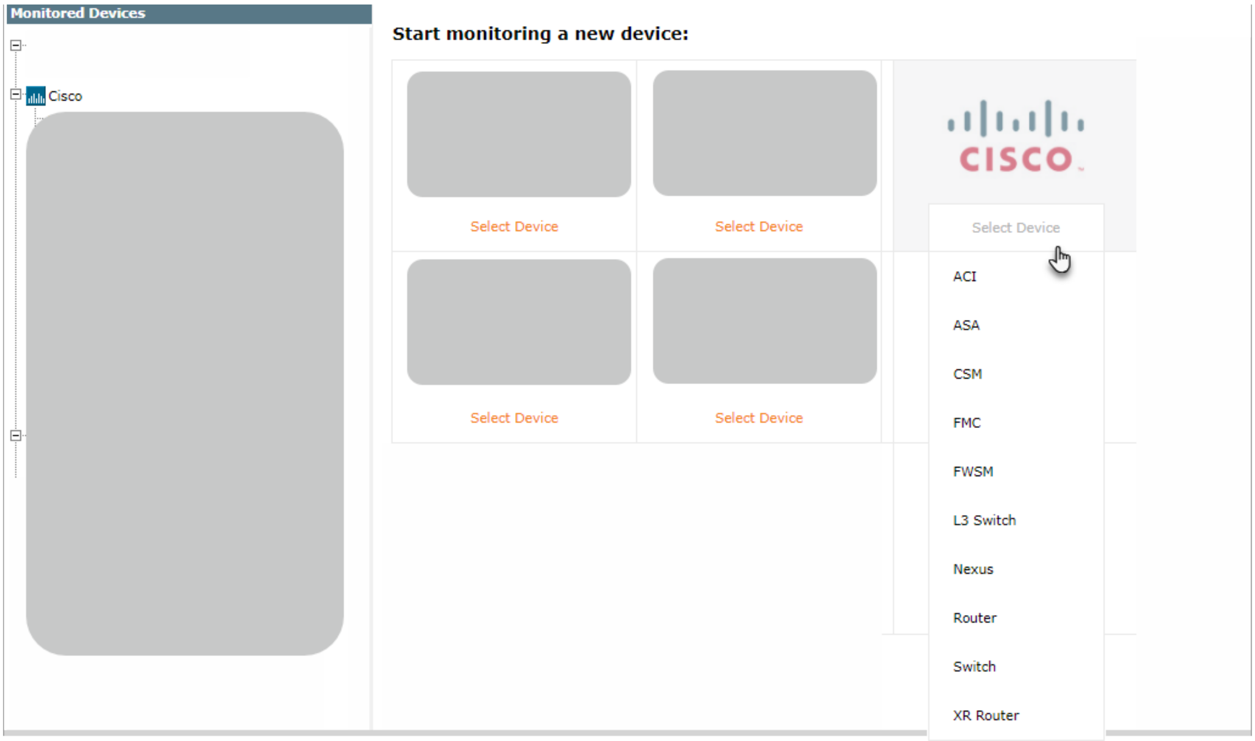
- Provisioning:

  ```
  changeto system
  show context
  ```

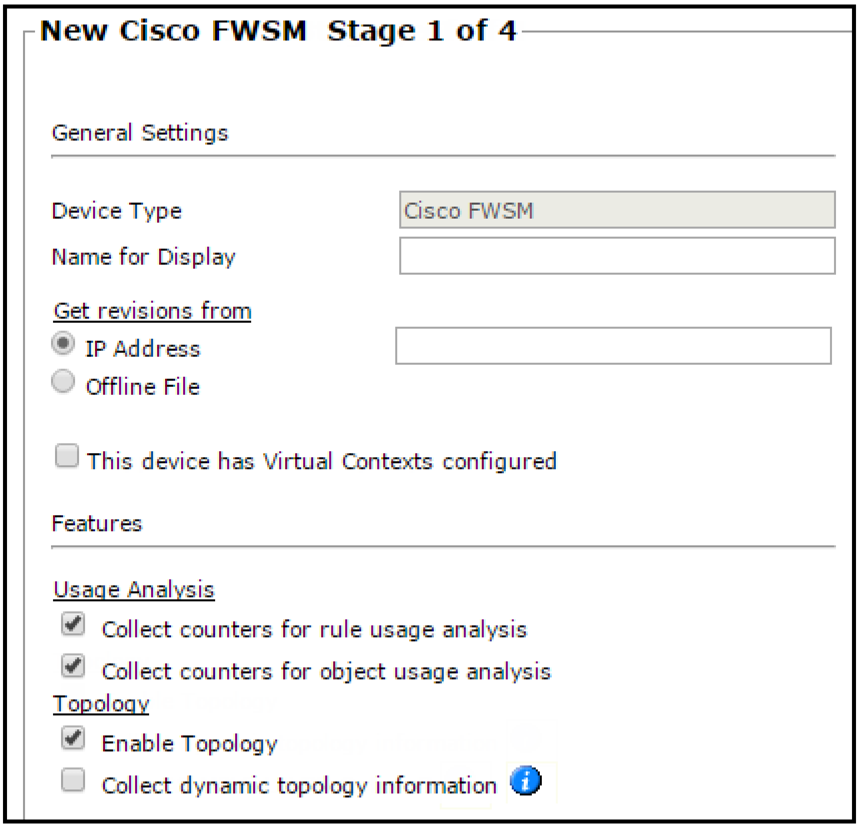
Monitor a Cisco Device

To configure TOS Classic to monitor the policy revisions of a Cisco device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Cisco FWSM Stage 1 of 4

General Settings

Device Type: Cisco FWSM

Name for Display:

Get revisions from

● IP Address

○ Offline File

□ This device has Virtual Contexts configured

Features

Usage Analysis

☑ Collect counters for rule usage analysis

☑ Collect counters for object usage analysis

Topology

☑ Enable Topology

□ Collect dynamic topology information

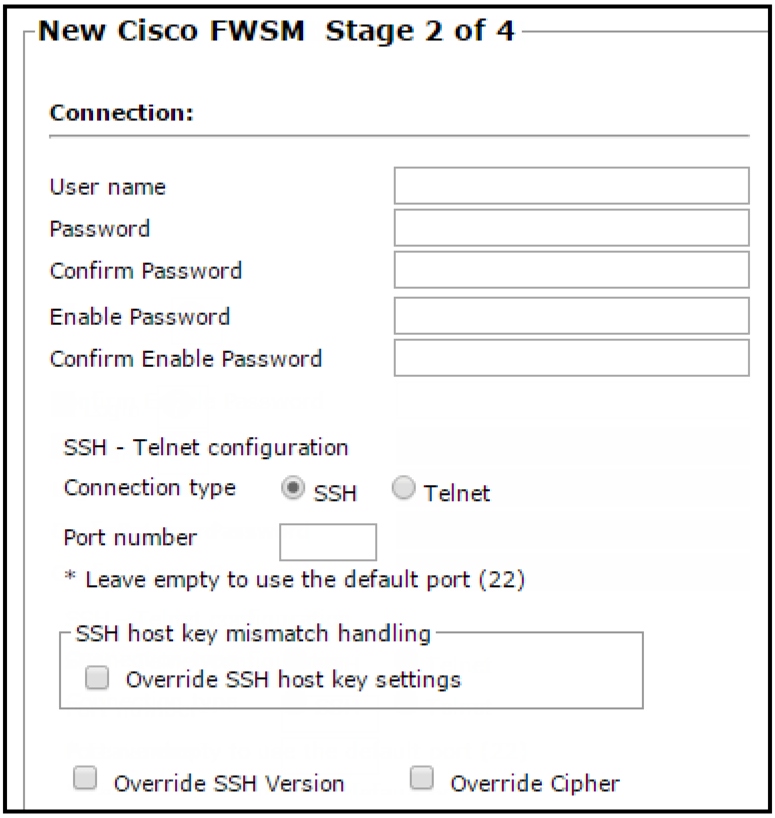
- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- To enable adding and monitoring Virtual Contexts, select **This device has Virtual Contexts configured**.
- **Collect counters for rule usage analysis** is necessary for Rule Usage reports.
- **Collect counters for object usage analysis** enables Rule Usage reports to include per-object usage information.

  > Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure TOS Classic to limit the number of days that data is kept.

  We recommend that you enable TOS Classic administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, TOS Classic sends an alert.
- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- If the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), also select **Collect dynamic topology information**. To collect dynamic topology information from Cisco routers using SNMP v2 or v3, select **SNMP** in the next stage and specify the protocol details for your device.

Click **Next**.

4. Configure the TOS Classic connection to the Cisco device, according to the parameters required by the device:



New Cisco FWSM Stage 2 of 4

Connection:

User name	
Password	
Confirm Password	
Enable Password	
Confirm Enable Password	

SSH - Telnet configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

□ Override SSH Version □ Override Cipher

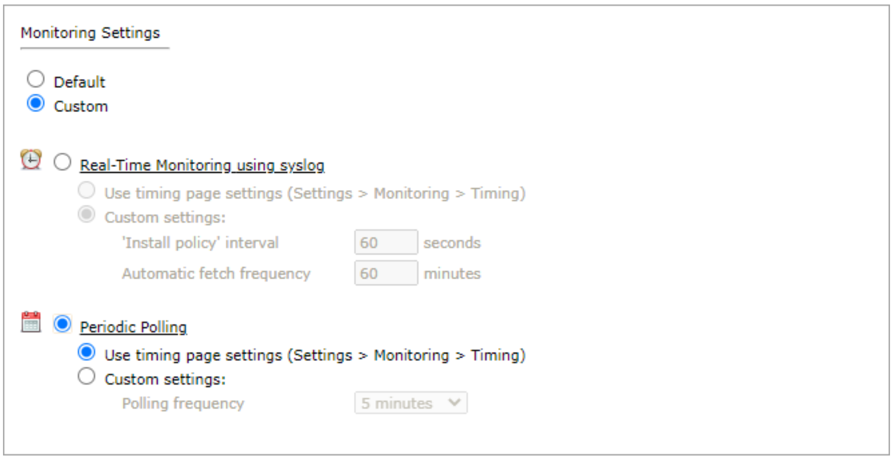
- Enter the authentication details needed to connect to the Cisco device.
  - **Username and password**: Enter the device username and password
  - **Enable password**: Enter the password to give TOS Classic elevated privileges on the device
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. The device can be configured to use either SSH version 1 or 2.
- To use default settings (recommended in most cases), leave the **Port number** and both **Override** options clear.
- If TOS Classic is configured to automatically replace the SSH host key when a new SSH host key is detected for a device, you can **Override SSH host key settings** to prevent the host key from being replaced for this device.

  You can then set TOS Classic to **Replace SSH host key automatically** for this specific device.

  Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.
- **Override SSH Version**: Select this option to force the device to use SSH-1 or SSH-2
- **Override Cipher**: Select this option to force the device to use DES or 3DES encryption

Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

Real-Time Monitoring: Applies only if syslogs "Sending Additional Information via Syslog" on page 239) are configured. Select **Custom settings** and configure:

- **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**.

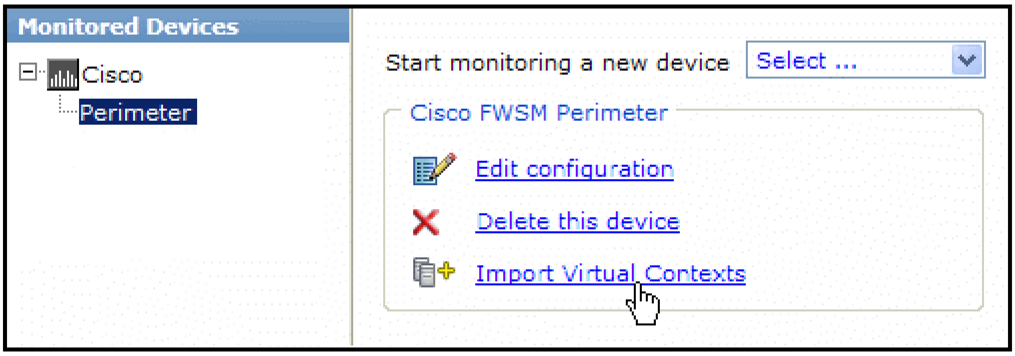
6. **Save** the configuration.

   The Cisco device now appears in the **Monitored Devices** tree.

7. To manually add Virtual Contexts to your device, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the Virtual Contexts:

   a. In the **Monitored Devices** tree, select the device.

   b. Click **Import Virtual Contexts** (only enabled for **Manual Import**):



   c. Select all the Virtual Contexts to be added.

      If the option to collect rule and object usage statistics for virtual contexts is available, it is enabled.

      If you do not want to collect these statistics, clear the options before you import the virtual contexts.

   d. Click **Save**.

For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Cisco Router Devices

TOS Classic monitors router devices for policy revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

TOS Classic can monitor Cisco routers for access lists, and configuration and routing information. For more about the features supported for each device, see the feature support table.

Prerequisites

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Make sure that the device user account that you use for TOS Classic monitoring has permission to run these commands:

- Retrieve revision:

  ```
  terminal no exec prompt timestamp
  ```

  ```
  show running-config
  ```

  or

  ```
  show configuration
  ```

  or

  ```
  show startup-config
  ```

  ```
  show ip route connected
  show ip route static
  show clock
  show version
  show access-lists
  ```

- Retrieve dynamic topology:

  ```
  show ip vrf detail
  ```

  For each VRF run:

  ```
  show ip route vrf <vrf name>
  show ip interface
  show mpls interface detail
  show ip bgp | inc ID
  ```

  If BGP is used, run:

  ```
  show ip bgp neighbors | inc BGP
  show ip bgp vpnv4 all labels
  show standby
  ```

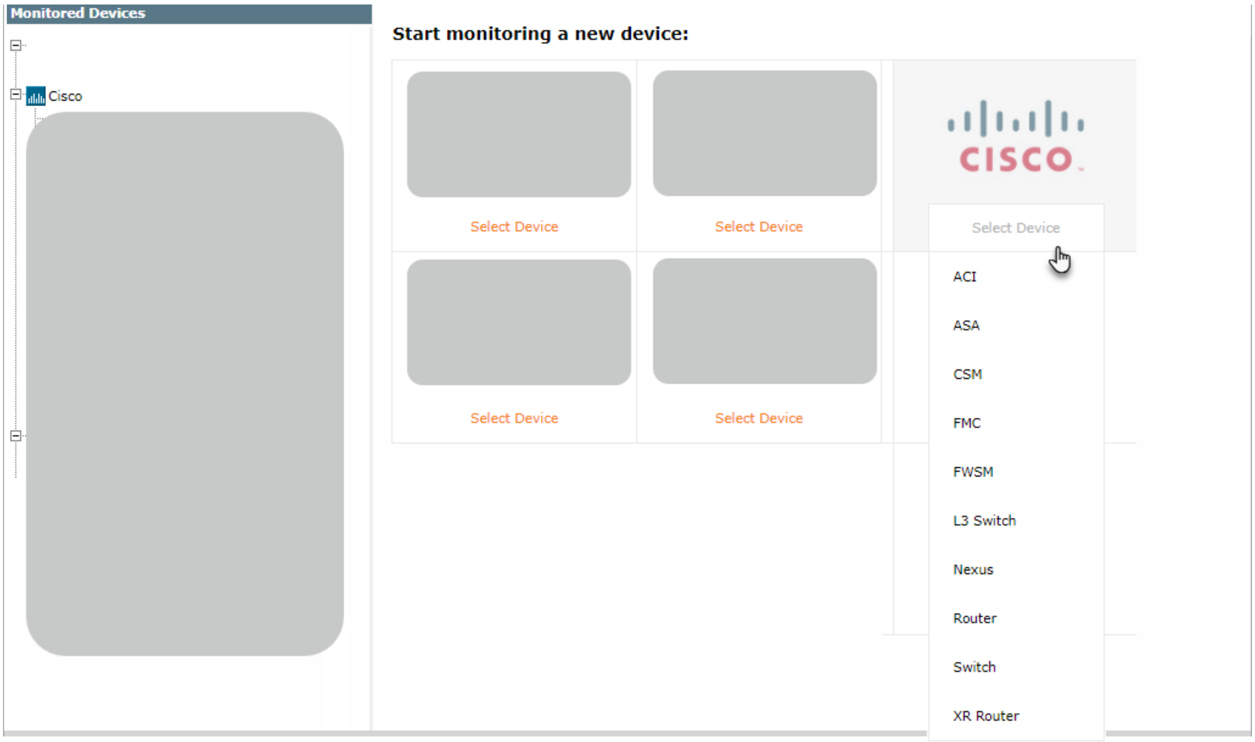
- Provisioning:

  ```
  changeto system
  show context
  ```

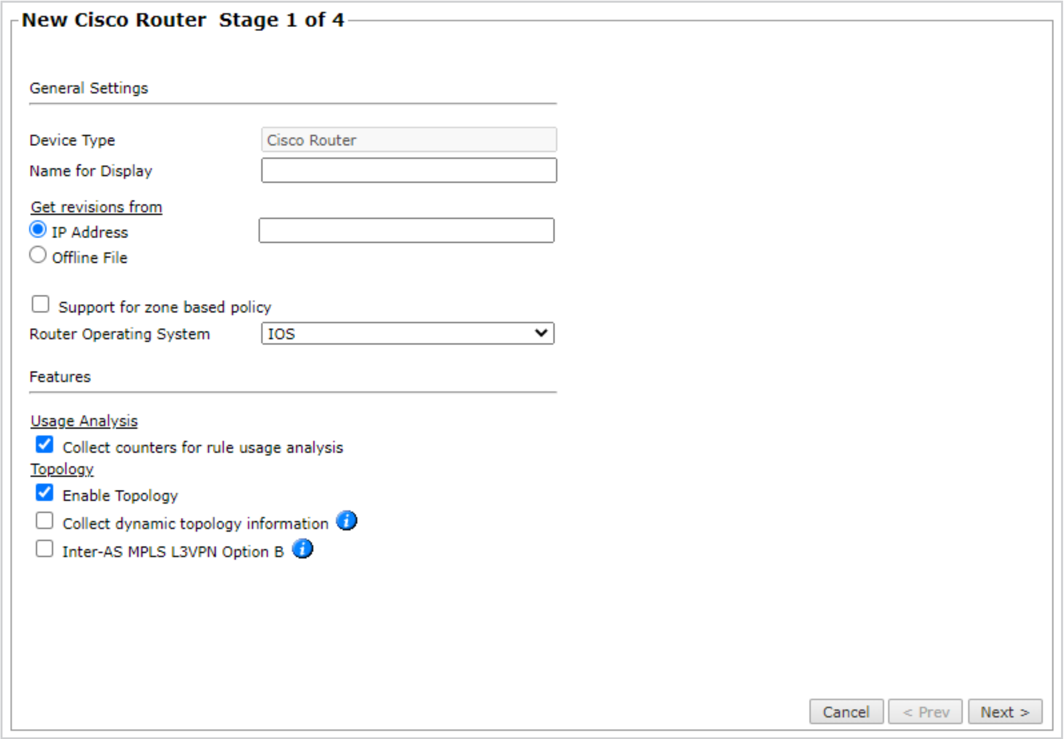
Monitor a Cisco Device

To configure TOS Classic to monitor the policy revisions of a Cisco device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Cisco Router Stage 1 of 4

General Settings

Device Type: Cisco Router

Name for Display:

Get revisions from

● IP Address

○ Offline File

□ Support for zone based policy

Router Operating System: IOS

Features

Usage Analysis

☑ Collect counters for rule usage analysis

Topology

☑ Enable Topology

□ Collect dynamic topology information

□ Inter-AS MPLS L3VPN Option B

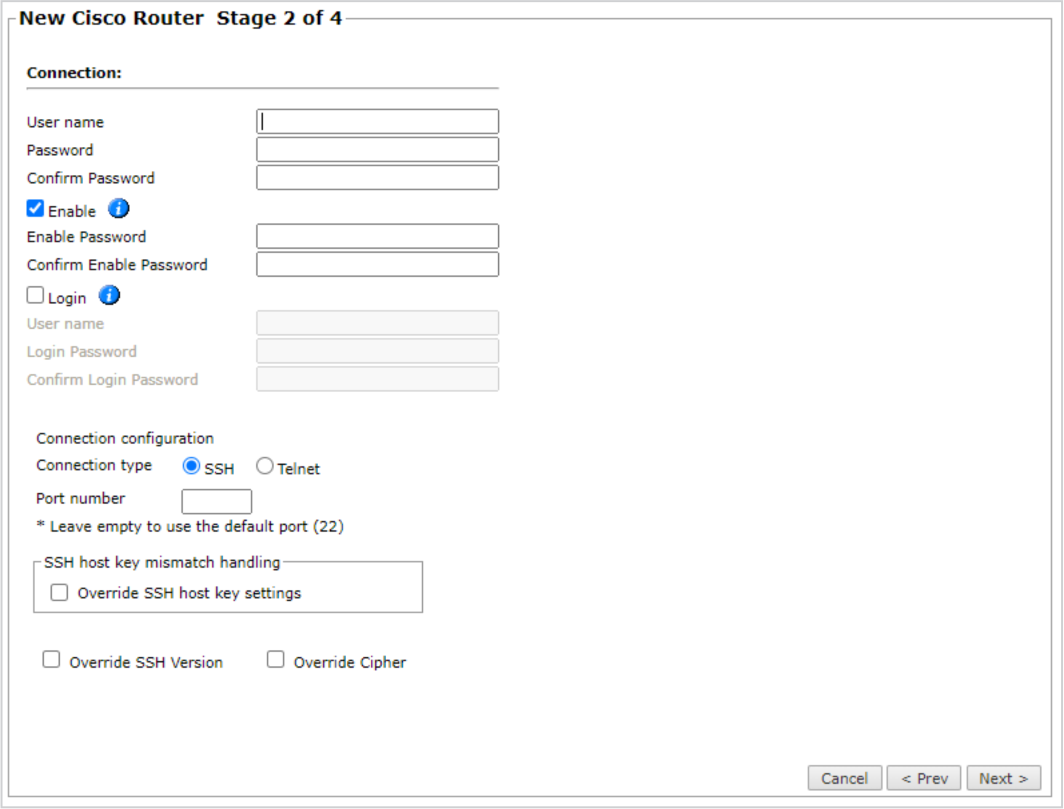
- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:

    - **IP Address**: Revisions are retrieved automatically
    - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **Support for zone based policy**: Select this option if the router uses the zone-based policy firewall feature
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- **Router Operating system**: IOS or IOS-XE
- **Collect counters for rule usage analysis**: Required for Rule Usage reports
- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.

  If the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), also select **Collect dynamic topology information**. You can specify in the next stage to retrieve the dynamic topology information using SNMP v2 or v3.
- **Inter-AS MPLS L3VPN Option B**: Select this option if this router is an autonomous system boundary router (ASBR) in an MPLS option B environment. This option retrieves VPNv4 labels associated with inter-AS communication.

Click **Next**.

4. Configure the TOS Classic connection to the Cisco device, according to the parameters required by the device:



New Cisco Router Stage 2 of 4

Connection:

User name

Password

Confirm Password

☑ Enable

Enable Password

Confirm Enable Password

□ Login

User name

Login Password

Confirm Login Password

Connection configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

□ Override SSH Version □ Override Cipher

- Enter the authentication details needed to connect to the Cisco device.
    - **Username and password**: The device username and password
    - **Enable** password: If your device requires sending the Enable command, select this option and enter the password to give TOS Classic elevated privileges on the device (required if automated Provisioning to the device will be used)
    - **Login** password: If your device requires the Login password, select this option and enter the username and password that is required for the login command
- Select whether to use **SSH** (preferred) or **Telnet**: The device can be configured to use either SSH version 1 or 2
- To use default settings (recommended in most cases), leave the **Port number** and both **Override** options clear.
- If TOS Classic is configured to automatically replace the SSH host key when a new SSH host key is detected for a device, you can **Override SSH host key settings** to prevent the host key from being replaced for this device.

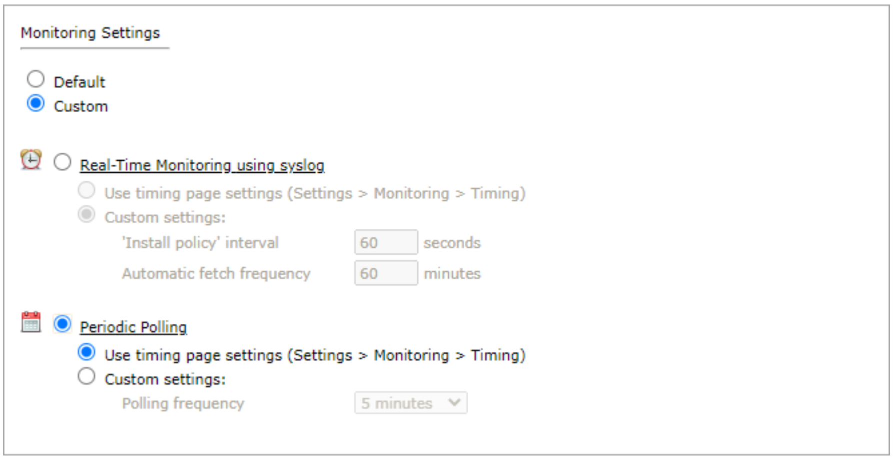
  You can then set TOS Classic to **Replace SSH host key automatically** for this specific device.

Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.

- **Override SSH Version**: Select this option to force the device to use SSH-1 or SSH-2
- **Override Cipher**: Select this option to force the device to use DES or 3DES encryption
- **SNMP**: Select this option to retrieve dynamic topology change information with SNMP instead of SSH, then enter the **port number** and SNMP **community name** to use for the SNMP connection to the device

Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

Real-Time Monitoring: (Not shown in image) Applies only if syslogs (Configuring Devices to Send Logs) are configured. Select **Custom settings** and configure:

- **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**.

6. **Save** the configuration.

The Cisco device now appears in the **Monitored Devices** tree.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Cisco XR Router Devices

TOS Classic monitors Cisco XR Router devices for policy revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

TOS Classic can monitor Cisco routers for access lists, and configuration and routing information.

Prerequisites

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Make sure that the device user account that you use for TOS Classic monitoring has permission to run these commands:

- Retrieve revision:

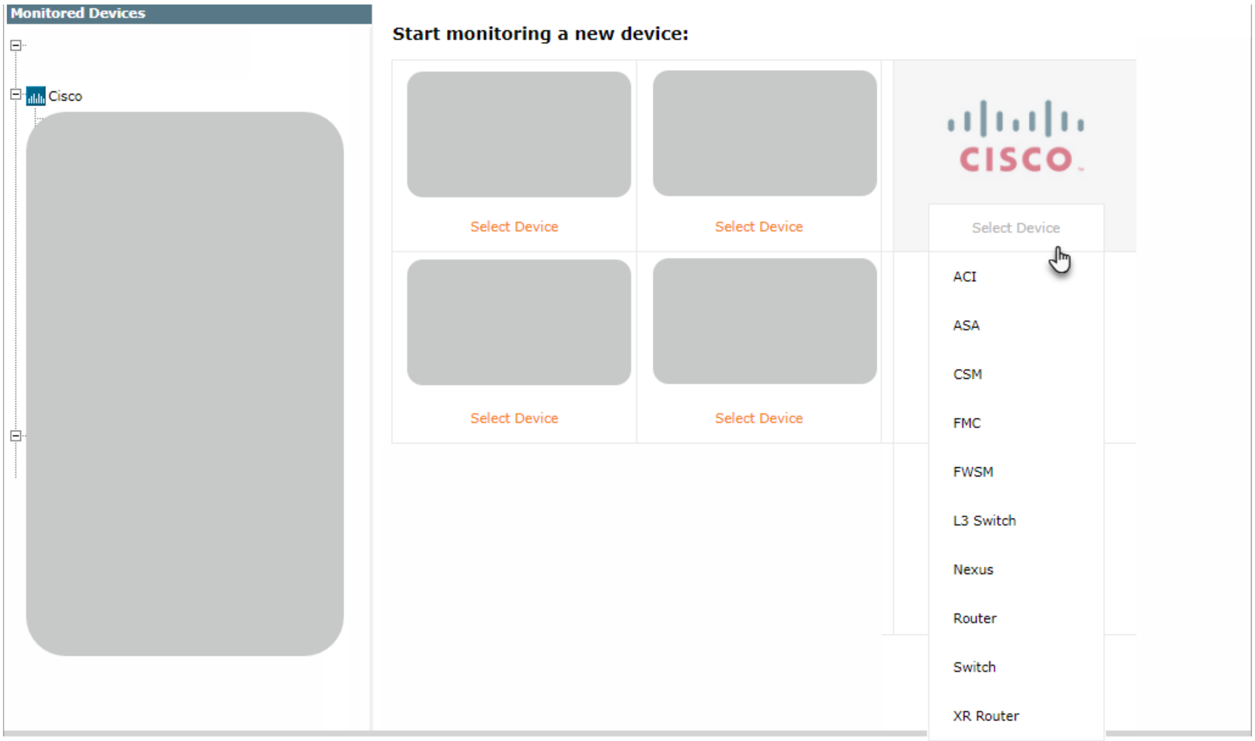
```
terminal exec prompt no-timestamp
terminal monitor disable
terminal length 512
show running-config
show route connected
show route static
show route ipv6 connected
show route ipv6 static
show clock
show version
show access-lists ipv4
```

- Retrieve dynamic topology:

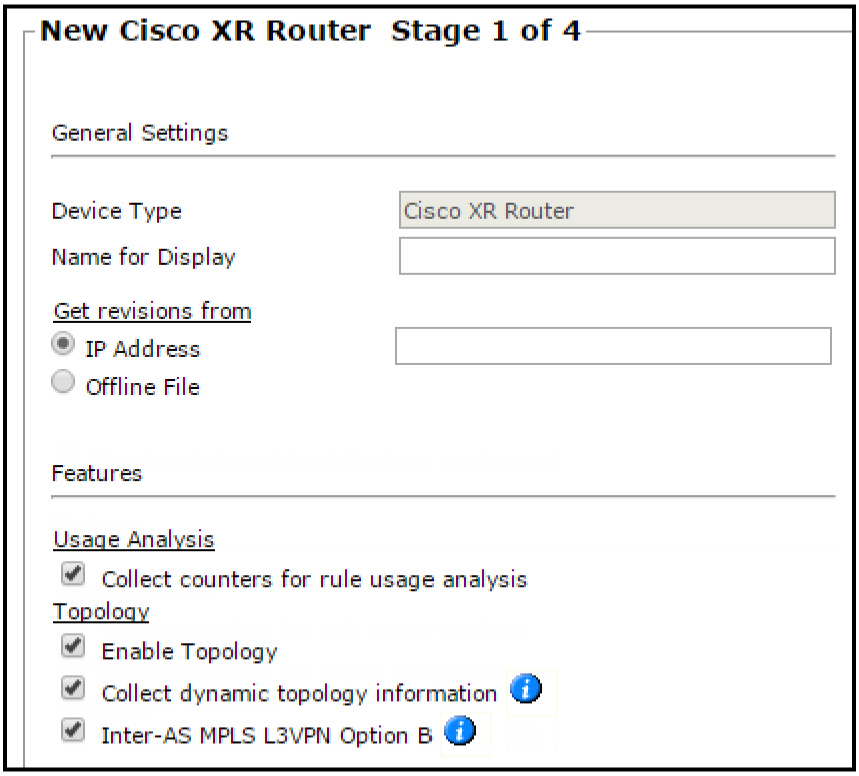
```
show route
show route vrf all
show ipv4 vrf all interface
show hsrp detail
show mpls interfaces detail
show bgp vpnv4 unicast labels
show bgp neighbors | inc BGP
```

Configure SecureTrack to Monitor a Cisco Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Cisco XR Router Stage 1 of 4

General Settings

Device Type: Cisco XR Router

Name for Display:

Get revisions from

● IP Address

○ Offline File

Features

Usage Analysis

☑ Collect counters for rule usage analysis

Topology

☑ Enable Topology

☑ Collect dynamic topology information

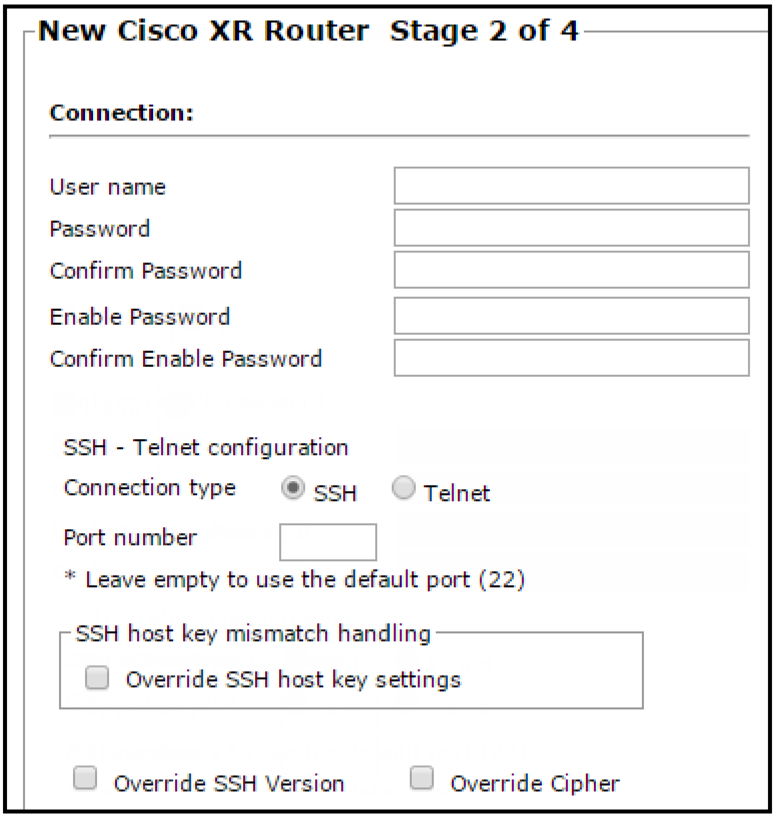
☑ Inter-AS MPLS L3VPN Option B

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- **Collect counters for rule usage analysis**: Required for Rule Usage reports
- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.

  If the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), also select **Collect dynamic topology information**.
- **Inter-AS MPLS L3VPN Option B**: Select this option if this router is an autonomous system boundary router (ASBR) in an MPLS option B environment. This option retrieves VPNv4 labels associated with inter-AS communication.

Click **Next**.

4. Configure the TOS Classic connection to the Cisco device, according to the parameters required by the device:



New Cisco XR Router Stage 2 of 4

Connection:

User name

Password

Confirm Password

Enable Password

Confirm Enable Password

SSH - Telnet configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

□ Override SSH Version □ Override Cipher

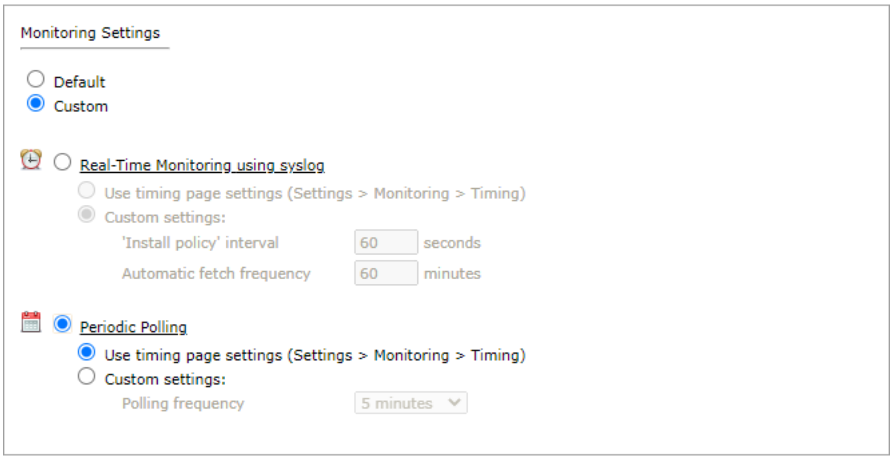
- Enter the authentication details needed to connect to the Cisco device.
  - **Username and password**: The device username and password
  - **Enable** password: Enter the enable password to give TOS Classic elevated privileges on the device
- Select whether to use **SSH** (preferred) or **Telnet**: The device can be configured to use either SSH version 1 or 2
- To use default settings (recommended in most cases), leave the **Port number** and both **Override** options clear.
- If TOS Classic is configured to automatically replace the SSH host key when a new SSH host key is detected for a device, you can **Override SSH host key settings** to prevent the host key from being replaced for this device.

  You can then set TOS Classic to **Replace SSH host key automatically** for this specific device.

  Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.
- **Override SSH Version**: Select this option to force the device to use SSH-1 or SSH-2
- **Override Cipher**: Select this option to force the device to use DES or 3DES encryption

Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog

○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling

● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

Real-Time Monitoring: Applies only if syslogs "Sending Additional Information via Syslog" on page 239) are configured. Select **Custom settings** and configure:

- **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**.

6. **Save** the configuration.

The Cisco device now appears in the **Monitored Devices** tree.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Cisco Switch Devices

TOS Classic monitors switch devices for revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Prerequisites

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Before you start, make sure that the device user account that you use for TOS Classic monitoring has permission to run these commands:

- Retrieve revision:

  `terminal no exec prompt timestamp`

  `show running-config` or `show configuration` or `show startup-config`

  `show clock`

  `show version`

  `show access-lists`

- Retrieve dynamic topology:

  `show ip route`

  `show ip interface`

  `show mpls interface detail`

  `show ip bgp | inc ID`

  if bgp is utilized run: `show ip bgp neighbors | inc BGP`

  `show ip bgp vpnv4 all labels`

  `show standby`

- Provisioning:

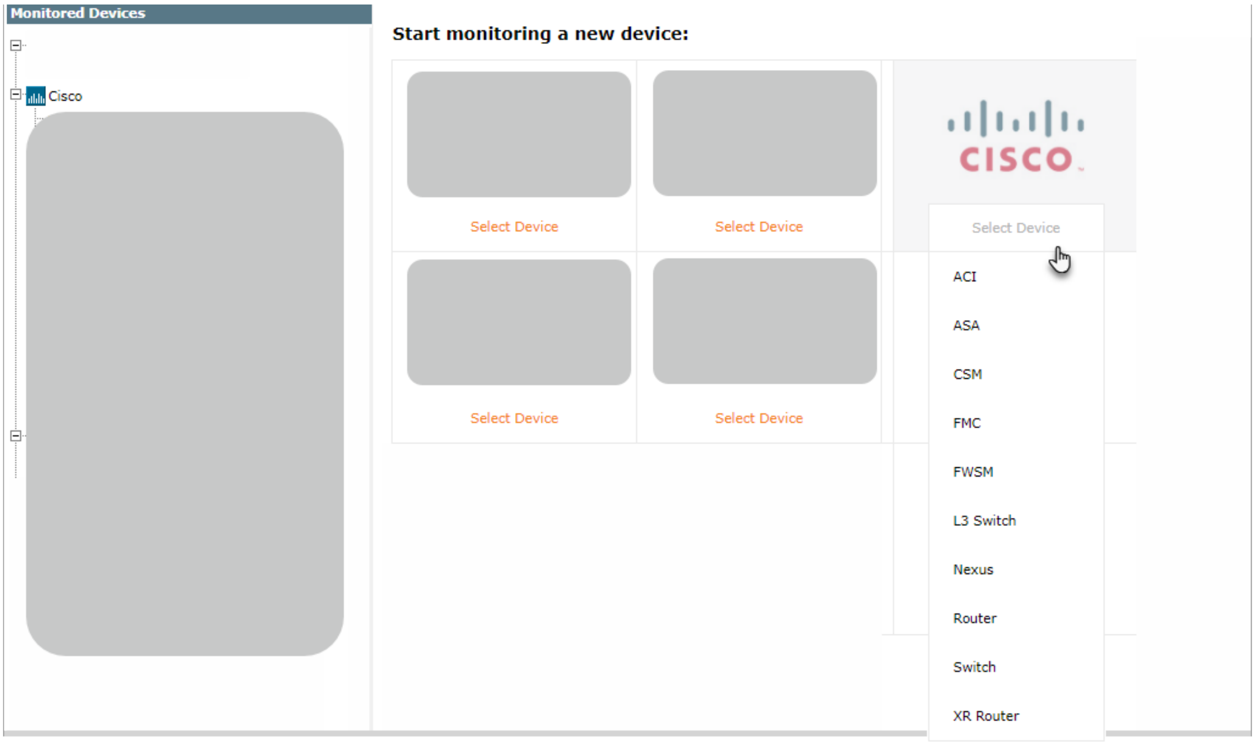
  `changeto system`

  `show context`

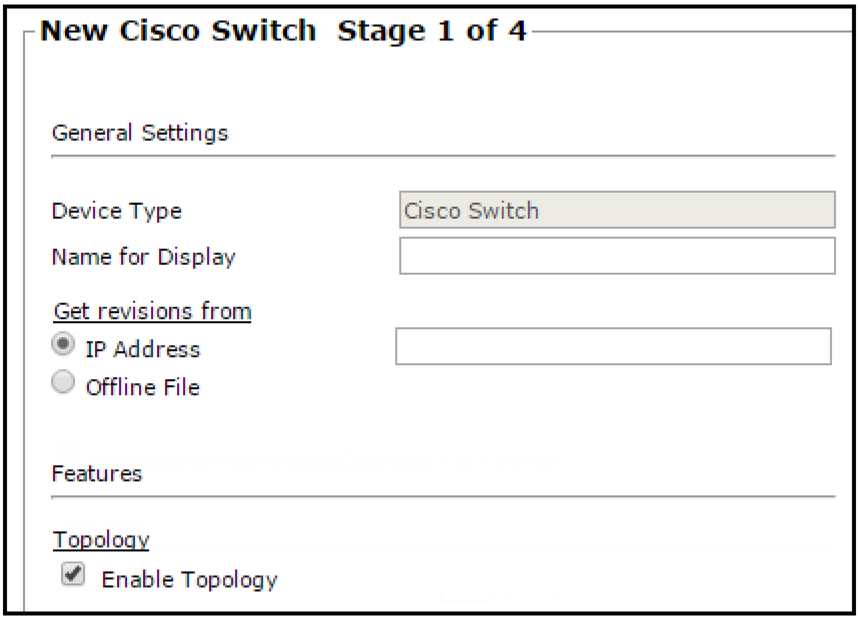
Adding a Cisco Switch Device

To configure TOS Classic to monitor the policy revisions of a Cisco device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:


New Cisco Switch Stage 1 of 4

General Settings

Device Type: Cisco Switch

Name for Display:

Get revisions from

● IP Address

○ Offline File

Features

Topology

☑ Enable Topology

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)

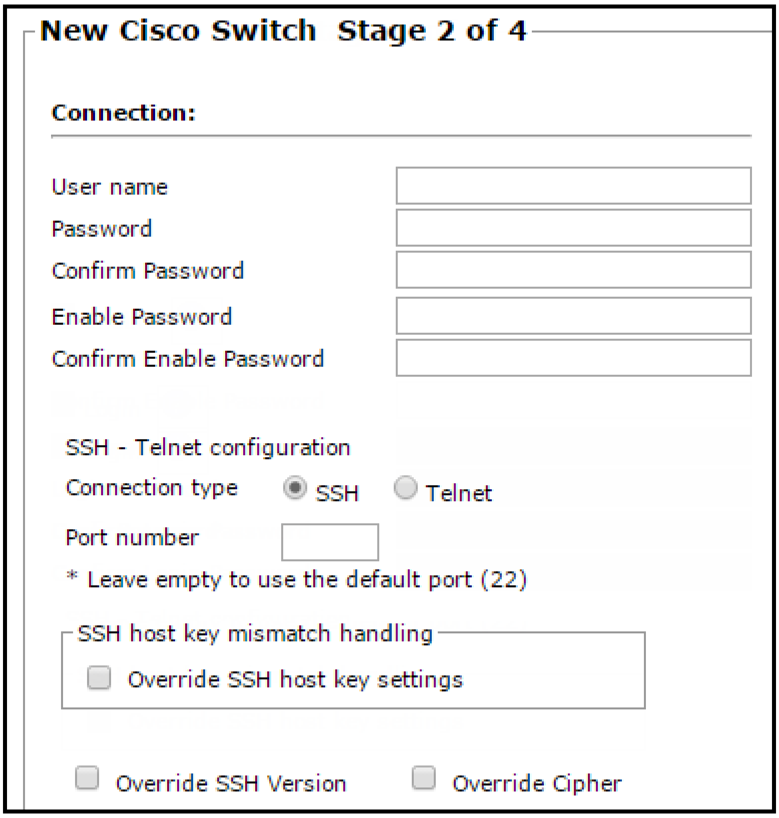
> Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure TOS Classic to limit the number of days that data is kept.

> We recommend that you enable TOS Classic administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, TOS Classic sends an alert.

- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.

Click **Next**.

4. Configure the TOS Classic connection to the Cisco device, according to the parameters required by the device:



New Cisco Switch Stage 2 of 4

Connection:

User name	
Password	
Confirm Password	
Enable Password	
Confirm Enable Password	

SSH - Telnet configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

□ Override SSH Version □ Override Cipher

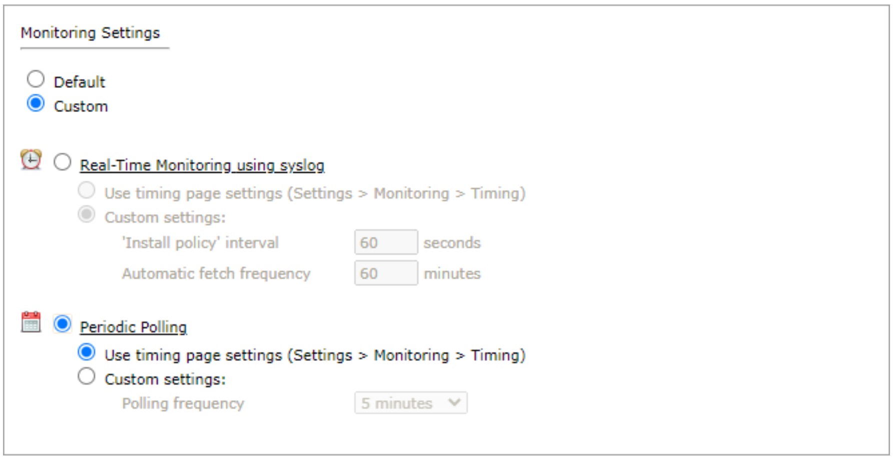
- Enter the authentication details needed to connect to the Cisco device.
  - **Username and password**: Enter the device username and password
  - **Enable password**: Enter the password to give TOS Classic elevated privileges on the device
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. The device can be configured to use either SSH version 1 or 2.
- To use default settings (recommended in most cases), leave the **Port number** and both **Override** options clear.
- If TOS Classic is configured to automatically replace the SSH host key when a new SSH host key is detected for a device, you can **Override SSH host key settings** to prevent the host key from being replaced for this device.

  You can then set TOS Classic to **Replace SSH host key automatically** for this specific device.

  Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.
- **Override SSH Version**: Select this option to force the device to use SSH-1 or SSH-2
- **Override Cipher**: Select this option to force the device to use DES or 3DES encryption

Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

Real-Time Monitoring: Applies only if syslogs "Sending Additional Information via Syslog" on page 239) are configured. Select **Custom settings** and configure:

- **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**.

6. **Save** the configuration.

   The Cisco device now appears in the **Monitored Devices** tree.

For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Using Cisco Switch Monitoring

> This is a Legacy Feature. We recommend you consider using the "Object Lookup" on page 334 feature.

To view a revision of IOS-level configuration data:

1. In **Compare** view, in the left-hand pane, select the relevant Cisco router or switch.
2. In the revisions list, select a revision.
3. Click **View Policy**.

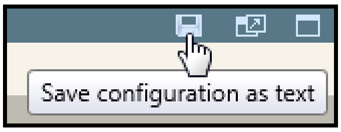
The configuration data is displayed.

To compare two revisions:

1. In **Compare** view, in the left-hand pane, select the relevant device.
2. In the revisions list, select two revisions.
3. Click **Compare**.

   When a change is detected, a "New Revision Report" is sent to SecureTrack users who are configured to receive them.

When viewing a single revision, you can export the policy as a text file:



Adding Cisco Nexus Switch Devices

TOS Classic monitors Cisco Nexus devices for policy revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

> TOS Classic can monitor Cisco switches for configuration and routing information. For more about the features supported for each device, see the feature support table.

Prerequisites

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Make sure that the device user account that you use for TOS Classic monitoring has permission to run these commands:

- Retrieve revision:

  ```
  terminal width 511
  terminal length 0
  show running-config
  show ip route direct vrf all
  show ip route static vrf all
  show clock
  ```

- Retrieve dynamic topology:

  ```
  show ip route vrf all
  show ip route bgp vrf all
  show ip interface vrf all
  show hsrp
  show vrrp detail
  show mpls interface detail
  show ip bgp | inc ID
  show ip bgp neighbors | inc BGP
  show bgp vpnv4 unicast labels vrf all
  ```

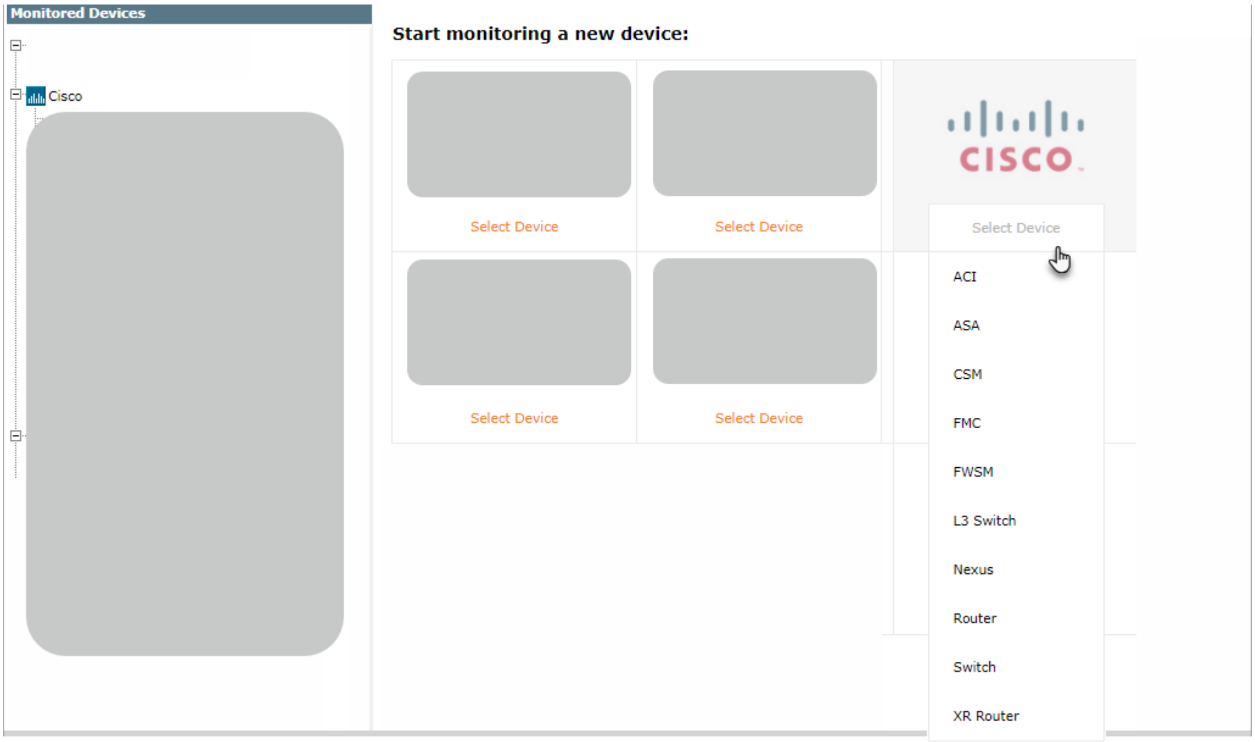
  `show nve vni` (for VXLAN protocol only)

- Provisioning:

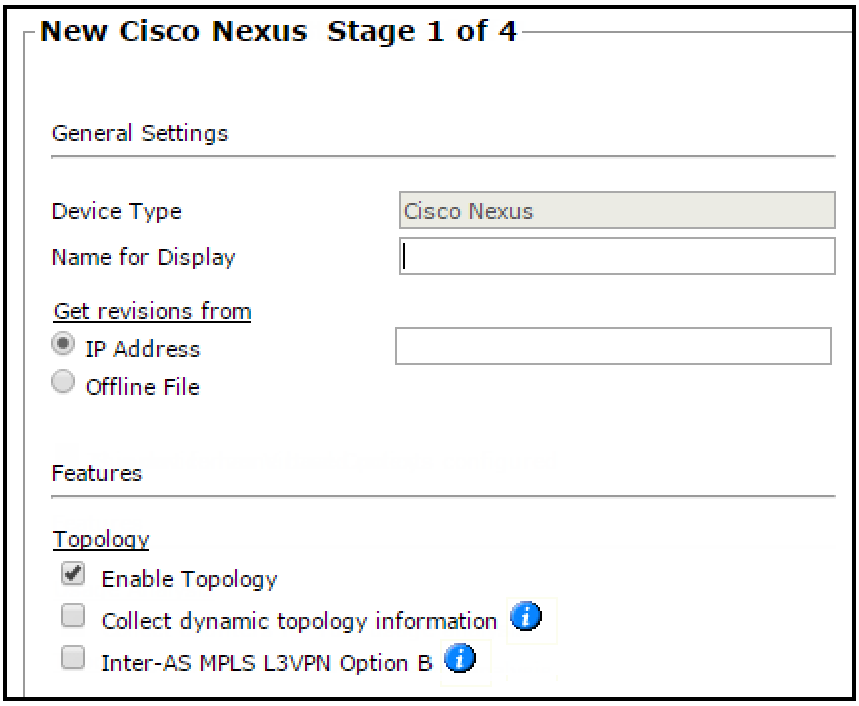
  ```
  changeto system
  show context
  ```

Monitor a Cisco Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Cisco Nexus Stage 1 of 4

General Settings

Device Type: Cisco Nexus

Name for Display:

Get revisions from

● IP Address

○ Offline File

Features

Topology

☑ Enable Topology

□ Collect dynamic topology information

□ Inter-AS MPLS L3VPN Option B

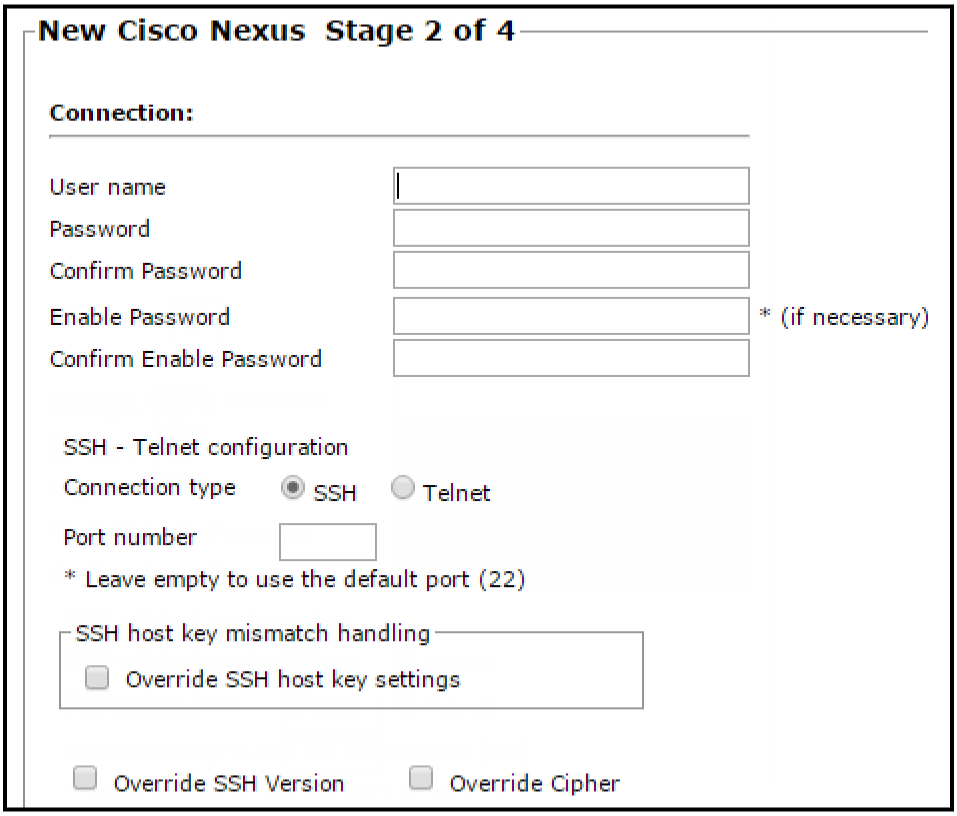
- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)

- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.

  If the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), also select **Collect dynamic topology information**.
- **Inter-AS MPLS L3VPN Option B**: Select this option if this router is an autonomous system boundary router (ASBR) in an MPLS option B environment. This option retrieves VPNv4 labels associated with inter-AS communication.

Click **Next**.

4. Configure the TOS Classic connection to the Cisco device, according to the parameters required by the device:



New Cisco Nexus Stage 2 of 4

Connection:

User name	
Password	
Confirm Password	
Enable Password	* (if necessary)
Confirm Enable Password	

SSH - Telnet configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

□ Override SSH Version □ Override Cipher

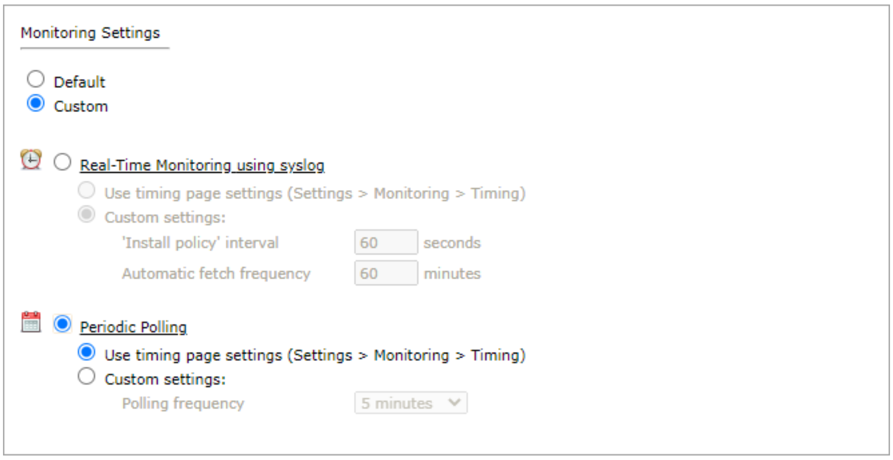
- Enter the authentication details needed to connect to the Cisco device.
  - **Username and password**: The device username and password
  - **Enable** password: Enter the enable password to give TOS Classic elevated privileges on the device
- Select whether to use **SSH** (preferred) or **Telnet**: The device can be configured to use either SSH version 1 or 2
- To use default settings (recommended in most cases), leave the **Port number** and both **Override** options clear.
- If TOS Classic is configured to automatically replace the SSH host key when a new SSH host key is detected for a device, you can **Override SSH host key settings** to prevent the host key from being replaced for this device.

  You can then set TOS Classic to **Replace SSH host key automatically** for this specific device.

  Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.
- **Override SSH Version**: Select this option to force the device to use SSH-1 or SSH-2
- **Override Cipher**: Select this option to force the device to use DES or 3DES encryption

Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

Real-Time Monitoring: Applies only if syslogs "Sending Additional Information via Syslog" on page 239) are configured. Select **Custom settings** and configure:

- **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**

6. **Save** the configuration.

The Cisco device now appears in the **Monitored Devices** tree.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Cisco L3 Switch Devices

TOS Classic monitors layer-3 switch devices for policy revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

TOS Classic can monitor Cisco layer-3 switches that have been added to TOS Classic for access lists, and configuration and routing information. For more about the features supported for each device, see the feature support table.

Prerequisites

TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Make sure that the device user account that you use for SecureTrack monitoring has permission to run these commands:

- Retrieve revision:

```
terminal no exec prompt timestamp
```

```
show running-config
```

or

```
show configuration
```

or

```
show startup-config
```

```
show ip route connected
show ip route static
show clock
show version
show access-lists
```

- Retrieve dynamic topology:

```
show ip vrf detail
```

For each VRF run:

```
show ip route vrf <vrf name>
show ip interface
show mpls interface detail
show ip bgp | inc ID
```

If BGP is used, run:

```
show ip bgp neighbors | inc BGP
show ip bgp vpnv4 all labels
show standby
```

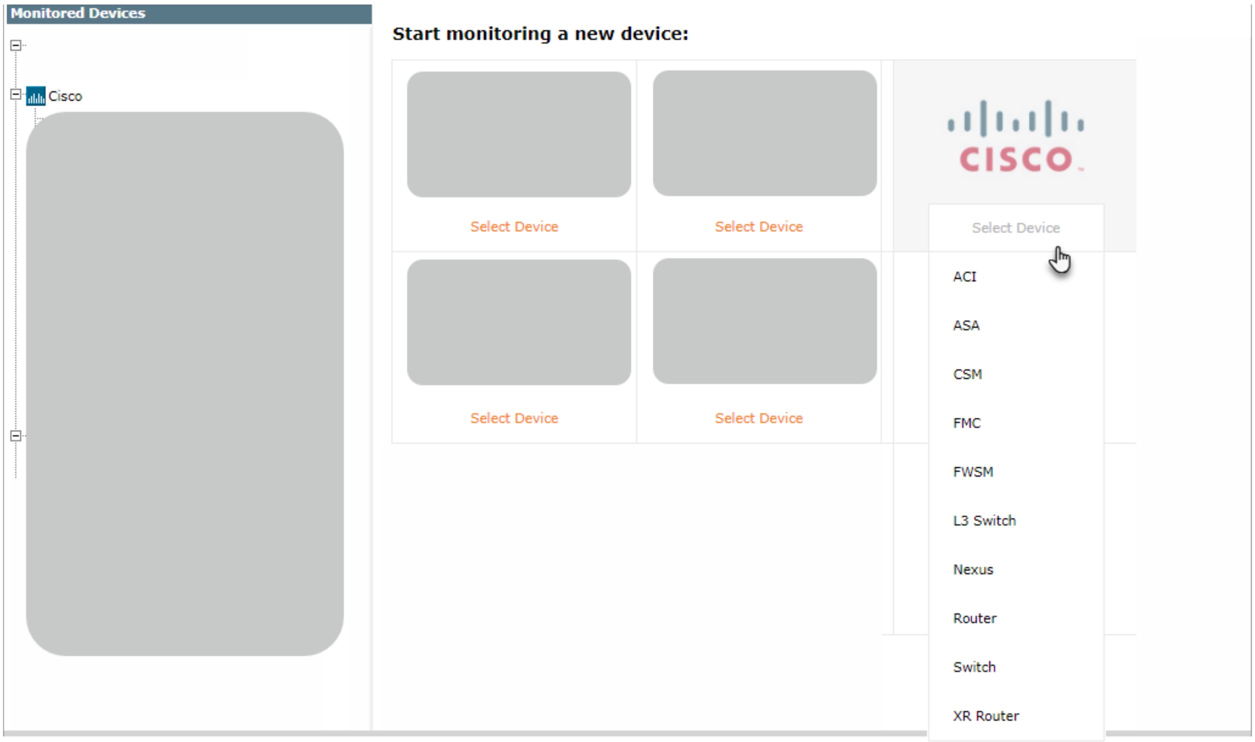
- Provisioning:

```
changeto system
show context
```

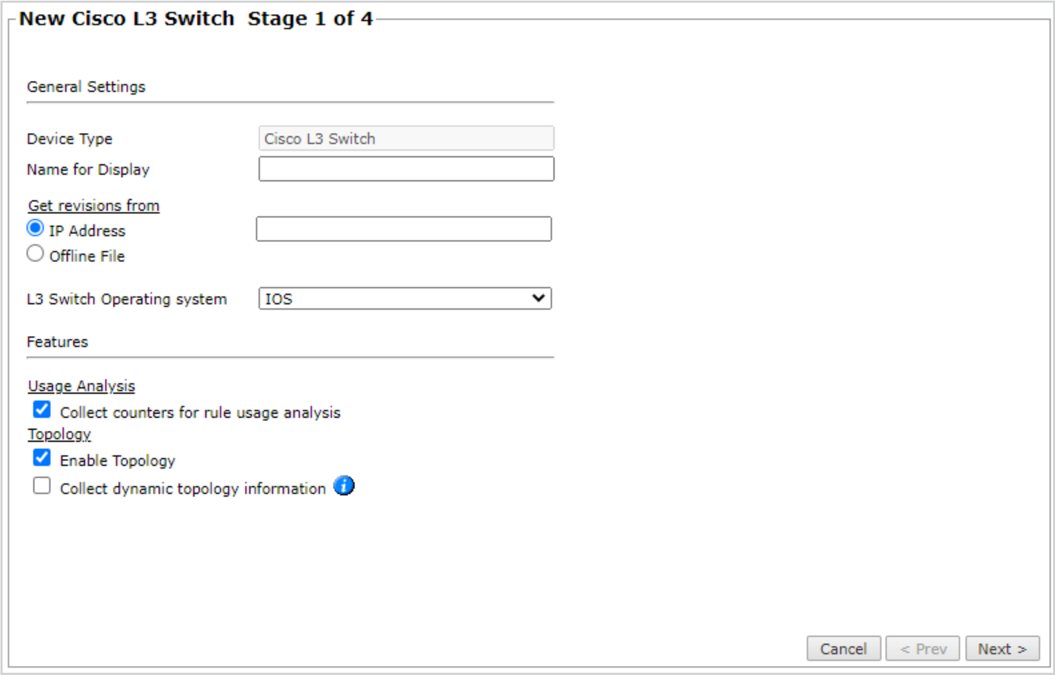
Monitor a Cisco Device

To configure SecureTrack to monitor the policy revisions of a Cisco device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Cisco L3 Switch Stage 1 of 4

General Settings

Device Type	Cisco L3 Switch
Name for Display	

Get revisions from

● IP Address

○ Offline File

L3 Switch Operating system: IOS

Features

Usage Analysis

☑ Collect counters for rule usage analysis

Topology

☑ Enable Topology

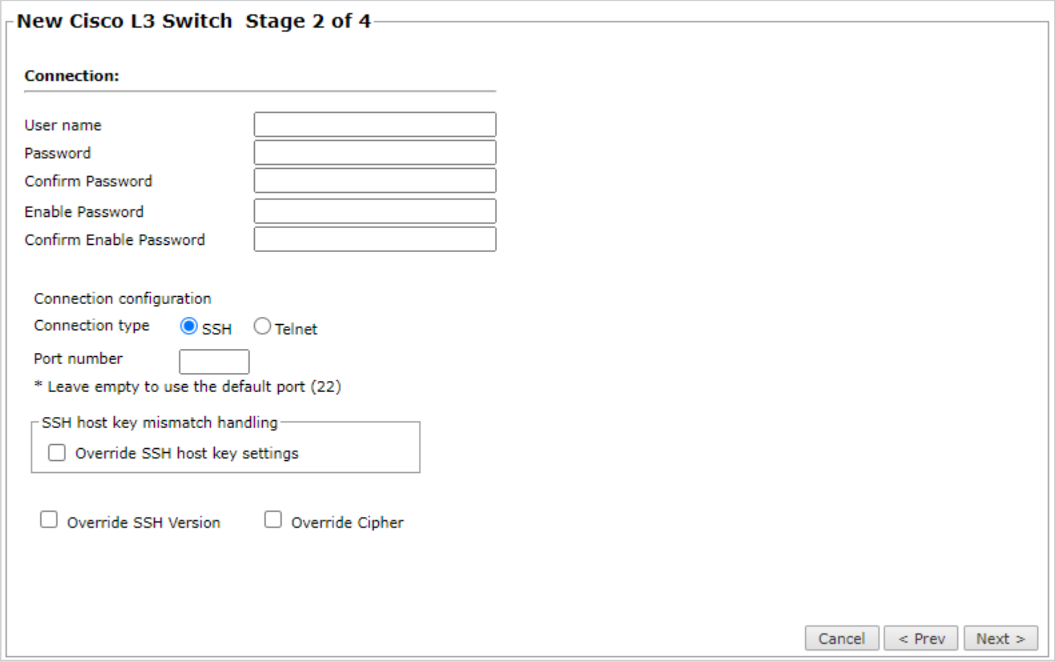
□ Collect dynamic topology information

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis
- **ST server**: In a distributed deployment, select which SecureTrack server monitors this device (Not shown in image)

- **L3 Switch Operating system**: IOS or IOS-XE
- **Collect counters for rule usage analysis**: Required for Rule Usage reports
- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- If the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), also select **Collect dynamic topology information**.

Click **Next**.

4. Configure the SecureTrack connection to the Cisco device, according to the parameters required by the device:



New Cisco L3 Switch Stage 2 of 4

Connection:

User name
Password
Confirm Password
Enable Password
Confirm Enable Password

Connection configuration
Connection type ● SSH ○ Telnet
Port number
* Leave empty to use the default port (22)

SSH host key mismatch handling
□ Override SSH host key settings

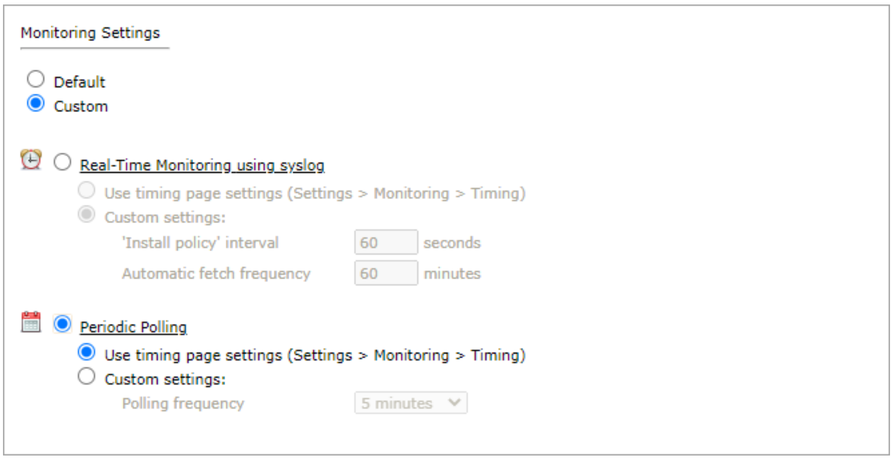
□ Override SSH Version □ Override Cipher

- Enter the authentication details needed to connect to the Cisco device.
  - **Username and Password**: The device username and password
  - **Enable Password**: If your device requires the Enable password, select this option and enter the password to give SecureTrack elevated privileges on the device
- Select whether to use **SSH** (preferred) or **Telnet**: The device can be configured to use either SSH version 1 or 2
- To use default settings (recommended in most cases), leave the **Port number** and both **Override** options clear.
- If SecureTrack is configured to automatically replace the SSH host key when a new SSH host key is detected for a device, you can **Override SSH host key settings** to prevent the host key from being replaced for this device.

  You can then set SecureTrack to **Replace SSH host key automatically** for this specific device.

  Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.
- **Override SSH Version**: Select this option to force the device to use SSH-1 or SSH-2
- **Override Cipher**: Select this option to force the device to use DES or 3DES encryption

5. Click **Next**.
6. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

Real-Time Monitoring: Applies only if syslogs "Sending Additional Information via Syslog" on page 239) are configured. Select **Custom settings** and configure:

- **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, SecureTrack combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**.

7. **Save** the configuration.

The Cisco device now appears in the **Monitored Devices** tree.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Cisco Security Manager (CSM) Devices

TOS Classic monitors Cisco Security Manager devices for policy revision changes. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

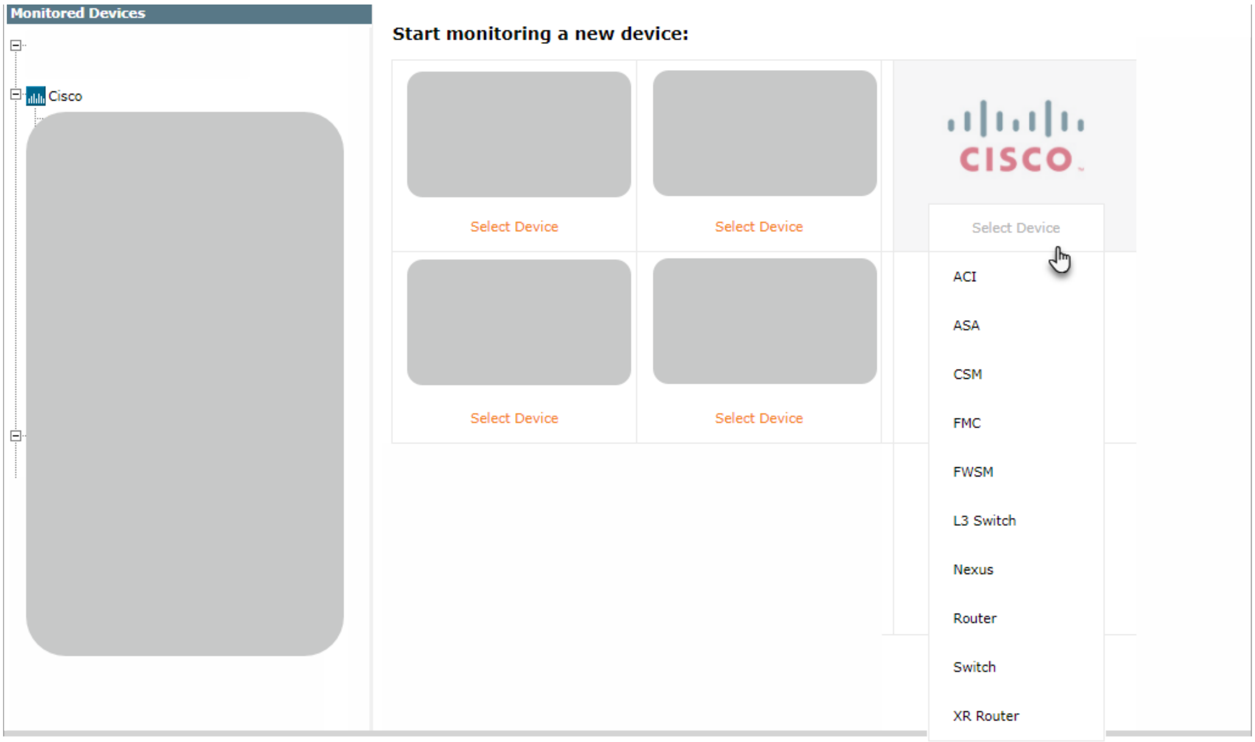
Prerequisites

TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

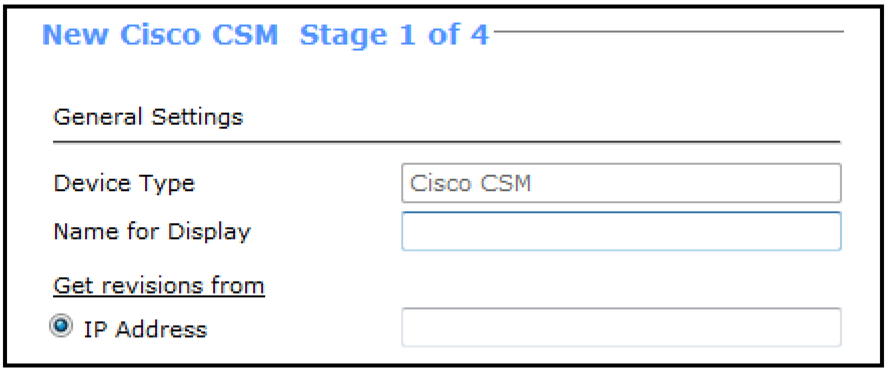
If you currently monitor your firewalls as standalone devices and you want to now monitor the firewall through the Cisco device that manages them, add the Cisco device and its firewalls as a new device and then disable your standalone firewalls (see Status). You can select the standalone devices from the device tree to see the historical device data. When the device data in the standalone firewalls is obsolete, you can remove the standalone firewall devices from TOS Classic.

Add a Cisco Security manager Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Cisco CSM Stage 1 of 4

General Settings

Device Type	Cisco CSM
Name for Display	

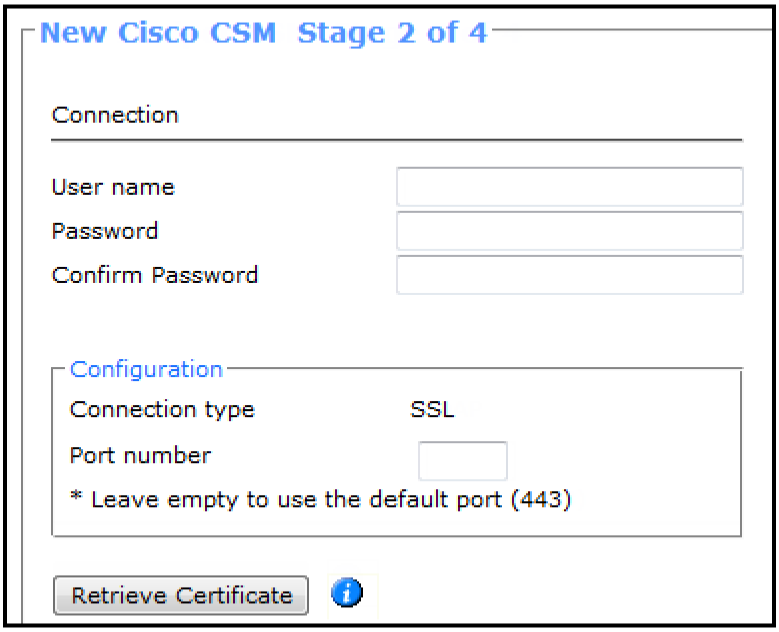
Get revisions from

● IP Address

- **Name for Display**
- Get revisions from **IP Address**
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)

Click **Next**.

4. Configure the TOS Classic connection to the Cisco device, according to the parameters required by the device:



New Cisco CSM Stage 2 of 4

Connection

User name

Password

Confirm Password

Configuration

Connection type SSL

Port number

* Leave empty to use the default port (443)

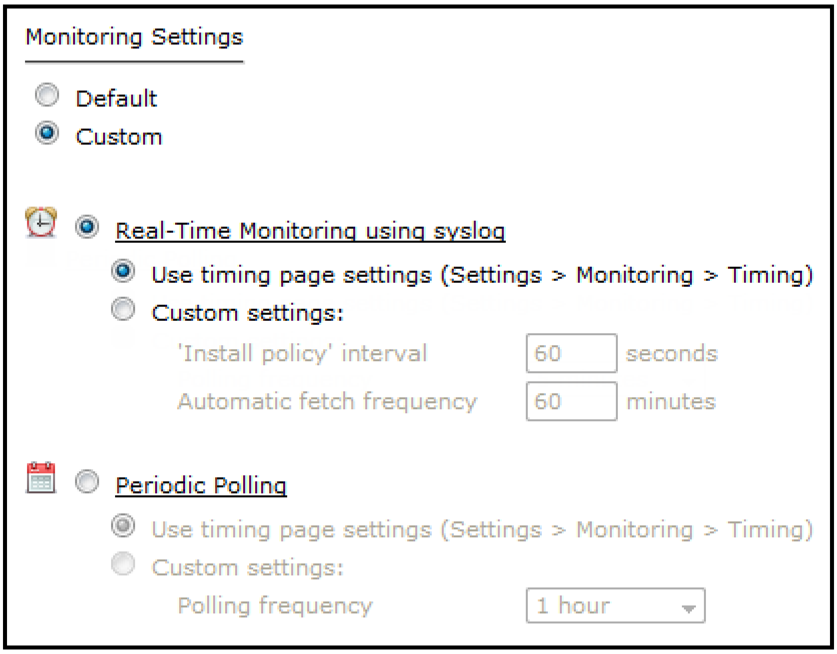
- Enter the authentication details needed to connect to the Cisco device.
- TOS Classic connects to Cisco devices with the SSL protocol. To use default settings (recommended in most cases), leave the **Port number** blank.
- Click **Retrieve Certificate** to setup encrypted communication between TOS Classic and the Cisco device.

  The certificate appears, and the following message is displayed:

The certificate was retrieved successfully.

Click **Next**.

5. The **Monitoring Settings** page appears:



Monitoring Settings

○ Default

● Custom

● Real-Time Monitoring using syslog

● Use timing page settings (Settings > Monitoring > Timing)

○ Custom settings:

'Install policy' interval 60 seconds

Automatic fetch frequency 60 minutes

○ Periodic Polling

● Use timing page settings (Settings > Monitoring > Timing)

○ Custom settings:

Polling frequency 1 hour

To use real-time monitoring when available, and timing settings from the Timing page, select **Default**. Otherwise, select **Custom** and configure the monitoring mode and settings:

Real-Time Monitoring using syslog: Select **Custom settings** and configure:

- **'Install policy' interval**: After a policy is saved, if the policy is installed within this interval, both actions are shown in TOS Classic as one revision.
- **Automatic fetch frequency**: How frequently the policy is retrieved even if there is no policy save or install action.
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**.

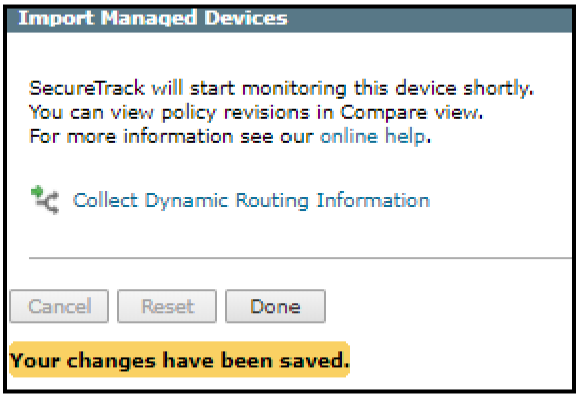
6. **Save** the configuration.

   The Cisco device now appears in the **Monitored Devices** tree.

To import devices or domains managed by the Cisco device into TOS Classic:

1. Make sure you receive the first Cisco policy revision.
2. Select the Cisco device from the device tree.
3. Click **Import Managed Devices** or **Import Domains and Managed Devices**.
4. From the list of devices managed by the Cisco device, select the devices to import and click **Import**.
5. Do one of the following:
   - Click **Reset** to update the list of managed devices.
   - Click **Done** to return to the device tree (**Manage Devices**).

     The managed devices appear under the Cisco device in the device tree.
   - If available, click ⇄ to **Collect Dynamic Routing Information** for the managed devices.



Import Managed Devices

SecureTrack will start monitoring this device shortly.
You can view policy revisions in Compare view.
For more information see our online help.

Your changes have been saved.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Cisco Firepower Management Center (FMC) Devices

Overview

SecureTrack monitors Cisco Firepower Management Center devices for policy revision changes. To help you organize the information for your devices, see the device information worksheet. For the full list of supported TOS features for your device, see the feature support table.

To monitor an FMC device (and its managed devices) in TOS Classic, you must complete the following procedures:

1. Add the Cisco FMC device to TOS Classic.
2. Import the domains and devices managed by the Cisco FMC device.
3. Select devices managed by the Cisco FMC device for which you want to retrieve dynamic topology information.
4. Edit the configuration of a managed Cisco firewall device, including enabling or disabling the option to **Collect dynamic topology information**.

Prerequisites

- Separate authentication credentials for both SecureTrack and SecureChange.
- TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.
- Monitoring Cisco Firepower Management Center (FMC) devices requires HTTP access via port 443.
- To collect Dynamic Topology information, make sure that SSH or Telnet access to the device is enabled.
- The following minimum user roles are required:
  - Administrator
  - Access Admin
  - Network Admin
- To collect usage, configure the FMC device to send syslogs to TOS Classic.
  - The syslog device ID for the FTD device managed by the FMC is required to enable TOS Classic to collect usage data.
- The following commands to collect Dynamic Topology:

Command	Description
`show route`	Extracts the routing table
`show interface`	Extracts the interfaces
`connect ftd`	Use this command to change the FTD context for running the `show route` and `show interface` commands

In the Cisco Firepower Management Center (FMC), the REST API is enabled by default:

- Before you begin, confirm that the REST API is enabled.
- If you use UCAPL mode, confirm that the REST API is disabled.

To enable the REST API:

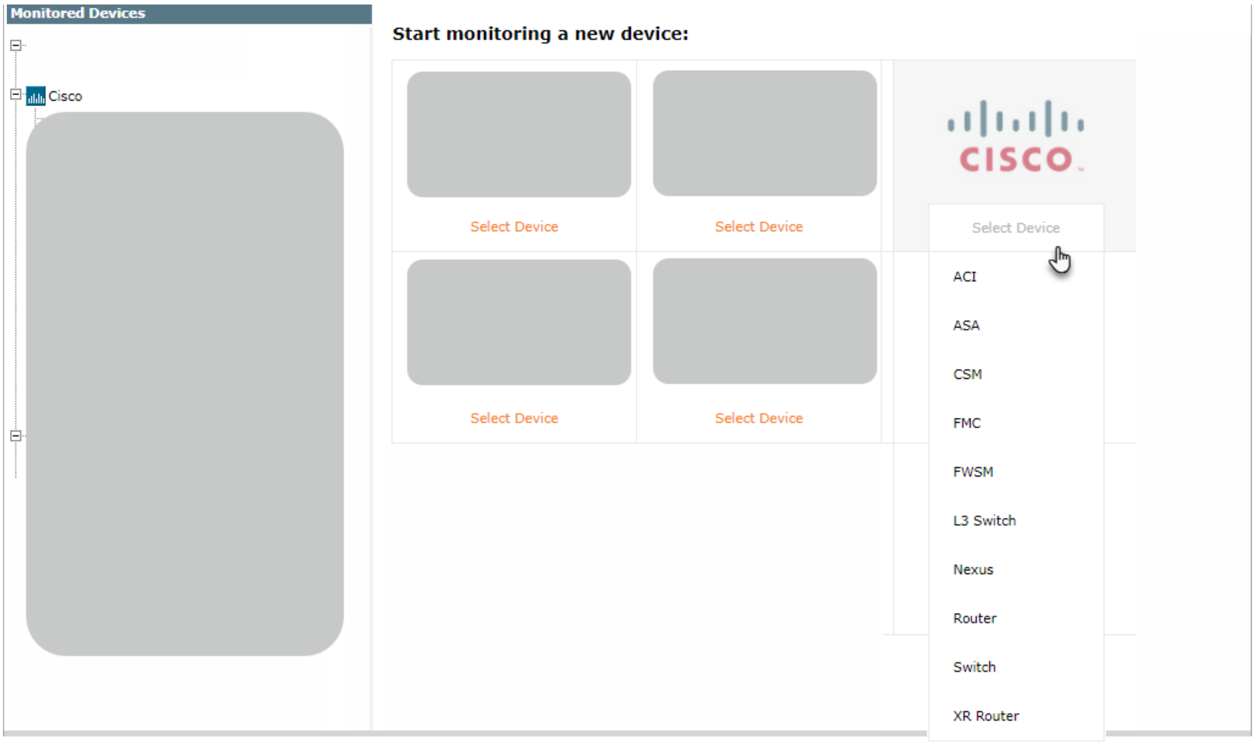
1. In the FMC, go to **System** > **Configuration** > **REST API Preferences** > **Enable REST API**.
2. Check **Enable REST API**.
3. Click **Save**.

   Save Successful displays when the REST API is enabled.

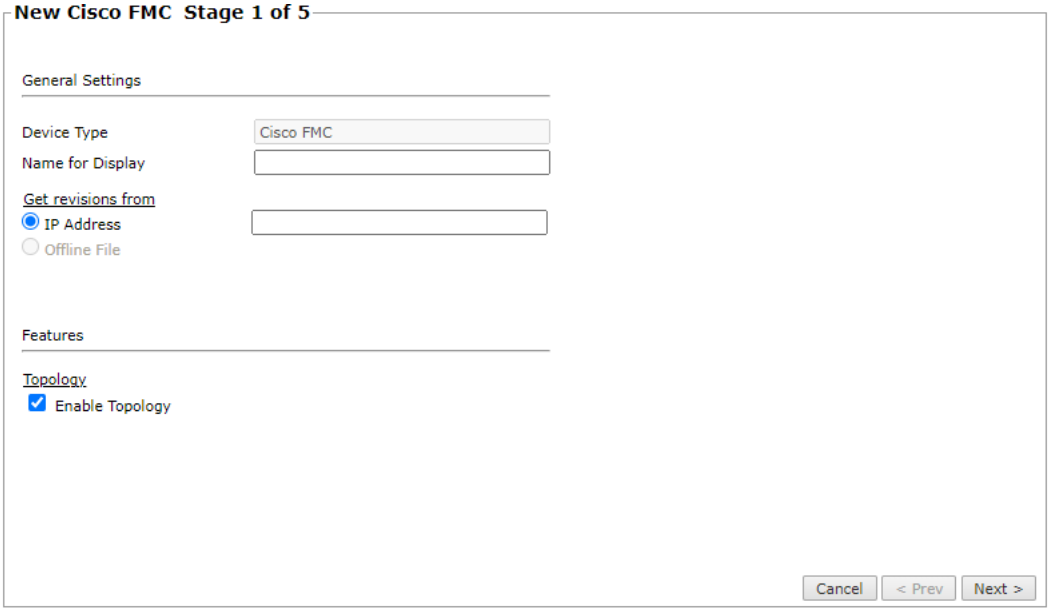
Monitor a Cisco Device

To configure TOS Classic to monitor the policy revisions of a Cisco device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Cisco FMC Stage 1 of 5

General Settings

Device Type	Cisco FMC
Name for Display	

Get revisions from

● IP Address

○ Offline File

Features

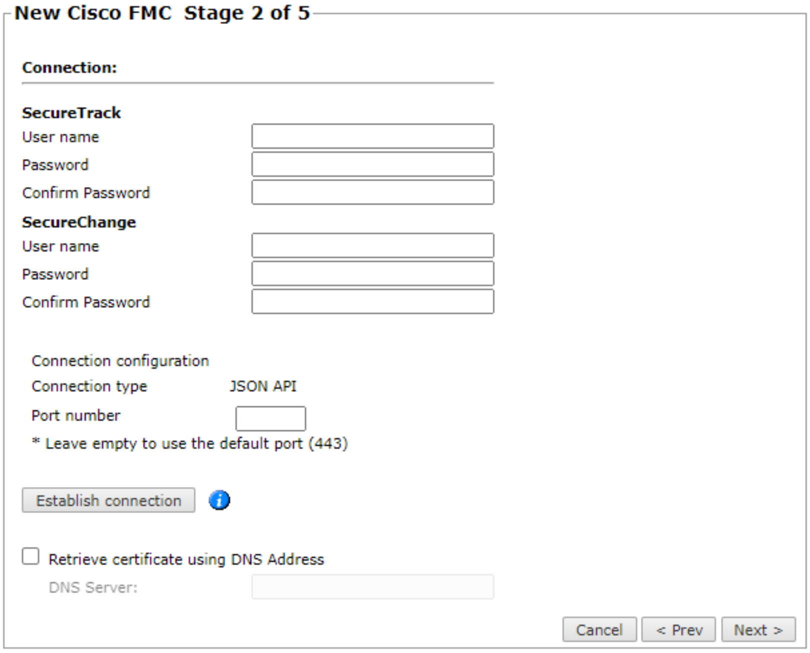
Topology

☑ Enable Topology

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically.
  - **Offline File**: This option is disabled for FMC devices.
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- **Enable Topology**: Collects routing information for building the network Interactive Map.

4. Click **Next**.

5. Configure the TOS Classic connection to the Cisco device, according to the parameters required by the device:



New Cisco FMC Stage 2 of 5

Connection:

SecureTrack

User name

Password

Confirm Password

SecureChange

User name

Password

Confirm Password

Connection configuration

Connection type JSON API

Port number

* Leave empty to use the default port (443)

☐ Retrieve certificate using DNS Address

DNS Server:

- Enter the authentication details needed to connect to the Cisco device.

  > ⚠ If you are using SecureChange, you need to enter separate access credentials for both SecureTrack and SecureChange. However, If you are only using SecureTrack, leave the **SecureChange** section empty.

  TOS Classic uses JSON API format to retrieve Cisco FMC device information.

- To use default settings (recommended in most cases), leave the **Port number** blank.

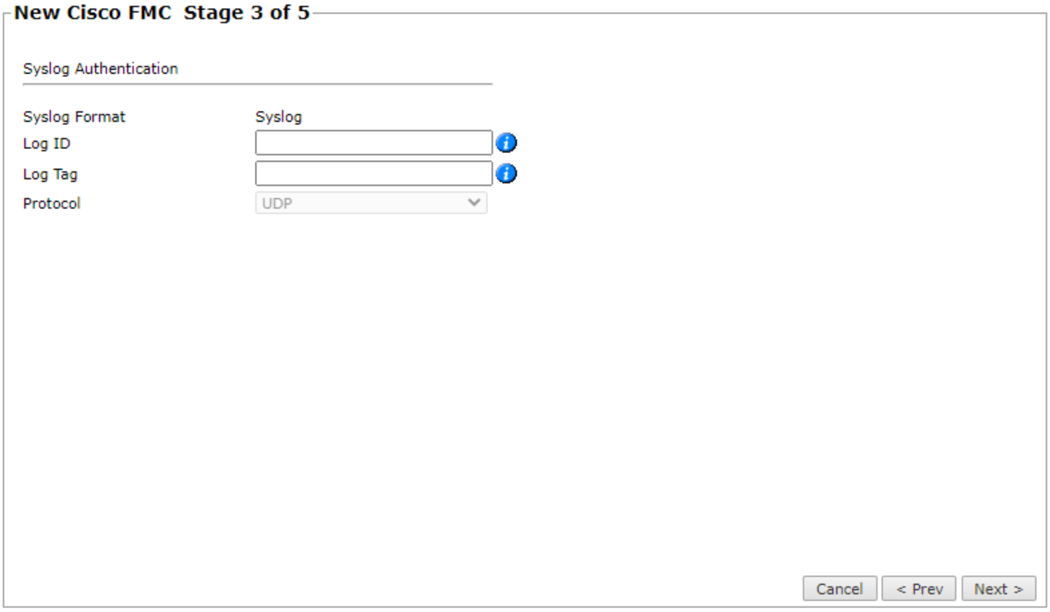
- Click **Establish connection** to set up encrypted communication between TOS Classic and the Cisco device. The following message appears:

  The connection was established successfully.

- To retrieve the FMC certificate using a DNS address, select **Retrieve certificate using DNS Address**, and enter the address of the DNS server.

6. Click **Next**.

7. Configure the Syslog authentication:



New Cisco FMC Stage 3 of 5

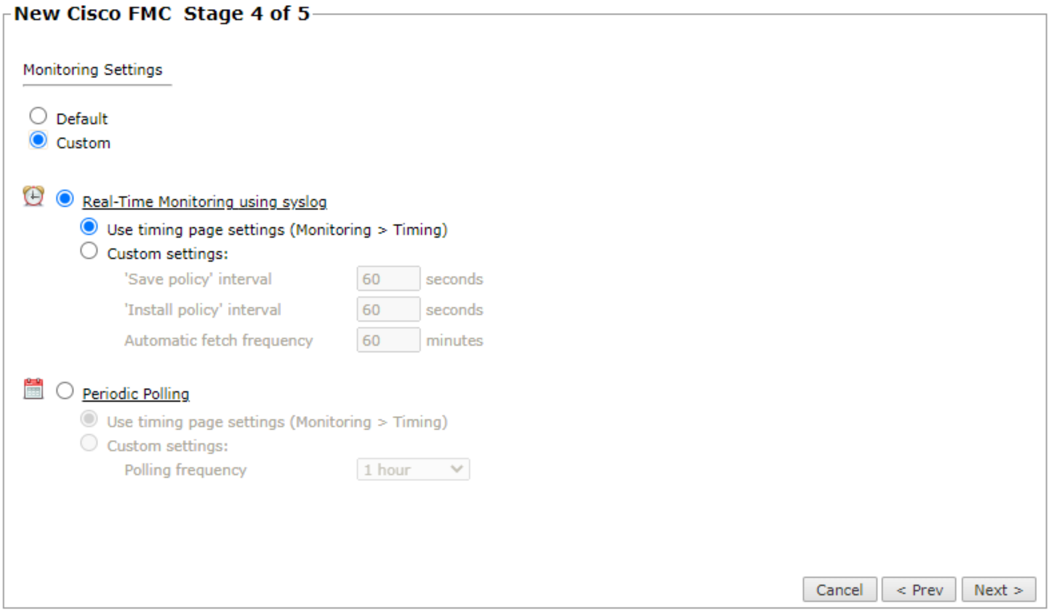
Syslog Authentication

Syslog Format	Syslog
Log ID	
Log Tag	
Protocol	UDP

- **Log ID**: The Log ID which corresponds to the User Defined ID in the FMC Syslog Settings. This tag is used for Data Usage.
- **Log Tag**: The Tag ID which corresponds to the Tag configured in Configuration > Audit Log > Tag. This tag is used for Accountability. You cannot define the same Tag ID in multiple FMC devices.
- **Protocol**: The Protocol is UDP by default and disabled.

8. Click **Next**.

9. In **Monitoring Settings**, do one of the following:



New Cisco FMC Stage 4 of 5

Monitoring Settings

○ Default
● Custom

● Real-Time Monitoring using syslog
- ● Use timing page settings (Monitoring > Timing)
- ○ Custom settings:
  - 'Save policy' interval 60 seconds
  - 'Install policy' interval 60 seconds
  - Automatic fetch frequency 60 minutes

○ Periodic Polling
- ● Use timing page settings (Monitoring > Timing)
- ○ Custom settings:
  - Polling frequency 1 hour

- Select **Default** to use the default time configured in **Periodic Polling** (1 hour).
- Select **Custom** and configure the monitoring mode and settings.

  For both **Custom** options, you can use the timing page settings

  - **Real-Time Monitoring using syslog** - Select **Custom settings** to configure the **'Save policy' interval**, **'Install policy interval'**, and **Automatic fetch frequency**.

    For more information, see Configuring a Cisco FMC to Send Syslogs.

- **Periodic Polling**: select **Custom settings** and configure the **Polling frequency** (jow often TOS Classic fetches the configuration from each device).

If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

10. Click **Next**.
11. **Save** the configuration.

    The Cisco device now appears in the **Monitored Devices** tree.

Import the domains or devices managed by the Cisco device

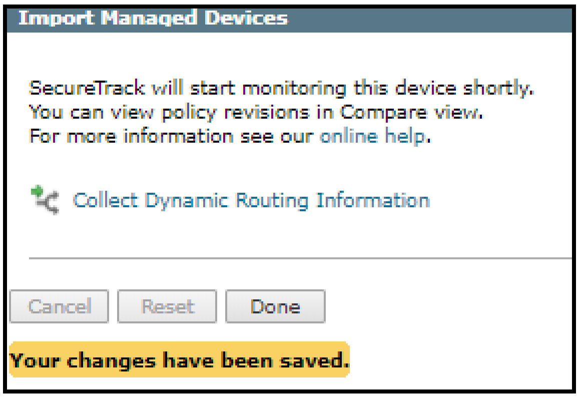
To import devices or domains managed by the Cisco device into TOS Classic:

1. Make sure you receive the first Cisco policy revision.
2. Select the Cisco device from the device tree.
3. Click **Import Managed Devices** or **Import Domains and Managed Devices**.
4. From the list of devices managed by the Cisco device, select the devices to import and click **Import**.
5. In the **Usage Tracking** section:
   - **Enable tracking of rule usage:** Select to enable usage for rules to be collected and saved in the SecureTrack database.
   - **Enable tracking of object usage:** Select to enable usage for objects in rules to be collected and saved in the SecureTrack database.

   If these options are selected:

   - The collected usage is displayed in the **Last Hit** column in Policy Browser.
   - Automatic Policy Generation (APG) is enabled.
   - The Rule and Object Usage Report is enabled.
6. Do one of the following:
   - Click **Reset** to update the list of managed devices.
   - Click **Done** to return to the device tree.

     The managed devices appear under the Cisco device in the device tree.
   - If available, click to **Collect Dynamic Routing Information** for the managed devices.



Import Managed Devices

SecureTrack will start monitoring this device shortly.
You can view policy revisions in Compare view.
For more information see our online help.

Collect Dynamic Routing Information

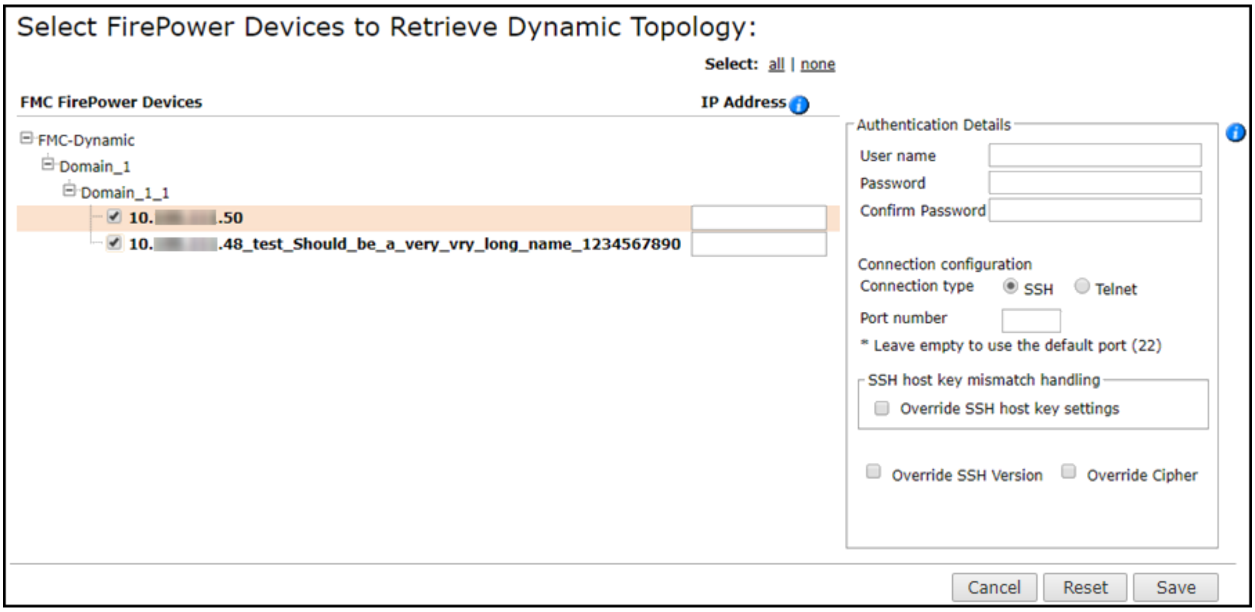
Your changes have been saved.

Edit the Dynamic Topology settings for devices managed by a Cisco FMC device

To collect Dynamic Topology information, make sure that SSH or Telnet access to the device is enabled.

To configure a Cisco FMC device to retrieve Dynamic Topology information for its managed devices in TOS Classic:

1. Select the Cisco FMC device from the device tree.
2. Click to **Collect Dynamic Routing Information**.
3. In **Select FirePower Devices to Retrieve Dynamic Topology:**



Select FirePower Devices to Retrieve Dynamic Topology:

Select: all | none

FMC FirePower Devices | IP Address

- ⊟ FMC-Dynamic
  - ⊟ Domain_1
    - ⊟ Domain_1_1
      - ☑ 10.[redacted].50
      - ☑ 10.[redacted].48_test_Should_be_a_very_vry_long_name_1234567890

Authentication Details

User name

Password

Confirm Password

Connection configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

□ Override SSH Version □ Override Cipher

a. Select the devices for which you want to retrieve Dynamic Topology.

b. For each device, provide an IP address that can be routed from TOS Classic.

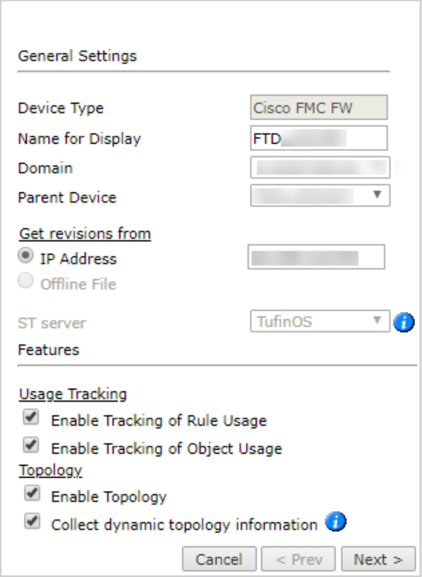
c. Enter the **Authentication Details** for the FMC FirePower devices and click **Save**.

All the selected devices must have the same user name and password.

Edit the configuration of a managed Cisco firewall device

To edit the configuration of a managed Cisco firewall device in TOS Classic:

1. Select the Cisco firewall device from the device tree.
2. Click **Edit Configuration**.



General Settings

Device Type: Cisco FMC FW

Name for Display: FTD[redacted]

Domain: [redacted]

Parent Device: [redacted]

Get revisions from

● IP Address [redacted]

○ Offline File

ST server: TufinOS

Features

Usage Tracking

☑ Enable Tracking of Rule Usage

☑ Enable Tracking of Object Usage

Topology

☑ Enable Topology

☑ Collect dynamic topology information

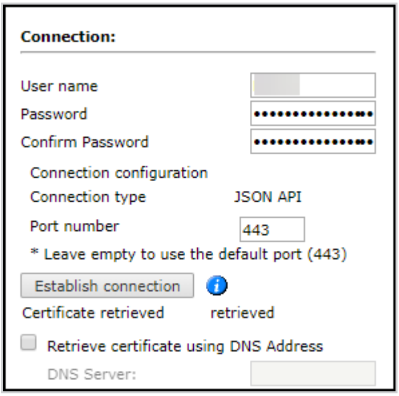
3. Edit the **General Settings**.
4. In the **Usage Tracking** section:
   - **Enable tracking of rule usage:** Select to enable usage for rules to be collected and saved in the SecureTrack database.
   - **Enable tracking of object usage:** Select to enable usage for objects in rules to be collected and saved in the SecureTrack database.

If these options are selected:

- The collected usage is displayed in the **Last Hit** column in Policy Browser.
- Automatic Policy Generation (APG) is enabled.
- The Rule and Object Usage Report is enabled.

5. In the **Topology** section:
   - **Enable Topology:** Collects routing information for building the network Interactive Map.
   - **Collect dynamic topology information:** Enables dynamic topology collection when dynamic addressing (DHCP) or routing protocols (OSPF and BGP) are in use.

     When dynamic topology is enabled:
     - Both static and dynamic routes are displayed on the interactive map.
     - Static routes are not shown as part of the revisions.
6. Click **Next**.



Connection:

User name

Password ••••••••••••••••

Confirm Password ••••••••••••••••

Connection configuration

Connection type JSON API

Port number 443

* Leave empty to use the default port (443)

Establish connection

Certificate retrieved retrieved

□ Retrieve certificate using DNS Address

DNS Server:

7. Edit the connection details and click **Next**.
8. Click **Save** to complete the device configuration.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Cisco ACI Devices

TOS Classic monitors Cisco ACI for policy revision changes. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Currently, only a single APIC is supported for each ACI fabric.
Only a single IP is supported for the APIC controller. If more than one IP is used for the APIC controller, a load balancer must be deployed.

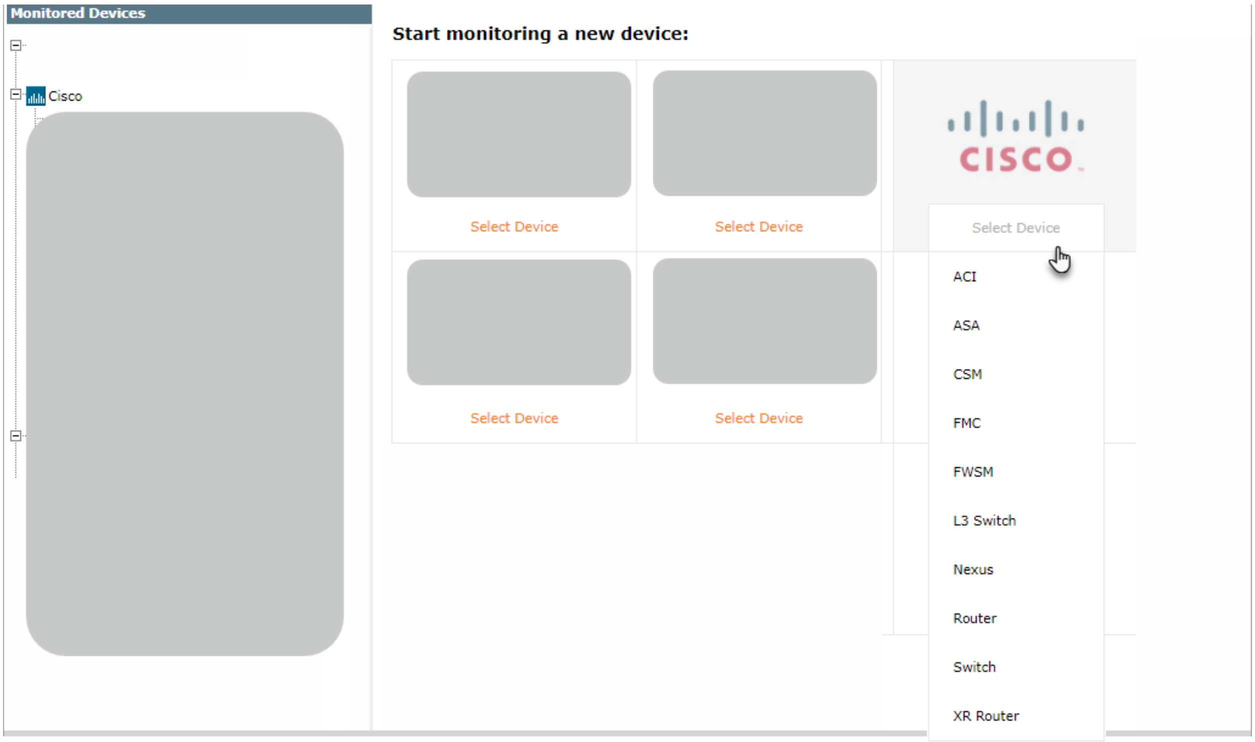
Prerequisites

Before you add Cisco ACI devices to TOS Classic, you must specify the ACI applications owner in the SecureApp settings.

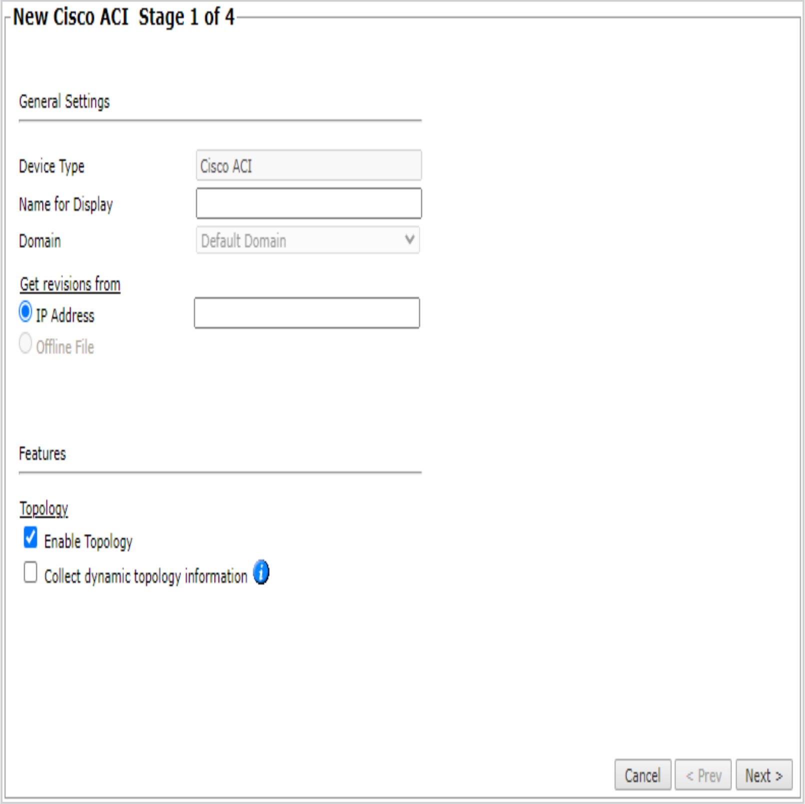
Monitor a Cisco ACI Device

To configure TOS Classic to monitor the policy revisions of a Cisco ACI device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select **Cisco** > **ACI**.



3. Configure the device settings:



New Cisco ACI Stage 1 of 4

General Settings

Device Type: Cisco ACI

Name for Display:

Domain: Default Domain

Get revisions from

● IP Address

○ Offline File

Features

Topology

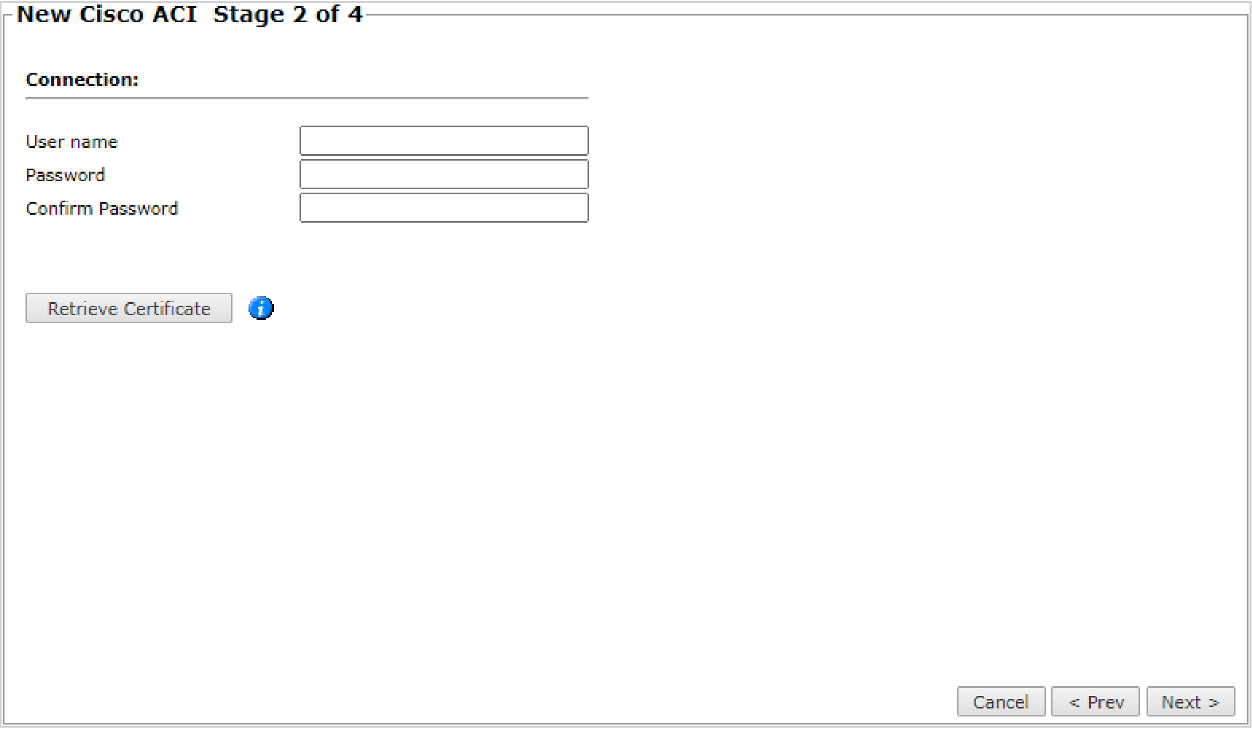
☑ Enable Topology

□ Collect dynamic topology information

- **General Settings**
  - **Name for Display**
  - **Domain** - Select the domain in a multidomain environment
- **Get revisions from**

    - **IP address** - Enter the IP address of the APIC controller
    - **Offline File** - Enter the file location
  - **Topology** - Click to enable Topology mode

4. Click **Next**
5. Configure the TOS Classic connection to the Cisco ACI device, according to the parameters required by the device and click **Next** to continue to the next stage:



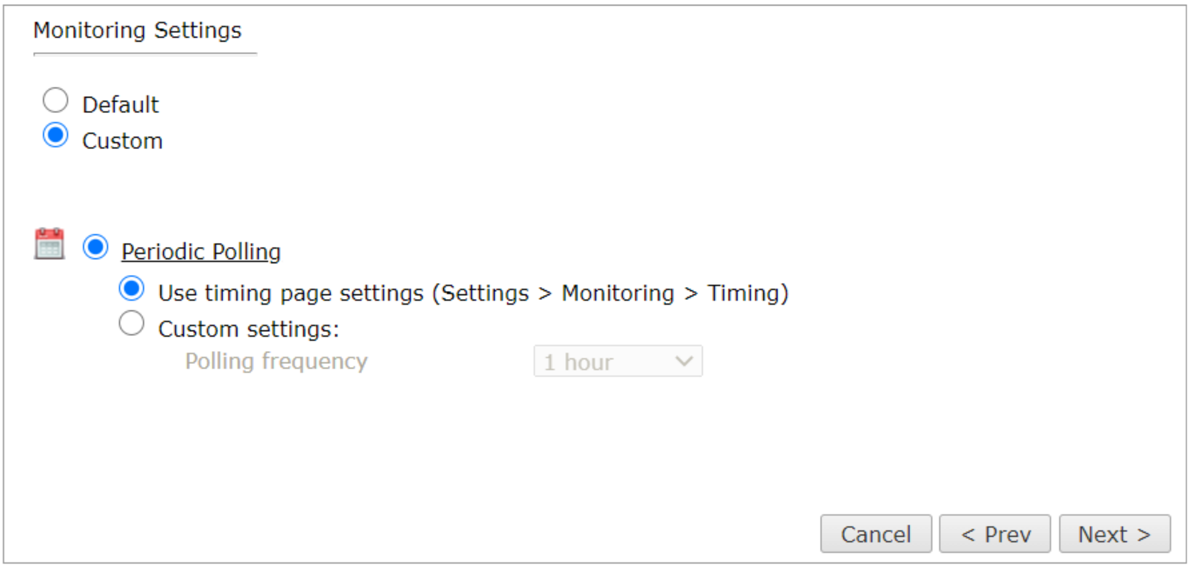
New Cisco ACI Stage 2 of 4

Connection:

User name
Password
Confirm Password

  - Enter the authentication details needed to connect to the Cisco APIC device. The user must have Read (Read Only, or Read/Write) permissions for all information on the Cisco ACI device.
  - Click **Retrieve Certificate** to setup encrypted communication between TOS Classic and the Cisco ACI device.

6. Click **Next**
7. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 1 hour

  - To use timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

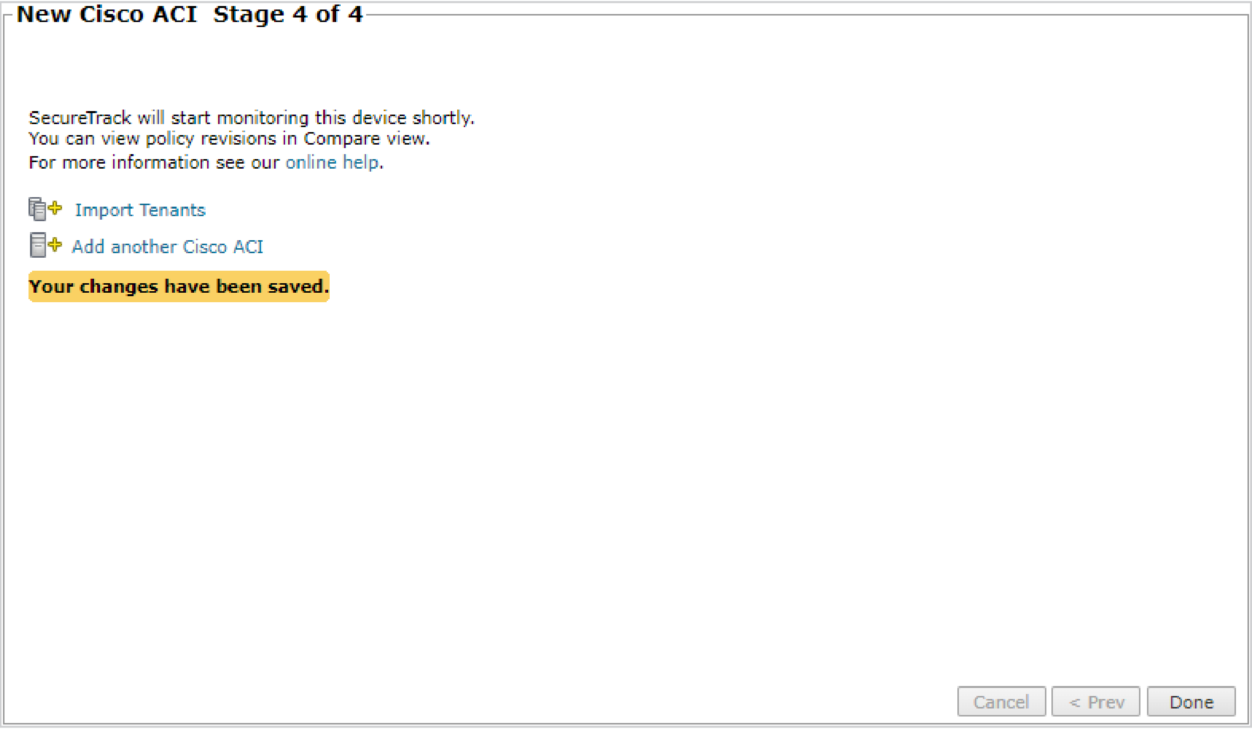
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

8. Click **Next**.
9. Click **Save**.

   The device now appears in the **Monitored Devices** tree.

10. To continue, select **Import Tenants** or **Add another Cisco ACI**



New Cisco ACI Stage 4 of 4

SecureTrack will start monitoring this device shortly.
You can view policy revisions in Compare view.
For more information see our online help.

Edit Cisco ACI Device Settings

To edit settings after you have added a Cisco ACI device:

1. Select the device and click **Edit configuration**.
2. Follow the stages described in steps 2, 3, 4, and 5 of the procedure to Monitor a Cisco ACI Device to edit **General Settings**, **Connection**, and **Monitoring Settings** and to **Save** your changes.

Import Tenants

To import tenants after you have added a Cisco ACI device:

1. Select the device and click **Import Tenants**.
2. Select all the managed devices to be added, click **Import**, and then **Done**.

How Do I Get Here

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Cisco ACI Fabric Visibility in TOS Classic

Tufin integrates your Cisco ACI device by modeling the ACI fabric in TOS Classic. Each tenant is represented as a separate device

TOS Classic derives robust security access rules to interpret and emulate the allowed ACI traffic flows. This set of rules is less susceptible to changes caused by small shifts in ACI configuration. The resulting Tufin security policy enables, redirects, and blocks the same traffic that the ACI does.

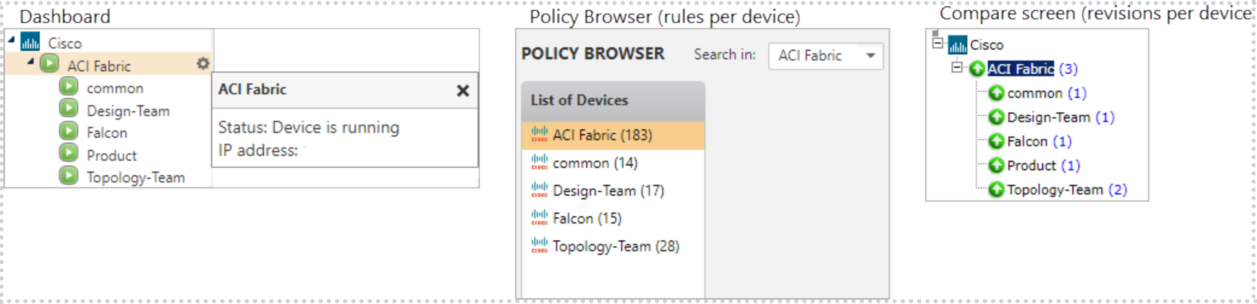
Each access rule includes metadata to indicate how it is derived from the ACI fabric, so you can track ACI configuration changes and search for relevant keywords. Rules that are built from ACI contracts indicate which contract and subject they are based on. Additional rules are derived from the configuration in the ACI, for example, vrf enforcement rules, which include implicit conditions that are external to contracts.

While the ACI zoning rules are not directly imported into TOS Classic, the access rules also simulate ACI zoning rule behavior, including emulating the priority ordering of the zoning rules.

When you associate a contract with VRFs as consumers or as providers and set the contract scope to Application-Profile, the behavior of Cisco ACI for this scope is non-deterministic. TOS Classic does not generate security rules for this situation, because the configuration may create different sets of zoning rules with different priorities at different times.

ACI Hierarchy Visibility

The image below displays the ACI hierarchy in the TOS Classic Dashboard, Policy Browser (with number of rules per devices), and in the Compare screen (with number of revisions per device).



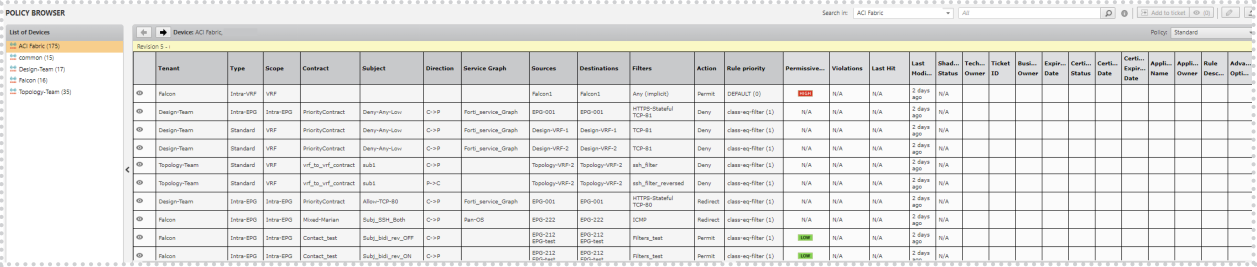
Status: Device is running
IP address:

ACI Fabric (183)
common (14)
Design-Team (17)
Falcon (15)
Topology-Team (28)

ACI Fabric (3)
common (1)
Design-Team (1)
Falcon (1)
Product (1)
Topology-Team (2)

ACI in the Policy Browser

At the parent ACI device level, for each tenant, Policy Browser displays a list of the security access rules that model the ACI traffic flows for that tenant, as well as the metadata related to the rules.

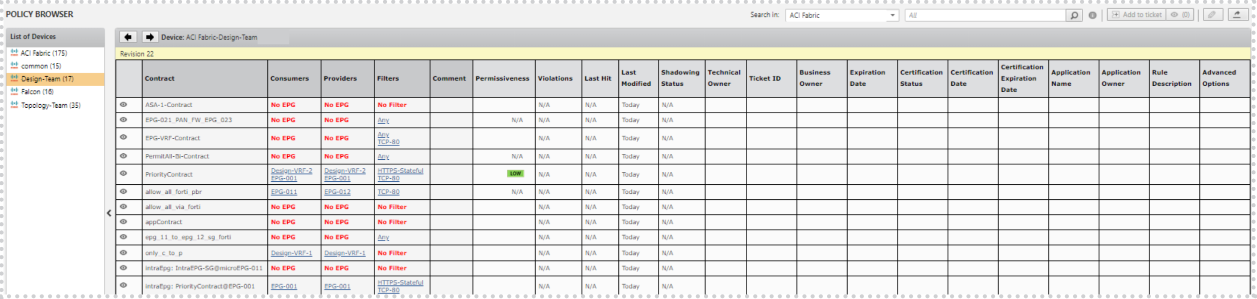


ACI Fabric (175)
common (15)
Design-Team (17)
Falcon (16)
Topology-Team (35)

Revision 5 -

Tenant	Type	Scope	Contract	Subject	Direction	Service Graph	Sources	Destinations	Filters	Action	Rule priority	Permissive...	Violations	Last Hit	Last Modi...	Shad... Status	Tech... Owner	Ticket ID	Busi... Owner	Expir... Date	Certi... Status	Certi... Date	Certi... Expir... Date	Appli... Name	Appli... Owner	Rule Desc...	Adva... Opti...
Falcon	Intra-VRF	VRF					Falcon1	Falcon1	Any (implicit)	Permit	DEFAULT (0)	HIGH	N/A	N/A	2 days ago	N/A											
Design-Team	Intra-EPG	Intra-EPG	PriorityContract	Deny-Any-Low	C->P	Forti_service_Graph	EPG-001	EPG-001	HTTPS-Stateful TCP-81	Deny	class-eq-filter (1)	N/A	N/A	N/A	2 days ago	N/A											
Design-Team	Standard	VRF	PriorityContract	Deny-Any-Low	C->P	Forti_service_Graph	Design-VRF-1	Design-VRF-1	TCP-81	Deny	class-eq-filter (1)	N/A	N/A	N/A	2 days ago	N/A											
Design-Team	Standard	VRF	PriorityContract	Deny-Any-Low	C->P	Forti_service_Graph	Design-VRF-2	Design-VRF-2	TCP-81	Deny	class-eq-filter (1)	N/A	N/A	N/A	2 days ago	N/A											
Topology-Team	Standard	VRF	vrf_to_vrf_contract	sub1	C->P		Topology-VRF-2	Topology-VRF-2	ssh_filter	Deny	class-eq-filter (1)	N/A	N/A	N/A	2 days ago	N/A											
Topology-Team	Standard	VRF	vrf_to_vrf_contract	sub1	P->C		Topology-VRF-2	Topology-VRF-2	ssh_filter_reversed	Deny	class-eq-filter (1)	N/A	N/A	N/A	2 days ago	N/A											
Design-Team	Intra-EPG	Intra-EPG	PriorityContract	Allow-TCP-80	C->P	Forti_service_Graph	EPG-001	EPG-001	HTTPS-Stateful TCP-80	Redirect	class-eq-filter (1)	N/A	N/A	N/A	2 days ago	N/A											
Falcon	Intra-EPG	Intra-EPG	Mixed-Marian	Subj_SSH_Both	C->P	Pan-OS	EPG-222	EPG-222	ICMP	Redirect	class-eq-filter (1)	N/A	N/A	N/A	2 days ago	N/A											
Falcon	Intra-EPG	Intra-EPG	Contact_test	Subj_bidi_rev_OFF	C->P		EPG-212 EPG-test	EPG-212 EPG-test	Filters_test	Permit	class-eq-filter (1)	LOW	N/A	N/A	2 days ago	N/A											
Falcon	Intra-EPG	Intra-EPG	Contact_test	Subj_bidi_rev_ON	C->P		EPG-212 EPG-test	EPG-212 EPG-test	Filters_test	Permit	class-eq-filter (1)	LOW	N/A	N/A	2 days ago	N/A											

At the tenant level, Policy Browser lists the contracts, consumers, providers, filters, and metadata for the tenant's access rules.



ACI Fabric (175)
common (15)
Design-Team (17)
Falcon (16)
Topology-Team (35)

Revision 22

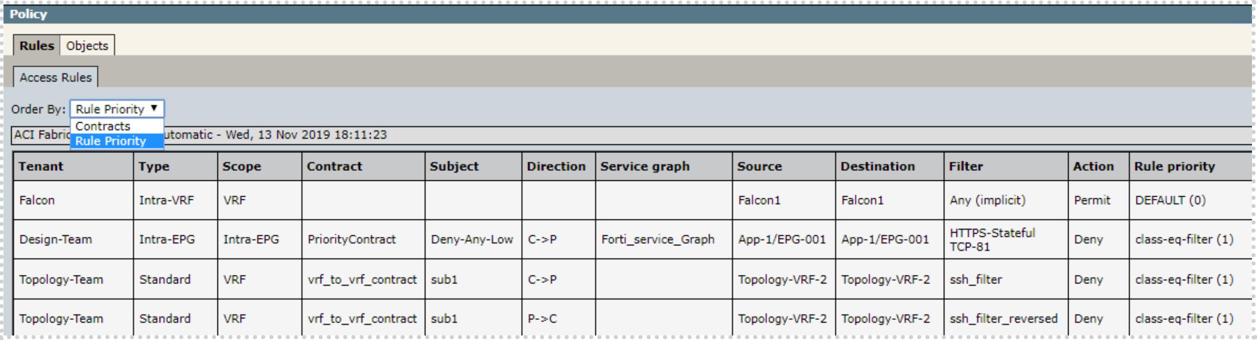
Contract	Consumers	Providers	Filters	Comment	Permissiveness	Violations	Last Hit	Last Modified	Shadowing Status	Technical Owner	Ticket ID	Business Owner	Expiration Date	Certification Status	Certification Date	Certification Expiration Date	Application Name	Application Owner	Rule Description	Advanced Options
ASA-1-Contract	No EPG	No EPG	No Filter			N/A	N/A	Today	N/A											
EPG-021_PAN_FW_EPG_023	No EPG	No EPG	Any		N/A	N/A	N/A	Today	N/A											
EPG-VRF-Contract	No EPG	No EPG	Any TCP-80			N/A	N/A	Today	N/A											
PermitAll-Bi-Contract	No EPG	No EPG	Any		N/A	N/A	N/A	Today	N/A											
PriorityContract	Design-VRF-2 EPG-001	Design-VRF-2 EPG-001	HTTPS-Stateful TCP-80		LOW	N/A	N/A	Today	N/A											
allow_all_forti_pbr	EPG-011	EPG-012	TCP-80		N/A	N/A	N/A	Today	N/A											
allow_all_via_forti	No EPG	No EPG	No Filter			N/A	N/A	Today	N/A											
appContract	No EPG	No EPG	No Filter			N/A	N/A	Today	N/A											
epg_11_to_epg_12_sg_forti	No EPG	No EPG	Any			N/A	N/A	Today	N/A											
only_c_to_p	Design-VRF-1	Design-VRF-1	No Filter			N/A	N/A	Today	N/A											
intraEpg: IntraEPG-SG@microEPG-011	No EPG	No EPG	No Filter			N/A	N/A	Today	N/A											
intraEpg: PriorityContract@EPG-001	EPG-001	EPG-001	HTTPS-Stateful TCP-80			N/A	N/A	Today	N/A											

Access Rules and ACI Revisions

At the parent device level, for each policy revision, the Access Rules table (**Compare Revisions > View Policy > Rules > Access Rules**) displays a list of the access rules that model the fabric, grouped or ordered by tenant, type, and scope.

The Access Rules in a TOS Classic policy present the source, destination, filters for protocol services, action, and the priority of the ACI zoning rule they emulate. Access rules that are generated from an ACI contract may also include the contract, subject, direction and related service graph information.

When the contracts in the Common tenant include the EPGs of other tenants, the Access Rules may include cross tenant rules generated from Standard and Taboo contracts that also model the traffic between those EPGs.



utomatic - Wed, 13 Nov 2019 18:11:23

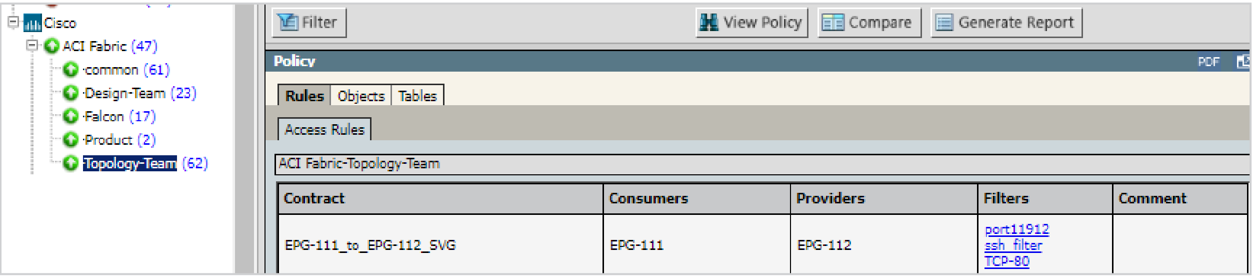
Tenant	Type	Scope	Contract	Subject	Direction	Service graph	Source	Destination	Filter	Action	Rule priority
Falcon	Intra-VRF	VRF					Falcon1	Falcon1	Any (implicit)	Permit	DEFAULT (0)
Design-Team	Intra-EPG	Intra-EPG	PriorityContract	Deny-Any-Low	C->P	Forti_service_Graph	App-1/EPG-001	App-1/EPG-001	HTTPS-Stateful TCP-81	Deny	class-eq-filter (1)
Topology-Team	Standard	VRF	vrf_to_vrf_contract	sub1	C->P		Topology-VRF-2	Topology-VRF-2	ssh_filter	Deny	class-eq-filter (1)
Topology-Team	Standard	VRF	vrf_to_vrf_contract	sub1	P->C		Topology-VRF-2	Topology-VRF-2	ssh_filter_reversed	Deny	class-eq-filter (1)

Column	Description
Tenant	Which tenant the access rule is associated with
Type	Defines the rule mechanism type: • Intra-EPG: Derived from the ACI Intra-EPG Isolation Enforcement setting at the EPG level. • Taboo: A single deny rule for traffic directed to the provider (**->P**), derived from contract, subject, and filter. Associated with the black-list zoning rule. • Standard: Rules derived from the combination of contract, subject, direction, and filter to enable, block, or redirect traffic between EPGs. • Preferred-Group: A rule that enables all EPGs in the specified VRF that belong to the preferred group to communicate with each other. Derived from the ACI Preferred-Group Member settings at the VRF and EPG levels • Intra-VRF: An intra-VRF allow rule is created when the VRF is configured to not enforce traffic control. An intra-VRF deny rule is created when the VRF is configured to enforce traffic contol. Derived from the VRF Policy Control Preference settings at the VRF level. • Cleanup: An added deny rule to deal with vendors not covered by an explicit deny rule
Scope	Defines which providers can communicate with which consumers: • Global: Any consumer EPG can connect to any provider EPG • Tenant: Any consumer EPG can connect to any provider EPG in the same tenant • VRF: Any consumer EPG can connect to any provider EPG within the same VRF • Application Profile: Any consumer EPG can connect to any provider EPG in the same Application Profile • Intra-EPG: Scope defined by Tufin. Any EPG may connect to itself
Contract	Contract from which the access rule is derived
Subject	Sub contracts within the contract
Direction	Rule traffic direction • Unidirectional ◦ consumer (C) to provider (P) **C->P** ◦ provider (P) to consumer (C) **P->C** • Bidirectional **C<->P**
Service graph	External firewall used as a filter for traffic redirection and access decisions
Source	Entity from which traffic originates
Destination	Entity to which traffic arrives
Filter	Set of services
Action	How to handle the traffic defined by the rule: • Permit • Deny • Redirect

Rule priority	Priority of the emulated ACI zoning rule

Viewing Tenant Access Rules

When you select the ACI tenant device and a revision, **View Policy > Rules > Access Rules** summarizes the contract, consumers, providers, and filters for each rule.

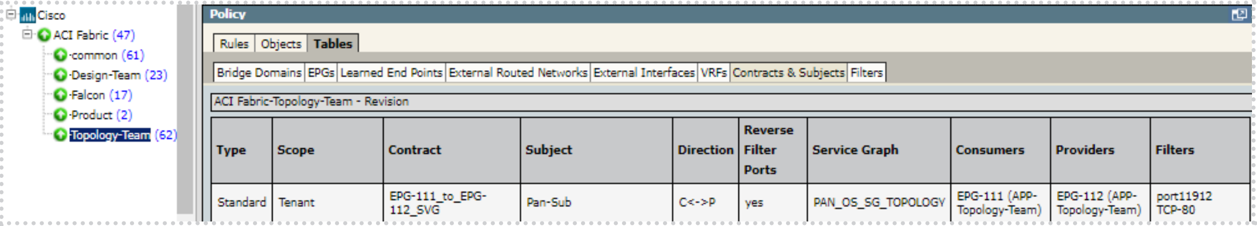


ACI Fabric-Topology-Team

Contract	Consumers	Providers	Filters	Comment
EPG-111_to_EPG-112_SVG	EPG-111	EPG-112	port11912 ssh_filter TCP-80	

Viewing the Tenant

When you select the ACI tenant device and a revision, **View Policy > Tables** presents tabs to explore the TOS Classic model of the tenant information.



ACI Fabric-Topology-Team - Revision

Type	Scope	Contract	Subject	Direction	Reverse Filter Ports	Service Graph	Consumers	Providers	Filters
Standard	Tenant	EPG-111_to_EPG-112_SVG	Pan-Sub	C<->P	yes	PAN_OS_SG_TOPOLOGY	EPG-111 (APP-Topology-Team)	EPG-112 (APP-Topology-Team)	port11912 TCP-80

Tufin provides added value by collecting information for each ACI tenant in a single location within the **Tables** tab, grouped by sub tabs:

Sub tab	Description
Bridge Domains	Presents the bridge domain details for the subnets and VRFs related to each bridge domain in the tenant. The table includes the following information: Name of the bridge domain, related VRFs and subnets, subnet type, and relevant segment
EPGs	Presents the application profile for each EPG in the tenant. The table includes the following information: EPG name and Class ID, related VRFs and bridge domains, Intra EPG Isolation status (enforced or unenforced), the Contract Master, Preferred Group Member action (include or exclude), and the related EPG Subnets
Learned End Points	Presents the end point details and related EPG information. The table includes the following information for the tenant: Application Profile, EPG name and Class ID, VRF, Bridge Domain, Contract Master, Preferred Group Member action (include or exclude), Intra EPG Isolation status (enforced or unenforced), and the EPG Subnets and End Points
External Routed Networks	Presents the information for the External Routed Networks. The table displays which VRFs, protocols and External Routed Domain are related to each external routed domain in the tenant
External Interfaces	Presents the information for External Interfaces. The table includes the External Network Name, the VRF information for the External Interfaces, as well as the Node, Interfaces. IP address, and the Designated Router and Backup Designated Router
VRFs	Presents the information for VRFs in the tenant, by VRF name. The table includes the relevant Segment and Class ID, Policy control status (enforced or unenforced), EPG collection for VRG (vzAny) , Preferred group status (enabled or disabled) and Preferred group members
Contracts & Subjects	For each tenant, presents the details for each subject and each direction in the contracts. The table includes the Contract Type and scope, and the Contract and Subject names, the Direction of the contract, whether

	Reverse Filter Ports are used (yes or no), the related Service Graph name, names of the Consumers and Providers, and Filters
Filters	Presents the filter details for the tenant. The table includes the Filter and Entry names, Ether type, IP protocol, whether Fragments only, whether the filter is Stateful, and the Source and Destination ports

At the tenant level:

- **View Policy > Tables** displays the same information presented in **Objects > Network Objects**
- **View Policy > Tables > Filters** includes the same information presented in **Objects > Services**

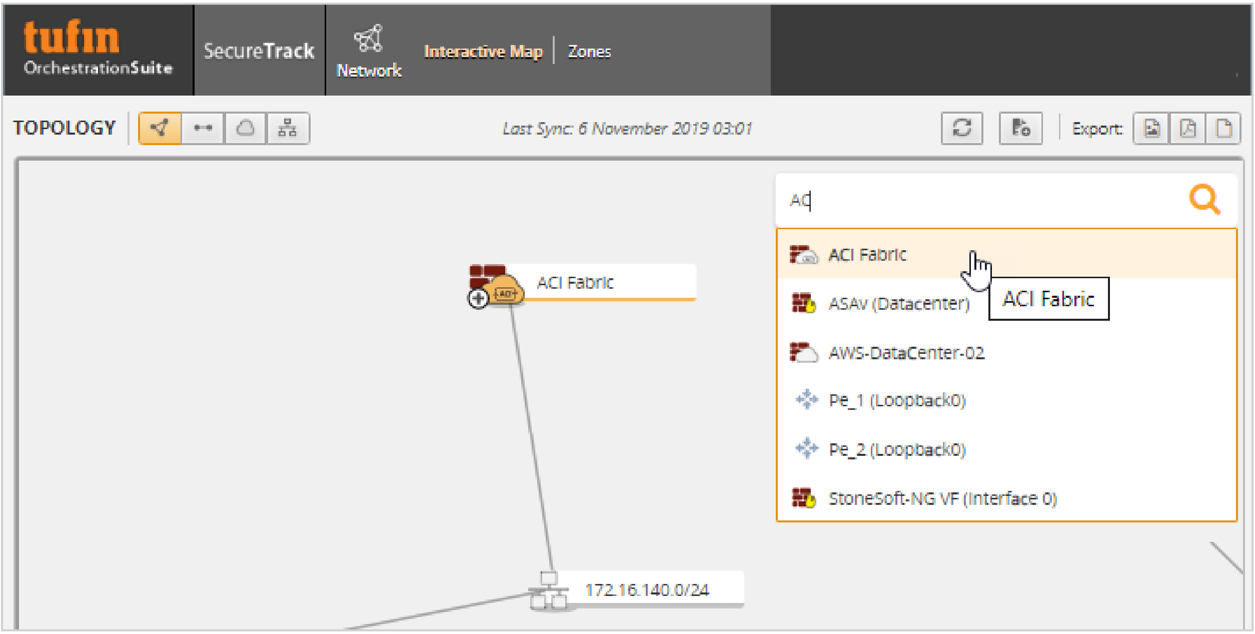
> **Tufin Tip:** At the parent device level, the most useful information is collected in **View Policy > Rules > Access Rules** and in **View Policy > Tables** at the tenant device level.

Viewing the ACI in the Interactive Map

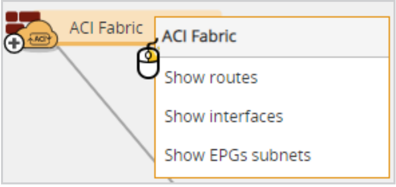
For Cisco ACI devices, Tufin supports path calculations in the Interactive Map with security simulations and with service graph calculations. You get to search for paths that cross the ACI fabric on the way from source to destination in Path Analysis. We show you the access rules from the Tufin model that enable, redirects, or denies the traffic that crosses the ACI.

You can search the Interactive Map for paths that simulate East/West and North/South connectivity both with and without redirection to Service Graph elements.

When you search for the ACI device in the Interactive Map, the ACI is presented as a single firewall in the Interactive Map and displays the aggregated information from the different tenants.



Right click and select an option to display lists of routes, interfaces, and the EPG subnets for the ACI:



- **Show routes** displays the network, interface name and gateway per route.
- **Show interfaces** displays the consumer or provider interface name, the IP, the bridge domain and interface type (either an external or service graph interface).

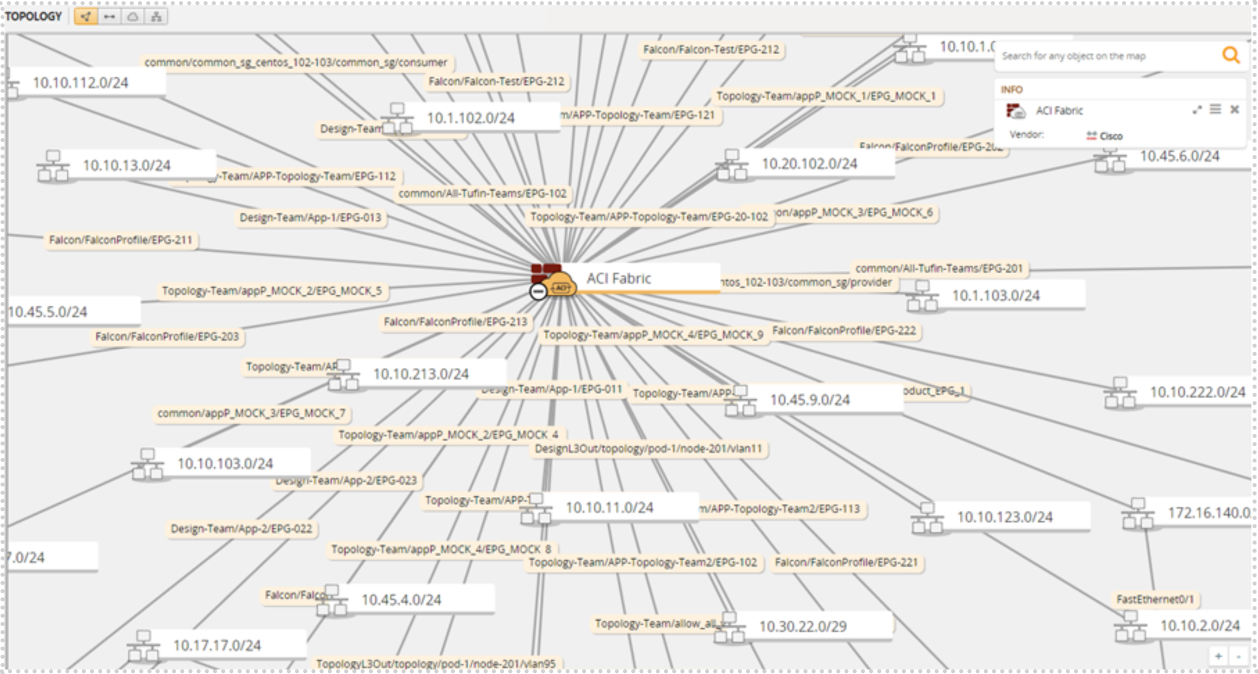
  A service graph interface name specifies the tenant, the contract name, the service graph template name, and whether the interface is serving as provider or consumer.

  For example, **common/common_sg_centos_192-103/common_sg/consumer**
- **Show EPGs subnets** displays the subnet name, IP, and bridge domain. Subnets are connected to the ACI by logical interfaces.

The Interactive Map displays a single interface per subnet, even if several EPGs are associated with this subnet. An EPG is associated with all subnets that are configured on the EPG's bridge domain.

Click ⊕ to expand the subnets:

- If a single EPG leads to a subnet, the EPG name appears in the Interactive Map
- If more than a single EPG leads to the same subnet, the names of the EPGs do not appear


TOPOLOGY
Search for any object on the map
INFO
ACI Fabric
Vendor:
Cisco
ACI Fabric
common/common_sg_centos_102-103/common_sg/consumer
10.10.112.0/24
Falcon/Falcon-Test/EPG-212
Falcon/Falcon-Test/EPG-212
10.10.1.0
Topology-Team/appP_MOCK_1/EPG_MOCK_1
Design-Team
10.1.102.0/24
n/APP-Topology-Team/EPG-121
10.10.13.0/24
-Team/APP-Topology-Team/EPG-112
common/All-Tufin-Teams/EPG-102
Falcon/FalconProfile/EPG-20
10.20.102.0/24
10.45.6.0/24
Design-Team/App-1/EPG-013
Topology-Team/APP-Topology-Team/EPG-20-102
on/appP_MOCK_3/EPG_MOCK_6
Falcon/FalconProfile/EPG-211
common/All-Tufin-Teams/EPG-201
ntos_102-103/common_sg/provider
10.1.103.0/24
Topology-Team/appP_MOCK_2/EPG_MOCK_5
10.45.5.0/24
Falcon/FalconProfile/EPG-213
Falcon/FalconProfile/EPG-203
Topology-Team/appP_MOCK_4/EPG_MOCK_9
Falcon/FalconProfile/EPG-222
Topology-Team/AP
10.10.213.0/24
Design-Team/App-1/EPG-011
Topology-Team/APP
10.45.9.0/24
oduct_EPG_1
10.10.222.0/24
common/appP_MOCK_3/EPG_MOCK_7
Topology-Team/appP_MOCK_2/EPG_MOCK_4
DesignL3Out/topology/pod-1/node-201/vlan11
10.10.103.0/24
Design-Team/App-2/EPG-023
Topology-Team/APP-1
10.10.11.0/24
n/APP-Topology-Team2/EPG-113
10.10.123.0/24
172.16.140.0
Design-Team/App-2/EPG-022
.0/24
Topology-Team/appP_MOCK_4/EPG_MOCK_8
Topology-Team/APP-Topology-Team2/EPG-102
Falcon/FalconProfile/EPG-221
Falcon/Falco
10.45.4.0/24
FastEthernet0/1
Topology-Team/allow_all
10.30.22.0/29
10.10.2.0/24
10.17.17.0/24
TopologyL3Out/topology/pod-1/node-201/vlan95

Using the ACI in Path Analysis

You can search for paths which simulate the traffic flow for east/west and north/south connectivity and the traffic that redirects to Service Graph.

Search Paths can calculate the paths for traffic that the ACI redirects to firewalls when the ACI is configured as follows:

- The firewalls are configured in the ACI as unmanaged service graph elements.
- Service graph templates were created for the firewalls.
- Bridge domains were created for the various firewall interfaces.
- PBR entries containing the interface IP and MAC address were created for firewall interfaces that are connected to the ACI (optional).
- Device selection policies were created, containing:
  - Contract name
  - Service graph template name
  - Consumer and Provider interfaces include:
    - IP addresses
    - Bridge domain
    - PBR entry (optional)

External EPGs in the Source or Destination Field

You can add an external EPG to the Source/Destination fields (North/South).

The external EPG is displayed as fully qualified.

Autocomplete works with external EPG IPs and External EPG names.

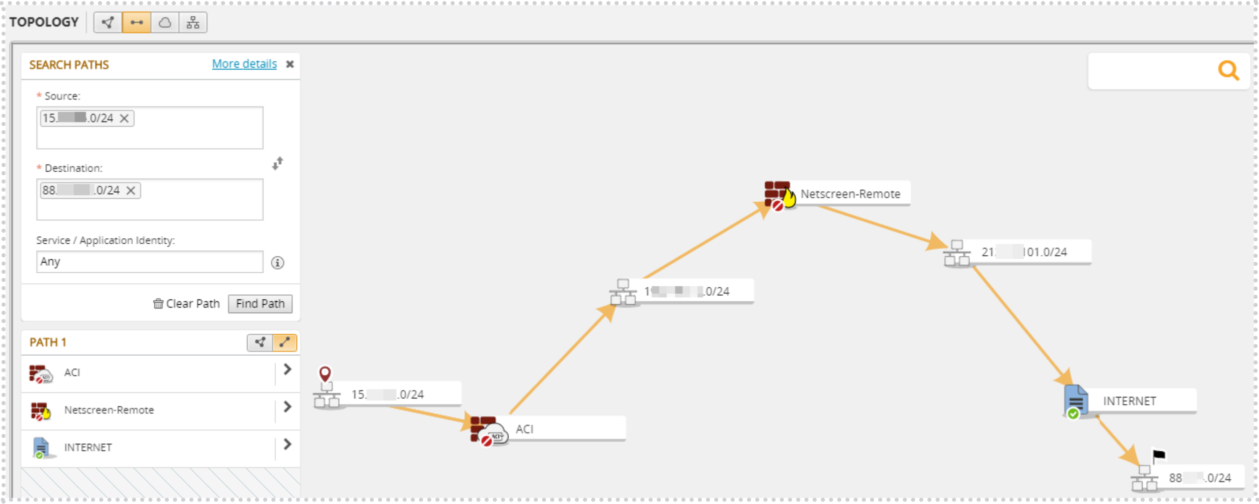
IP to EPG (East/West) in the Source or Destination Field

You can add an IP or an EPG to the Source/Destination fields.

EPGs are displayed as fully qualified.

Autocomplete suggests the most exact results for an EPG that contain the requested IP address:

- Learned end-point autocomplete is applied only on full IP match
- Autocomplete task starts only after the third octet of the IP



TOPOLOGY

SEARCH PATHS More details

* Source: 15.[redacted].0/24

* Destination: 88.[redacted].0/24

Service / Application Identity: Any

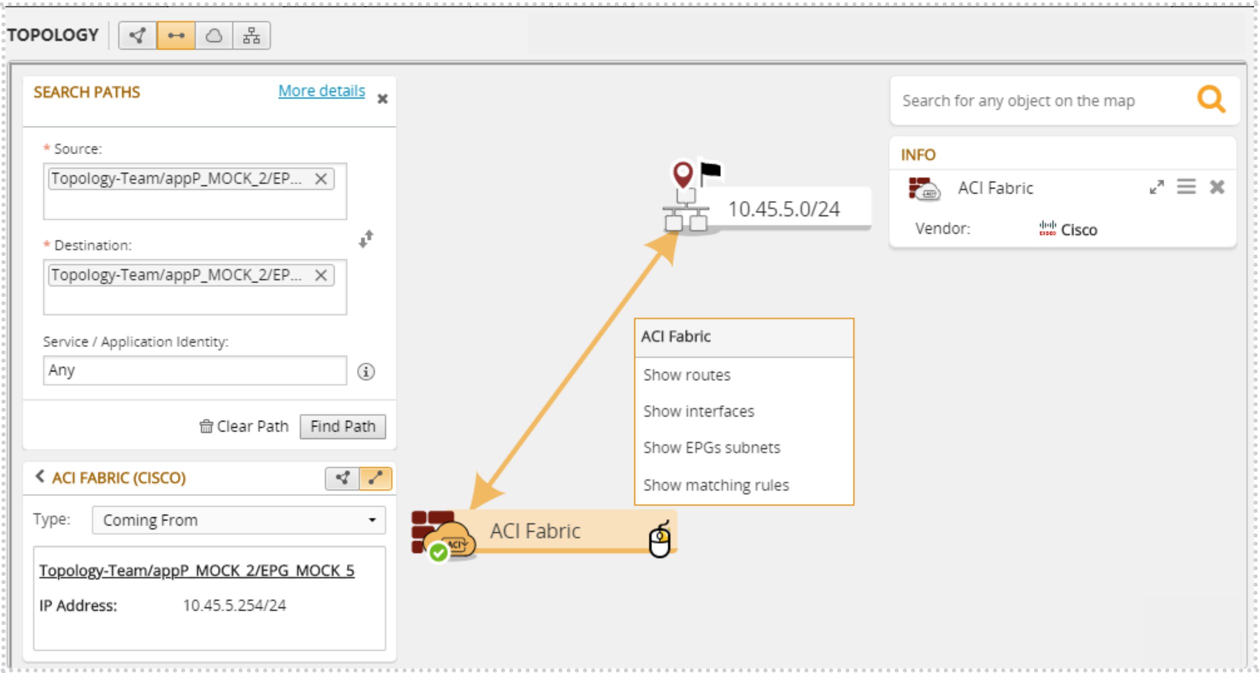
Clear Path Find Path

PATH 1

ACI

Netscreen-Remote

INTERNET



TOPOLOGY

SEARCH PATHS More details

* Source: Topology-Team/appP_MOCK_2/EP...

* Destination: Topology-Team/appP_MOCK_2/EP...

Service / Application Identity: Any

Clear Path Find Path

ACI FABRIC (CISCO)

Type: Coming From

Topology-Team/appP_MOCK_2/EPG_MOCK_5

IP Address: 10.45.5.254/24

Search for any object on the map

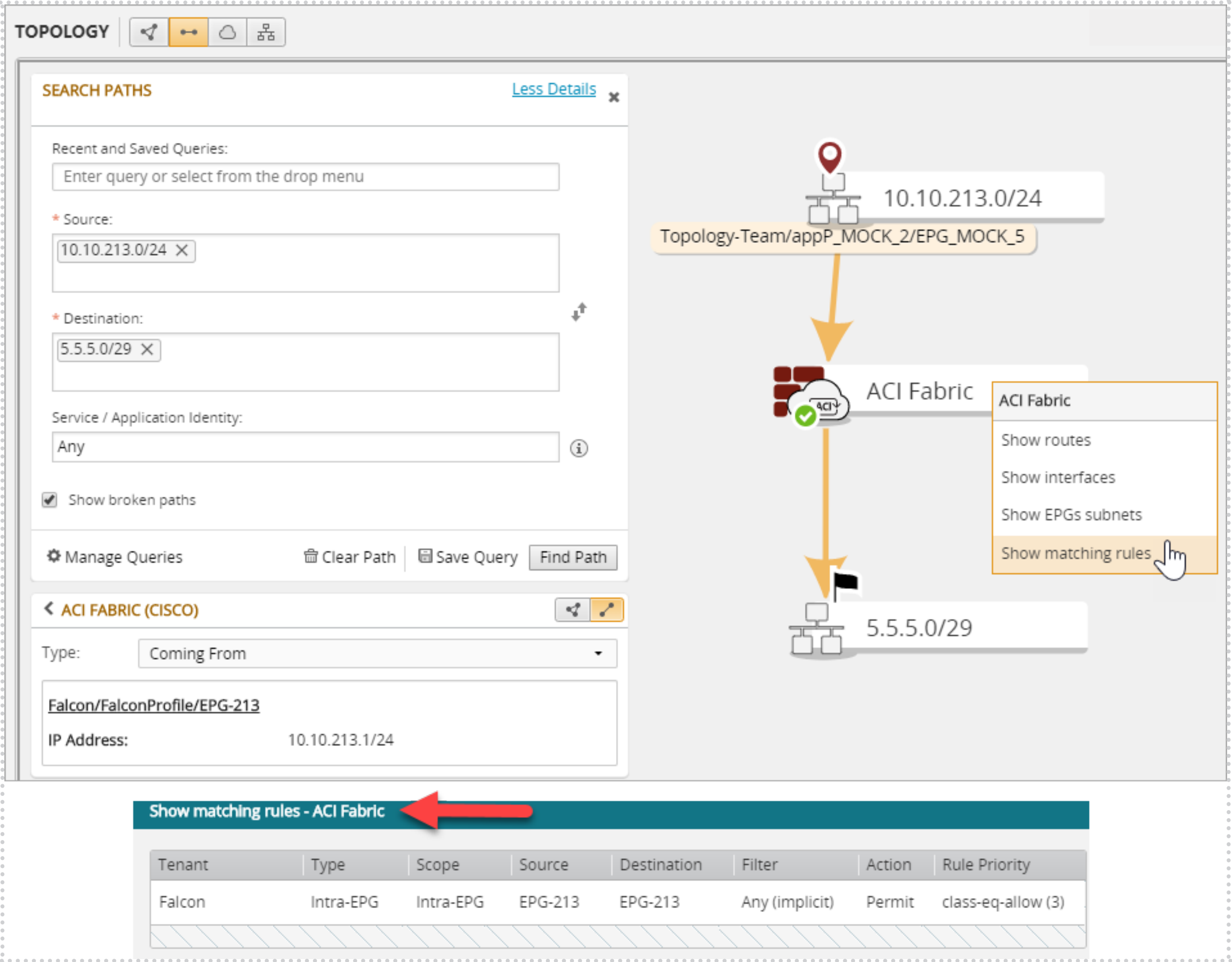
INFO

ACI Fabric

Vendor: Cisco

Show Matching Rules

Path calculation between EPGs, matched by an intra-EPG traffic rule that permits traffic.



Recent and Saved Queries: Enter query or select from the drop menu

* Source: 10.10.213.0/24

* Destination: 5.5.5.0/29

Service / Application Identity: Any

☑ Show broken paths

Type: Coming From

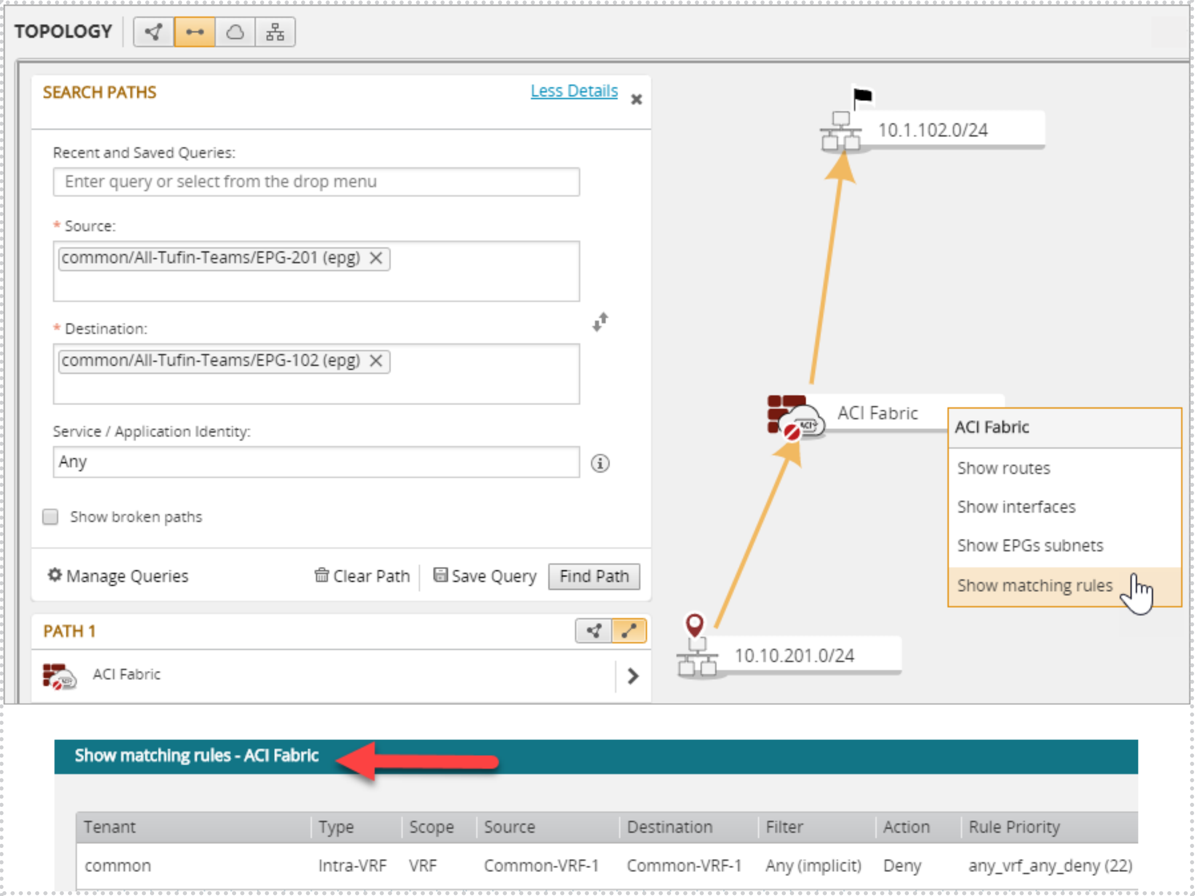
Falcon/FalconProfile/EPG-213

IP Address: 10.10.213.1/24

Show matching rules - ACI Fabric

Tenant	Type	Scope	Source	Destination	Filter	Action	Rule Priority
Falcon	Intra-EPG	Intra-EPG	EPG-213	EPG-213	Any (implicit)	Permit	class-eq-allow (3)

Path calculation between EPGs matched by an intra-VRF rule that denies traffic.



Recent and Saved Queries: Enter query or select from the drop menu

* Source: common/All-Tufin-Teams/EPG-201 (epg)

* Destination: common/All-Tufin-Teams/EPG-102 (epg)

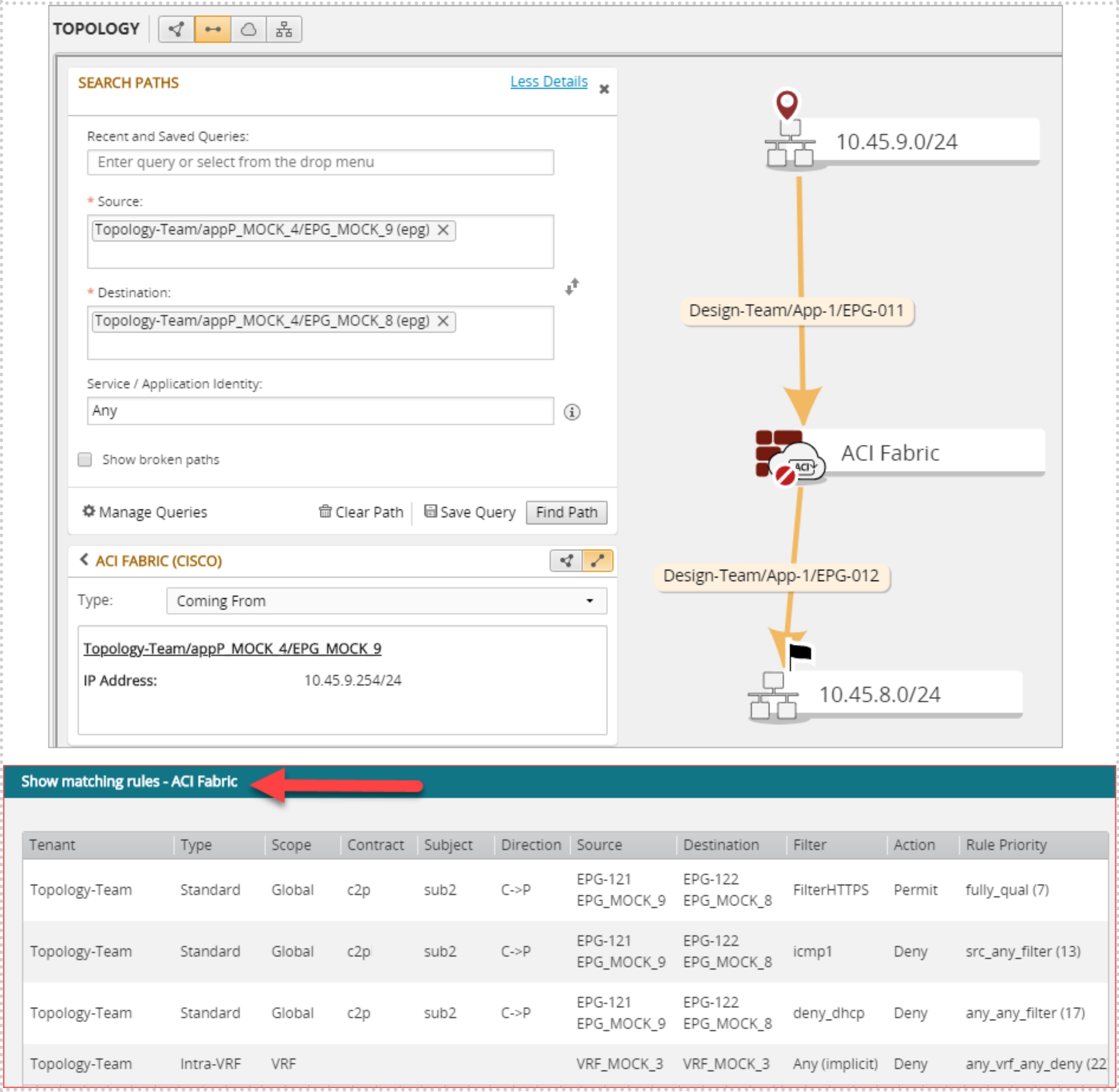
Service / Application Identity: Any

□ Show broken paths

Show matching rules - ACI Fabric

Tenant	Type	Scope	Source	Destination	Filter	Action	Rule Priority
common	Intra-VRF	VRF	Common-VRF-1	Common-VRF-1	Any (implicit)	Deny	any_vrf_any_deny (22)

Path calculation between EPGs matched by rules from a standard contract.



TOPOLOGY

SEARCH PATHS

Less Details

Recent and Saved Queries: Enter query or select from the drop menu

* Source: Topology-Team/appP_MOCK_4/EPG_MOCK_9 (epg)

* Destination: Topology-Team/appP_MOCK_4/EPG_MOCK_8 (epg)

Service / Application Identity: Any

□ Show broken paths

Manage Queries | Clear Path | Save Query | Find Path

ACI FABRIC (CISCO)

Type: Coming From

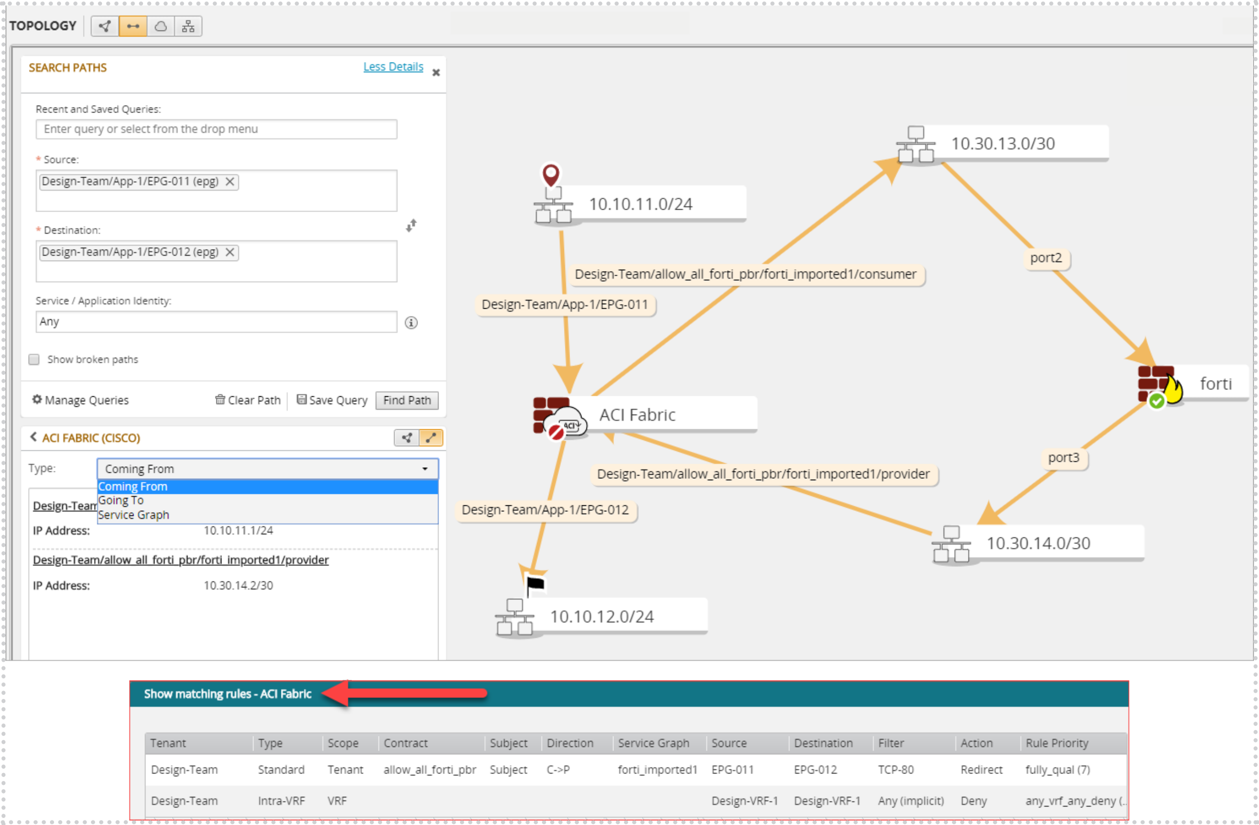
Topology-Team/appP_MOCK_4/EPG_MOCK_9

IP Address: 10.45.9.254/24

Show matching rules - ACI Fabric

Tenant	Type	Scope	Contract	Subject	Direction	Source	Destination	Filter	Action	Rule Priority
Topology-Team	Standard	Global	c2p	sub2	C->P	EPG-121 EPG_MOCK_9	EPG-122 EPG_MOCK_8	FilterHTTPS	Permit	fully_qual (7)
Topology-Team	Standard	Global	c2p	sub2	C->P	EPG-121 EPG_MOCK_9	EPG-122 EPG_MOCK_8	icmp1	Deny	src_any_filter (13)
Topology-Team	Standard	Global	c2p	sub2	C->P	EPG-121 EPG_MOCK_9	EPG-122 EPG_MOCK_8	deny_dhcp	Deny	any_any_filter (17)
Topology-Team	Intra-VRF	VRF				VRF_MOCK_3	VRF_MOCK_3	Any (implicit)	Deny	any_vrf_any_deny (22

Path calculation between EPGs with Service Graph - two arms


TOPOLOGY
10.10.11.0/24
10.30.13.0/30
Design-Team/allow_all_forti_pbr/forti_imported1/consumer
Design-Team/App-1/EPG-011
port2
forti
ACI Fabric
ACI
port3
Design-Team/allow_all_forti_pbr/forti_imported1/provider
Design-Team/App-1/EPG-012
10.30.14.0/30
10.10.12.0/24

SEARCH PATHS Less Details ✖

Recent and Saved Queries: Enter query or select from the drop menu

* Source: Design-Team/App-1/EPG-011 (epg) ✕

* Destination: Design-Team/App-1/EPG-012 (epg) ✕

Service / Application Identity: Any

□ Show broken paths

Manage Queries | Clear Path | Save Query | Find Path

ACI FABRIC (CISCO)

Type: Coming From
- Coming From
- Going To
- Service Graph

Design-Team

IP Address: 10.10.11.1/24

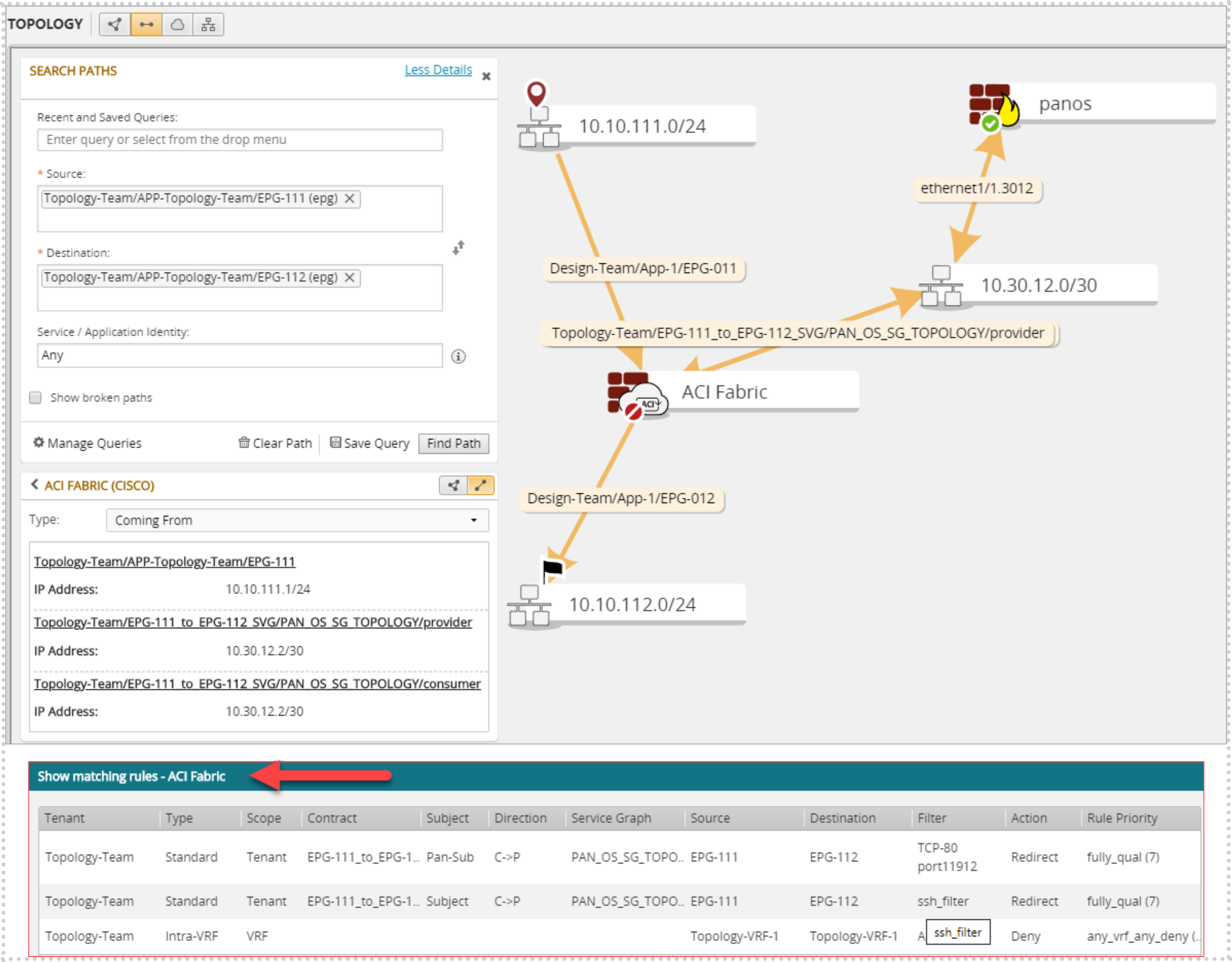
Design-Team/allow_all_forti_pbr/forti_imported1/provider

IP Address: 10.30.14.2/30

Show matching rules - ACI Fabric

Tenant	Type	Scope	Contract	Subject	Direction	Service Graph	Source	Destination	Filter	Action	Rule Priority
Design-Team	Standard	Tenant	allow_all_forti_pbr	Subject	C->P	forti_imported1	EPG-011	EPG-012	TCP-80	Redirect	fully_qual (7)
Design-Team	Intra-VRF	VRF					Design-VRF-1	Design-VRF-1	Any (implicit)	Deny	any_vrf_any_deny (..

Path between EPGs with Service Graph - single arm


TOPOLOGY
10.10.111.0/24
panos
ethernet1/1.3012
Design-Team/App-1/EPG-011
10.30.12.0/30
Topology-Team/EPG-111_to_EPG-112_SVG/PAN_OS_SG_TOPOLOGY/provider
ACI Fabric
ACI
Design-Team/App-1/EPG-012
10.10.112.0/24

SEARCH PATHS Less Details ✖

Recent and Saved Queries: Enter query or select from the drop menu

* Source: Topology-Team/APP-Topology-Team/EPG-111 (epg) ✕

* Destination: Topology-Team/APP-Topology-Team/EPG-112 (epg) ✕

Service / Application Identity: Any

□ Show broken paths

Manage Queries | Clear Path | Save Query | Find Path

ACI FABRIC (CISCO)

Type: Coming From

Topology-Team/APP-Topology-Team/EPG-111

IP Address: 10.10.111.1/24

Topology-Team/EPG-111_to_EPG-112_SVG/PAN_OS_SG_TOPOLOGY/provider

IP Address: 10.30.12.2/30

Topology-Team/EPG-111_to_EPG-112_SVG/PAN_OS_SG_TOPOLOGY/consumer

IP Address: 10.30.12.2/30

Show matching rules - ACI Fabric

Tenant	Type	Scope	Contract	Subject	Direction	Service Graph	Source	Destination	Filter	Action	Rule Priority
Topology-Team	Standard	Tenant	EPG-111_to_EPG-1..	Pan-Sub	C->P	PAN_OS_SG_TOPO..	EPG-111	EPG-112	TCP-80 port11912	Redirect	fully_qual (7)
Topology-Team	Standard	Tenant	EPG-111_to_EPG-1..	Subject	C->P	PAN_OS_SG_TOPO..	EPG-111	EPG-112	ssh_filter	Redirect	fully_qual (7)
Topology-Team	Intra-VRF	VRF					Topology-VRF-1	Topology-VRF-1	A ssh_filter	Deny	any_vrf_any_deny (..

How Do I Get Here?

To view revisions, in TOS Classic, go to **Compare** > **Compare Revisions**

To view the interactive map:

In TOS Classic, click **Network** > **Interactive Map**.

Adding F5 BIG-IP Devices

TOS Classic monitors F5 BIG-IP devices for policy revision changes. You can add these devices as TOP plugins for change management of textual revisions, but you can add F5 BIG-IP Local Traffic Manager (LTM) devices without the plugin to see the graphical display of revisions and to include the devices in Topology calculations. To help you organize the information for your devices, you can use the device information worksheet.

To see which TOS features are supported for your device, review the feature support table.

Prerequisites

TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

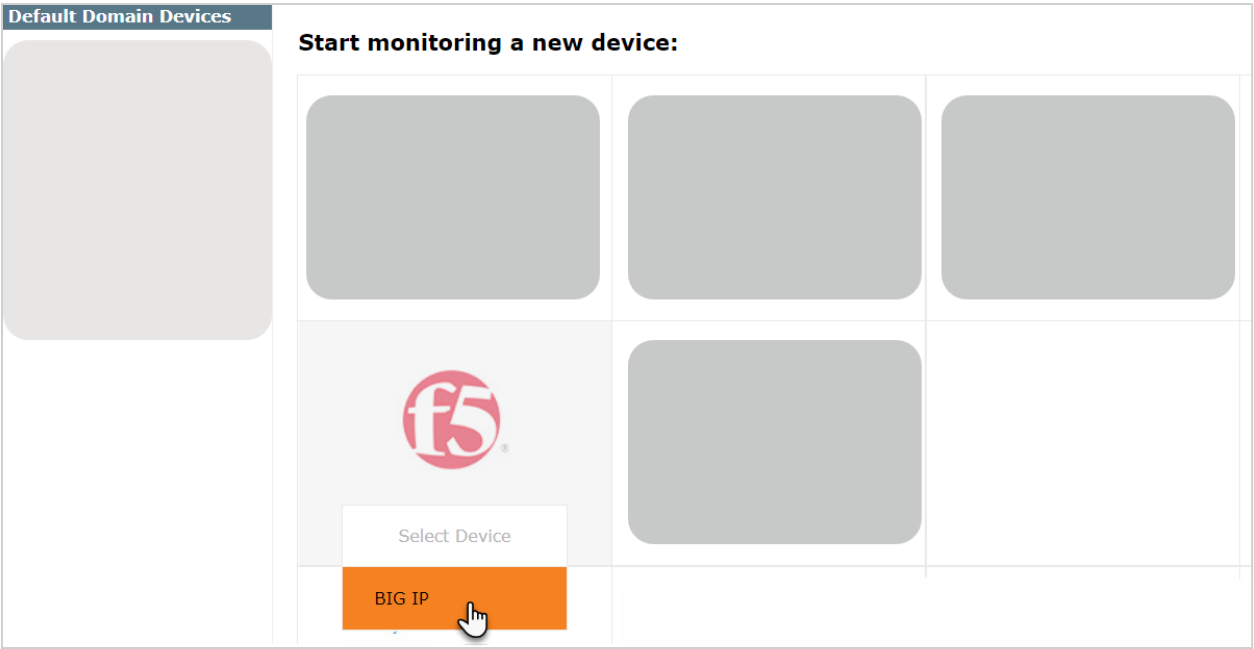
Before you begin, make sure that you have an F5 user that has a policy that has all the permissions you require for the TOS features you will be using. The user must have Terminal Access set to `tmsh`. If the user is not logged into TMSH directly, run the command `tmsh` before running the commands below.

Feature	Permissions
Visibility and Change Tracking	list auth partition list ltm node list ltm node recursive list ltm pool list ltm pool recursive list ltm snat-translation recursive list ltm snatpool recursive list ltm virtual recursive list net route-domain partition id strict vlans list net route list net self show running-config show running-config recursive show sys clock show sys version show running-config sys global-settings
Dynamic Topology	list auth partition list ltm node list ltm pool list net route-domain partition id strict vlans list net self show net route static dynamic field-fmt

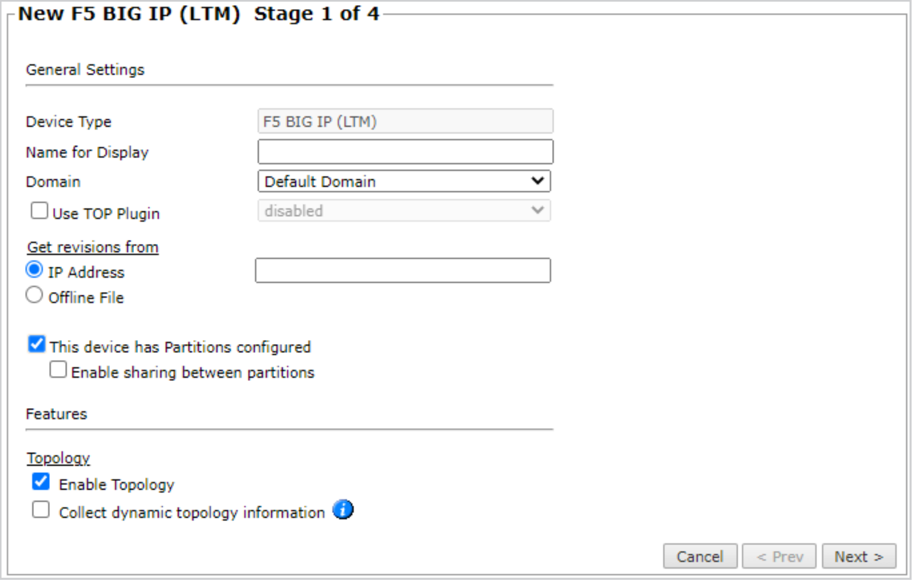
Monitor a F5 BIG-IP Device

To configure TOS Classic to monitor the policy revisions of a F5 BIG-IP device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New F5 BIG IP (LTM) Stage 1 of 4

General Settings

Device Type	F5 BIG IP (LTM)
Name for Display	
Domain	Default Domain
□ Use TOP Plugin	disabled

Get revisions from

● IP Address
○ Offline File

☑ This device has Partitions configured
□ Enable sharing between partitions

Features

Topology

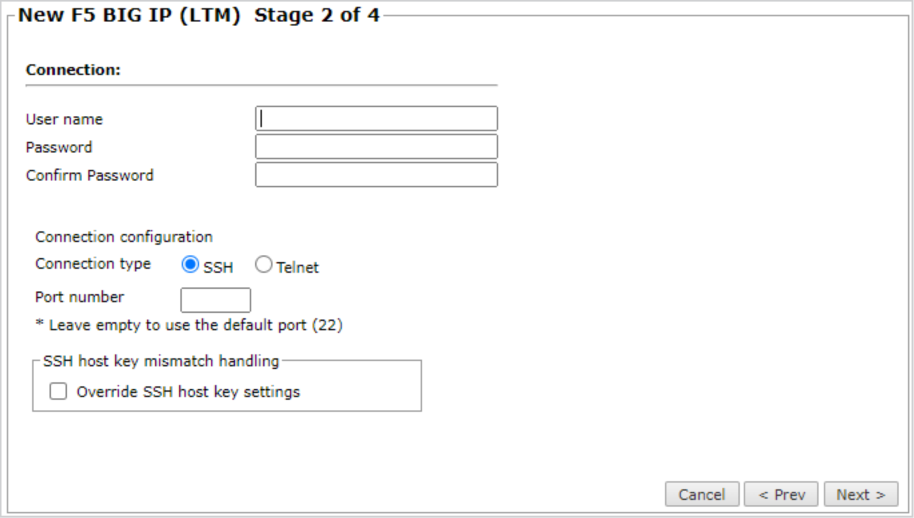
☑ Enable Topology
□ Collect dynamic topology information

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Use TOP plugin**: To get expanded support for a F5 BIG-IP LTM device, do not select this option. To get basic support of any F5 BIG-IP device, select this option to add the device with the TOP plugin.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **This device has Partitions configured**: If your device has administrative partitions, select this option so that you can import the partitions to the device monitoring after you complete the device monitoring wizard.
  - **Enable sharing between partitions**: Always select this option when partitions share objects from the Common partition, unless you are managing partitions on different MSSP domains.
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)

- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- If the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), also select **Collect dynamic topology information**.

  Topology is supported only for devices not added with the TOP plugin.

4. Click **Next**.
5. Configure the TOS Classic connection to the F5 BIG-IP device, according to the parameters required by the device:



New F5 BIG IP (LTM) Stage 2 of 4

Connection:

User name
Password
Confirm Password

Connection configuration

Connection type ● SSH ○ Telnet

Port number

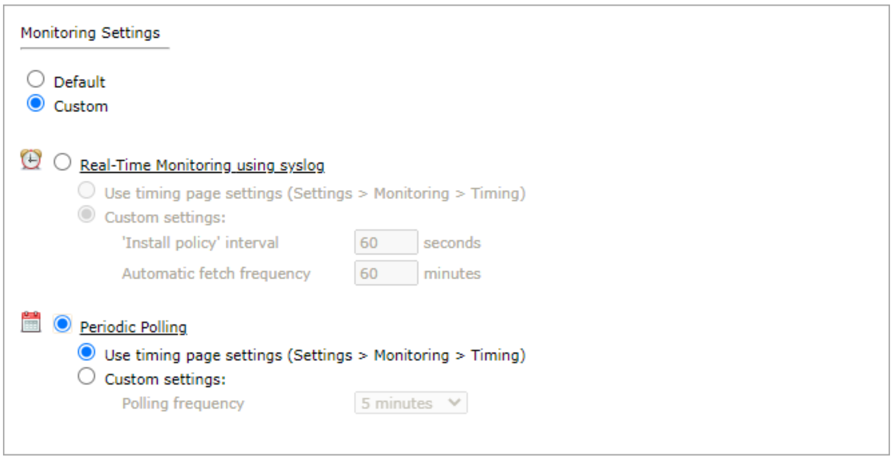
* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

- Enter the authentication details needed to connect to the F5 BIG-IP device. The user must have permissions for the commands listed in the prerequisites above.
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
  The device must be configured to use SSH version 2.

6. Click **Next**.
7. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog

○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling

● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

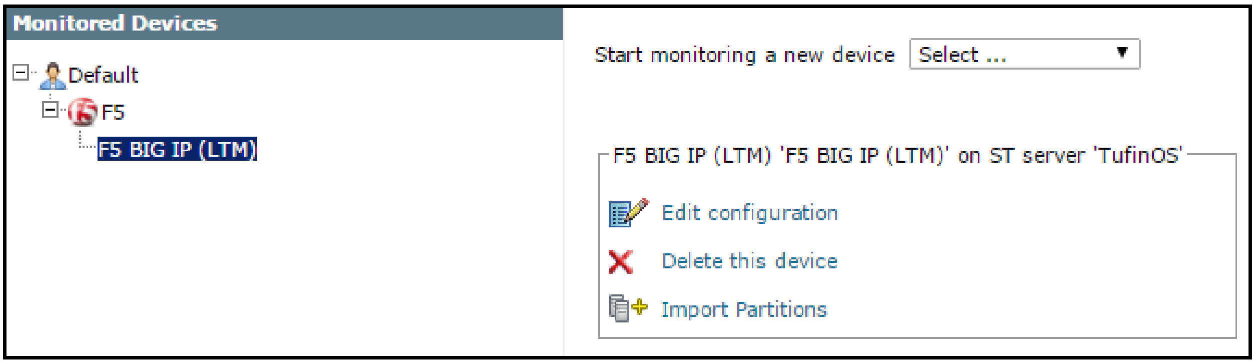
8. Click **Next**.
9. **Save** the configuration.

The F5 BIG-IP device now appears in the **Monitored Devices** tree.

10. If the device has administrative partitions, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the partitions:

    a. In the **Monitored Devices** tree, select the device.

    b. Click **Import partitions**:



    c. Select all the partitions to be added.

    d. Click **Save**.

After you import an F5 device with partitions, the parent device receives a single empty revision. You can safely ignore this revision.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Forcepoint Devices

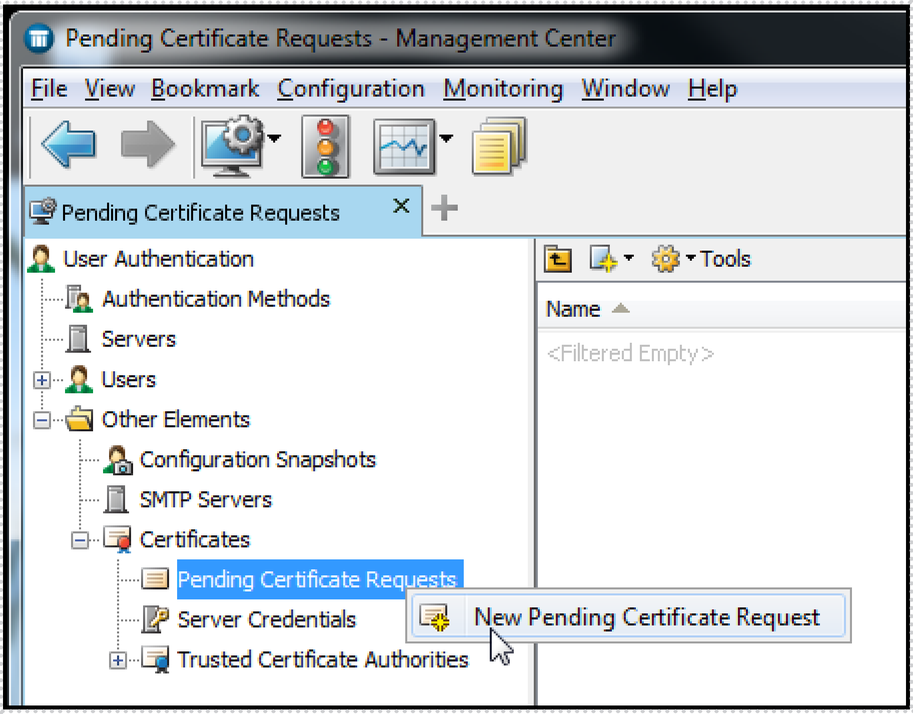
Adding Forcepoint Stonesoft Management Center (SMC) Devices

TOS Classic monitors Forcepoint devices for policy revision changes. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Before you add a Forcepoint Stonesoft Management Center (SMC) device to TOS Classic, you must prepare the SMC with a certificate for the SMC API. The firewalls must be configured under the Share Domain.

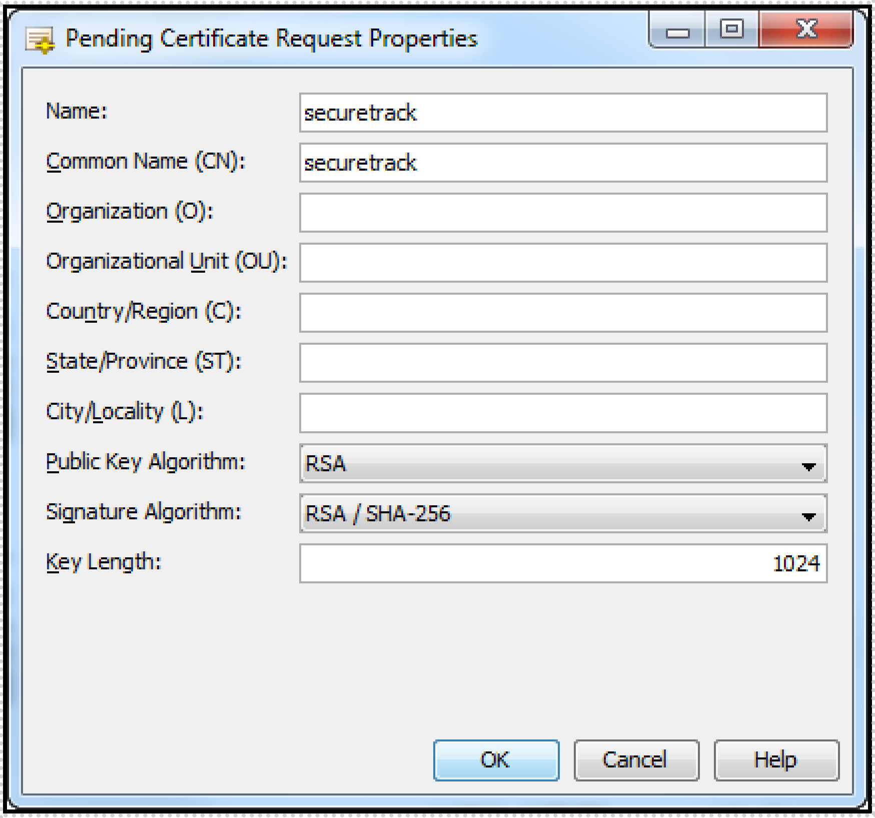
To prepare the Forcepoint Stonesoft Management Center (SMC)

1. Log in to the device interface.
2. Go to: **Configuration** > **User Authentication**
3. Navigate to **Administration** > **Certificates** > **TLS Credentials**.


Pending Certificate Requests - Management Center
File View Bookmark Configuration Monitoring Window Help
Pending Certificate Requests
User Authentication
Authentication Methods
Servers
Users
Other Elements
Configuration Snapshots
SMTP Servers
Certificates
Pending Certificate Requests
Server Credentials
Trusted Certificate Authorities
Tools
Name
<Filtered Empty>
New Pending Certificate Request

4. In the top right-hand corner, select **New**.

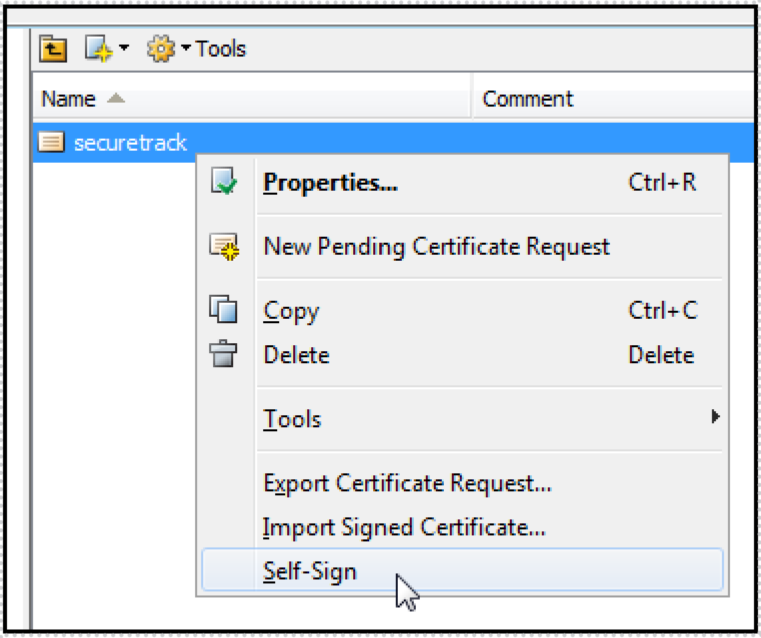
5. Enter `TOS Classic` as the name and common name of the request, and click **Next**.



Pending Certificate Request Properties

Name:	securetrack
Common Name (CN):	securetrack
Organization (O):	
Organizational Unit (OU):	
Country/Region (C):	
State/Province (ST):	
City/Locality (L):	
Public Key Algorithm:	RSA
Signature Algorithm:	RSA / SHA-256
Key Length:	1024

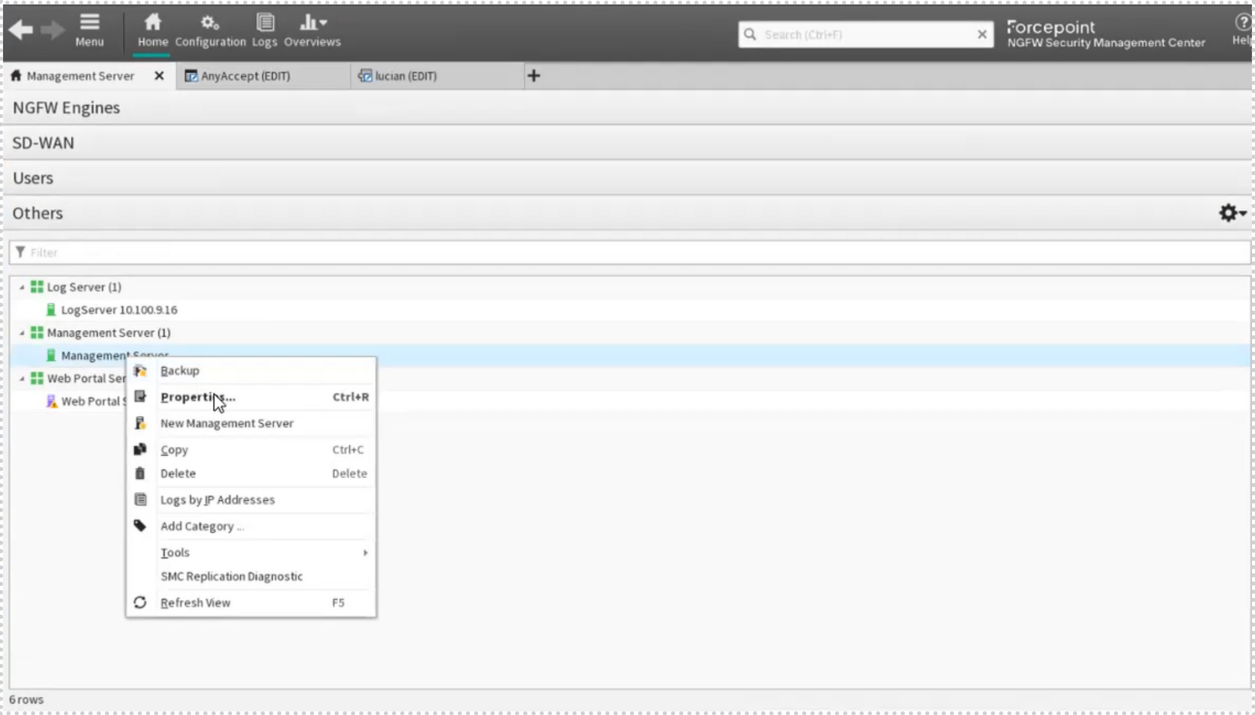
6. Select **Self-Sign**.


Tools
Name
Comment
securetrack
Properties... Ctrl+R
New Pending Certificate Request
Copy Ctrl+C
Delete Delete
Tools
Export Certificate Request...
Import Signed Certificate...
Self-Sign

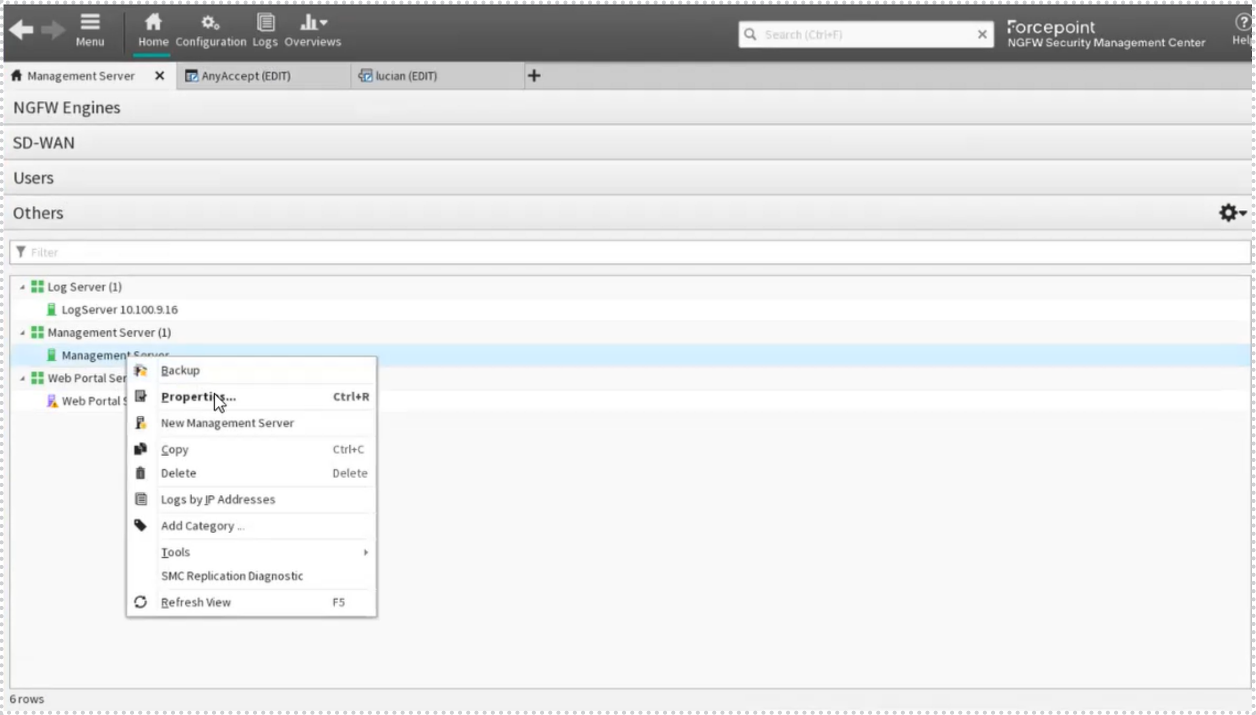
7. Select **Finish**.

8. Go to: **Home** .

9. From the **Others** list, right-click on **Management Server** and select **Properties**.



10. In the **SMC API** tab of **Management Server -Properties**choose the certificate that you just created. Click **Select**.



11. Click **OK** to close the Management Server properties.
12. Go to: **Configuration** > **Administration** > **Access Rights** > **API Clients**
13. Right-click on **API Clients** and select **New API Client**.
14. In the **General** tab, enter the name `securetrack_api`, copy the authentication key, and click **OK**.

    Copy the key to a temporary location because you cannot get the same key again from the API client settings.

    If the key is lost before you enter it into SecureTrack, you must generate a new key.
15. In the **Permissions** tab, select **Unrestricted Permissions** and select the **Superuser** role.
16. Click **OK**.

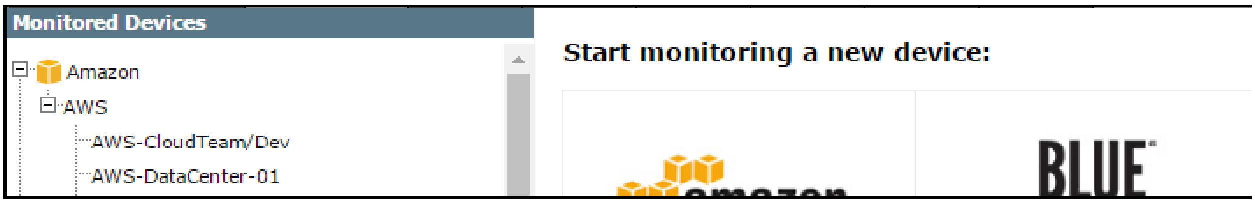
You can now add the Forcepoint device to SecureTrack.

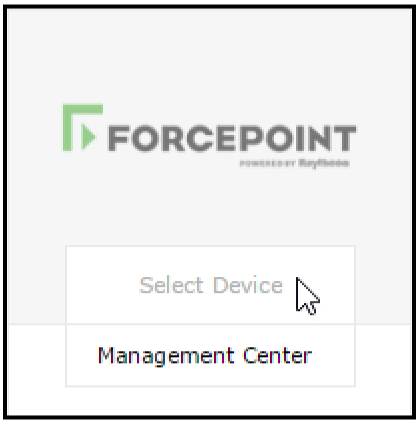
SecureTrack and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Monitor a Forcepoint Device

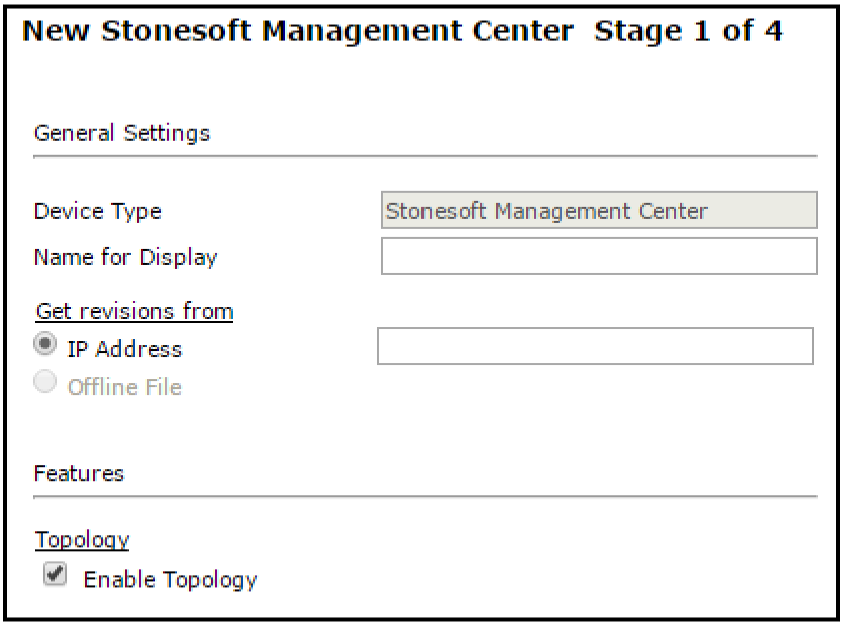
To configure SecureTrack to monitor the policy revisions of a Forcepoint device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:





3. Configure the device settings:



New Stonesoft Management Center Stage 1 of 4

General Settings

Device Type: Stonesoft Management Center

Name for Display:

Get revisions from

● IP Address

○ Offline File

Features

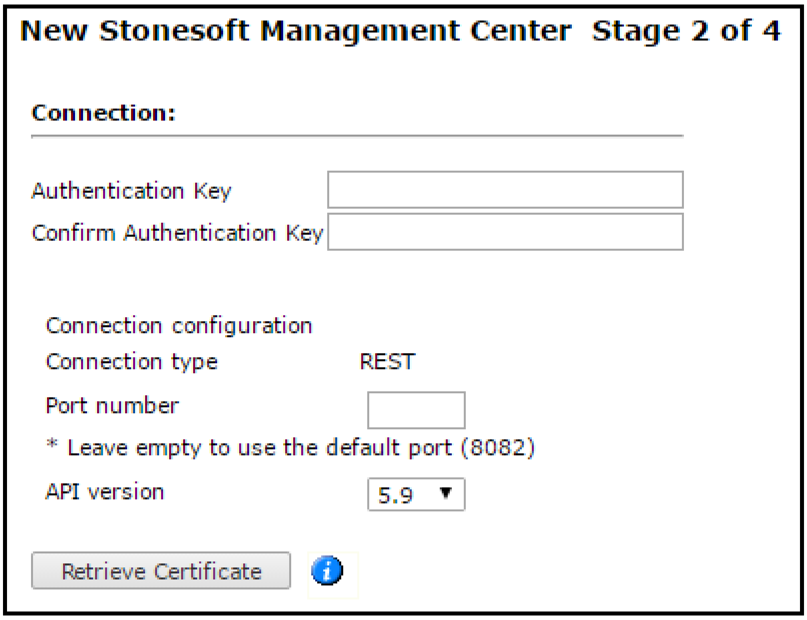
Topology

☑ Enable Topology

- **Name for Display**
- Get revisions from **IP Address**
- **ST server**: In a distributed deployment, select which SecureTrack server monitors this device (Not shown in image)

Click **Next**.

4. Configure the SecureTrack connection to the Forcepoint device, according to the parameters required by the device:



New Stonesoft Management Center Stage 2 of 4

Connection:

Authentication Key

Confirm Authentication Key

Connection configuration

Connection type REST

Port number

* Leave empty to use the default port (8082)

API version 5.9

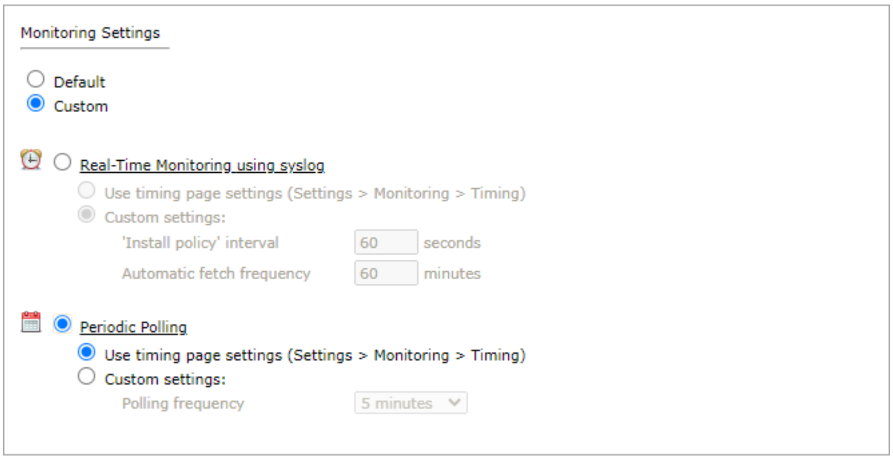
- Enter the authentication details needed to connect to the Forcepoint device.
- TOS Classic connects to Forcepoint devices with the REST protocol. To use default settings (recommended in most cases), leave the **Port number** blank.
- Specify the version of that is installed on the Forcepoint device. To use default settings (recommended in most cases), leave the **Port number** blank.
- Click **Retrieve Certificate** to setup encrypted communication between TOS Classic and the Forcepoint device.

  The certificate appears, and the following message is displayed:

  The certificate was retrieved successfully.

Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**.

6. **Save** the configuration.

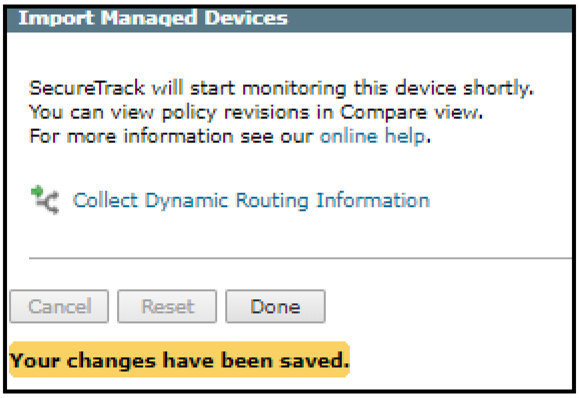
   The Forcepoint device now appears in the **Monitored Devices** tree.

To customize the device object that represents the Internet, see Define Internet Object.

To import devices or domains managed by the Forcepoint device into TOS Classic

1. Make sure you receive the first Forcepoint policy revision.
2. Select the Forcepoint device from the device tree.
3. Click **Import Managed Devices** or **Import Domains and Managed Devices**.
4. From the list of devices managed by the Forcepoint device, select the devices to import and click **Import**.
5. Do one of the following:
   - Click **Reset** to update the list of managed devices.
   - Click **Done** to return to the device tree.

     The managed devices appear under the Forcepoint device in the device tree.
   - If available, click to **Collect Dynamic Routing Information** for the managed devices.



Import Managed Devices

SecureTrack will start monitoring this device shortly.
You can view policy revisions in Compare view.
For more information see our online help.

Collect Dynamic Routing Information

Your changes have been saved.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Forcepoint Firewall Enterprise Devices

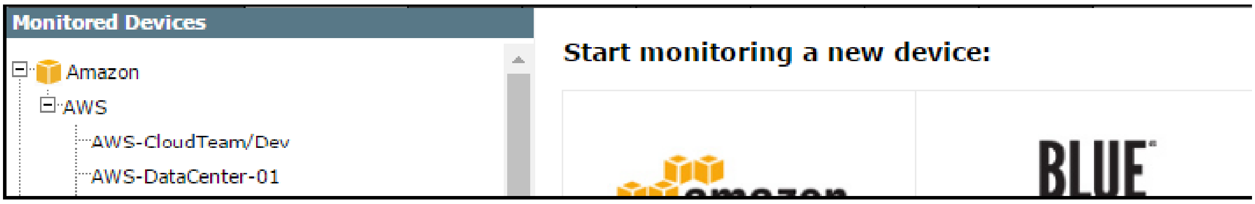
TOS Classic monitors Forcepoint Firewall Enterprise devices for policy revision changes. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

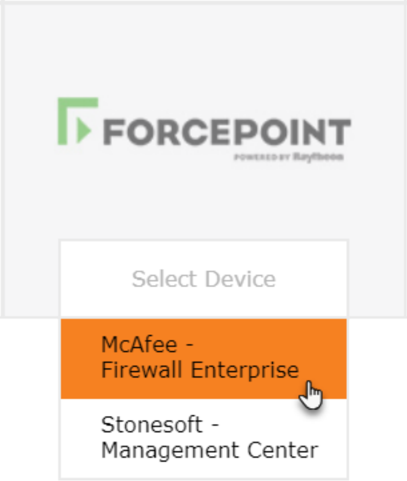
> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Monitor a Forcepoint Device

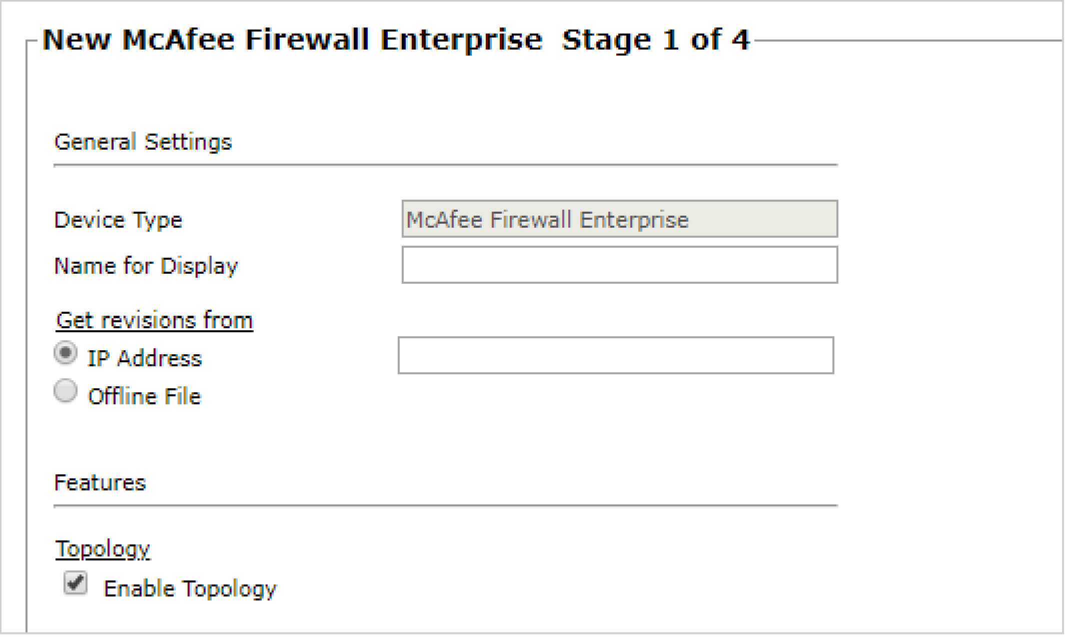
To configure TOS Classic to monitor the policy revisions of a Forcepoint device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:





3. Configure the device settings:



New McAfee Firewall Enterprise Stage 1 of 4

General Settings

Device Type	McAfee Firewall Enterprise
Name for Display	

Get revisions from

● IP Address

○ Offline File

Features

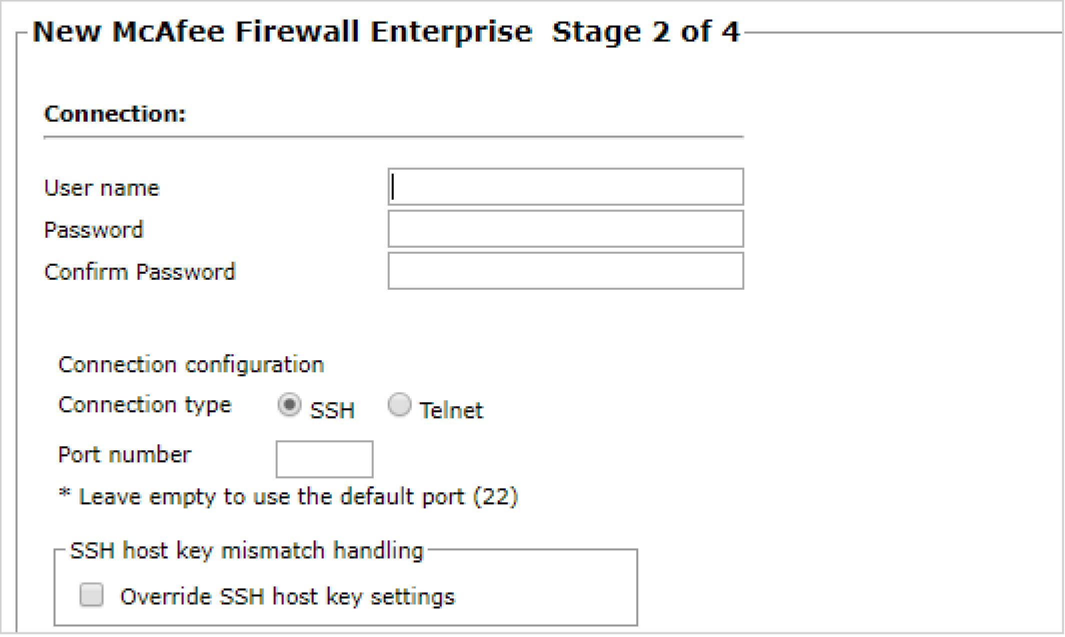
Topology

☑ Enable Topology

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)

Click **Next**.

4. Configure the TOS Classic connection to the Forcepoint device, according to the parameters required by the device:



New McAfee Firewall Enterprise Stage 2 of 4

Connection:

User name
Password
Confirm Password

Connection configuration
Connection type ● SSH ○ Telnet
Port number
* Leave empty to use the default port (22)

SSH host key mismatch handling
□ Override SSH host key settings

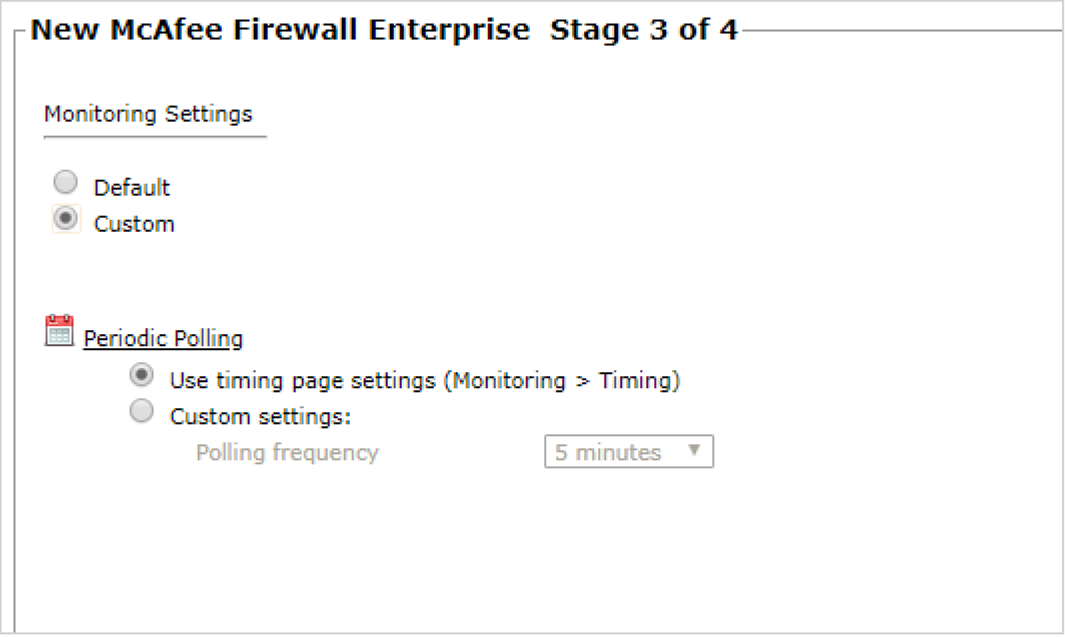
Enter the necessary authentication information to connect to the Forcepoint Firewall Enterprise device.

> Make sure to enter the username of a user with administrator privileges of the firewall device.

Select the whether you connect to the device with **SSH** or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** clear.

Click **Next**.

5. The Monitoring Settings page appears:



New McAfee Firewall Enterprise Stage 3 of 4

Monitoring Settings

○ Default
● Custom

Periodic Polling
● Use timing page settings (Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use timing settings from the Timing page, select **Default**. Otherwise, select **Custom**, **Custom settings**, and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Fortinet Devices

Adding Fortinet Firewall Devices

TOS Classic monitors Fortinet devices for policy revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made) and rule and object usage, you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

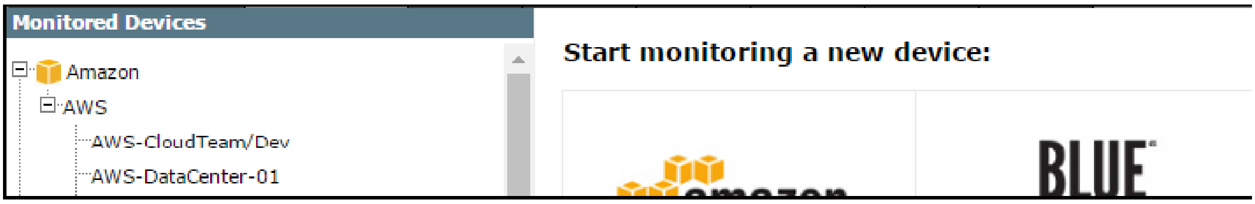
Prerequisites

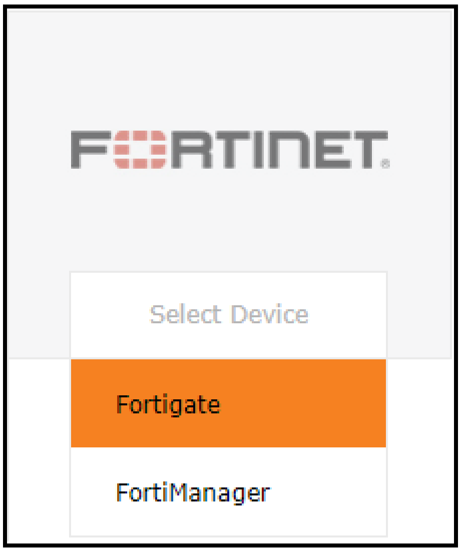
Make sure to use a username that has Read (Read Only, or Read/Write) permissions for all information on the Fortinet device. If your device has VDOMs, make sure that your RO user is configured correctly according to this Fortinet article.

Monitor a Fortinet Device

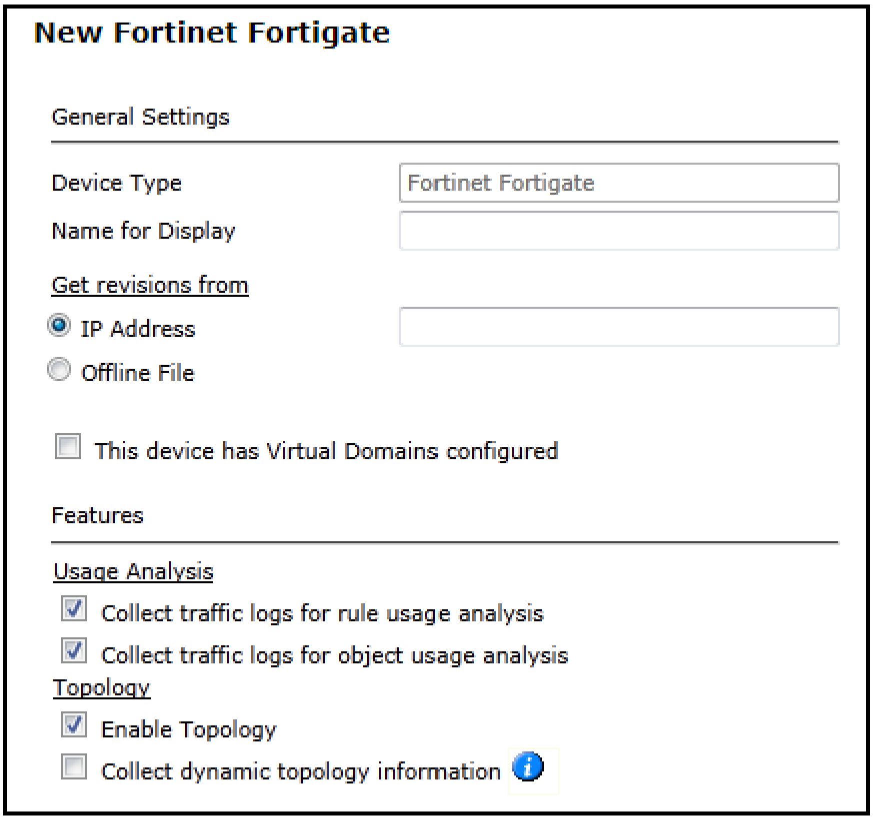
To configure TOS Classic to monitor the policy revisions of a Fortinet device:

1. Select the appropriate device type:





2. Configure the device settings:



New Fortinet Fortigate

General Settings

Device Type: Fortinet Fortigate

Name for Display:

Get revisions from

● IP Address

○ Offline File

□ This device has Virtual Domains configured

Features

Usage Analysis

☑ Collect traffic logs for rule usage analysis

☑ Collect traffic logs for object usage analysis

Topology

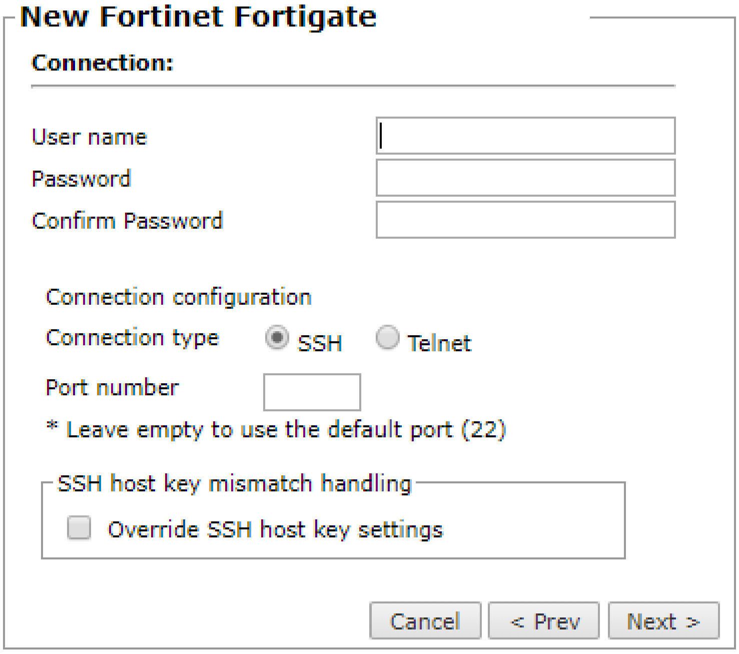
☑ Enable Topology

□ Collect dynamic topology information

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- To enable adding and monitoring Virtual Domains, select **This device has Virtual Domains configured**.

Click **Next**.

3. Configure the TOS Classic connection to the Fortinet device, according to the parameters required by the device:



New Fortinet Fortigate

Connection:

User name

Password

Confirm Password

Connection configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

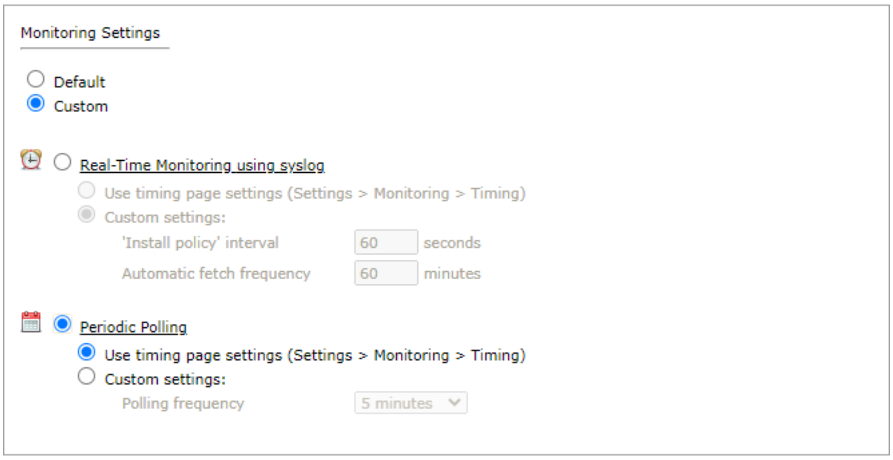
SSH host key mismatch handling

□ Override SSH host key settings

- Enter the authentication details needed to connect to the Fortinet device.
    - **Username and password**: Enter the device username and password
    - **Enable password**: Enter the password to give TOS Classic elevated privileges on the device
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
  The device must be configured to use SSH version 2.

4. Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default

● Custom

○ Real-Time Monitoring using syslog

○ Use timing page settings (Settings > Monitoring > Timing)

● Custom settings:

'Install policy' interval 60 seconds

Automatic fetch frequency 60 minutes

● Periodic Polling

● Use timing page settings (Settings > Monitoring > Timing)

○ Custom settings:

Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

Real-Time Monitoring: Applies only if syslogs "Sending Additional Information via Syslog" on page 239) are configured. Select **Custom settings** and configure:

- **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration

from each device.

If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

6. Click **Next**.
7. **Save** the configuration.

   The Fortinet device now appears in the **Monitored Devices** tree.

8. To manually add Virtual Domains to your device, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the Virtual Domains:
   a. In the **Monitored Devices** tree, select the device.
   b. Click **Import Virtual Domains** (only enabled for **Manual Import**):
   c. Select all the Virtual Domains to be added.

      If the option to collect rule and object usage statistics for virtual contexts is available, it is enabled.

      If you do not want to collect these statistics, clear the options before you import the virtual contexts.

   d. Click **Save**.

For TOS Classic to show full accountability details (who made the policy changes and when the changes were made) and rule and object usage, you must also configure the device to send syslogs.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Fortinet FortiManager Devices

TOS Classic monitors FortiManager devices for revision changes. When you add a FortiManager device to TOS Classic, you can select the devices and virtual domains (VDOMs) managed by the FortiManager that you want TOS Classic to monitor by periodic polling.

Process Overview

To monitor a Fortinet FortiManager device (and its managed devices) in TOS Classic, you must complete the following procedures:

1. Add the Fortinet FortiManager device to TOS Classic.
2. Import the domains and/or devices managed by the Fortinet FortiManager device.

   When you select the Administrative Domains (ADOMs) and devices to be managed by the Fortinet FortiManager device, if you have configured Advanced monitoring mode, you can also select the **Collect dynamic topology information** option.

3. Edit the configuration of a managed FortiManager firewall device, including enabling or disabling the option to **Collect dynamic topology information**.

   If you currently monitor your firewalls as standalone devices and you want to now monitor the firewall through the FortiManager device that manages them, add the FortiManager device and its firewalls as a new device and then disable your standalone firewalls (see Status). You can select the standalone devices from the device tree to see the historical device data. When the device data in the standalone firewalls is obsolete, you can remove the standalone firewall devices from TOS Classic.

After you add the FortiManager and its managed devices, you can monitor the managed devices the same as when you add the managed devices directly to TOS Classic. In addition, you can:

- View and compare in graphical format the policy packages on the FortiManager device according to their administrative domains (ADOMs), including those that are not installed on a firewall device
- View the global object database on the FortiManager device
- Create New Revision and Advanced Change reports for the policy packages on the FortiManager device

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

To help you organize the information for your devices, you can use the device information worksheet.

> From R19-3, support for Fortinet FortiManager (FMG) devices (up to and including version 5.2) in Basic firewall management mode is deprecated for new devices. If you are upgrading to R19-3, the existing FortiManager devices in Basic mode will

> continue to be monitored in TOS Classic. For more information about supported features in each monitoring mode, see the TOS Classic Features by Vendor.

Prerequisites

Read/Write Permissions

- JSON API access with read/write permission
- Create a device user with Read/Write permissions for all information on the FortiManager device.

  You can configure these permissions either in the Fortimanager command line interface, or in the user interface for the device.

Setting Permissions using the Command Line Interface

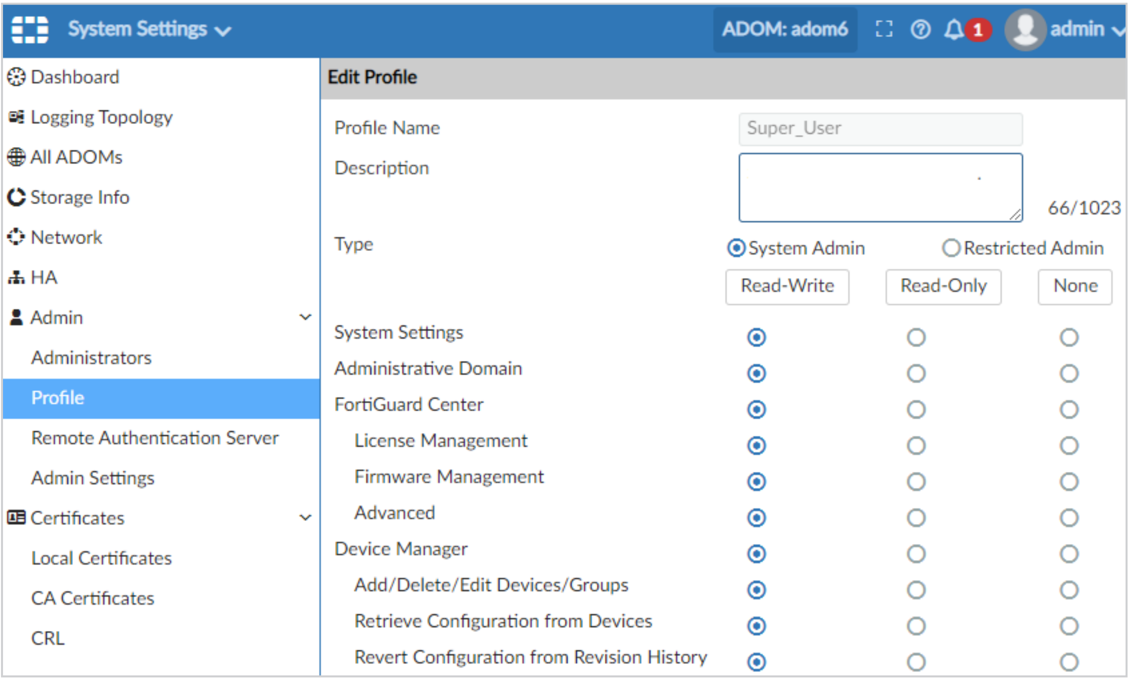
To configure Read/Write permissions for the FortiManager device, in the FortiManager command line interface run:

```
config system admin user
edit <username configured in TOS>
set rpc-permit read-write
end
```

Setting Permissions in FortiManager Interface

To configure Read/Write permissions for a FortiManager device, in the device user interface:

1. Log into the device and select **System Settings**.
2. In the navigation pane, select **Admin** > **Profile**.
3. Create/Edit the device profile that is associated with a Tufin Orchestration Suite user account.
4. Select **Read-Write** for all the profile settings.



Edit Profile

Profile Name: Super_User

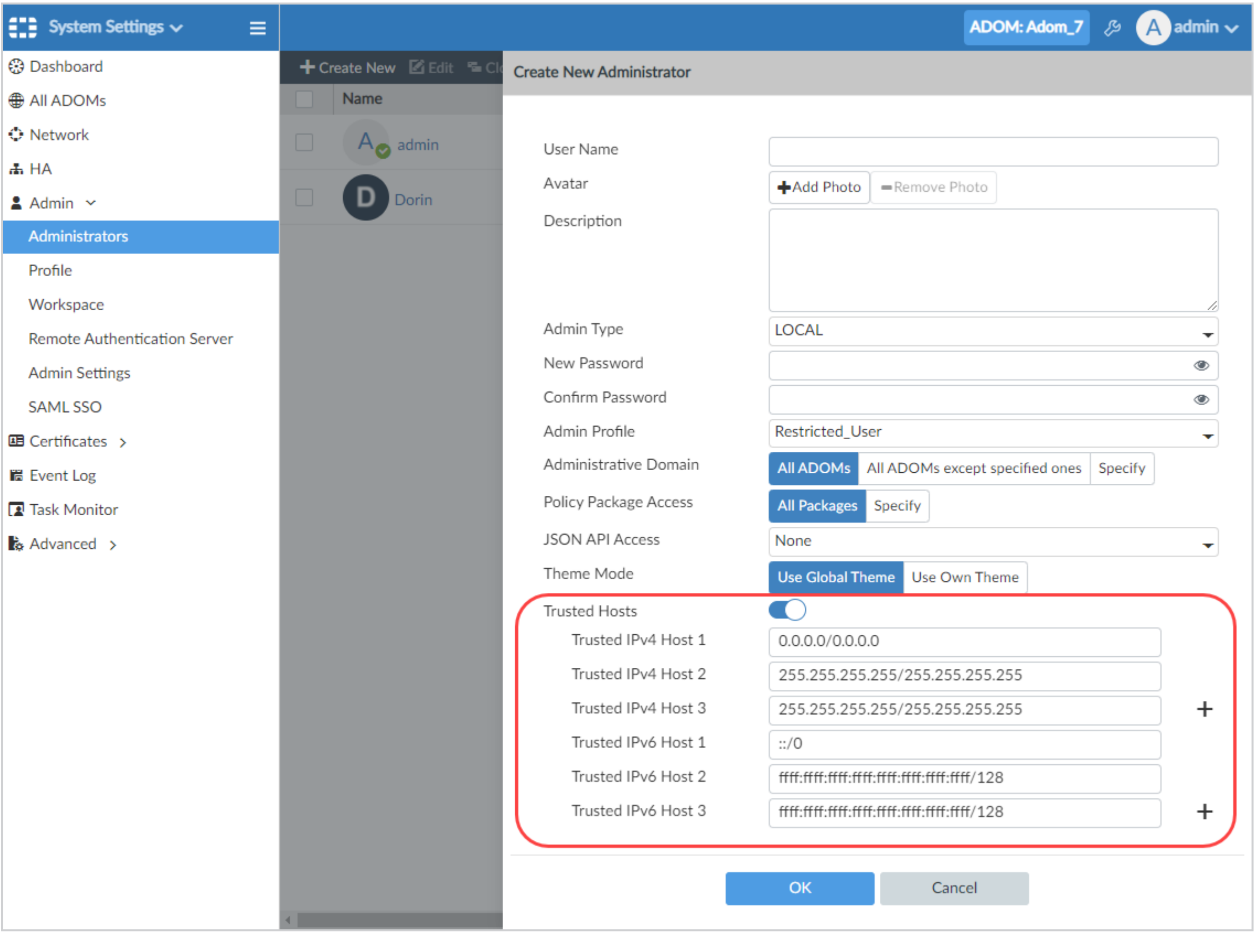
Description: 66/1023

Type: ● System Admin ○ Restricted Admin

	Read-Write	Read-Only	None
System Settings	●	○	○
Administrative Domain	●	○	○
FortiGuard Center	●	○	○
License Management	●	○	○
Firmware Management	●	○	○
Advanced	●	○	○
Device Manager	●	○	○
Add/Delete/Edit Devices/Groups	●	○	○
Retrieve Configuration from Devices	●	○	○
Revert Configuration from Revision History	●	○	○

Update the FortiManager List of Trusted Hosts

If you have enabled the **Trusted Hosts** setting in FortiManager, you will need to add the IP address of the TOS Classic host to enable certificate retrieval and communication.



Create New Administrator

User Name

Avatar: Add Photo | Remove Photo

Description

Admin Type: LOCAL

New Password

Confirm Password

Admin Profile: Restricted_User

Administrative Domain: [✓ All ADOMs] | All ADOMs except specified ones | Specify

Policy Package Access: [✓ All Packages] | Specify

JSON API Access: None

Theme Mode: [✓ Use Global Theme] | Use Own Theme

Trusted Hosts: ●

Trusted IPv4 Host 1	0.0.0.0/0.0.0.0
Trusted IPv4 Host 2	255.255.255.255/255.255.255.255
Trusted IPv4 Host 3	255.255.255.255/255.255.255.255
Trusted IPv6 Host 1	::/0
Trusted IPv6 Host 2	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
Trusted IPv6 Host 3	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128

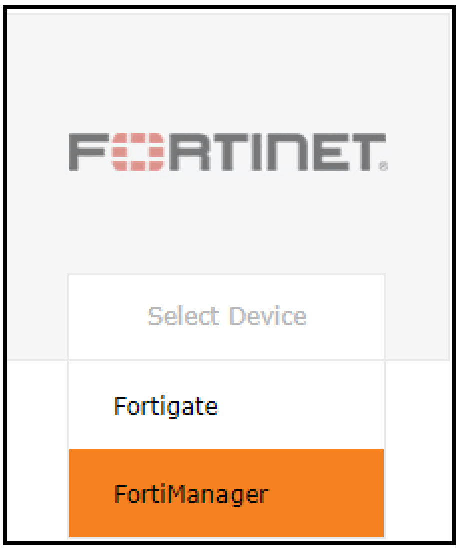
Add a SAN Signed Certificate to the FortiManager Device

See "Adding SAN signed certificates to FortiManager devices" on page 174.

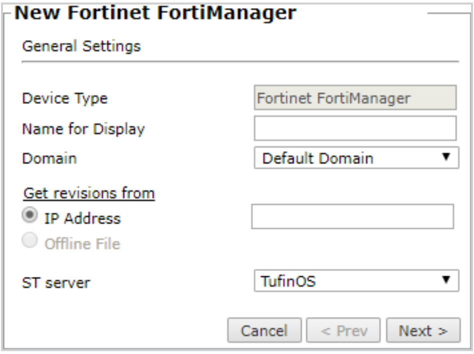
Monitor a FortiManager Device

To configure TOS Classic to monitor the policy revisions of a FortiManager device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Fortinet FortiManager

General Settings

Device Type	Fortinet FortiManager
Name for Display	
Domain	Default Domain

Get revisions from

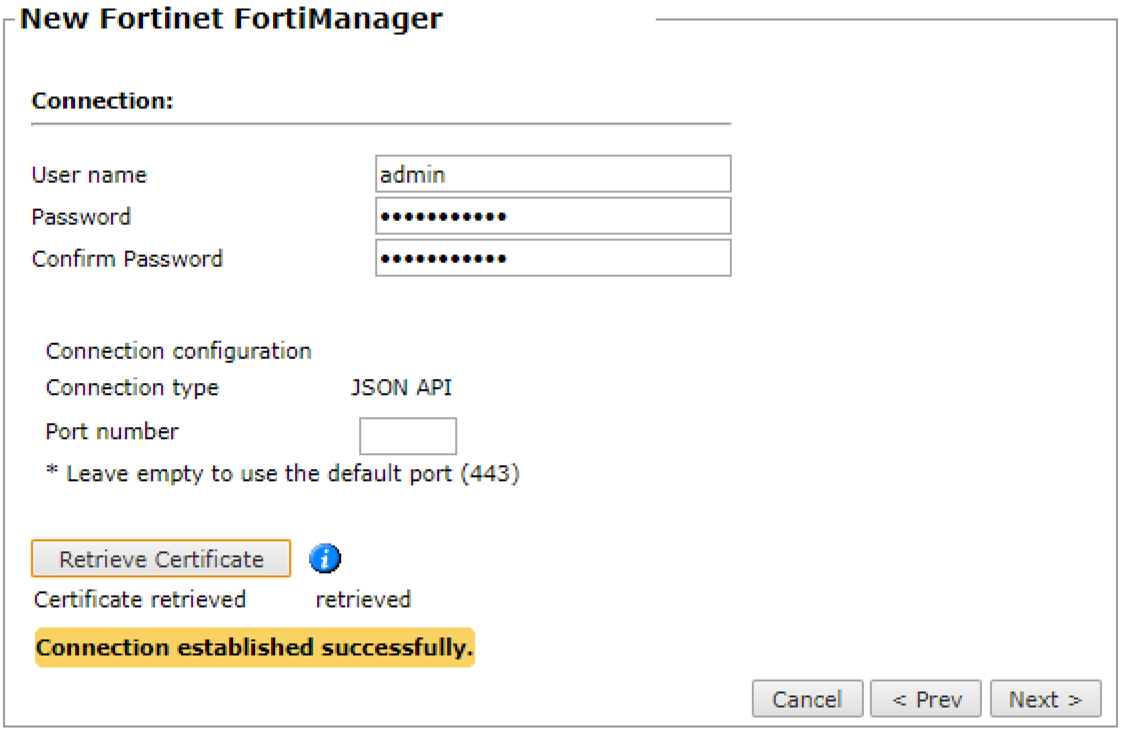
● IP Address

○ Offline File

ST server: TufinOS

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**:
  - **IP Address**: Enter the IP address of the FortiManager device.
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device.

4. Click **Next**.
5. Configure the TOS Classic connection to the FortiManager device, according to the parameters required by the device:



New Fortinet FortiManager

Connection:

User name	admin
Password	•••••••••••
Confirm Password	•••••••••••

Connection configuration

Connection type JSON API

Port number

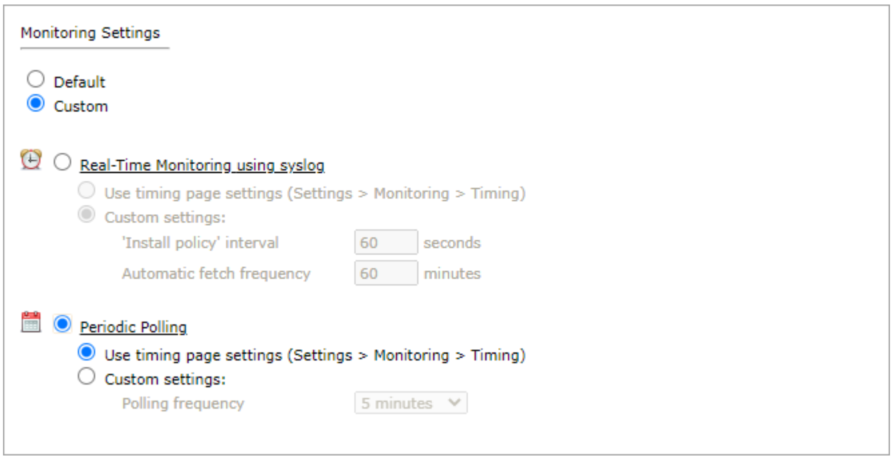
* Leave empty to use the default port (443)

Certificate retrieved retrieved

Connection established successfully.

- Enter the authentication details needed to connect to the FortiManager device.
  - **Username and password**: Enter the device username and password
  - **Enable password**: Enter the password to give TOS Classic elevated privileges on the device
  - **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
    The device must be configured to use SSH version 2. For Advanced management, the connection type is **JSON API**.
  - **Port number**: Leave empty to use the default port (port 22 for Basic firewall management, port 443 for Advanced management)

6. Click **Next**.
7. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

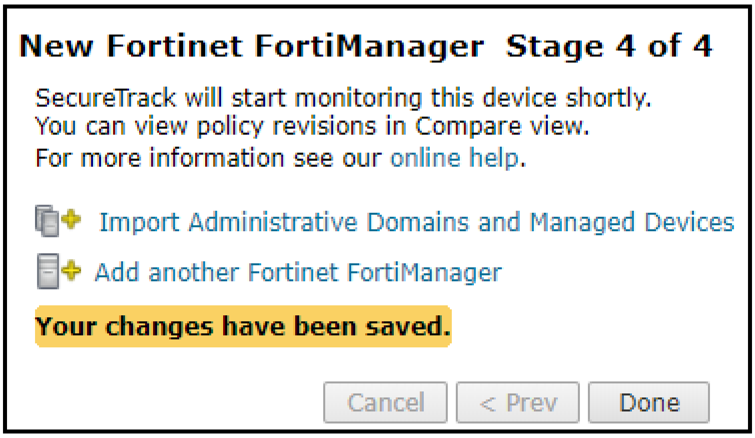
- To use real-time monitoring and timing settings from the Timing page, select **Default**.
- Otherwise, select **Custom** and configure the monitoring mode and settings.
- In **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

8. Click **Next**.
9. **Save** the configuration.

   The FortiManager device now appears in the **Monitored Devices** tree.
10. To complete the configuration, do one of the following:
    - Click **Done**.
    - Click **Import Managed Devices** (or **Import Administrative Domains and Managed Devices/Import Device Groups and Managed Devices** if available), select all the managed devices to be added, and click **Save** or **Import**.

      To import managed devices later, you can select the device and click **Import Managed Devices** (or **Import Administrative Domains and Managed Devices/Import Device Groups and Managed Devices** if available).
    - Add another device.



New Fortinet FortiManager Stage 4 of 4

SecureTrack will start monitoring this device shortly.
You can view policy revisions in Compare view.
For more information see our online help.

Import Administrative Domains and Managed Devices

Add another Fortinet FortiManager

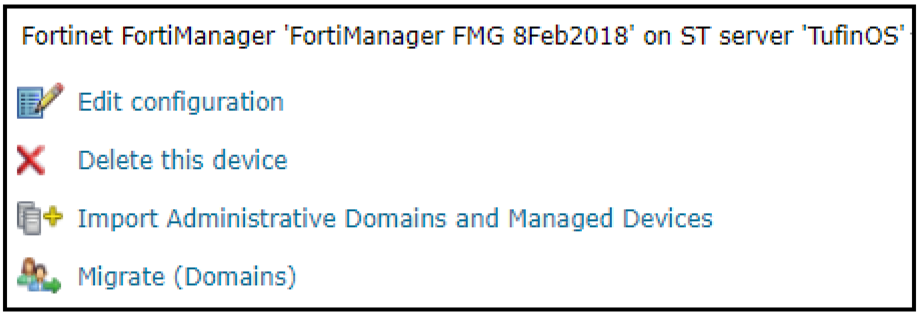
Your changes have been saved.

Topology options to collect routing information for building the network Interactive Map are configured when you import managed devices.

Import the domains or devices managed by the FortiManager device

To import devices or domains managed by the FortiManager device into TOS Classic:

1. Select the FortiManager device from the device tree.
2. Click **Import Administrative Domains and Managed Devices**.

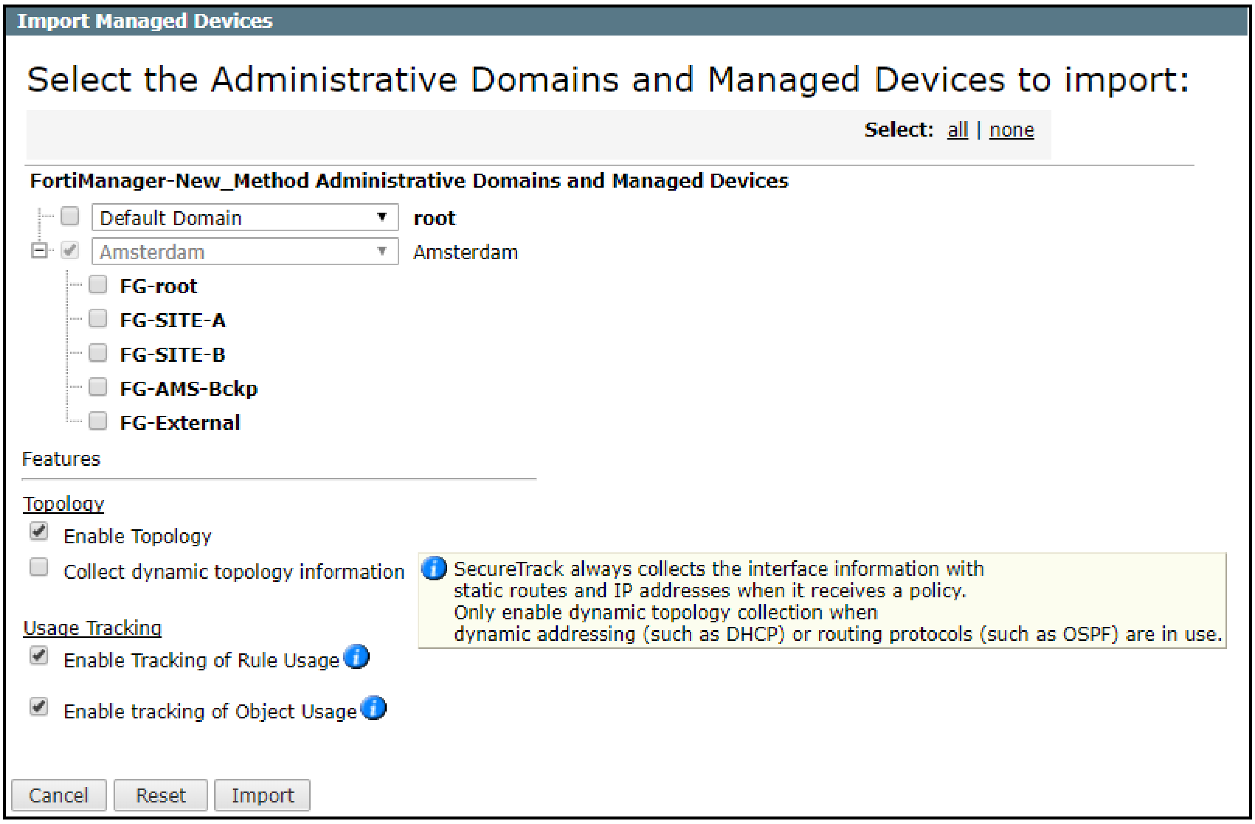


Fortinet FortiManager 'FortiManager FMG 8Feb2018' on ST server 'TufinOS'

3. From the list of devices managed by the FortiManager device, select the devices to import.
4. Configure the **Topology** options.

   Enable Topology: Collects routing information for building the network Interactive Map.
   Topology options for **Advanced management** mode are configured when you import managed devices.

   - **Collect dynamic topology information** when dynamic addressing (DHCP) or routing protocols (OSPF and BGP) are in use. (This option is available if you have configured Advanced monitoring mode).



Import Managed Devices

Select the Administrative Domains and Managed Devices to import:

FortiManager-New_Method Administrative Domains and Managed Devices

- □ Default Domain ▾ **root**
- ☑ Amsterdam ▾ Amsterdam
  - □ **FG-root**
  - □ **FG-SITE-A**
  - □ **FG-SITE-B**
  - □ **FG-AMS-Bckp**
  - □ **FG-External**

Features

Topology

☑ Enable Topology

□ Collect dynamic topology information

SecureTrack always collects the interface information with static routes and IP addresses when it receives a policy.
Only enable dynamic topology collection when dynamic addressing (such as DHCP) or routing protocols (such as OSPF) are in use.

Usage Tracking

☑ Enable Tracking of Rule Usage

☑ Enable tracking of Object Usage

5. Configure the **Usage Tracking** options:
   - **Enable Tracking of Rule Usage** - Monitor last hit information for rules in the managed devices being imported.
   - **Enable Tracking of Application and User Usage** - Monitor last hit information for applications and users in the managed devices being imported.
6. Click **Import**.
7. Do one of the following:
   - Click **Reset** to update the list of managed devices.
   - Click **Done** to return to the device tree.

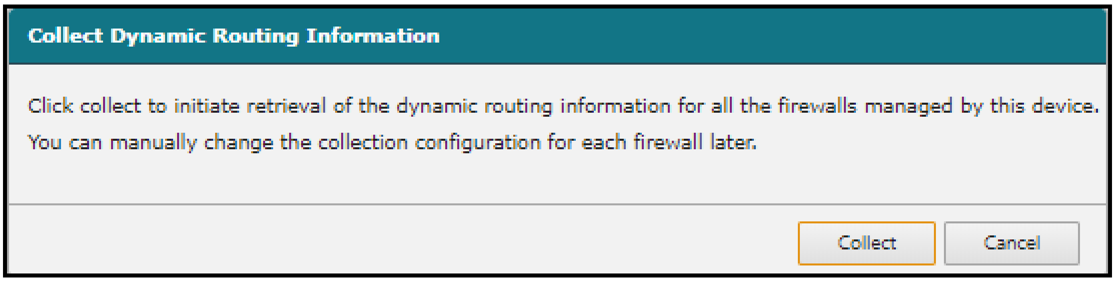
     The managed devices appear under the FortiManager device in the device tree.

For TOS Classic to show full accountability details (who made the policy changes and when the changes were made) and rule and object usage, you must also configure the device to send syslogs.

Edit the Dynamic Topology Settings for Devices

To configure a Fortinet FortiManager device to retrieve Dynamic Topology information for its managed devices in TOS Classic:

1. Select the Fortinet FortiManager device from the device tree.
2. Click **Collect Dynamic Routing Information** and click **Collect**.

   Collect Dynamic Routing Information

   Click collect to initiate retrieval of the dynamic routing information for all the firewalls managed by this device.
   You can manually change the collection configuration for each firewall later.

   Collect dynamic topology information is enabled for all the managed devices.

   For Fortinet FortiManager devices, dynamic topology information is retrieved for Administrative Domains (ADOMs) from version 5.4 and above.

How Do I Get Here?

In SecureTrack, go to **Monitoring** > **Manage Devices**.

Adding SAN signed certificates to FortiManager devices

Overview

TOS requires that all monitored FortiManager devices have a SAN signed certificate. Without a SAN signed certificate, SecureTrack will be unable to retrieve dynamic topology information. By default, FortiManager devices do not include a SAN certificate. Therefore, you are going to need to add a SAN certificate to each monitored FortiManager device.

Prerequisites

- Certificate (CSR) signed by a Certification Authority (CA).
  - The **Host IP** and **Subject Alternative Name** fields need to be the IP address of the device.
- Key used to generate the certificate.

Both the certificate and key need to be obtained independently from Fortinet

To add the SAN signed certificate to the FortiManager device

1. Sign into the FortiManager device as an Administrator.
2. In the FortiManager device, go to **System Settings** > **Certificates** > **Local Certificates**, and click **Import**.
3. In the **Import** dialog box:
   a. In the **Type** field, select **Certificate**.
   b. In the **Certificate File** and **Key File** fields, upload the certificate and key.
   c. In the **Certificate Name** field, enter the certificate name.
   d. Click **OK**.
4. Go to **System Settings** > **Admin** > **Admin Settings.**
5. In **Administration Settings** section > **HTTPS & Web Service Certificate**, select the certificate from the previous step.
6. **If the device was already imported into SecureTrack:**
   a. In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**, select the Fortimanager device, and click **Edit Configuration**.
   b. On page 2, click the **Retrieve Certificate** button.

Adding IPtables Devices

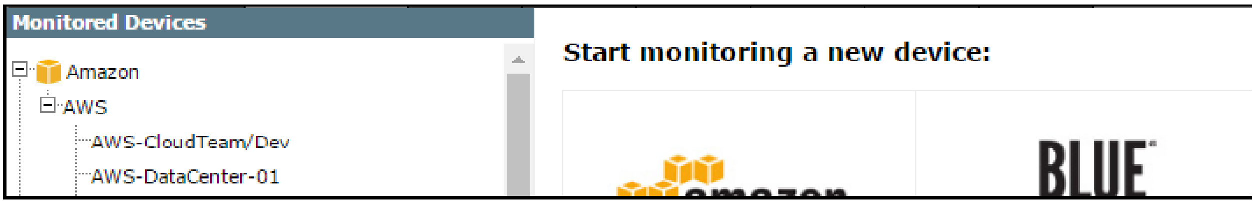
SecureTrack can monitor Netfilter devices with pre-installed TOP plugins. To help you organize the information for your devices, you can use the device information worksheet.

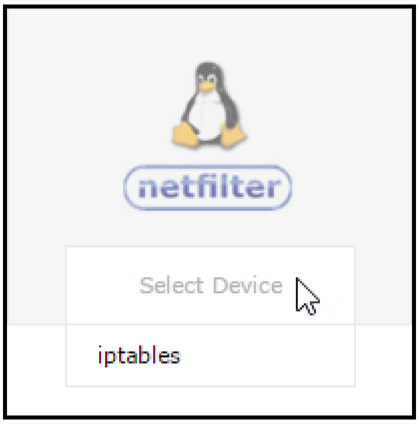
SecureTrack and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Monitor a Netfilter Device

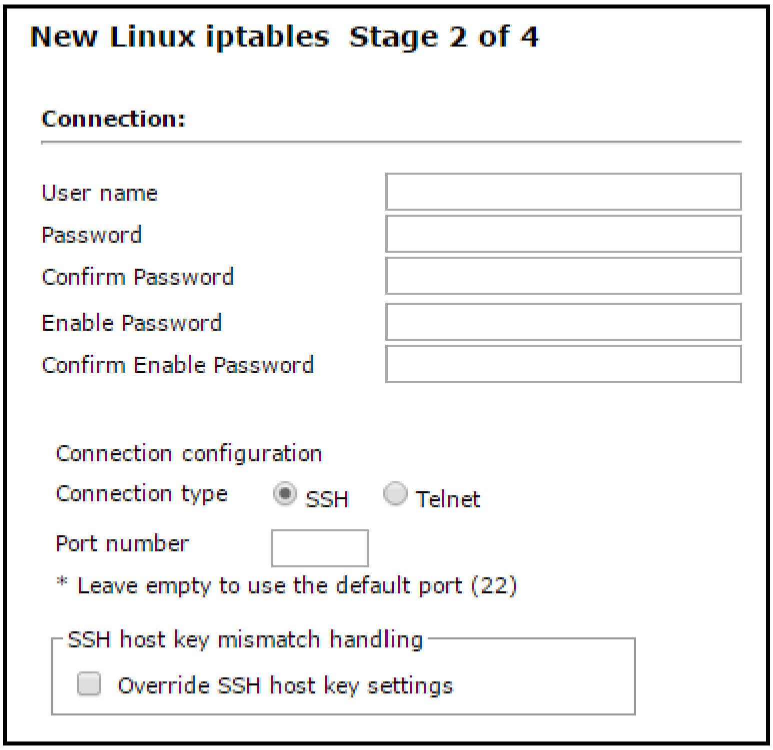
To configure SecureTrack to monitor the policy revisions of a Netfilter device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:





3. Configure the device settings:



New Linux iptables Stage 2 of 4

Connection:

User name
Password
Confirm Password
Enable Password
Confirm Enable Password

Connection configuration
Connection type ● SSH ○ Telnet
Port number
* Leave empty to use the default port (22)

SSH host key mismatch handling
□ Override SSH host key settings

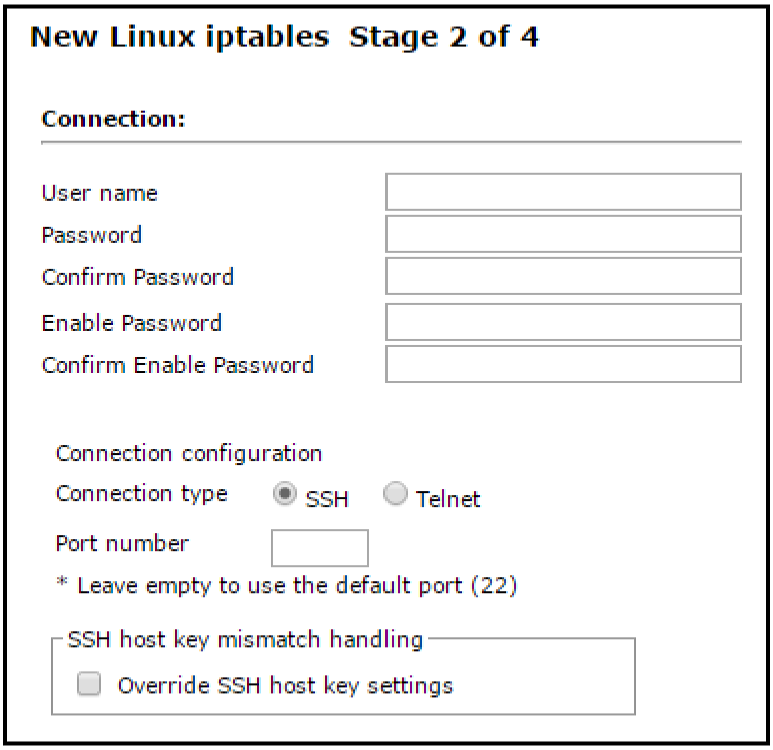
- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you

must migrate the device.

- **Plugin name**: If there are multiple plugins installed for the same device type, select the plugin for your device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis
- **ST server**: In a distributed deployment, select which SecureTrack server monitors this device (Not shown in image) TOP devices monitored via preinstalled TOP plugins can be monitored by any SecureTrack server (Central, Distribution, or Remote Collector).

Click **Next**.

4. Configure the SecureTrack connection to the Netfilter device, according to the parameters required by the device:



New Linux iptables Stage 2 of 4

Connection:

User name

Password

Confirm Password

Enable Password

Confirm Enable Password

Connection configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

SSH host key mismatch handling

□ Override SSH host key settings

- Depending on the device type, Enter the authentication details needed to connect to the Netfilter device.
  - **Username and password**: Enter the device username and password
  - **Enable password**: Enter the password to give SecureTrack elevated privileges on the device
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
  The device must be configured to use SSH version 2.

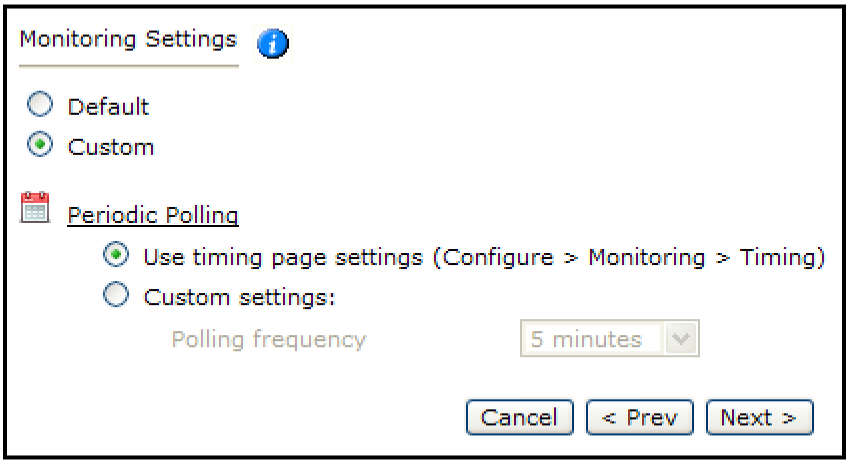
  Special characters in the password are not supported for some plugins.

  Depending on your device configuration, SecureTrack web interface may include more fields than are necessary for logging into the device. Make sure not to fill in these fields, as this may cause monitoring to fail.

  Make sure to use a username representing a user account that has Read (Read Only, or Read/Write) permissions for all information on the Netfilter device. For **iptables**, the user must have permission to run the `iptables-save` command.

Click **Next**.

5. The Monitoring Settings page appears:



Monitoring Settings

○ Default

● Custom

Periodic Polling

● Use timing page settings (Configure > Monitoring > Timing)

○ Custom settings:

Polling frequency 5 minutes

To use timing settings from the Timing page for this device, select **Default**.

- To define specific timing settings for this device, select **Custom**, then select **Custom settings**, and configure the **Polling frequency**: How often SecureTrack fetches the configuration from each device.

If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

6. **Save** the configuration.

   The Netfilter device now appears in the Device Configuration list.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Juniper Devices

Adding Juniper M or MX Devices

TOS Classic monitors M Series and MX Series devices for policy revision changes. To see which TOS features are supported for your device, review the feature support table.

Prerequisites

Before you add the device to TOS Classic:

1. SecureTrack and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.
2. Make sure that the Juniper device user account permission to run the following commands:
   - Retrieve revision

   ```
   show configuration
   show configuration policy-options
   show system uptime
   show version
   show configuration system
   ```

   - Virtual context

   ```
   show logical-system
   ```

   - Dynamic topology

   ```
   show configuration routing-instances
   show route active-path
   show interfaces terse
   ```

```
show vrrp
show interfaces
show bgp neighbor
```

- Export versions of JunOS devices may not support SSH.

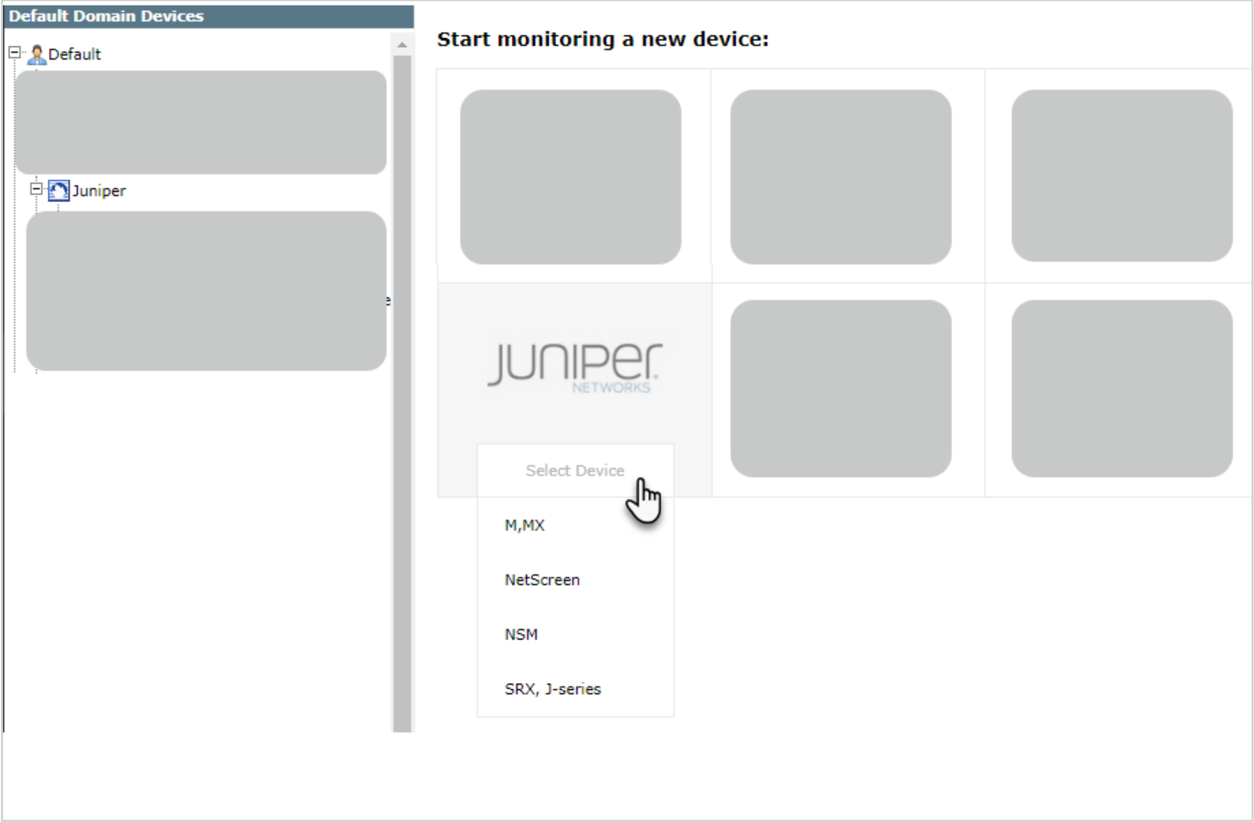
3. If you want to use commit scripts, update `stconf` as follows:

```
<JunOS_Use_Commit_Scripts>
       <management_ids>16,17,18,19,20,21, 22,23,24,25</management_ids>
</JunOS_Use_Commit_Scripts>
```

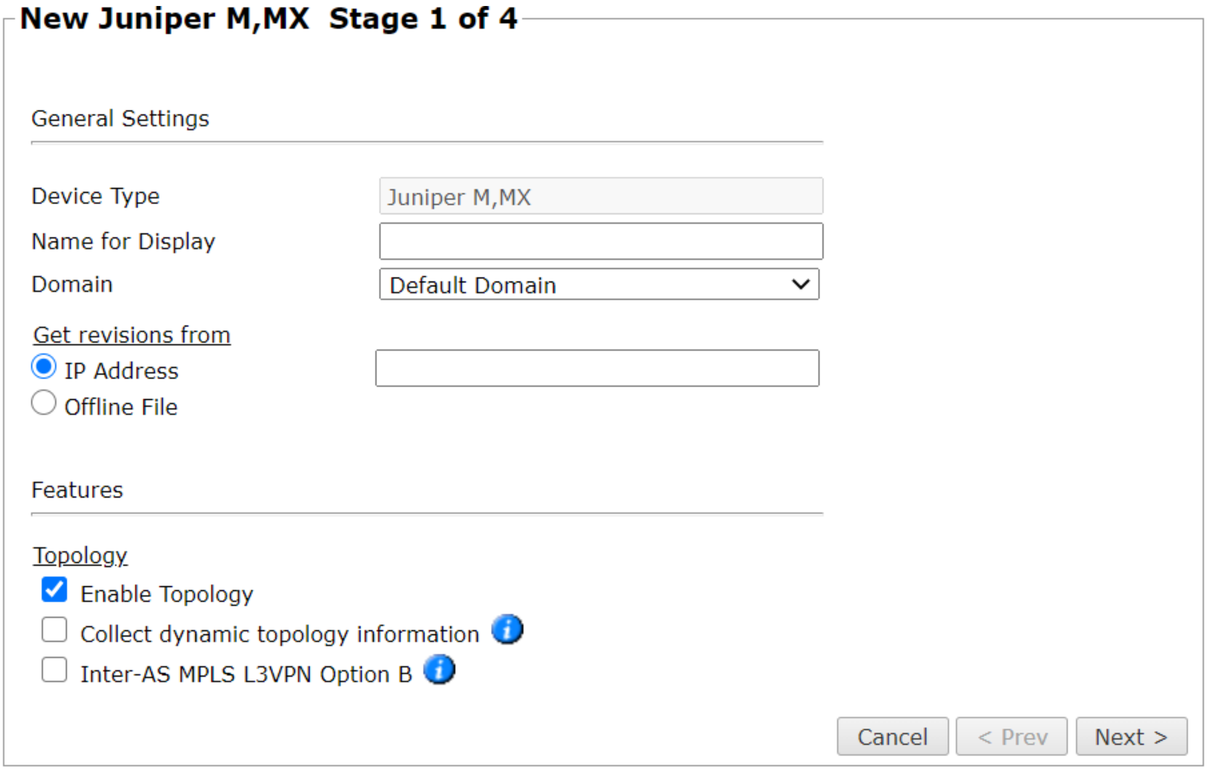
Monitor a M or MX Series Device

To configure TOS Classic to monitor the policy revisions of a M or MX Series Device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select **M, MX**.



3. Configure the device settings:



New Juniper M,MX Stage 1 of 4

General Settings

Device Type: Juniper M,MX

Name for Display:

Domain: Default Domain

Get revisions from

● IP Address

○ Offline File

Features

Topology

☑ Enable Topology

□ Collect dynamic topology information

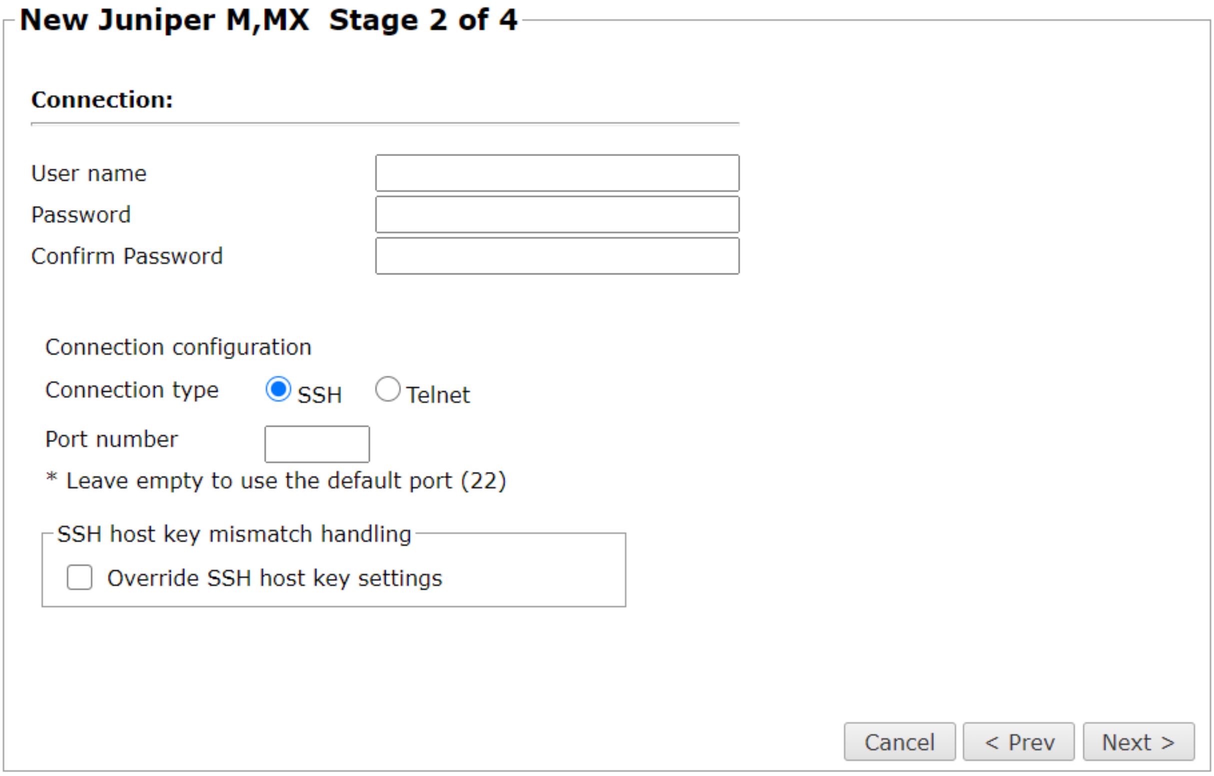
□ Inter-AS MPLS L3VPN Option B

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis

    For **IP Address**, if SecureTrack is configured or will be configured as a syslog server for the NSM, make sure to use the same Juniper device IP address here as is configured in the NSM.
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- **Enable Topology**: Collects routing information for building the network Interactive Map.

  Topology options for **Advanced management** mode are configured when you import managed devices.
- **Collect dynamic topology information**: Select if the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF).
- **Inter-AS MPLS L3VPN Option**: Select if this router is an ASBR in an MPLS option B environment. This option will retrieve VPNv4 labels associated with inter-AS communication.

4. Click **Next**.
5. Configure the TOS Classic connection to the NSM device, according to the parameters required by the device:



New Juniper M,MX Stage 2 of 4

Connection:

User name
Password
Confirm Password

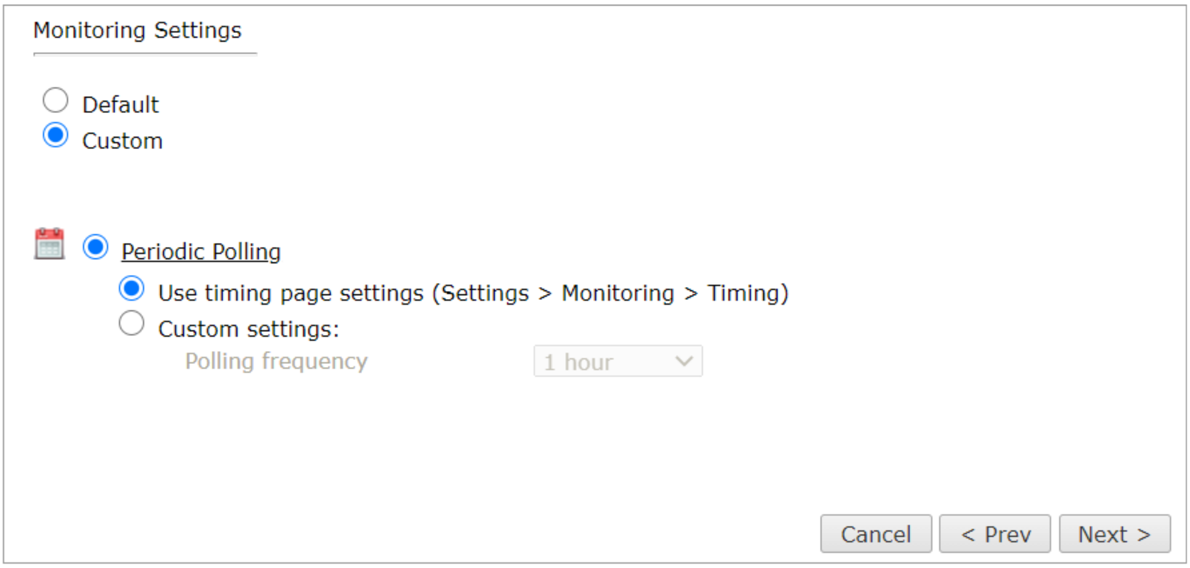
Connection configuration
Connection type ● SSH ○ Telnet
Port number
* Leave empty to use the default port (22)

SSH host key mismatch handling
□ Override SSH host key settings

Make sure you have a user configured on the device with the privileges required by SecureTrack. See the prerequisites section for a list of required privileges.

- Enter the authentication details (**User name** and **Password**) needed to connect to the Juniper device.
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
  The device must be configured to use SSH version 2.

6. Click **Next**.
7. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 1 hour

- To use timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

8. Click **Next**.
9. **Save** the configuration.

   The device now appears in the **Monitored Devices** tree.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Juniper NetScreen Devices

SecureTrack monitors Juniper devices for policy revision changes. For SecureTrack to show full accountability details (who made the policy changes and when the changes were made) and rule and object usage, you must also configure the device to send syslogs.

Prerequisites

Before you add the device to SecureTrack:

1. SecureTrack and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.
2. Make sure that the Juniper device user account permission to run the following commands:

   Netscreen

   - Retrieve revision

     ```
     get config
     get service pre-defined
     get service <service>
     get service group
     get service group <group name>
     get clock
     get system
     get hostname
     get zone all
     get zone
     get zone id <zone_id>
     exit
     ```

   - Retrieve dynamic topology

     ```
     get route
     get route v4
     get interface all
     get interface <interface name>
     ```

   - Virtual context

     ```
     get vsys
     enter vsys <vsys name>
     ```

   JunOS

   - Retrieve revision

     ```
     show configuration
     show version
     show uptime
     ```

- Virtual context

```
show logical-system
```

- Dynamic topology

```
show configuration routing-instances
show route active-path
show interface
show vrrp
show bgp neighbor
```

- Provisioning

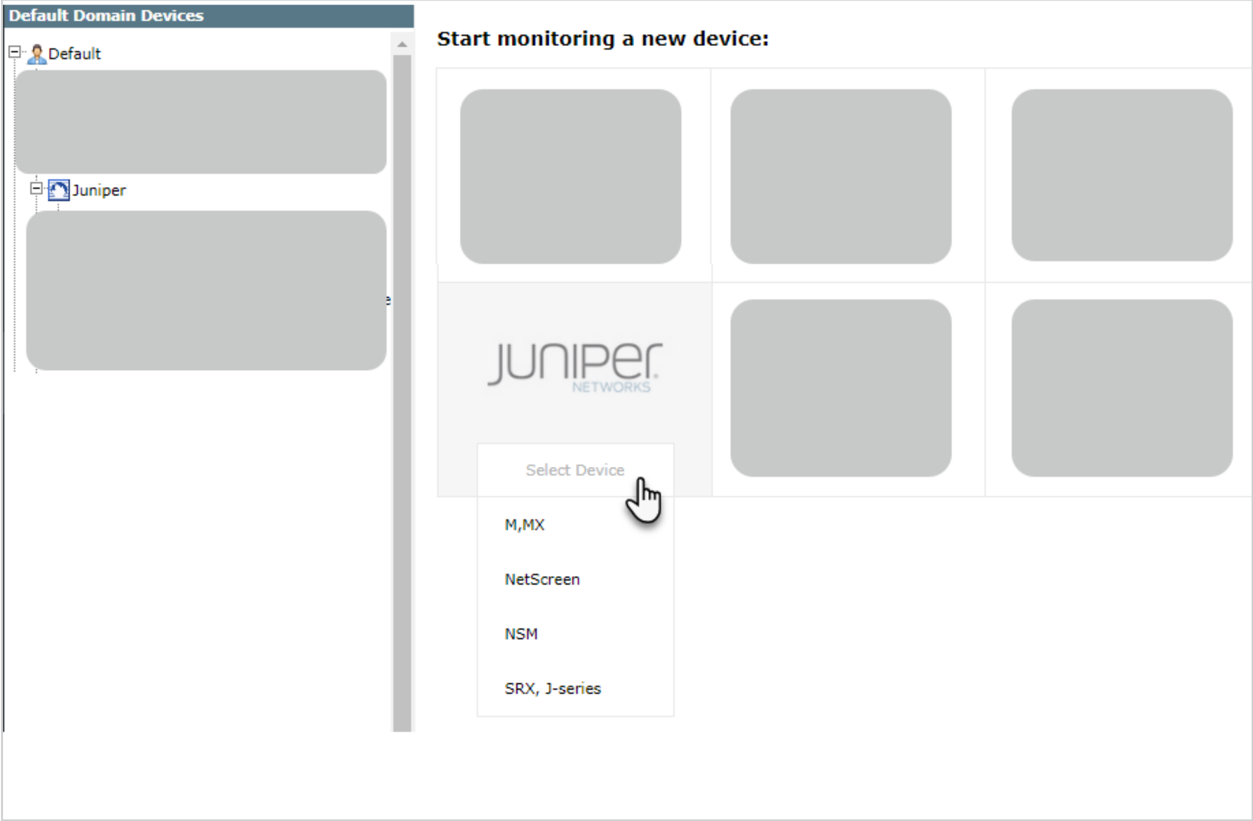
```
edit
configure
edit logical-system (for provisioning FW with logical system)
```

Export versions of JunOS devices may not support SSH.

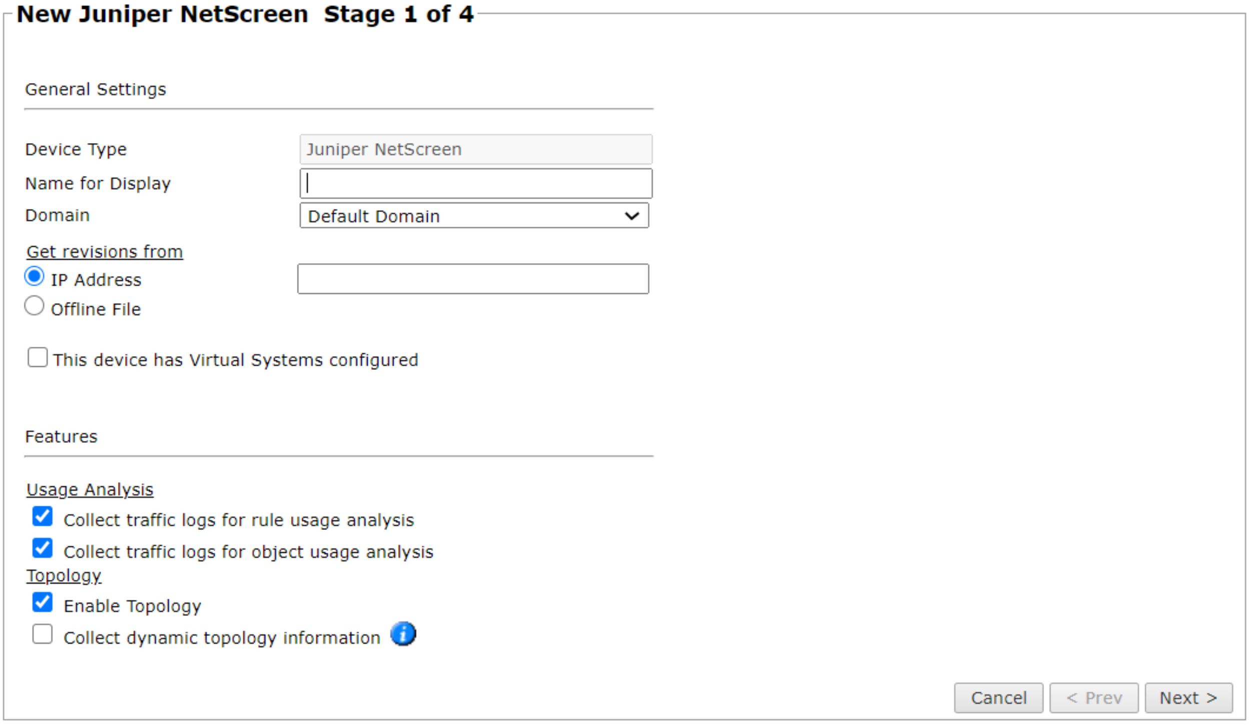
Monitor a Juniper NetScreen Device

To configure SecureTrack to monitor the policy revisions of a Juniper device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select **NetScreen**.



3. Configure the device settings:



New Juniper NetScreen Stage 1 of 4

General Settings

Device Type: Juniper NetScreen

Name for Display:

Domain: Default Domain

Get revisions from

● IP Address

○ Offline File

□ This device has Virtual Systems configured

Features

Usage Analysis

☑ Collect traffic logs for rule usage analysis

☑ Collect traffic logs for object usage analysis

Topology

☑ Enable Topology

□ Collect dynamic topology information

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis

    For **IP Address**, if SecureTrack is configured or will be configured as a syslog server for the NSM, make sure to use the same Juniper device IP address here as is configured in the NSM.
- **ST server**: In a distributed deployment, select which SecureTrack server monitors this device (Not shown in image)
- **This device has Virtual Systems configured**: Select to enable adding and monitoring Virtual Systems.

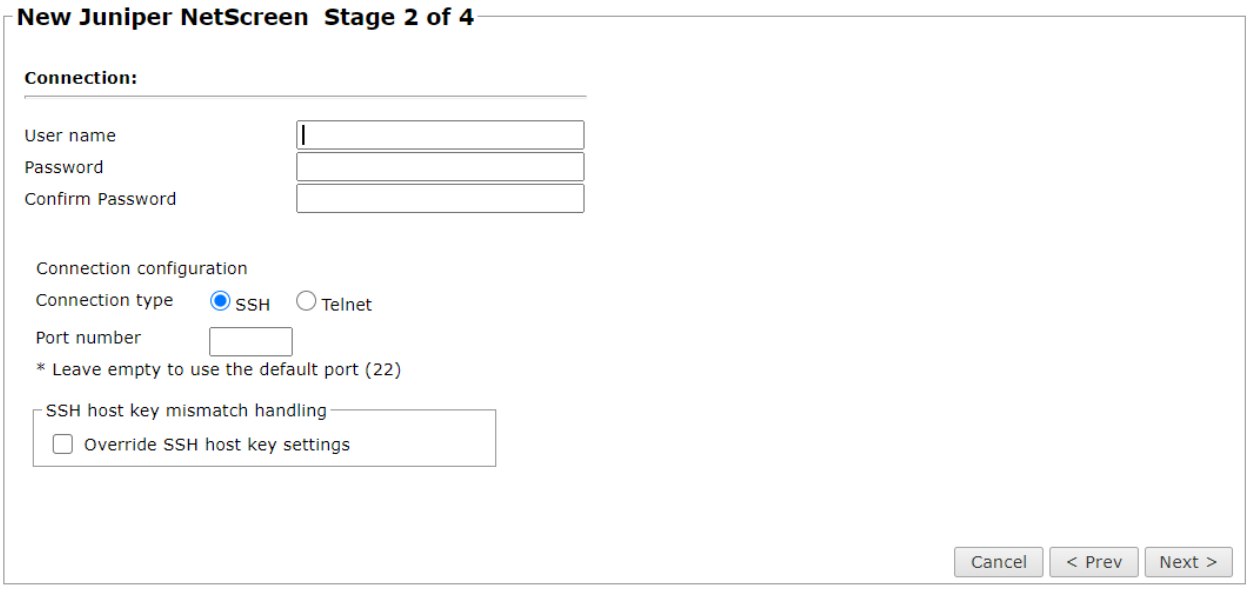
  If you have virtual systems, you can monitor clustered Netscreen devices. You can only do this when you first add the device to SecureTrack. To monitor a Netscreen cluster that has virtual systems, select **This device has Virtual Systems configured** and select **Cluster**.
- **Collect traffic logs for rule usage analysis** is necessary for Rule Usage reports.
  - **Collect traffic logs for object usage analysis** is necessary for reporting on unused objects and services in Rule Usage Reports.

  Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure SecureTrack to limit the number of days that data is kept.

  We recommend that you enable SecureTrack administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, SecureTrack sends an alert.
- **Enable Topology**: Collects routing information for building the network Interactive Map.

  Topology options for **Advanced management** mode are configured when you import managed devices.
- **Collect dynamic topology information**: Select if the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF).

4. Click **Next**.
5. Configure the SecureTrack connection to the Juniper device, according to the parameters required by the device:



New Juniper NetScreen Stage 2 of 4

Connection:

User name
Password
Confirm Password

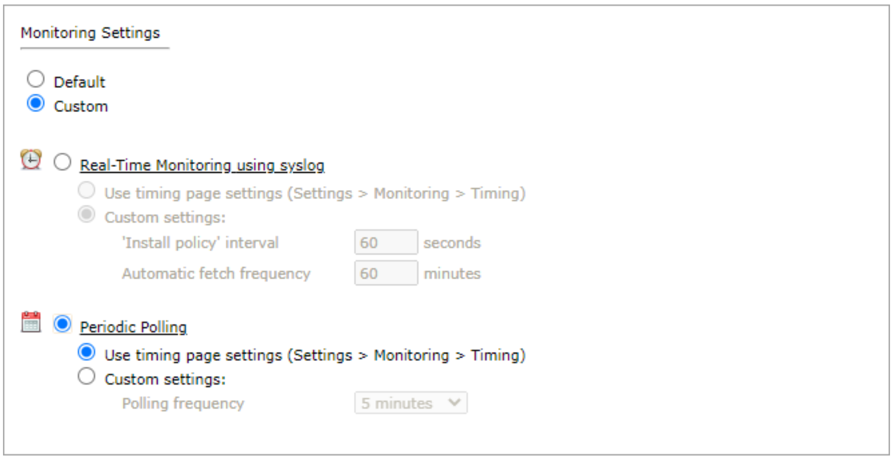
Connection configuration
Connection type ● SSH ○ Telnet
Port number
* Leave empty to use the default port (22)

SSH host key mismatch handling
□ Override SSH host key settings

Make sure you have a user configured on the device with the privileges required by SecureTrack. See the prerequisites section for a list of required privileges.

- Enter the authentication details (**User name** and **Password**) needed to connect to the Juniper device.
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
  The device must be configured to use SSH version 2.

6. Click **Next**.
7. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings:

- **Real-Time Monitoring**: Applies only if syslogs "Sending Additional Information via Syslog" on page 239) are configured. Select **Custom settings** and configure:
  - **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, SecureTrack combines the events into a single Install Policy revision (Default: 60 seconds)
  - **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often SecureTrack fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

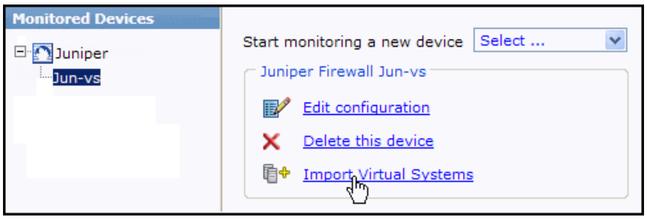
8. Click **Next**.
9. **Save** the configuration.

The Juniper device now appears in the **Monitored Devices** tree.

10. To manually add Virtual Systems to your device, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the Virtual Systems:

    a. In the **Monitored Devices** tree, select the device.

    b. Click **Import Virtual Systems** (only enabled for **Manual Import**):

    c. Select all the Virtual Systems to be added.

    If the option to collect rule and object usage statistics for virtual contexts is available, it is enabled.

    If you do not want to collect these statistics, clear the options before you import the virtual contexts.

    d. Click **Save**.

For SecureTrack to show full accountability details (who made the policy changes and when the changes were made) and rule and object usage, you must also configure the device to send syslogs.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Juniper NSM Devices

TOS Classic monitors NSM devices for policy revision changes. To see which TOS features are supported for your device, review the feature support table.

In addition to the change management monitoring and reporting, you can run these reports for devices managed by NSM: Best Practices, Compliance Policies, Policy Analysis, Rule Documentation and Recertification, and Firewall Module Change.

If you currently monitor your firewalls as standalone devices and you want to now monitor the firewall through the NSM device that manages them, add the NSM device and its firewalls as a new device and then disable your standalone firewalls (see Status). You can select the standalone devices from the device tree to see the historical device data. When the device data in the standalone firewalls is obsolete, you can remove the standalone firewall devices from TOS Classic.

Prerequisites

Before you add the device to TOS Classic:

1. SecureTrack and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

2. Make sure that the Juniper device user account permission to run the following commands:

   Netscreen

   - Retrieve revision

     ```
     get config
     get service pre-defined
     get service <service>
     get service group
     get service group <group name>
     get clock
     get system
     get hostname
     get zone all
     get zone
     get zone id <zone_id>
     exit
     ```

   - Retrieve dynamic topology

```
get route
get route v4
get interface all
get interface <interface name>
```

- Virtual context

```
get vsys
enter vsys <vsys name>
```

JunOS

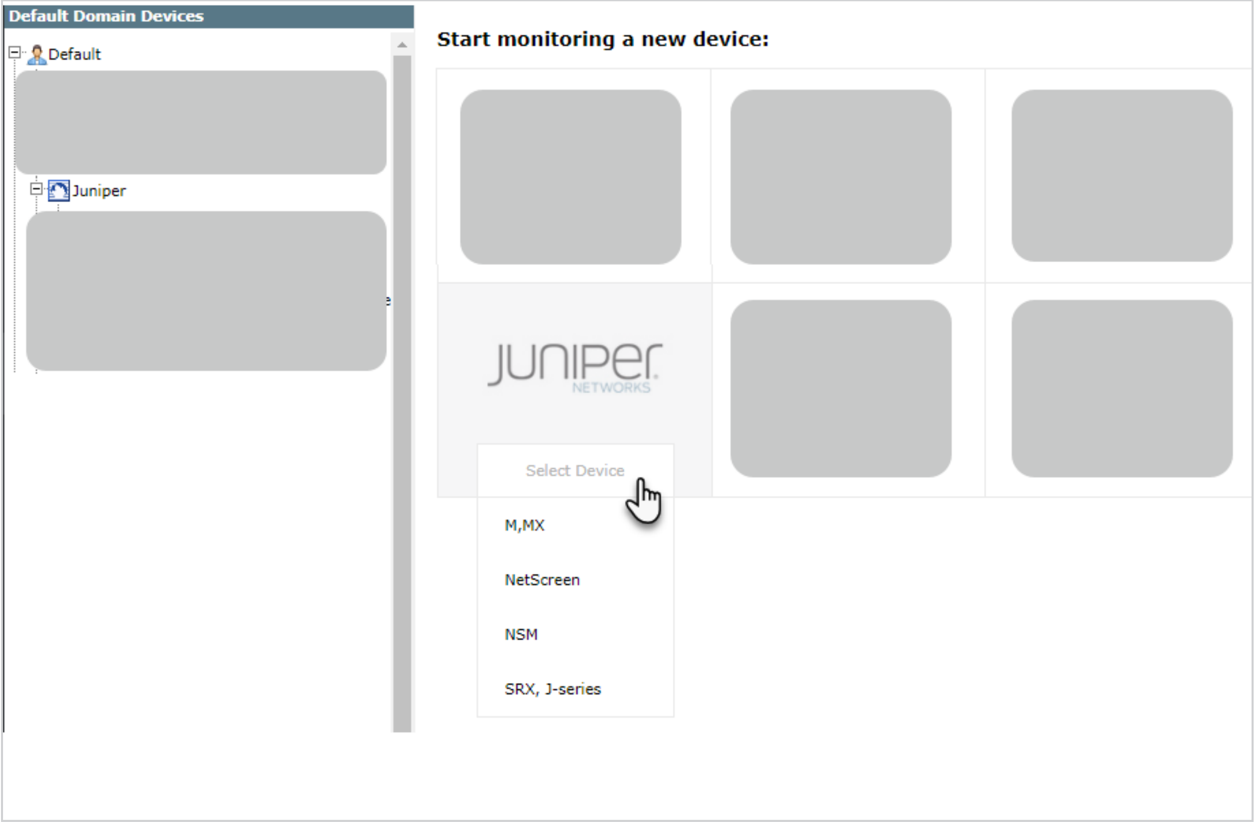
- Permissions

```
set system login class stClass
permissions view-configuration
permissions secret
allow-commands "set cli screen-width"
allow-commands "show *"
set cli logical-system <lsys>
clear cli logical-system
```

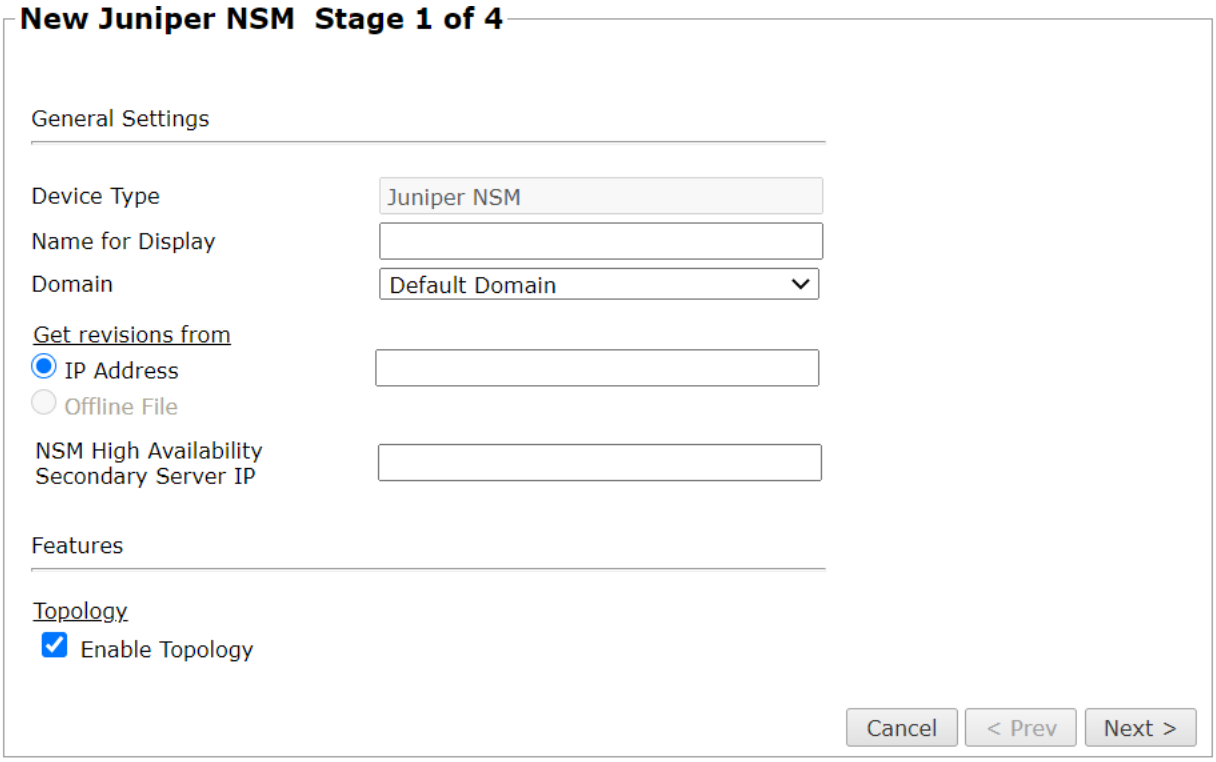
Monitor a NSM Device

To configure TOS Classic to monitor the policy revisions of a NSM device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select **NSM**.



3. Configure the device settings:



New Juniper NSM Stage 1 of 4

General Settings

Device Type: Juniper NSM

Name for Display:

Domain: Default Domain

Get revisions from

● IP Address

○ Offline File

NSM High Availability Secondary Server IP:

Features

Topology

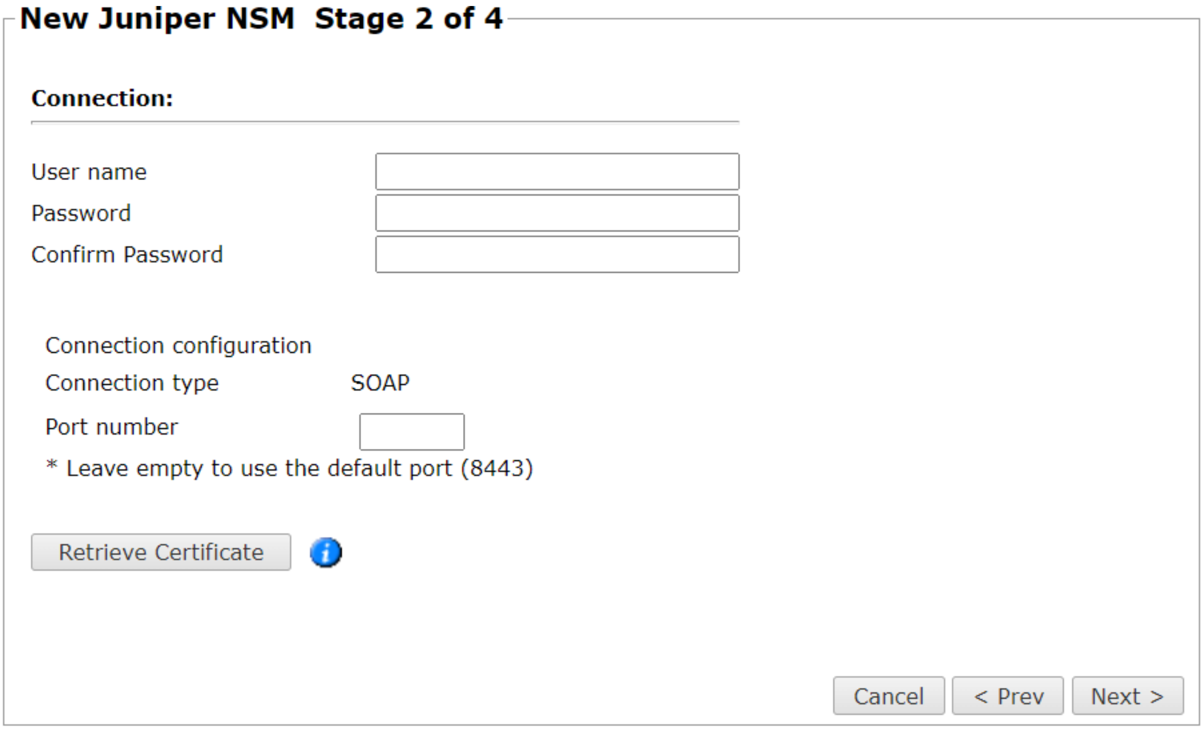
☑ Enable Topology

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- Get revisions from **IP Address**

  For **IP Address**, if TOS Classic is configured or will be configured as a syslog server for the NSM, make sure to use the same Juniper device IP address here as is configured in the NSM.
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- **NSM High Availability Secondary Server IP**: For an NSM HA cluster, enter the IP address of the secondary server. If you change the primary IP address for an NSM HA cluster, you must retrieve the certificate again on the next page.
- **Enable Topology**: Collects routing information for building the network Interactive Map.

  Topology options for **Advanced management** mode are configured when you import managed devices.

4. Click **Next**.
5. Configure the TOS Classic connection to the NSM device, according to the parameters required by the device:



New Juniper NSM Stage 2 of 4

Connection:

User name

Password

Confirm Password

Connection configuration

Connection type SOAP

Port number

* Leave empty to use the default port (8443)

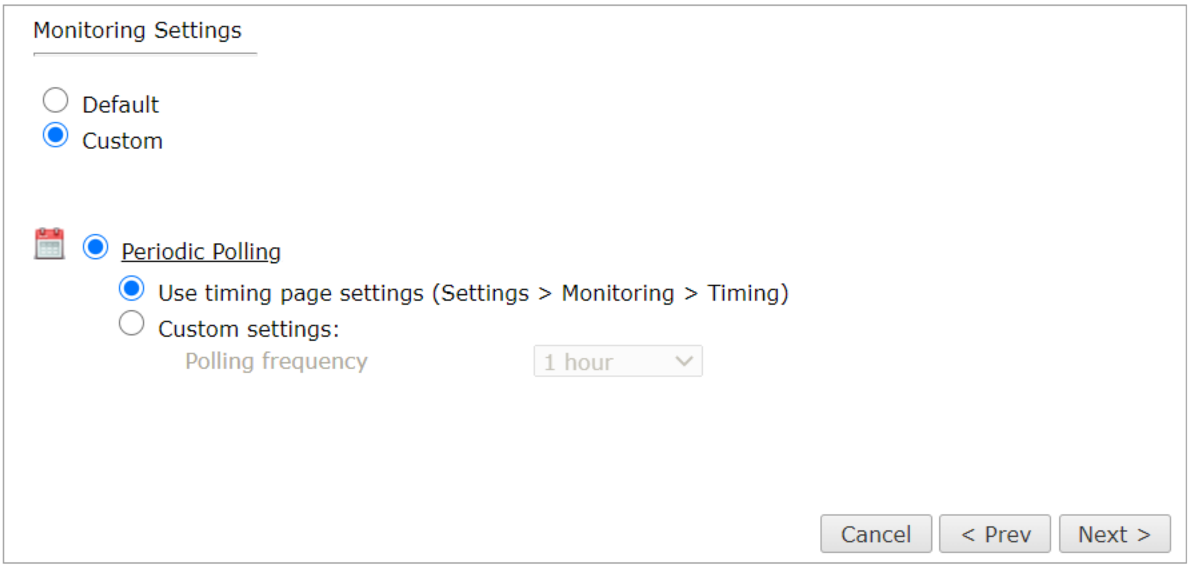
Make sure you have a user configured on the device with the privileges required by TOS Classic. See the prerequisites section for a list of required privileges.

- Enter the authentication details (**User name** and **Password**) needed to connect to the NSM device.
- TOS Classic connects to NSM devices with the SOAP protocol. To use default settings (recommended in most cases), leave the **Port number** blank.
- Click **Retrieve Certificate** to setup encrypted communication between TOS Classic and the NSM device.

  The certificate appears, and the following message is displayed:

  The certificate was retrieved successfully.

6. Click **Next**.
7. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default

● Custom

● Periodic Polling

● Use timing page settings (Settings > Monitoring > Timing)

○ Custom settings:

Polling frequency 1 hour

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

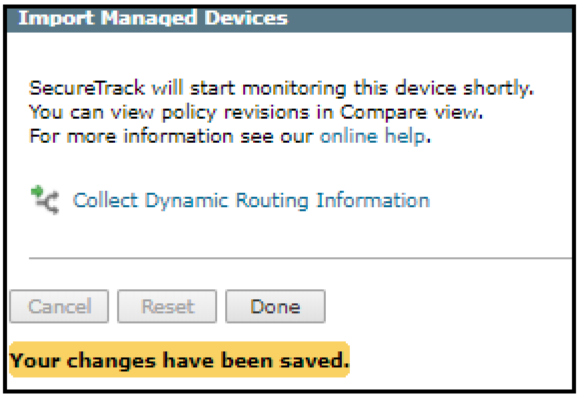
8. Click **Next**.
9. **Save** the configuration.

   The NSM device now appears in the **Monitored Devices** tree.

To import devices or domains managed by the NSM device into TOS Classic:

1. Make sure you receive the first NSM policy revision.
2. Select the NSM device from the device tree.
3. Click **Import Managed Devices** or **Import Domains and Managed Devices**.
4. From the list of devices managed by the NSM device, select the devices to import and click **Import**.
5. Do one of the following:
   - Click **Reset** to update the list of managed devices.
   - Click **Done** to return to the device tree.

     The managed devices appear under the NSM device in the device tree.
   - If available, click ⤨ to **Collect Dynamic Routing Information** for the managed devices.



Import Managed Devices

SecureTrack will start monitoring this device shortly.
You can view policy revisions in Compare view.
For more information see our online help.

Your changes have been saved.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Juniper SRX or J Series Devices

TOS Classic monitors SRX or J Series devices for policy revision changes. To see which TOS features are supported for your device, review the feature support table.

Prerequisites

Before you add the device to TOS Classic:

1. SecureTrack and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.
2. Make sure that the Juniper device user account permission to run the following commands:
   - Retrieve revision

```
show configuration
show configuration policy-options
show system uptime
show version
show configuration system
```

   - Virtual context

```
show logical-system
```

- Dynamic topology

```
show configuration routing-instances
show route active-path
show interfaces terse
show vrrp
show interfaces
show bgp neighbor
```

- Provisioning

```
SET
EDIT
INSERT
DELETE
EXIT
```

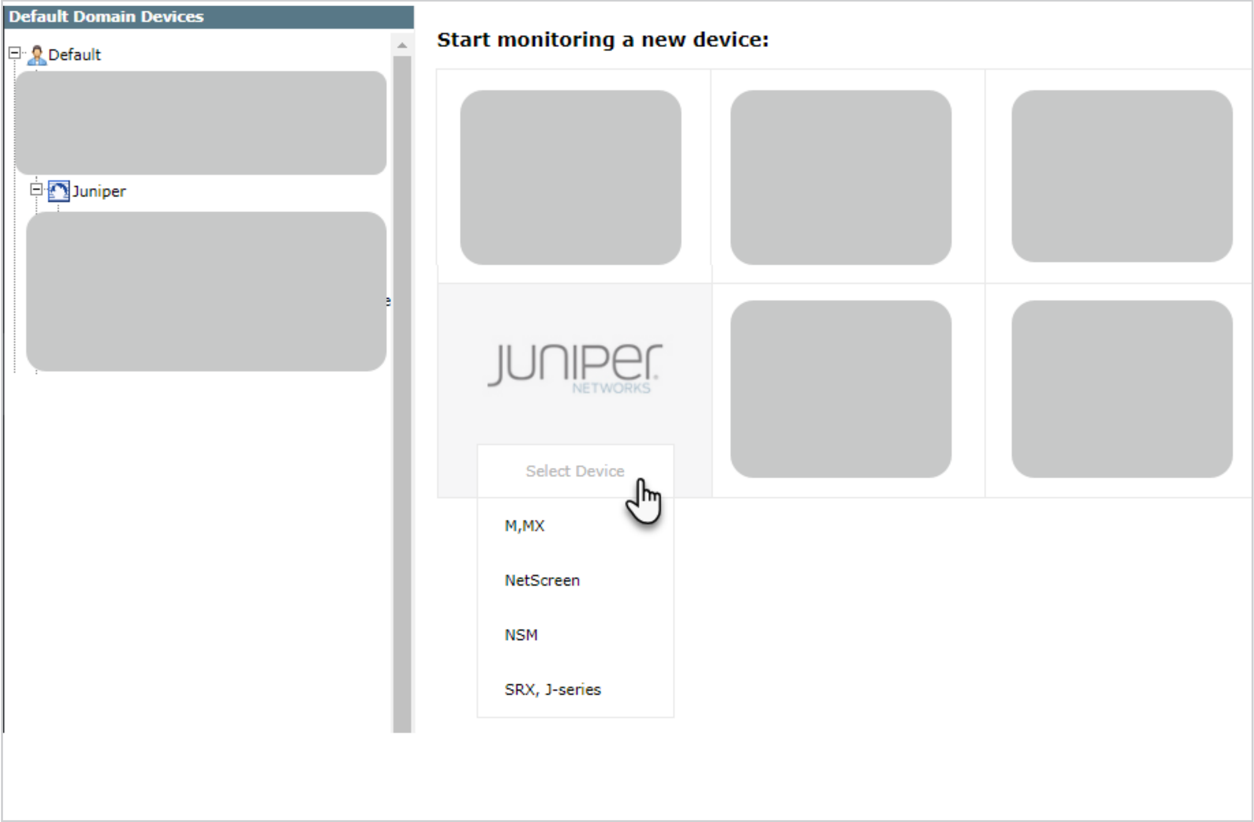
- Export versions of JunOS devices may not support SSH.

3. If you want to use commit scripts, update `stconf` as follows:

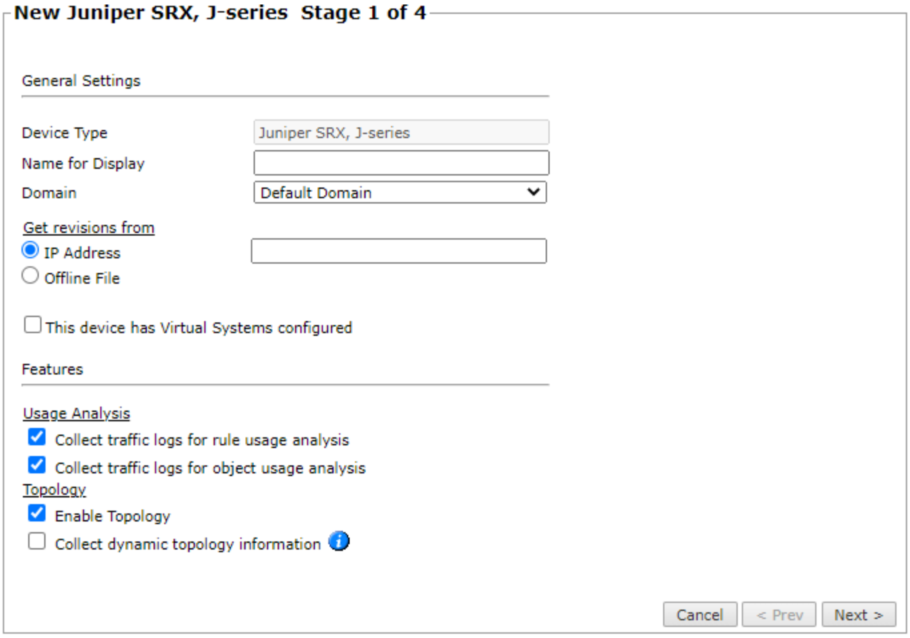
```
<JunOS_Use_Commit_Scripts>
       <management_ids>16,17,18,19,20,21, 22,23,24,25</management_ids>
</JunOS_Use_Commit_Scripts>
```

Adding an SRX or J Series Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select **SRX, J-Series**.



3. Configure the device settings:



New Juniper SRX, J-series Stage 1 of 4

General Settings

Device Type	Juniper SRX, J-series
Name for Display	
Domain	Default Domain

Get revisions from
● IP Address
○ Offline File

□ This device has Virtual Systems configured

Features

Usage Analysis
☑ Collect traffic logs for rule usage analysis
☑ Collect traffic logs for object usage analysis

Topology
☑ Enable Topology
□ Collect dynamic topology information

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically
  - **Offline File**: (If available) Revisions are manually uploaded to SecureTrack for Offline Analysis

For **IP Address**, if SecureTrack is configured or will be configured as a syslog server for the NSM, make sure to use the same Juniper device IP address here as is configured in the NSM.

- **This device has Virtual Systems configured**: Select to enable adding and monitoring Virtual Systems.

  If you have virtual systems, you can monitor clustered Netscreen devices. You can only do this when you first add the device to SecureTrack. To monitor a Netscreen cluster that has virtual systems, select **This device has Virtual Systems configured** and select **Cluster**.

- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- **Collect traffic logs for rule usage analysis** is necessary for Rule Usage reports.
  - **Collect traffic logs for object usage analysis** is necessary for reporting on unused objects and services in Rule Usage Reports.

  Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure SecureTrack to limit the number of days that data is kept.

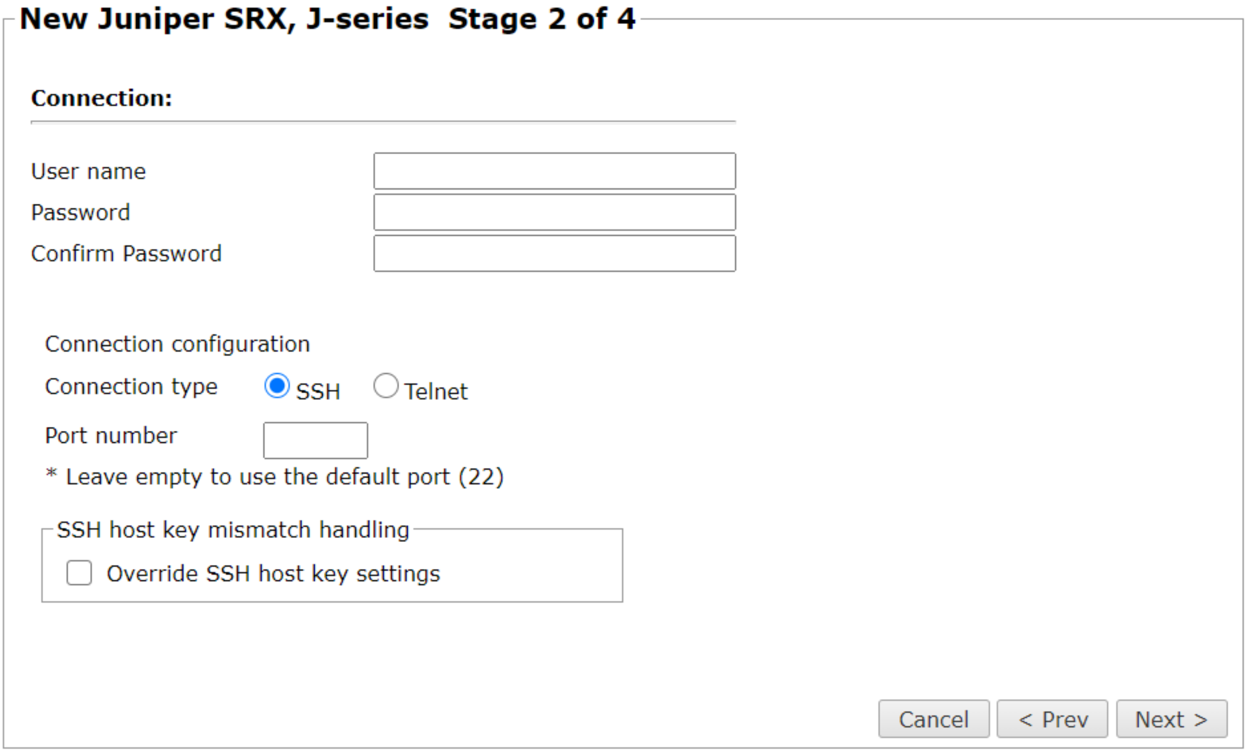
  We recommend that you enable SecureTrack administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, SecureTrack sends an alert.

- **Enable Topology**: Collects routing information for building the network Interactive Map.

  Topology options for **Advanced management** mode are configured when you import managed devices.

- **Collect dynamic topology information**: Select if the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF).

4. Click **Next**.
5. Configure the TOS Classic connection to the NSM device, according to the parameters required by the device:



New Juniper SRX, J-series Stage 2 of 4

Connection:

User name

Password

Confirm Password

Connection configuration

Connection type ● SSH ○ Telnet

Port number

* Leave empty to use the default port (22)

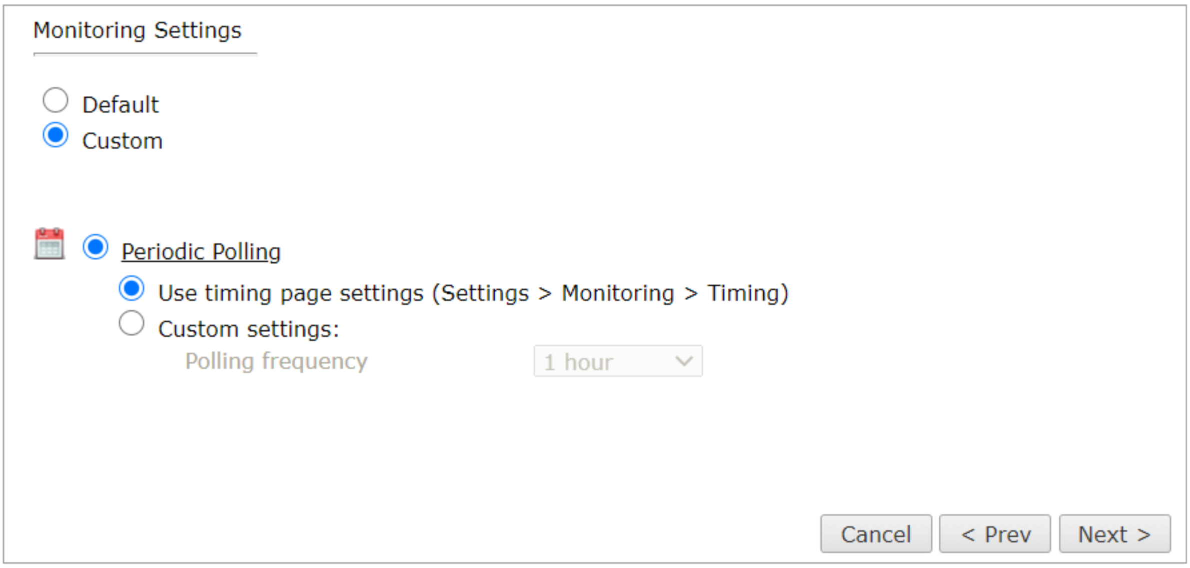
SSH host key mismatch handling

□ Override SSH host key settings

Make sure you have a user configured on the device with the privileges required by SecureTrack. See the prerequisites section for a list of required privileges.

- Enter the authentication details (**User name** and **Password**) needed to connect to the Juniper device.
- **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
  The device must be configured to use SSH version 2.

6. Click **Next**.
7. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency: 1 hour

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

8. Click **Next**.
9. **Save** the configuration.

   The device now appears in the **Monitored Devices** tree.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Configuring Juniper SRX Logging

Introduction

Tufin lets you configure Juniper SRX logging to occur at the beginning or end of a session with `session-init` or `session-close`.

By default, logging for both a new and an upgraded R18-3 installation occurs at the start of the session. If session processing is overloaded or backed-up, configure SRX logging to occur at the end of the session.

The Juniper logging option in StConf affects only the provisioning command logging for all the SRX devices managed in Secure Track.

How do I do it?

We recommend that you backup the stconf table prior to making any changes.

To configure the Juniper logging option for provisioning:

1. Navigate to: `https://<SecureTrack_IP>/securetrack/admin/stcgitest.htm`
2. Navigate to **Edit StConf > Fetch StConf**.
3. In the StConf file, navigate to the `<provisioning>` section and verify that the `<junos_log_options>` flag is present.
4. If the `<junos_log_options>` flag is not present, manually insert it into the `<provisioning>` section.
5. In the `<provisioning>` section of the StConf file, set the `<junos_log_options>` flag to configure logging to occur at the beginning of the session `(session-init)` or at the end of the session (`session-close`).

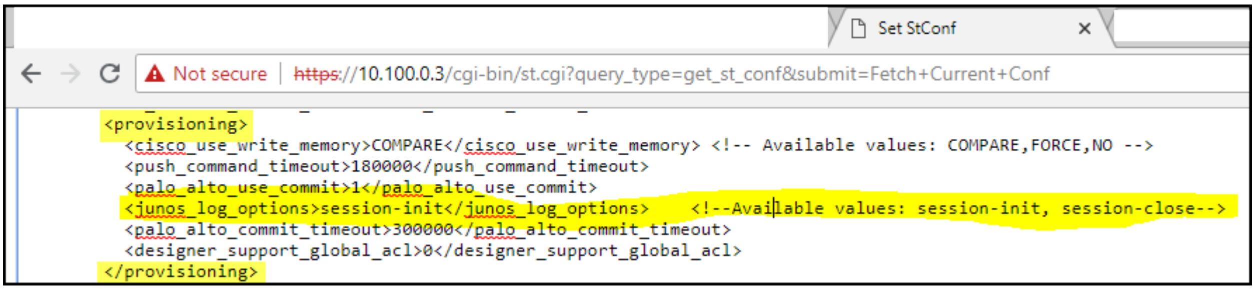
   The logging default is `session-init`
6. Click **Submit New Conf**.

Sample code

```
<provisioning>
 <junos_log_options>session-close</junos_log_options> <!--Available values: session-init, session-
```

```
close-->
</provisioning>
```

Example



Set StConf
Not secure
https://10.100.0.3/cgi-bin/st.cgi?query_type=get_st_conf&submit=Fetch+Current+Conf

```
<provisioning>
  <cisco_use_write_memory>COMPARE</cisco_use_write_memory> <!-- Available values: COMPARE,FORCE,NO -->
  <push_command_timeout>180000</push_command_timeout>
  <palo_alto_use_commit>1</palo_alto_use_commit>
  <junos_log_options>session-init</junos_log_options>    <!--Available values: session-init, session-close-->
  <palo_alto_commit_timeout>300000</palo_alto_commit_timeout>
  <designer_support_global_acl>0</designer_support_global_acl>
</provisioning>
```

Adding Microsoft Azure Cloud Platform

Overview

TOS Classic monitors the Microsoft Azure Resource Manager (RM) platform for policy revision changes. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Prerequisites

To complete the Microsoft Azure configuration procedures, you must have the following connection information for Microsoft Azure Resource Manager:

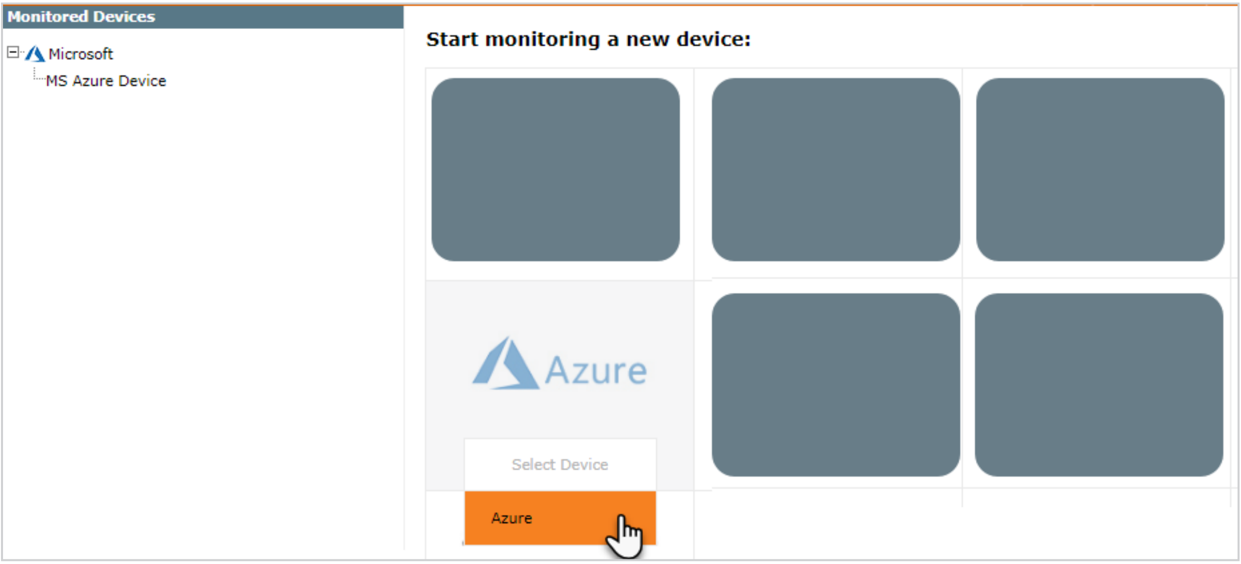
ID Information	Description
Subscription ID	The ID for an active Azure subscription - see Find your Azure subscription (Microsoft documentation)
Tenant ID	A Tenant represents a single organization, and is the dedicated instance of Azure Active Directory (AD) you receive when you sign up for Azure AD services. Each Tenant is completely isolated, and all your data and identity information is kept distinct and separate from other Tenants - see Get Tenant ID.
Application ID	An Application ID (also referred to as a Client ID) is the unique ID provided by Azure Active Directory (AD) for any registered application. You must register an application in your Tenant to authenticate the application to access to your network or data. See • Get application ID and authentication key • Create a Tufin application in Azure Active Directory • Assign Tufin application to Contributor role • Check Azure Active Directory permissions
Application Secret	An Application Secret (also known as a Client Secret, Shared Secret, or Keys) is credentials used by an application to authenticate itself to a Tenant when signing in to Azure AD - see Get application ID and authentication key. These keys do not refer to key vaults.

Additional information from Microsoft documentation:

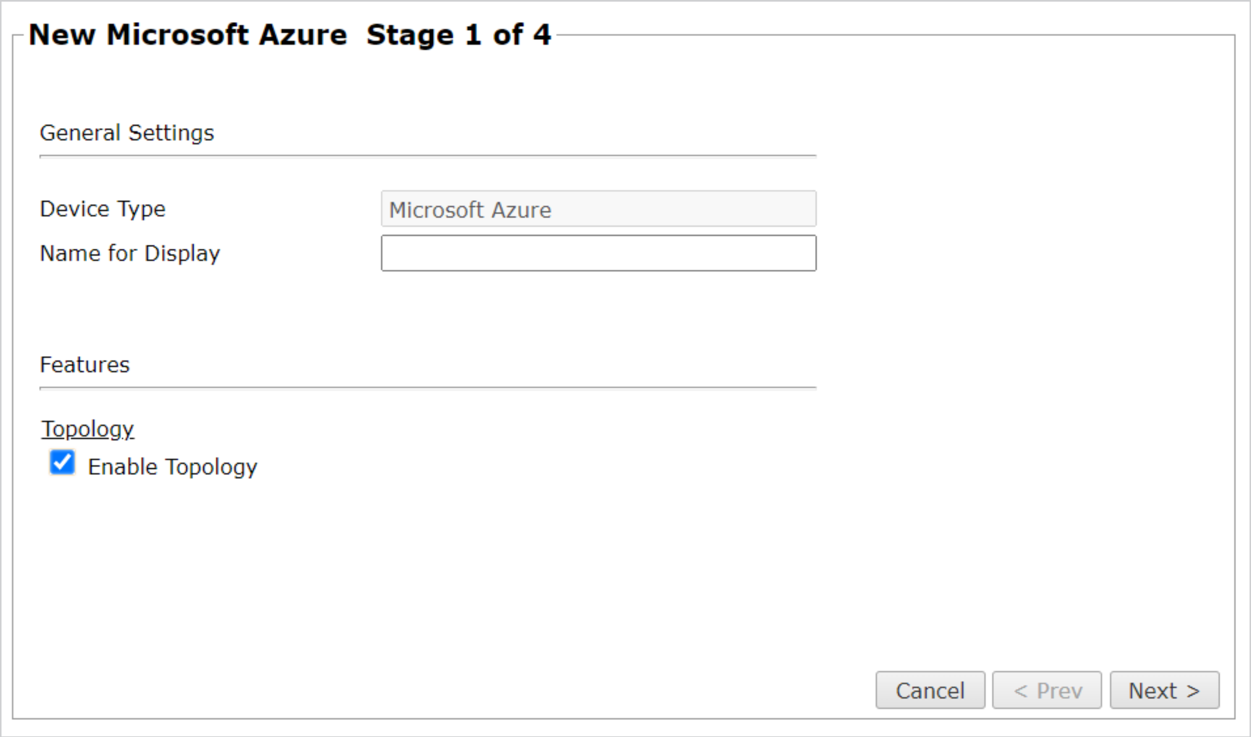
1. Azure management portal
2. Manage Resource Groups
3. Get Tenant ID

Adding a Microsoft Azure Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Microsoft Azure Stage 1 of 4

General Settings

Device Type	Microsoft Azure
Name for Display	

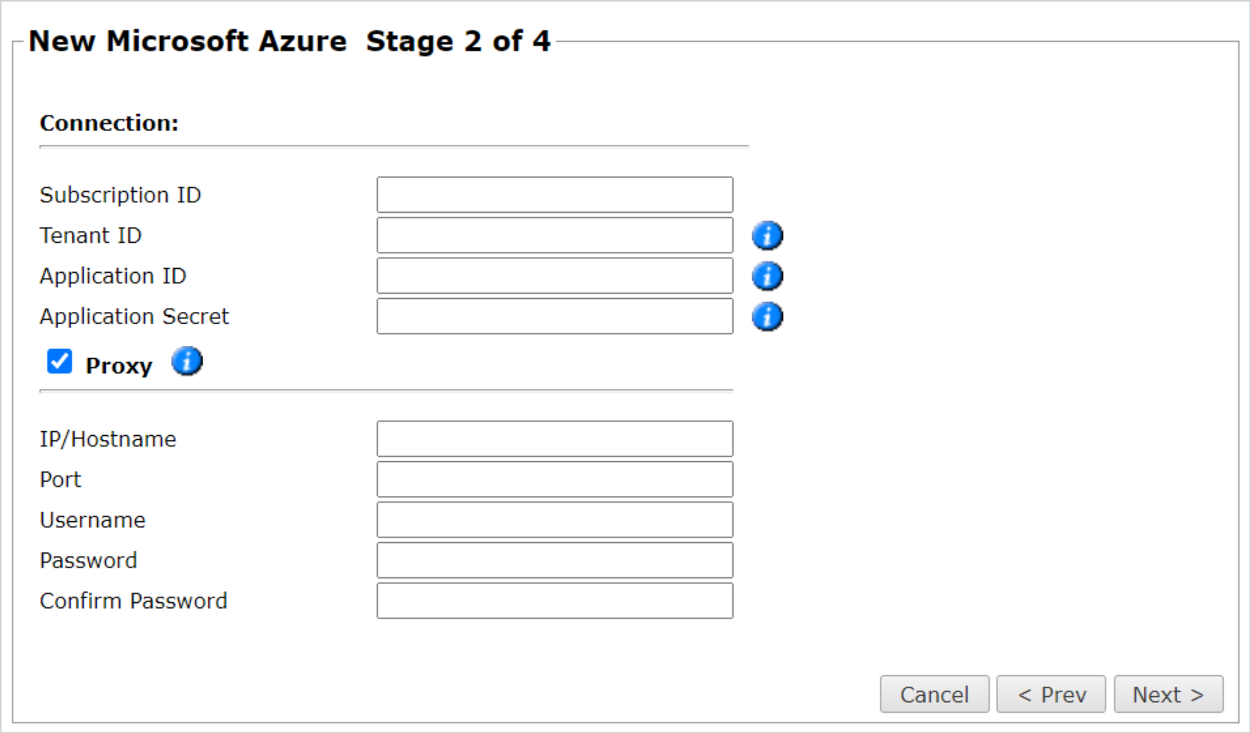
Features

Topology

☑ Enable Topology

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Enable Topology**: Collects routing information for building the network Interactive Map.

4. Click **Next**.
5. Configure the TOS Classic connection to the Microsoft Azure device, according to the parameters required by the device:



New Microsoft Azure Stage 2 of 4

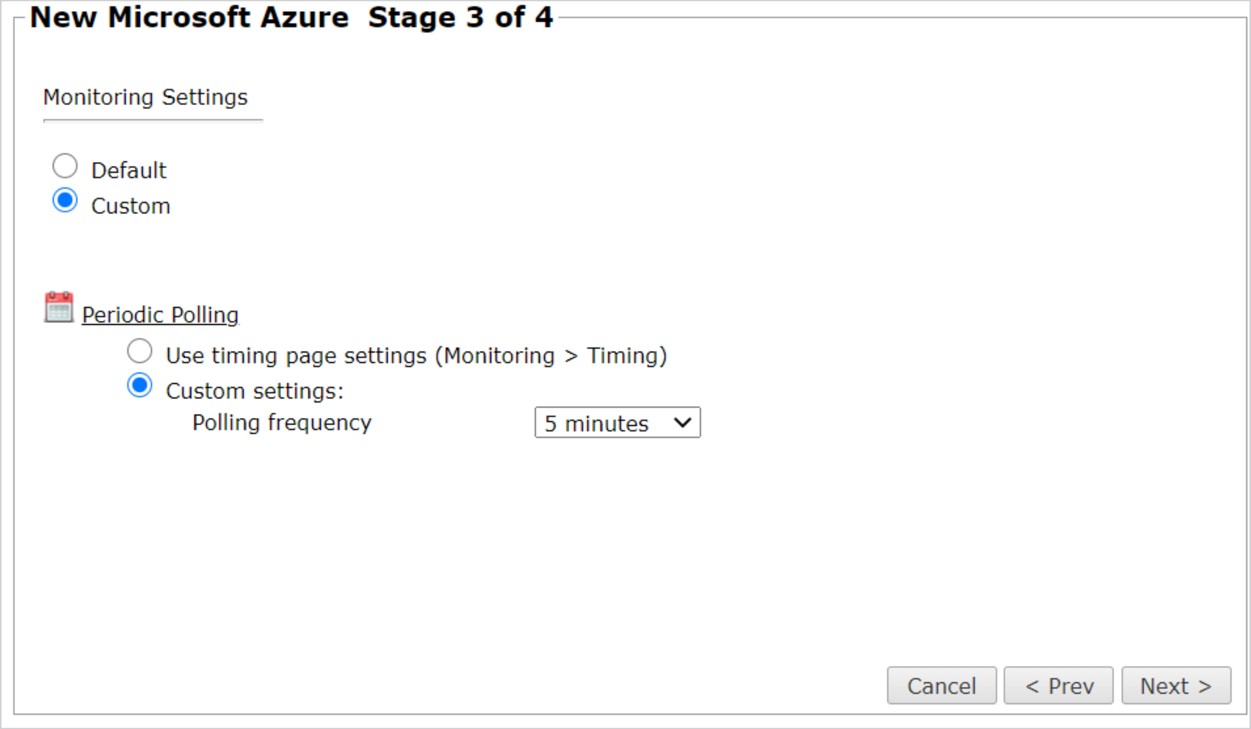
Connection:

Subscription ID	
Tenant ID	
Application ID	
Application Secret	

☑ **Proxy**

IP/Hostname	
Port	
Username	
Password	
Confirm Password	

6. If you connect to the device with a proxy server, select **Proxy** and enter the Hostname, Port, Username, and Password.
7. Click **Next**.
8. In **Monitoring Settings**, do one of the following:



New Microsoft Azure Stage 3 of 4

Monitoring Settings

○ Default
● Custom

Periodic Polling

○ Use timing page settings (Monitoring > Timing)
● Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

- In **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

9. Click **Next**.

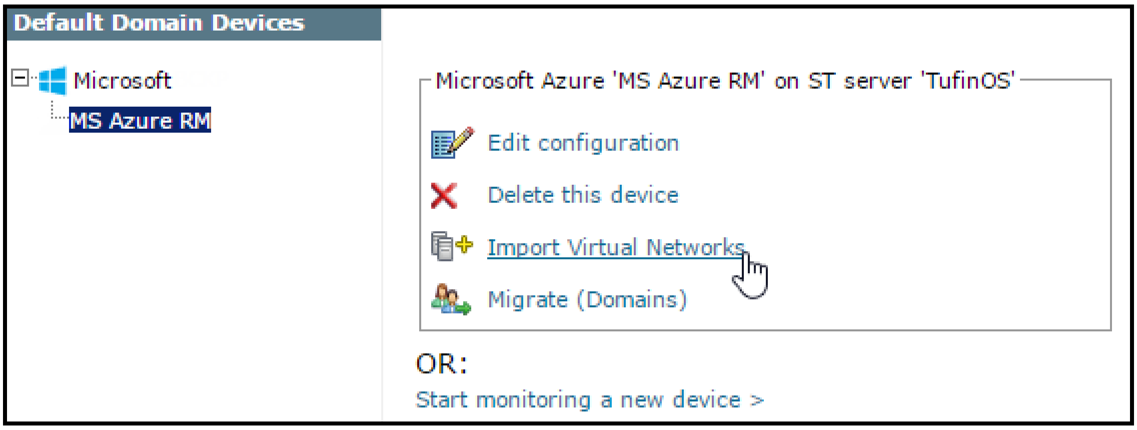
10. **Save** the configuration.

    The Microsoft Azure device now appears in the **Monitored Devices** tree.

11. To manually add Virtual Networks to your device, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the Virtual Networks:

    a. In the **Monitored Devices** tree, select the device. Only Virtual Networks with a vNic are imported.

    b. Click **Import Virtual Networks** (only enabled for **Manual Import**):



    c. Select all the Virtual Networks to be added.

    If the option to collect rule and object usage statistics for virtual contexts is available, it is enabled.

    If you do not want to collect these statistics, clear the options before you import the virtual contexts.

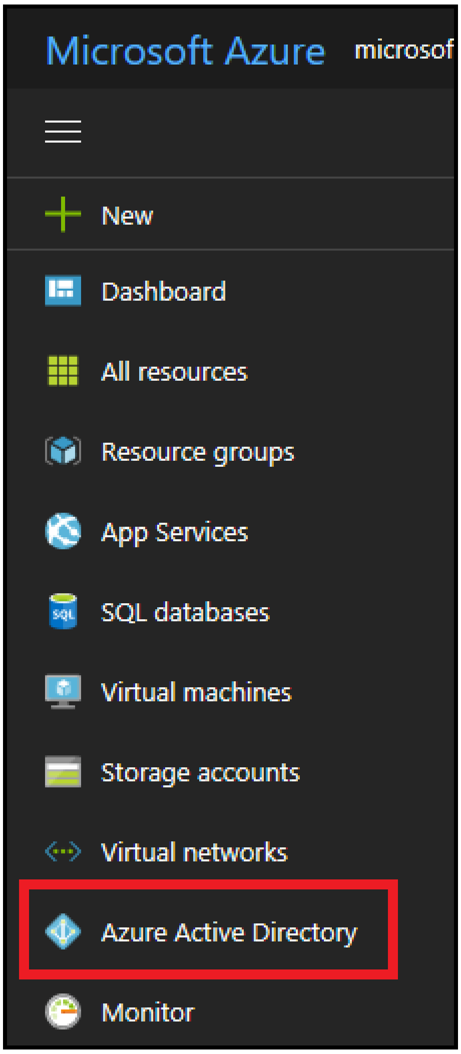
12. Click **Save**.

How Do I Get Here?

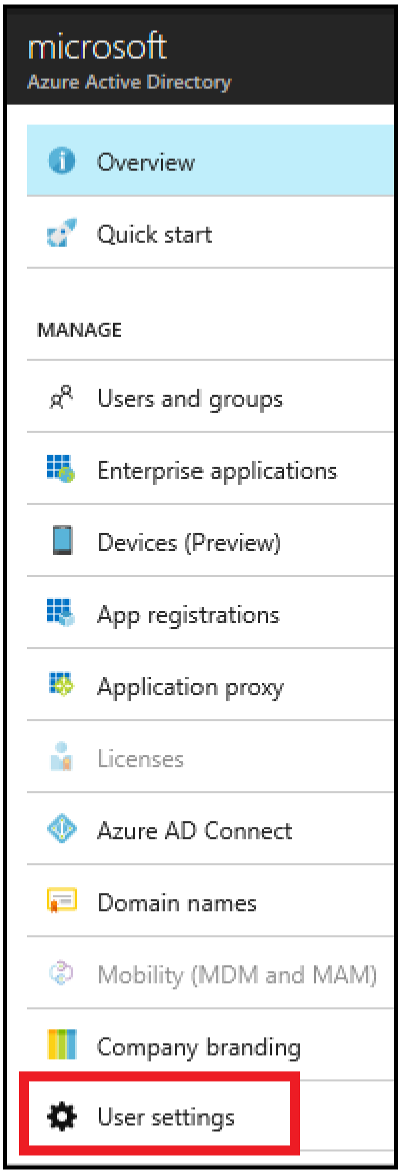
In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Check Azure Active Directory permissions

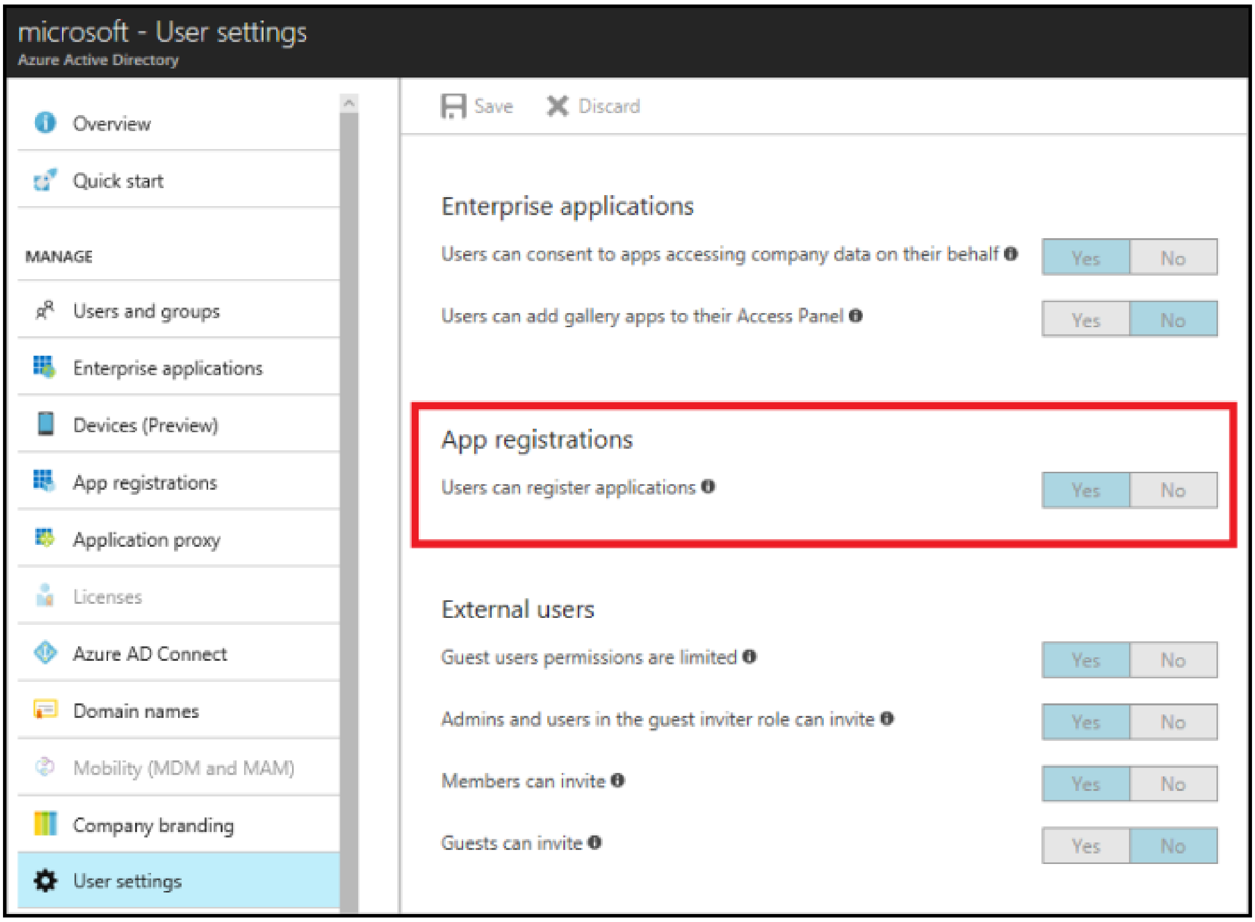
1. Log in to your Azure Account through the Azure portal.
2. Select **Azure Active Directory**.



3. In Azure Active Directory, select **User settings**.



4. Check the **App registrations** setting.
   - If **App registrations** is set to **Yes**, non-admin users can register AD apps. This setting means any user in the Azure AD tenant can register an app.
     You can proceed to Check Azure subscription permissions.



microsoft - User settings
Azure Active Directory

Enterprise applications

Users can consent to apps accessing company data on their behalf [✓ Yes] No

Users can add gallery apps to their Access Panel Yes [✓ No]

App registrations

Users can register applications [✓ Yes] No

External users

Guest users permissions are limited [✓ Yes] No

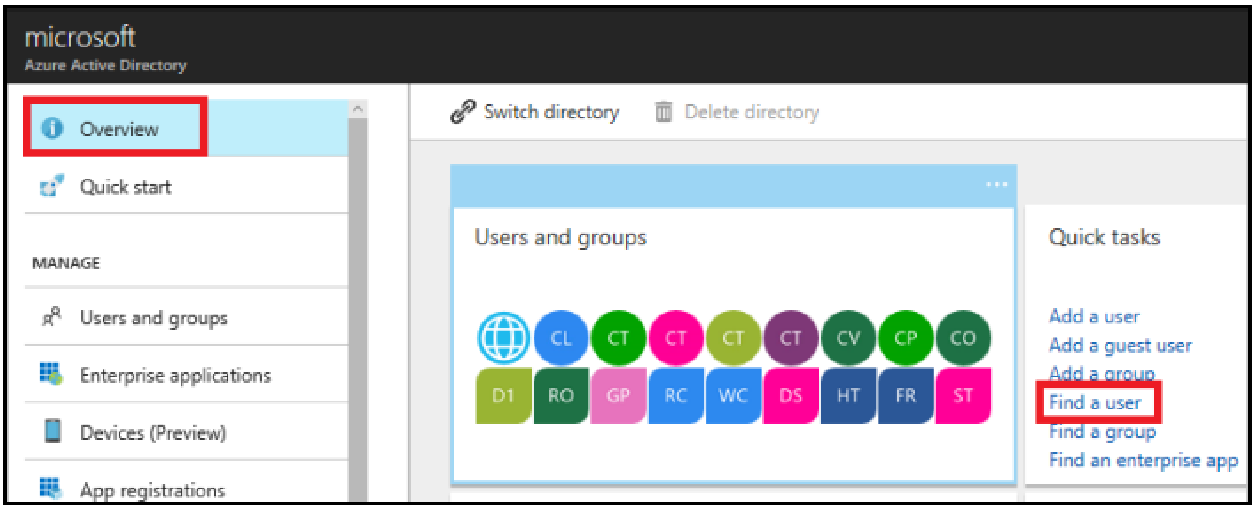
Admins and users in the guest inviter role can invite [✓ Yes] No

Members can invite [✓ Yes] No

Guests can invite Yes [✓ No]

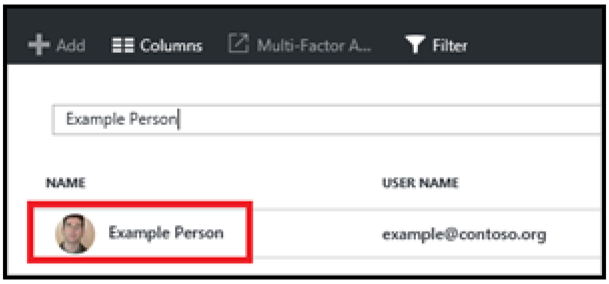
- If **App registrations** is set to **No**, only admin users can register apps: Check whether your account is an admin for the Azure AD tenant.

5. Select **Overview** and **Find a user** from **Quick tasks**.

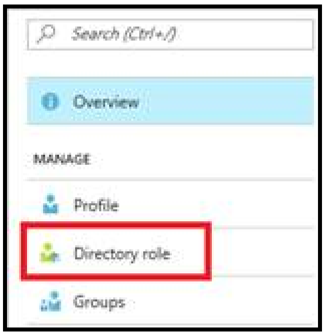


microsoft
Azure Active Directory

6. Search for your account, and select it when you find it.



7. For your account, select **Directory role**.

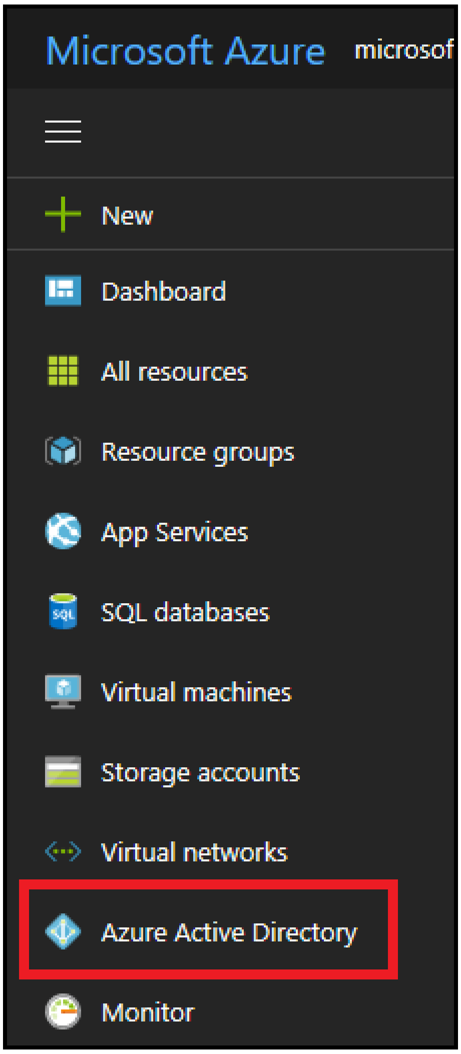


8. View your assigned directory role in Azure AD.

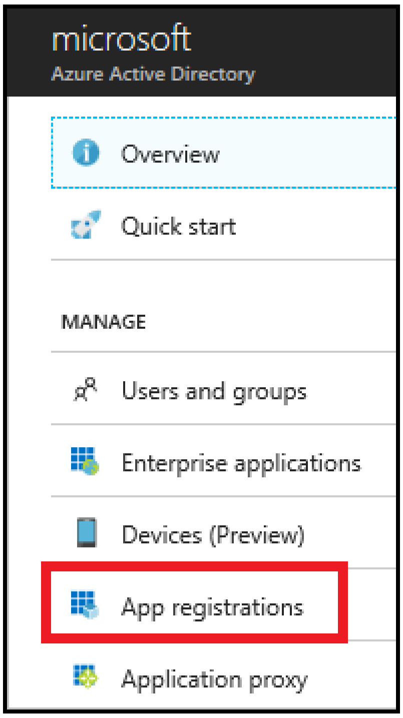
   If your account is assigned to the User role, but the app registration setting (from the preceding steps) is limited to admin users, ask your administrator to either assign you to an administrator role, or to enable users to register apps.

Create a Tufin application in Azure Active Directory

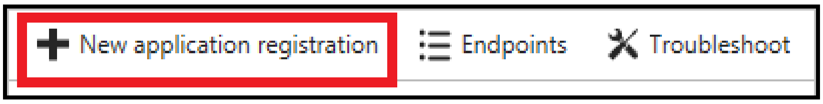
1. Log in to your Azure Account through the Azure portal.
2. Select **Azure Active Directory**.



3. In Azure Active Directory, select **App registrations**.



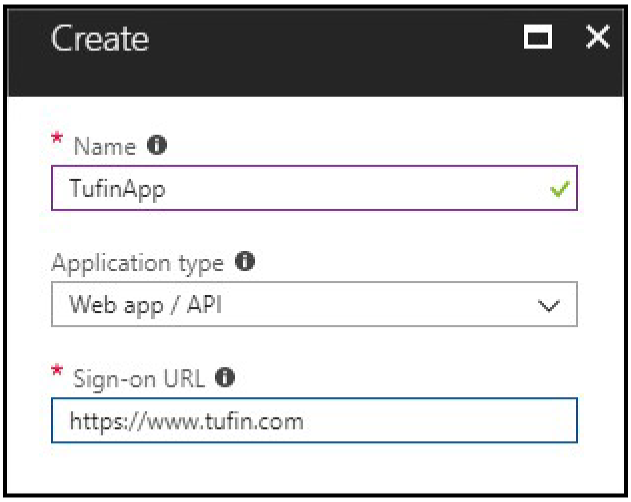
4. Select **New application registration**.



5. Type a name and a Redirect URI for the application.

   We recommend that you use your company's public domain URI.

6. In the **Application type** field, select **Web app/API**.
7. After setting the values, select **Create**.



* Name: TufinApp

Application type: Web app / API

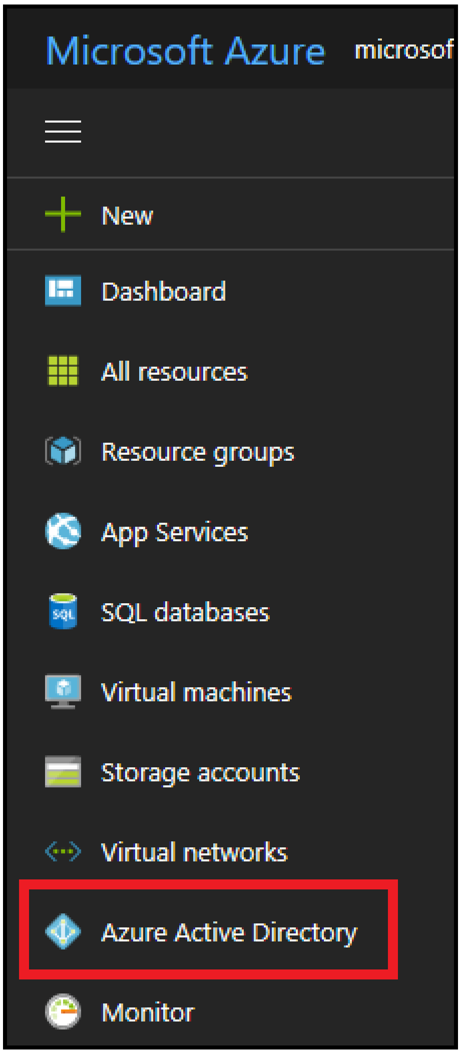
* Sign-on URL: https://www.tufin.com

Your application is created.

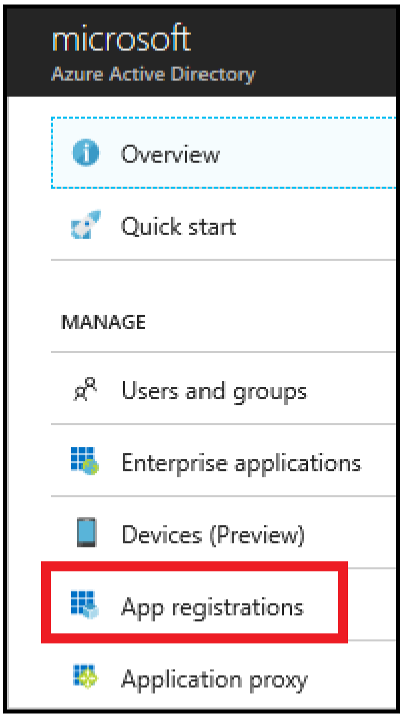
Get application ID and authentication key

When logging in programmatically, you need the ID for your application and an authentication key. To get those values, use the following steps:

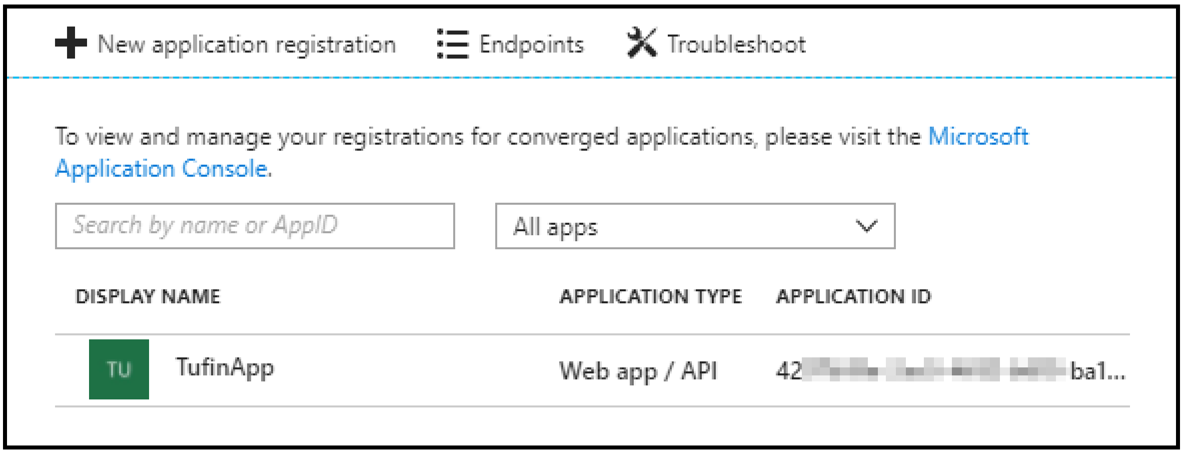
1. Log in to your Azure Account through the Azure portal.
2. Select **Azure Active Directory**.



3. In Azure Active Directory, select **App registrations**.



4. In Azure Active Directory > **App registrations**, select your application.

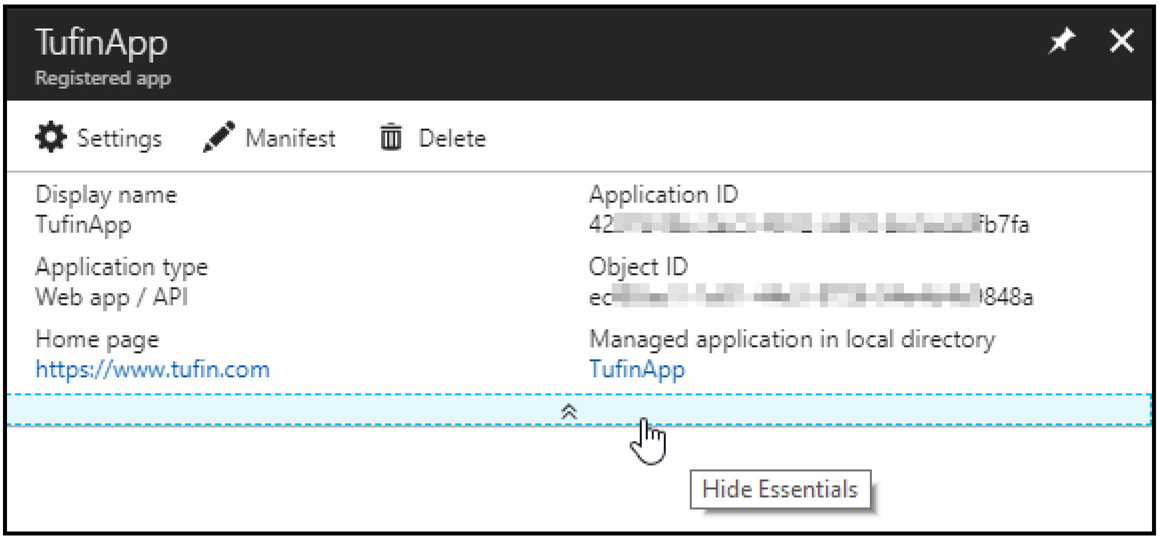


To view and manage your registrations for converged applications, please visit the Microsoft Application Console.

DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
TU TufinApp	Web app / API	42[redacted]ba1...

5. Copy the **Application ID** and store it.

   This value is the Azure **Application ID** in the Tufin wizard.



TufinApp
Registered app

Settings | Manifest | Delete

Display name
TufinApp

Application type
Web app / API

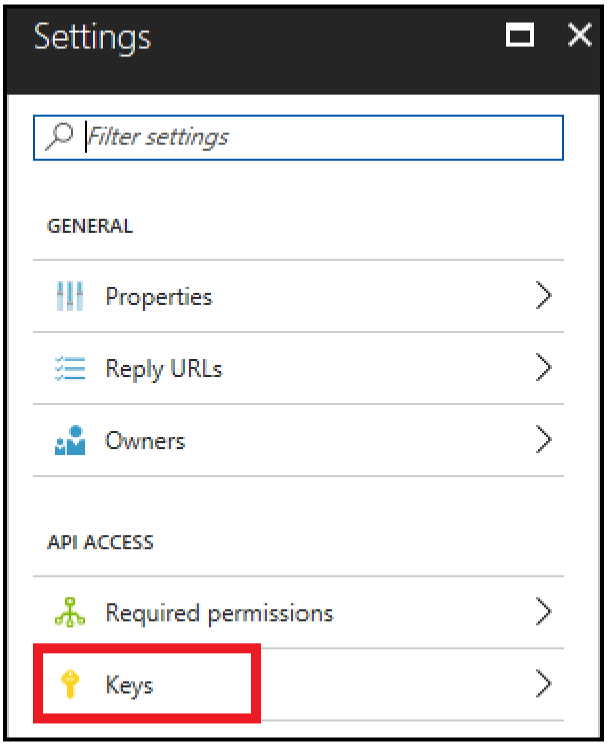
Home page
https://www.tufin.com

Application ID
42[redacted]fb7fa

Object ID
ec[redacted]848a

Managed application in local directory
TufinApp

6. In Settings, select **Keys** to generate an authentication key.



Settings

Filter settings

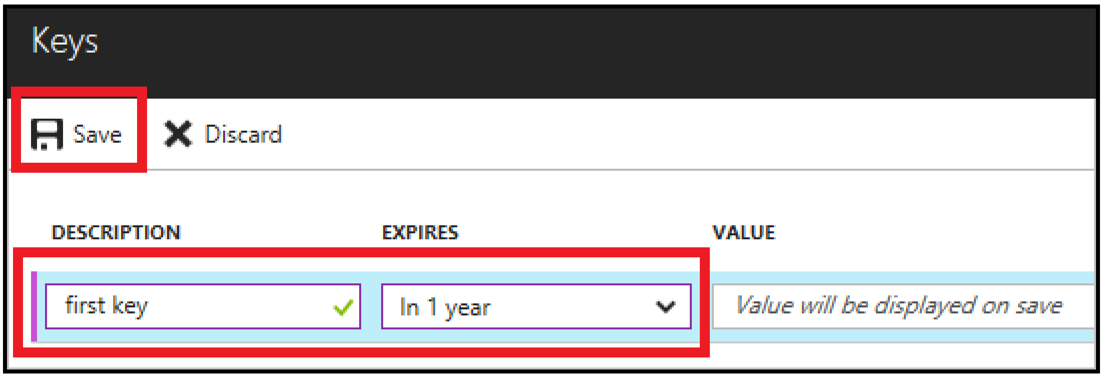
GENERAL

- Properties
- Reply URLs
- Owners

API ACCESS

- Required permissions
- Keys

7. Type a description and a duration for the key and select **Save**.



Keys

Save | Discard

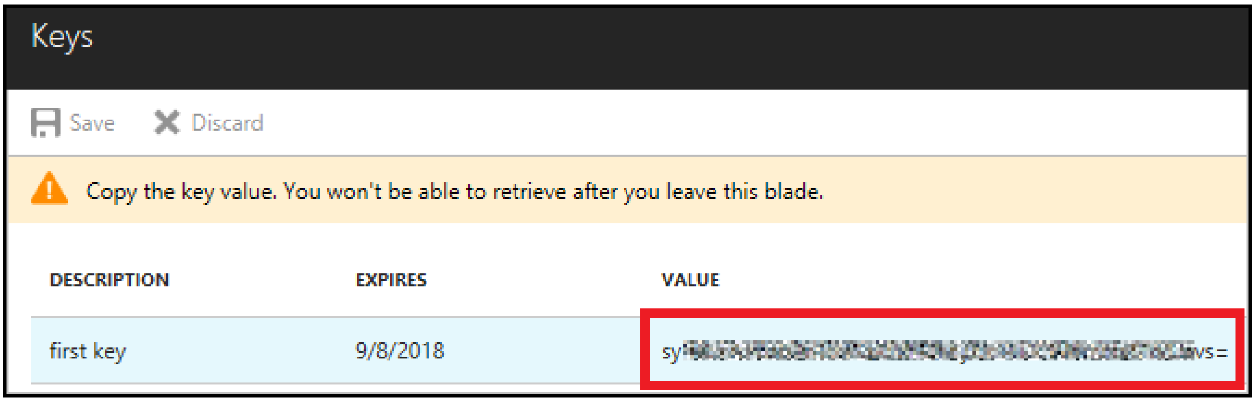
DESCRIPTION	EXPIRES	VALUE
first key	In 1 year	*Value will be displayed on save*

The key value is displayed after you save the key.

8. Copy the key value: You will not be able to retrieve the key later.

   You provide the key value with the application ID to log in as the application.

   This value is the Azure **Application Secret** in the Tufin wizard.



Keys

Save Discard

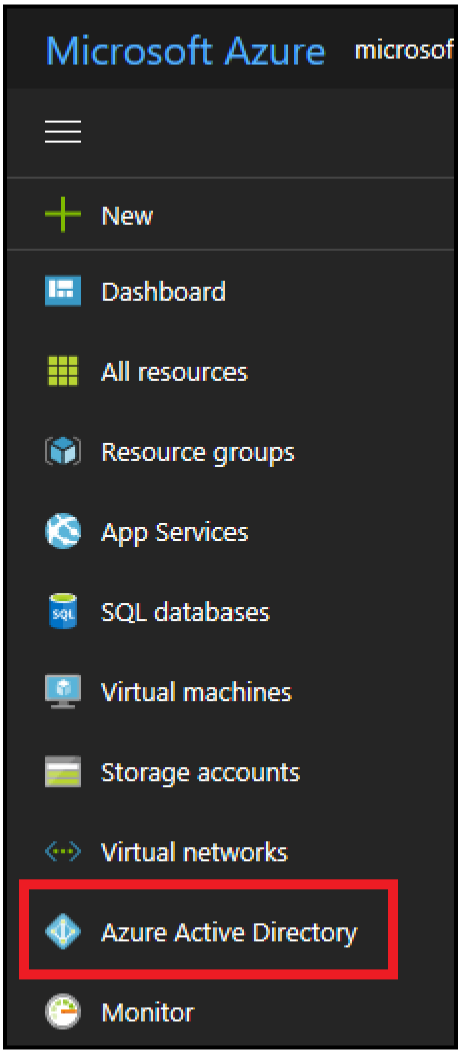
Copy the key value. You won't be able to retrieve after you leave this blade.

DESCRIPTION	EXPIRES	VALUE
first key	9/8/2018	sy[redacted]vs=

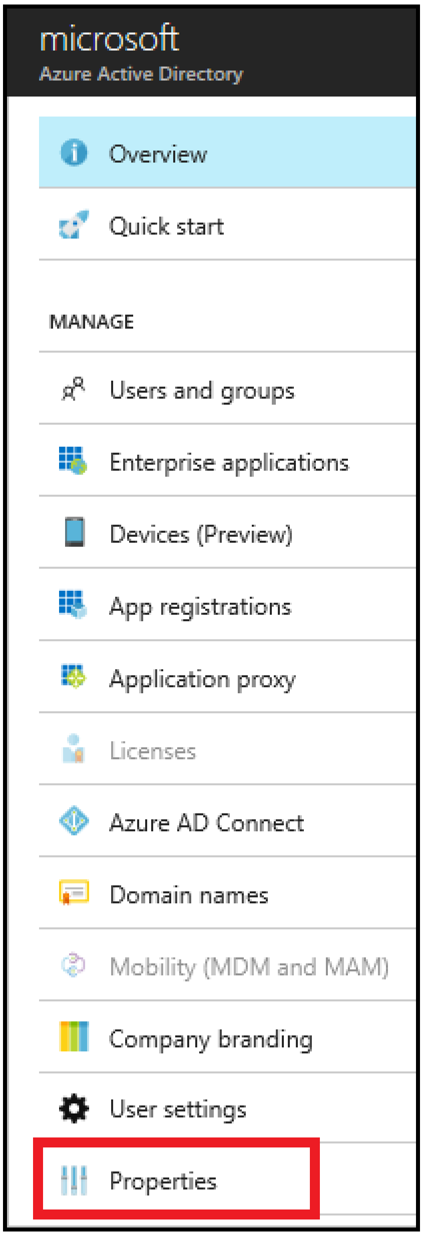
Get tenant ID

When logging in programmatically, you need to include the tenant ID with your authentication request. To get those values, use the following steps:

1. Log in to your Azure Account through the Azure portal.
2. Select **Azure Active Directory**.

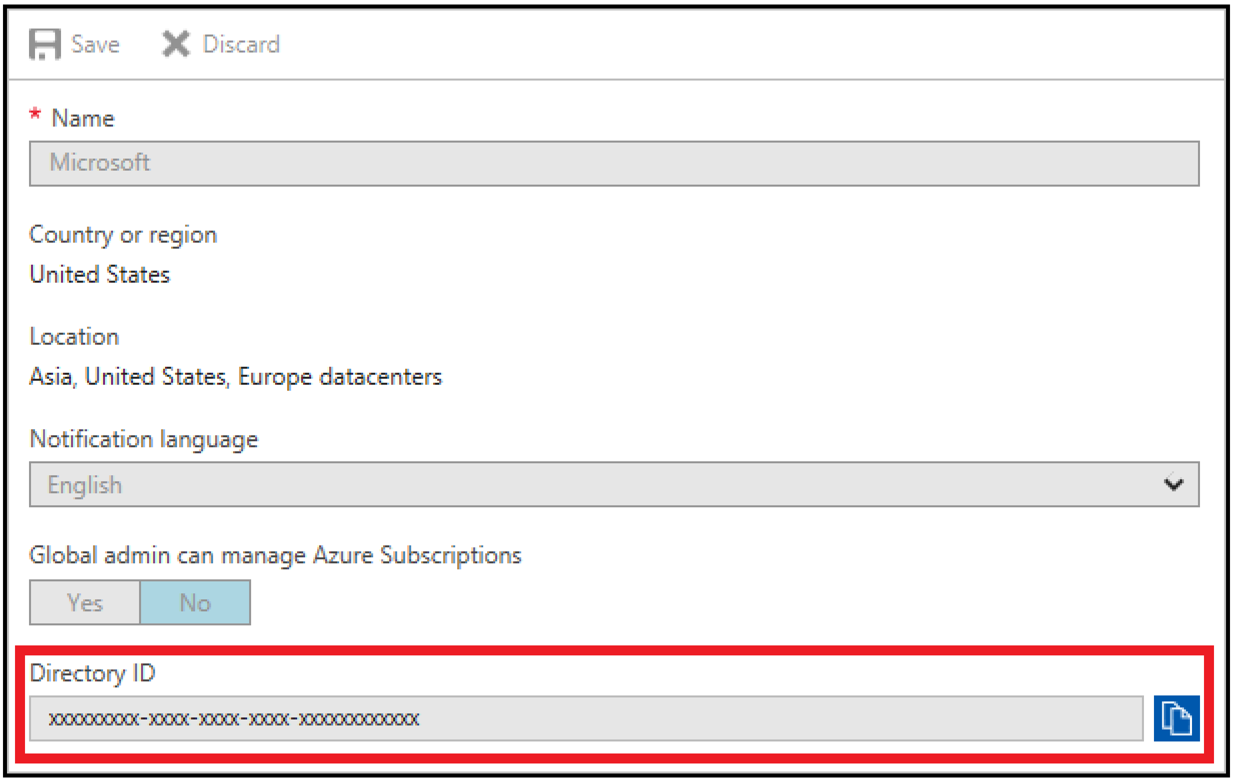


3. To get the tenant ID, select **Properties** for your Azure AD tenant.



4. Copy the **Directory ID**.

   This value is the Azure **tenant ID** in the Tufin wizard.



* Name

Microsoft

Country or region

United States

Location

Asia, United States, Europe datacenters

Notification language

English

Global admin can manage Azure Subscriptions

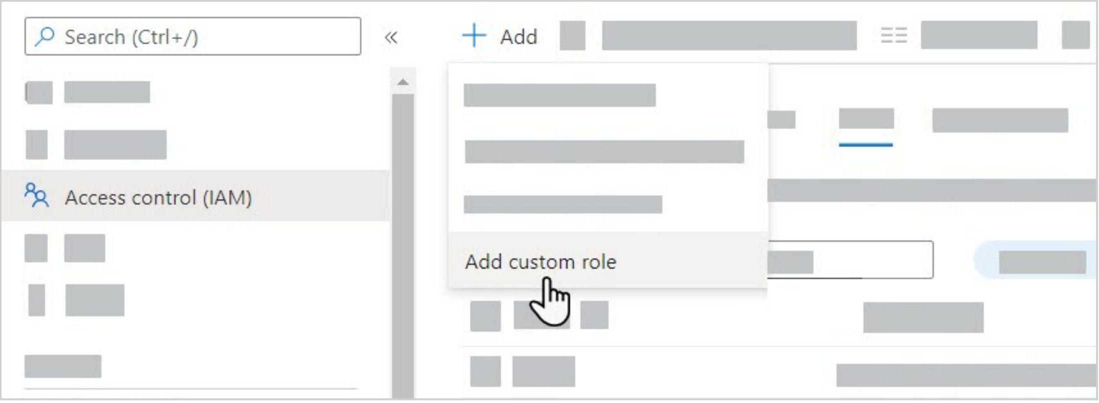
Yes [✓ No]

Directory ID

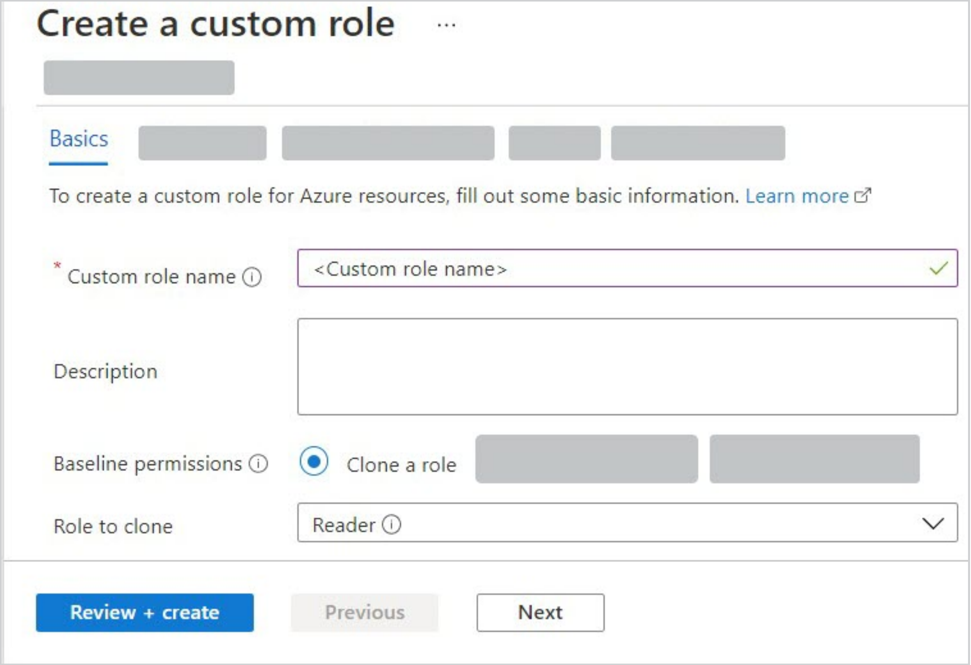
xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Configuring a Custom Role and Assigning it to a Tufin Application

1. Log in to your Azure Account through the Azure portal.
2. Go to the **Access Control** page, and click **Add** > **Add Custom Role**.



The Custom Role Editor is displayed.



Create a custom role ···

Basics

To create a custom role for Azure resources, fill out some basic information. Learn more

* Custom role name ⓘ <Custom role name> ✓

Description:

Baseline permissions ⓘ: ● Clone a role

Role to clone: Reader ⓘ

3. In the **Basics** tab, fill out the following information:

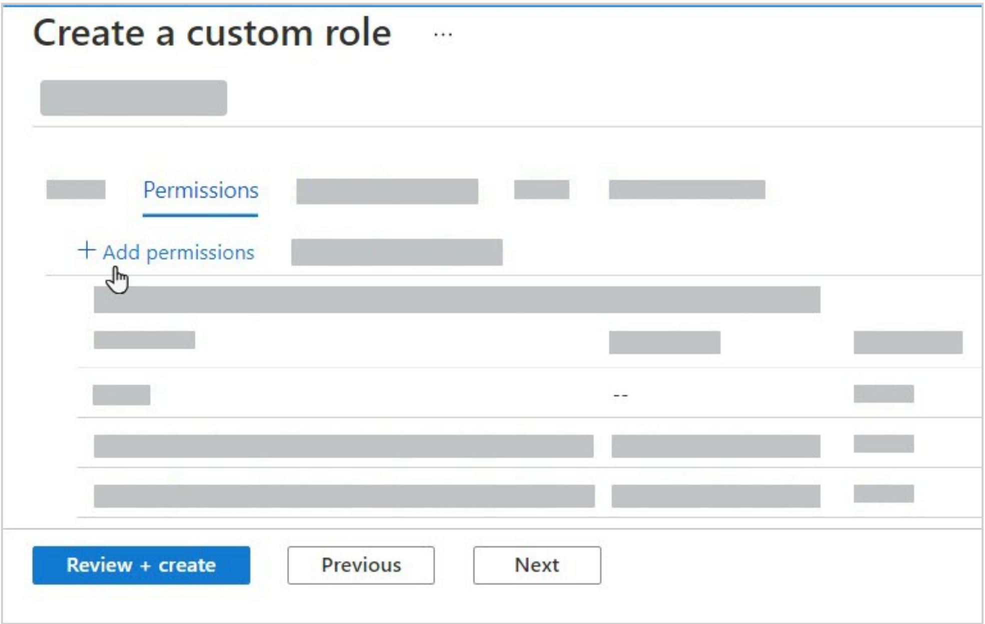
   a. **Custom role name** and **Description**: Enter a name and description for the custom role.

   b. **Baseline Permissions:** Select **Clone a role**.

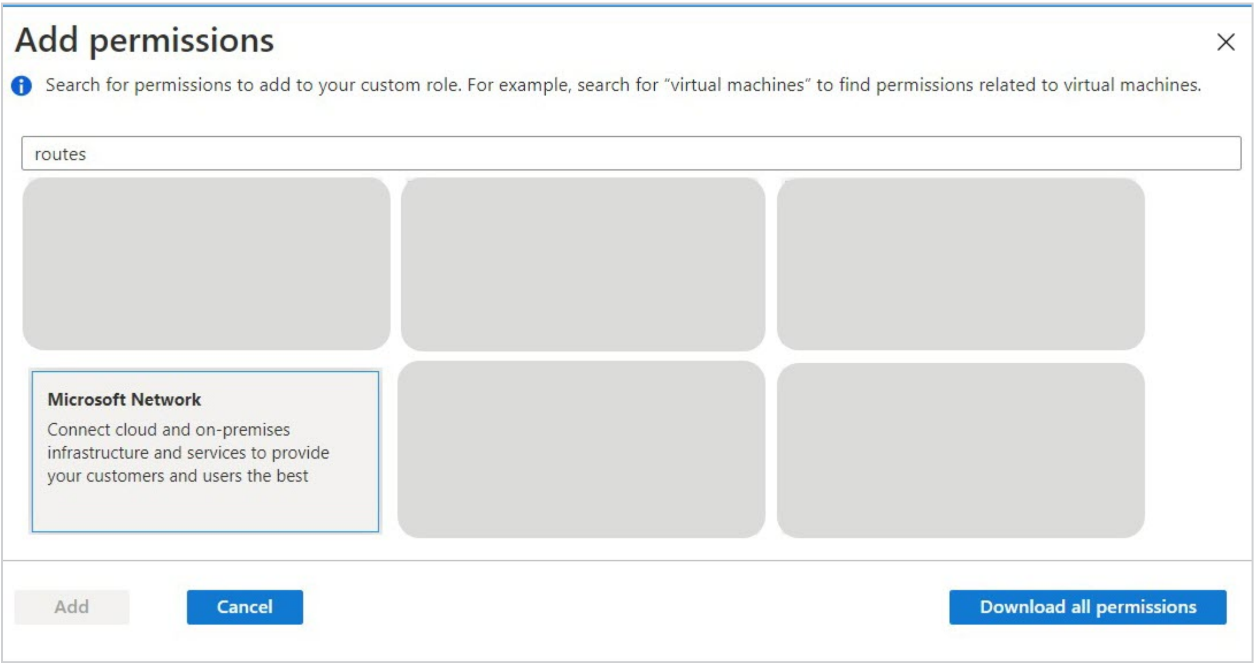
   c. **Role to clone:** Select **Reader.**

4. Click **Next** to move to the **Permissions** tab.

5. Click **Add Permissions**.



6. Search for **Microsoft Network**.



Add permissions

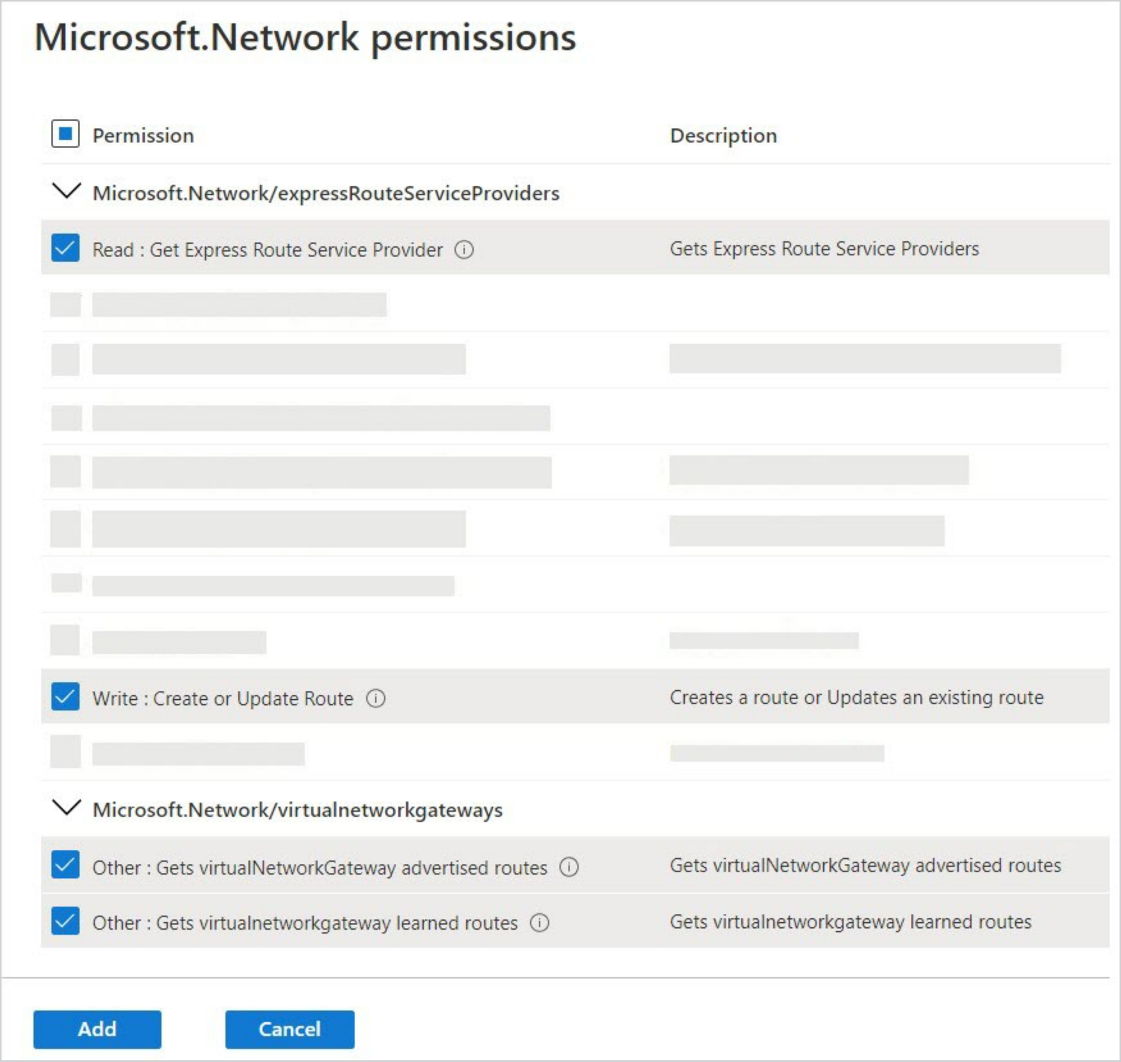
Search for permissions to add to your custom role. For example, search for "virtual machines" to find permissions related to virtual machines.

routes

Microsoft Network

Connect cloud and on-premises infrastructure and services to provide your customers and users the best

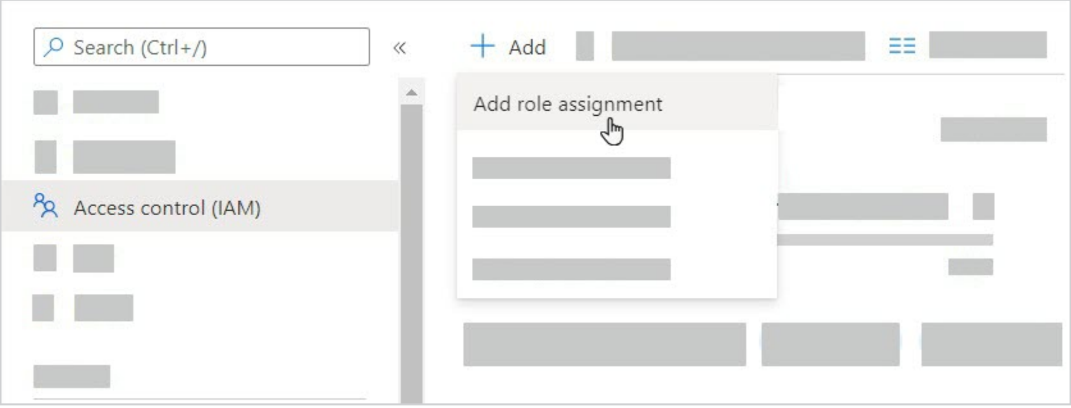
7. Click on the **Microsoft Network** tile, and select the following permissions:
   - `Read: Get Express Route Service Provider`
   - `Write: Create or Update Route`
   - `Other: Gets virtualNetworkGateway advertised routes`
   - `Other: Gets virtualnetworkgateway learned routes`



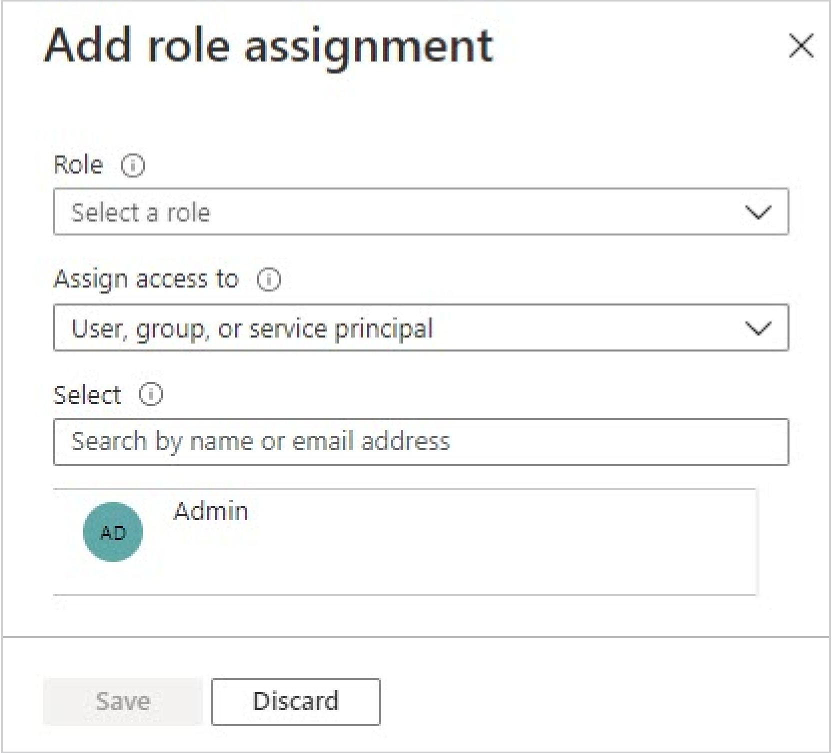
Microsoft.Network permissions

■ Permission	Description
Microsoft.Network/expressRouteServiceProviders	
☑ Read : Get Express Route Service Provider ⓘ	Gets Express Route Service Providers
☑ Write : Create or Update Route ⓘ	Creates a route or Updates an existing route
Microsoft.Network/virtualnetworkgateways	
☑ Other : Gets virtualNetworkGateway advertised routes ⓘ	Gets virtualNetworkGateway advertised routes
☑ Other : Gets virtualnetworkgateway learned routes ⓘ	Gets virtualnetworkgateway learned routes

8. Click **Add**.
9. Create the custom role by clicking **Review+Create**.
10. In the **Access Control** page, click **Add** > **Add Role Assignment.**



The **Add Role Assignment** pane is displayed.


Add role assignment

Role

Select a role

Assign access to

User, group, or service principal

Select

Search by name or email address

11. In the **Role** field, select the role you created.
12. In the **Select** field, select the SecureTrack App registration.
13. Click **Save**.

Adding TOP Devices

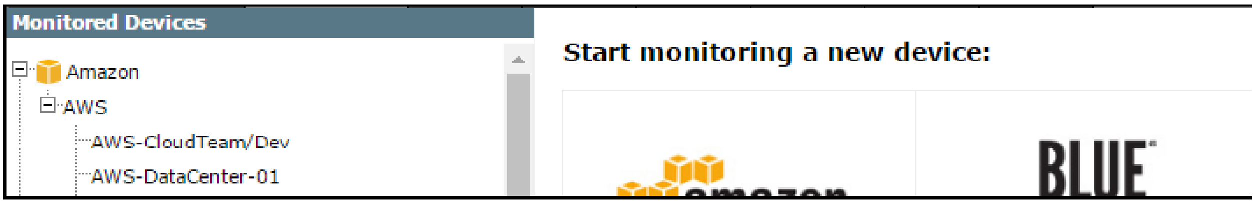
TOS Classic can monitor devices with vendor-specific TOP plugins. TOP plugins for Blue Coat ProxySG and Linux iptables come preinstalled in the current version of TOS Classic. TOP plugins for any other device type must be manually installed before adding devices of that type. To help you organize the information for your devices, you can use the device information worksheet.

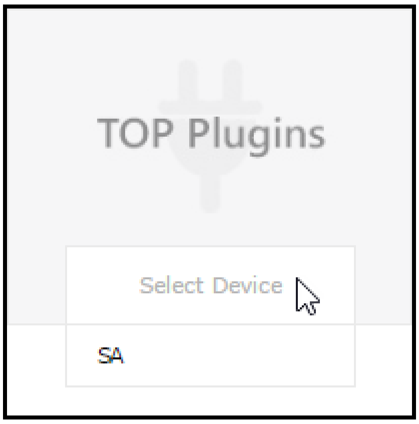
> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Monitor a TOP Device

To configure TOS Classic to monitor the policy revisions of a TOP device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



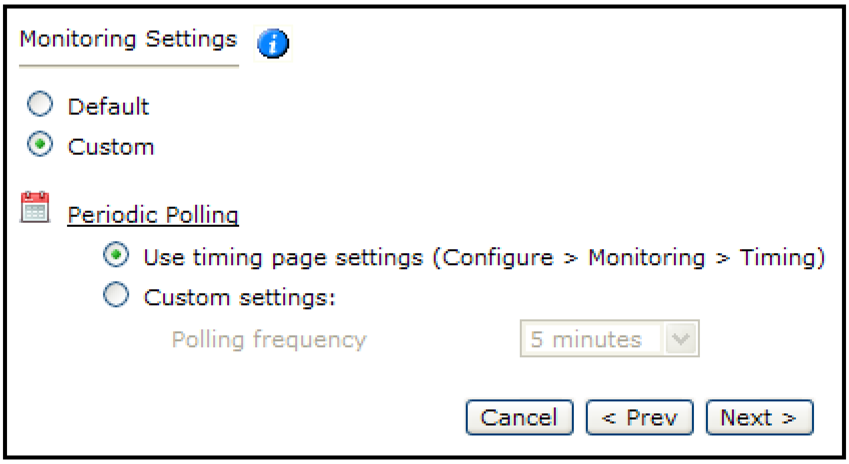


3. Configure the device settings:
   - **Name for Display**
   - **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
   - **Plugin name**: If there are multiple plugins installed for the same device type, select the desired one.
   - **Get revisions from**: One of the following:
     - **IP Address**: Revisions are retrieved automatically
     - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
   - **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image) TOP devices monitored via preinstalled TOP plugins can be monitored by any TOS Classic server (Central, Distribution, or Remote Collector); TOP devices monitored via manually-installed TOP plugins can be monitored only by the TOS Classic Central server.

   Click **Next**.
4. Configure the TOS Classic connection to the TOP device, according to the parameters required by the device:
   - Enter the authentication details needed to connect to the TOP device.
     - **Username and password**: Enter the device username and password
     - **Enable password**: Enter the password to give TOS Classic elevated privileges on the device
   - **Connection configuration**: Select whether to use **SSH** (preferred) or **Telnet**. To use default settings (recommended in most cases), leave the **Port number** blank.
     The device must be configured to use SSH version 2.

     > Special characters in the password are not supported for some plugins.
     >
     > Depending on your device configuration, TOS Classic web interface may include more fields than are necessary for logging into the device. Make sure not to fill in these fields, as this may cause monitoring to fail.
     >
     > Make sure to use a username representing a user account that has Read (Read Only, or Read/Write) permissions for all information on the TOP device.

   Click **Next**.
5. The Monitoring Settings page appears:



Monitoring Settings

○ Default
● Custom

Periodic Polling

● Use timing page settings (Configure > Monitoring > Timing)
○ Custom settings:

Polling frequency: 5 minutes

To use timing settings from the Timing page for this device, select **Default**.

- To define specific timing settings for this device, select **Custom**, then select **Custom settings**, and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

6. **Save** the configuration.

   The TOP device now appears in the Device Configuration list.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

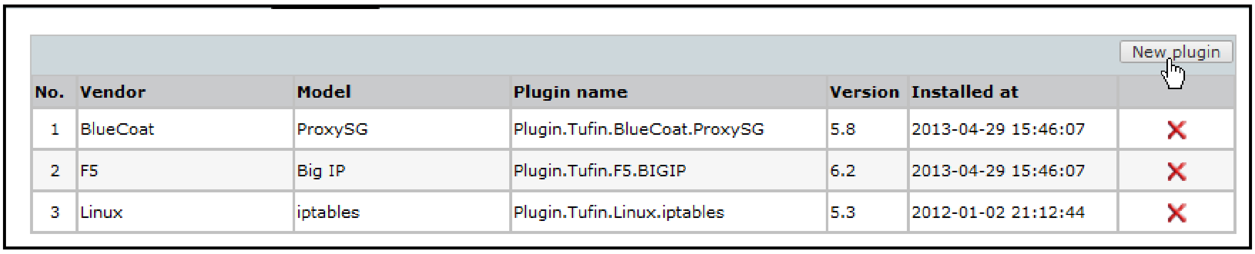
Installing a TOP Plugin

With an appropriate TOP plugin, TOS Classic can monitor any device's configuration that can be retrieved as a text file. To develop a TOP plugin, see the TOP Developer Alliance. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Before adding any TOP devices of a specific type, the plugin for that device type must be installed in TOS Classic.

To install a TOP plugin in TOS Classic:

1. Go to the Tufin Download Center and download the TOP plugin for your device.
2. Click **New Plugin**:



No.	Vendor	Model	Plugin name	Version	Installed at	
1	BlueCoat	ProxySG	Plugin.Tufin.BlueCoat.ProxySG	5.8	2013-04-29 15:46:07	✗
2	F5	Big IP	Plugin.Tufin.F5.BIGIP	6.2	2013-04-29 15:46:07	✗
3	Linux	iptables	Plugin.Tufin.Linux.iptables	5.3	2012-01-02 21:12:44	✗

   Navigate to the .tgz file, and click **Open**.

3. Wait for confirmation:

The plugin was installed successfully.

The plugin is installed. You can now add devices of the relevant type, from the **Devices** page.

How Do I Get Here?

In TOS Classic, go to Settings > **Monitoring** > **TOP Plugins**.

Adding OpenStack Devices

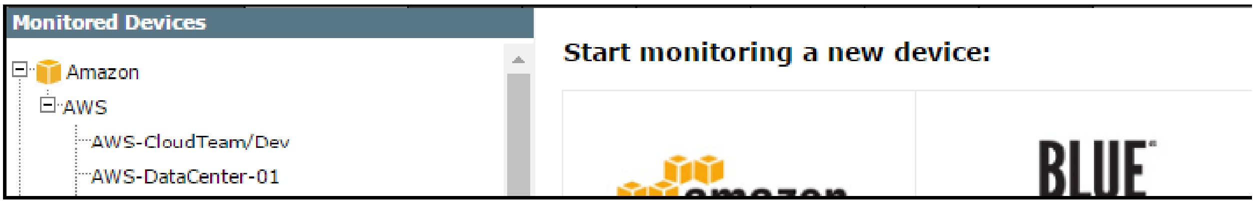
TOS Classic monitors the OpenStack platform for policy revision changes. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

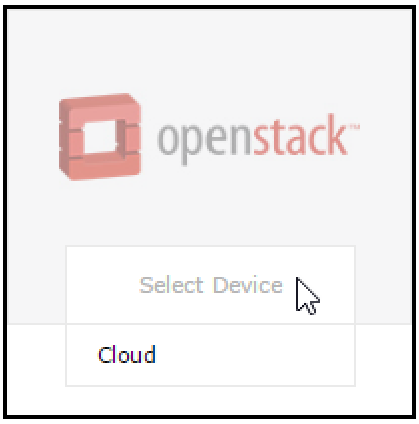
TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

Monitor a OpenStack Device

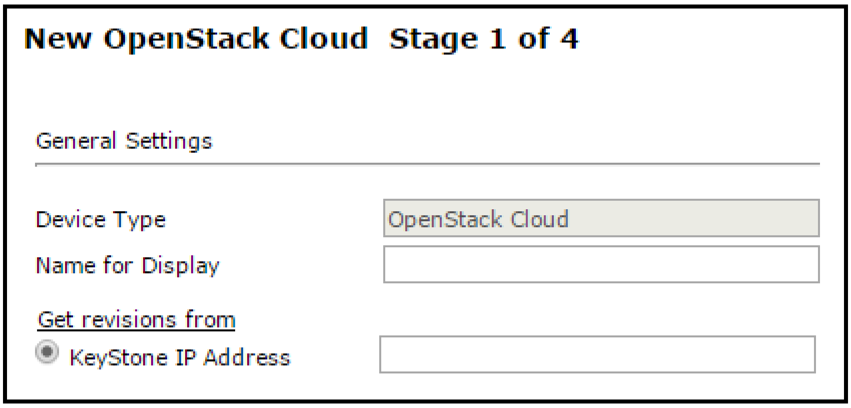
To configure TOS Classic to monitor the policy revisions of a OpenStack device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:





3. Configure the device settings:



New OpenStack Cloud Stage 1 of 4

General Settings

Device Type: OpenStack Cloud

Name for Display:

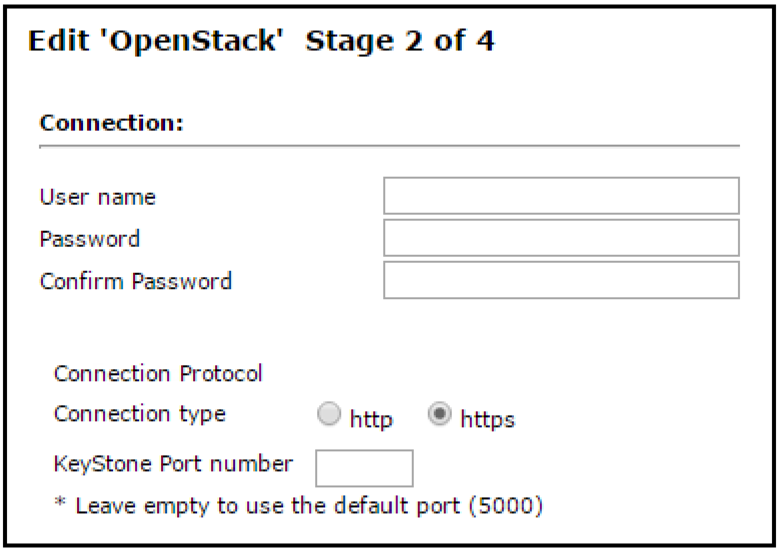
Get revisions from

● KeyStone IP Address:

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Keystone IP Address**: Enter the IP address of your OpenStack platform.
- **ST server**: In a distributed deployment, the OpenStack platform must be monitored by the Central server.

Click **Next**.

4. Configure the TOS Classic connection to the OpenStack device, according to the parameters required by the device:



Edit 'OpenStack' Stage 2 of 4

Connection:

User name

Password

Confirm Password

Connection Protocol

Connection type ○ http ● https

KeyStone Port number

* Leave empty to use the default port (5000)

a. Enter the user name of the OpenStack user that has permission to retrieve the policies.

The user can be a admin or a project member with read/write permissions.

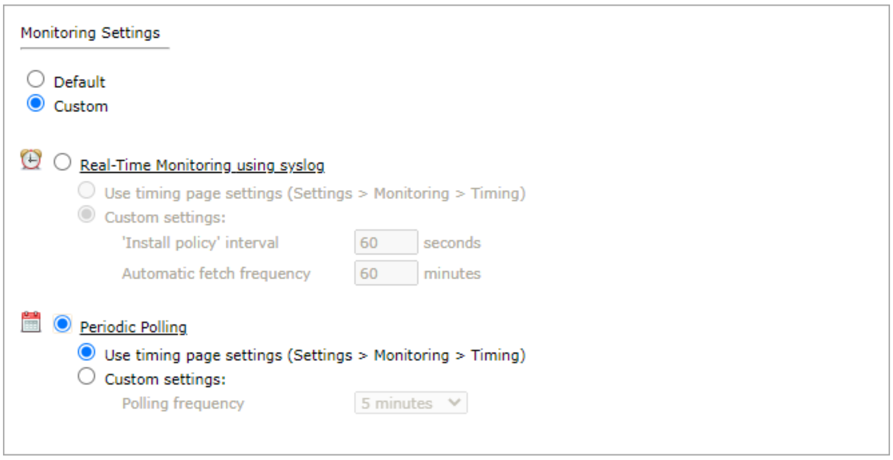
b. Enter and confirm the password of the OpenStack user.

c. Select to connect to OpenStack over http or https.

d. If your OpenStack system uses a custom port for connections, enter the **Keystone port number**.

e. Click **Next**.

5. In **Monitoring Settings**, do one of the following:



Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog
○ Use timing page settings (Settings > Monitoring > Timing)
● Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling
● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

Real-Time Monitoring: Applies only if syslogs "Sending Additional Information via Syslog" on page 239) are configured. Select **Custom settings** and configure:

- **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
- **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

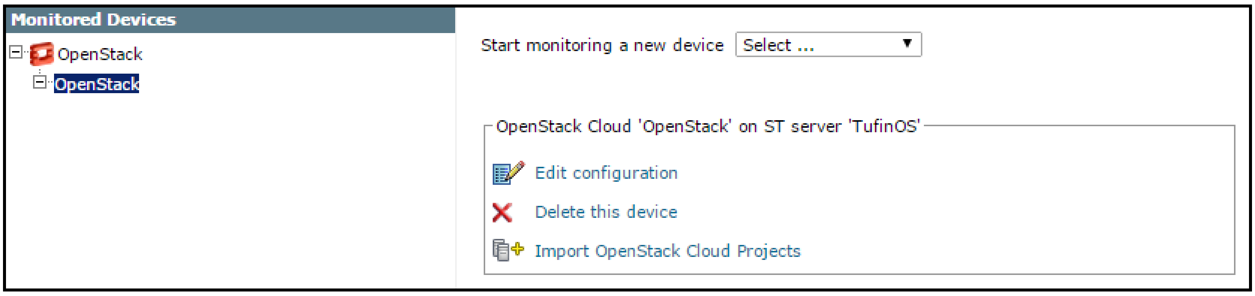
  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

Click **Next**.

6. **Save** the configuration.

The OpenStack device now appears in the **Monitored Devices** tree.

7. To manually add Virtual Cloud Projects to your device, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the Virtual Cloud Projects:
   a. In the **Monitored Devices** tree, select the device.
   b. Click **Import Virtual Cloud Projects** (only enabled for **Manual Import**):


Monitored Devices
OpenStack
OpenStack
Start monitoring a new device
Select ...
OpenStack Cloud 'OpenStack' on ST server 'TufinOS'
Edit configuration
Delete this device
Import OpenStack Cloud Projects

   c. Select all the Virtual Cloud Projects to be added.

      If the option to collect rule and object usage statistics for virtual contexts is available, it is enabled.

      If you do not want to collect these statistics, clear the options before you import the virtual contexts.
8. Click **Save**.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Palo Alto Devices

Adding Palo Alto PanOS Firewall Devices

TOS Classic monitors Palo Alto PanOS firewall devices for policy revision changes. For TOS Classic to show revision accountability and show rule and object usage, you must also configure the device to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

> TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.

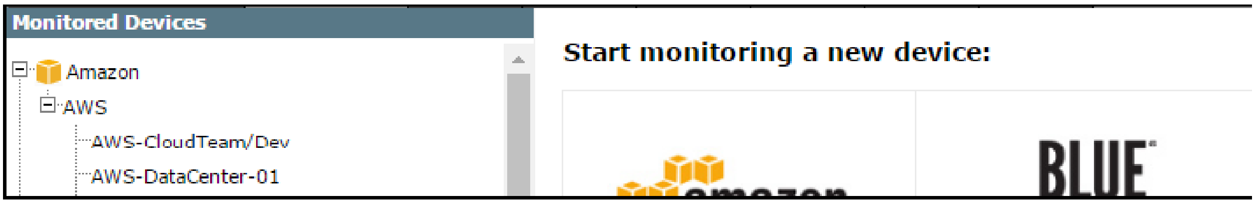
Prerequisites

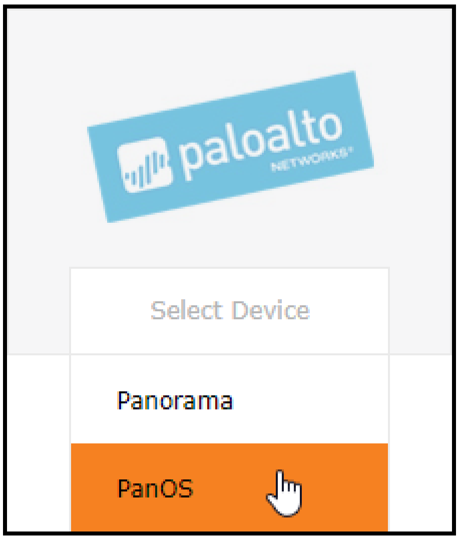
Monitoring: Create a user with the **Superuser** admin role for the Palo Alto PanOS firewall device. For PanOS 4.1 and higher you can also use a **Superuser (read-only)** user. TOS Classic does not write anything to the Palo Alto device for either user role.

Monitor a Palo Alto PanOS firewall Device

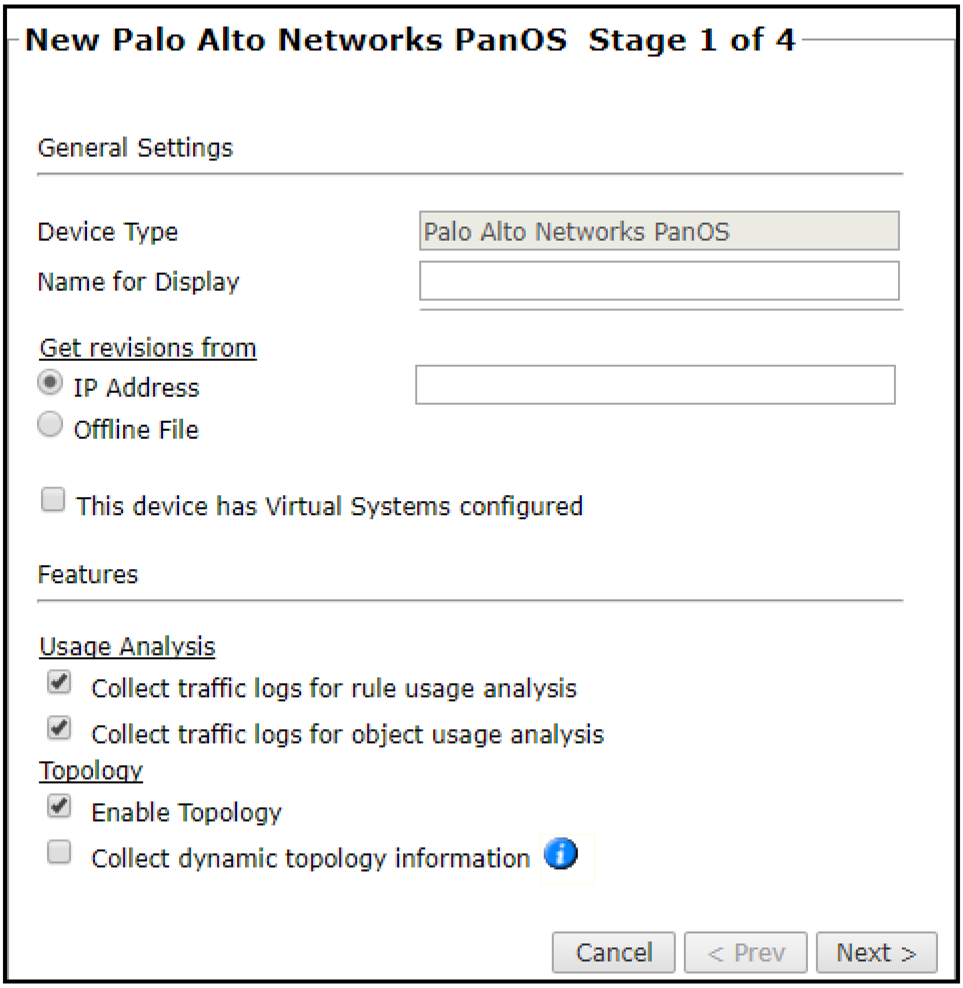
To configure TOS Classic to monitor the policy revisions of a Palo Alto PanOS firewall device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:





3. Configure the device settings:



New Palo Alto Networks PanOS Stage 1 of 4

General Settings

Device Type: Palo Alto Networks PanOS

Name for Display:

Get revisions from

● IP Address

○ Offline File

□ This device has Virtual Systems configured

Features

Usage Analysis

☑ Collect traffic logs for rule usage analysis

☑ Collect traffic logs for object usage analysis

Topology

☑ Enable Topology

□ Collect dynamic topology information

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:

- **IP Address**: Revisions are retrieved automatically
- **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis

  This option is disabled for Panorama devices.

- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)
- To enable adding and monitoring Virtual Systems, select **This device has Virtual Systems configured**. If selected, **Usage Analysis** is moved to the **Import Virtual Systems** step.

Usage Analysis

- **Collect traffic logs for rule usage analysis** is necessary for Rule Usage reports.
- **Collect counters for object usage analysis** enables Rule Usage reports to include per-object usage information.
  - **Collect traffic logs for object usage analysis** is necessary for reporting on unused objects and services in Rule Usage Reports.

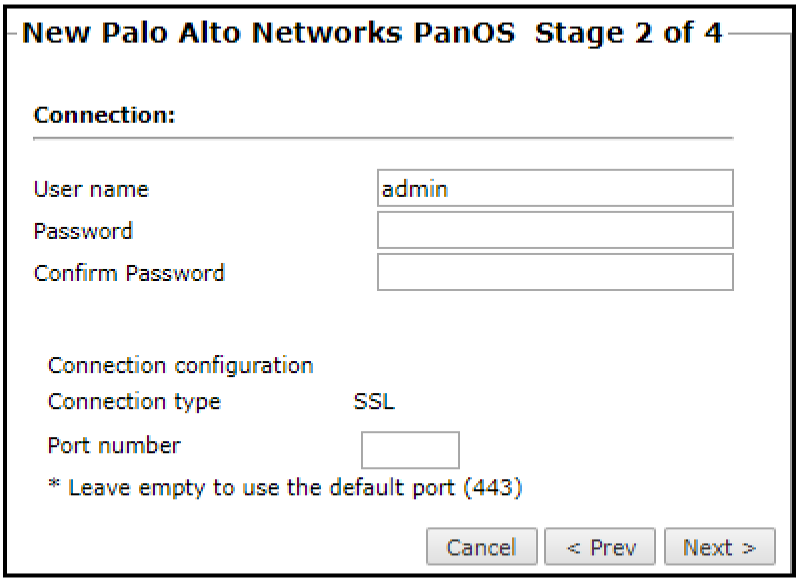
> Object usage analysis requires plenty of free disk space (depending on the number of gateways and the amount of traffic logs generated). If disk space is limited, you can configure TOS Classic to limit the number of days that data is kept.

> We recommend that you enable TOS Classic administrative alerts, which notify you if there is low disk space on the server. When disk utilization exceeds 90% in the partition that has the database, TOS Classic sends an alert.

Topology

- **Enable Topology**: Collects routing information for building the network Interactive Map.
  Topology options for **Advanced management** mode are configured when you import managed devices.
- If the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), also select **Collect dynamic topology information**. TOS Classic always collects the interface information with static routes and IP addresses when it receives a policy.

4. Click **Next**.
5. Configure the TOS Classic connection to the Palo Alto PanOS firewall device, according to the parameters required by the device:



New Palo Alto Networks PanOS Stage 2 of 4

Connection:

User name: admin

Password:

Confirm Password:

Connection configuration

Connection type: SSL

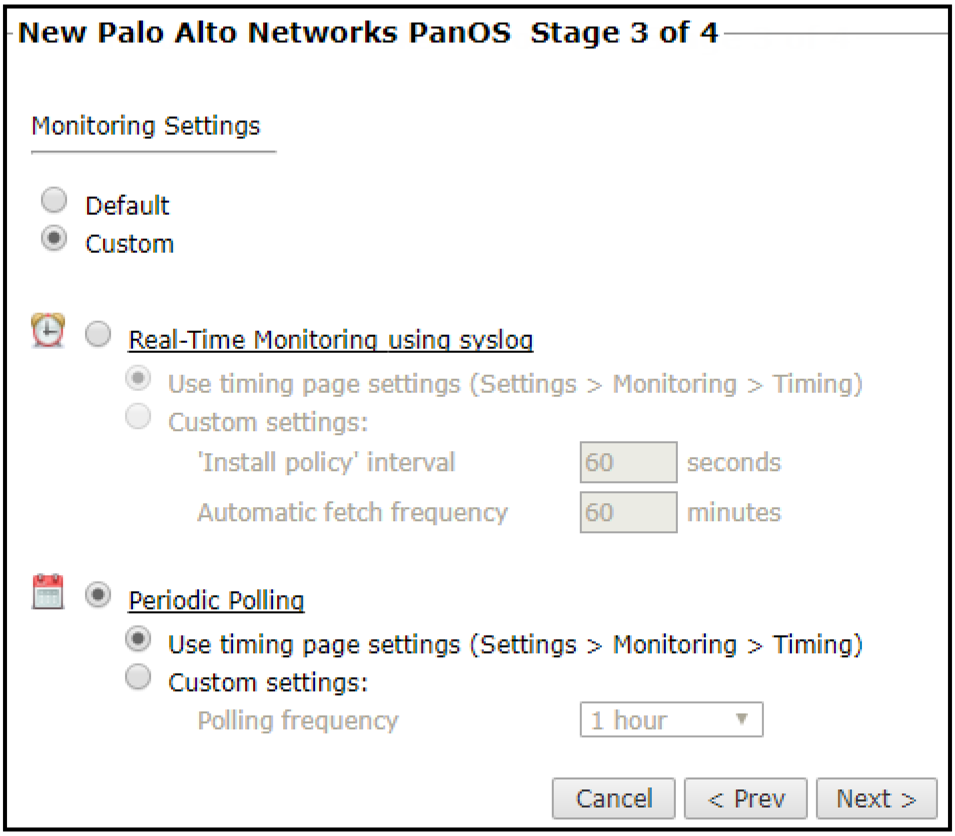
Port number:

* Leave empty to use the default port (443)

Enter the authentication details neeeded to connect to the Palo Alto PanOS firewall device.

To use default settings (recommended in most cases), leave the **Port number** blank.

6. Click **Next**.
7. The Monitoring Settings page appears:



New Palo Alto Networks PanOS Stage 3 of 4

Monitoring Settings

○ Default
● Custom

○ Real-Time Monitoring using syslog

● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

● Periodic Polling

● Use timing page settings (Settings > Monitoring > Timing)
○ Custom settings:
Polling frequency 1 hour

- To use timing settings from the Timing page, select **Default**. Otherwise, select **Custom**, **Custom settings**, and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

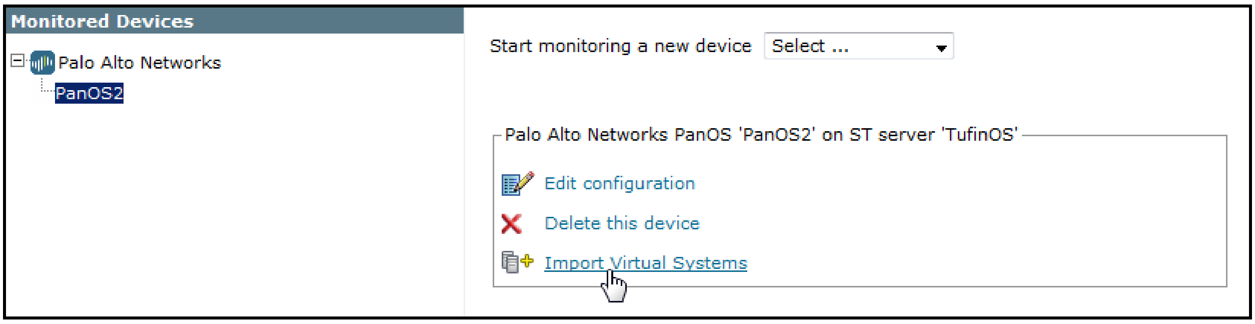
8. **Save** the configuration.

   The Palo Alto PanOS firewall device now appears in the **Monitored Devices** tree.

9. To manually add Virtual Systems to your device, wait for a revision to be received from the device (you can see the revision in **Compare** view). This may take several minutes. Then, add the Virtual Systems:

   a. In the **Monitored Devices** tree, select the device.

   b. Click **Import Virtual Systems** (only enabled for **Manual Import**):



Palo Alto Networks PanOS 'PanOS2' on ST server 'TufinOS'

   c. Select all the Virtual Systems to be added.

      If the option to collect rule and object usage statistics for virtual contexts is available, it is enabled.

      If you do not want to collect these statistics, clear the options before you import the virtual contexts.

   d. Click **Save**.

For TOS Classic to show revision accountability and show rule and object usage, you must also configure the device to send syslogs.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Adding Palo Alto Panorama Devices

TOS Classic monitors Palo Alto Panorama devices for policy revision changes. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Overview

To monitor a Palo Alto Panorama device (and its managed devices) in TOS Classic, you must complete the following procedures:

1. Add the Palo Alto Panorama device to TOS Classic.
2. Import the Device Groups (DGs) and devices managed by the Palo Alto Panorama device.

   When you select the DGs and devices to be managed by the Palo Alto Panorama device, if you have configured Advanced monitoring mode, you can also select the **Collect dynamic topology information** option.
3. Edit the configuration of a managed Palo Alto Panorama firewall device, including enabling or disabling the option to **Collect dynamic topology information**.

Additional considerations:

- If the device being added is an HA cluster of the managed firewall, TOS Classic will only provision the changes to the active HA server.
- TOS Classic and the monitored devices must be synchronized with the correct date and time, either manually or automatically. We recommend that you also configure the devices to resolve DNS queries.
- TOS R16-2 and higher includes improved support for Palo Alto Panorama versions 7.1 or higher. If you upgrade from TOS R16-1 or lower and want to use the advanced features, disable your Palo Alto Panorama devices to keep your device data and re-add the Palo Alto Panorama device and its firewalls as new devices. You can then remove the old Palo Alto Panorama device and its firewalls when the device data is obsolete.
- If you currently monitor your firewalls as standalone devices and you want to now monitor the firewall through the Palo Alto Panorama device that manages them, add the Palo Alto Panorama device and its firewalls as a new device and then disable your standalone firewalls (see Status). You can select the standalone devices from the device tree to see the historical device data. When the device data in the standalone firewalls is obsolete, you can remove the standalone firewall devices from TOS Classic.

After you add a Panorama device for monitoring, you can see the list of policy templates on the Panorama and which devices use each template. To see this information, go to: **Compare** > select the Panorama device from the device tree > click on the **Panorama** tab in the Policy pane > click on the **Templates** tab > expand the **Templates** tree.

In 2019, Palo Alto announced that online updates for Palo Alto Panorama software versions (up to and including version 7.1) will no longer be available. From R19-3, support for Panorama devices in Basic firewall management mode is deprecated for new devices. If you are upgrading to R19-3, the existing Panorama devices in Basic mode will continue to be monitored in TOS Classic. For more information about supported features in each monitoring mode, see the TOS Classic Features by Vendor.

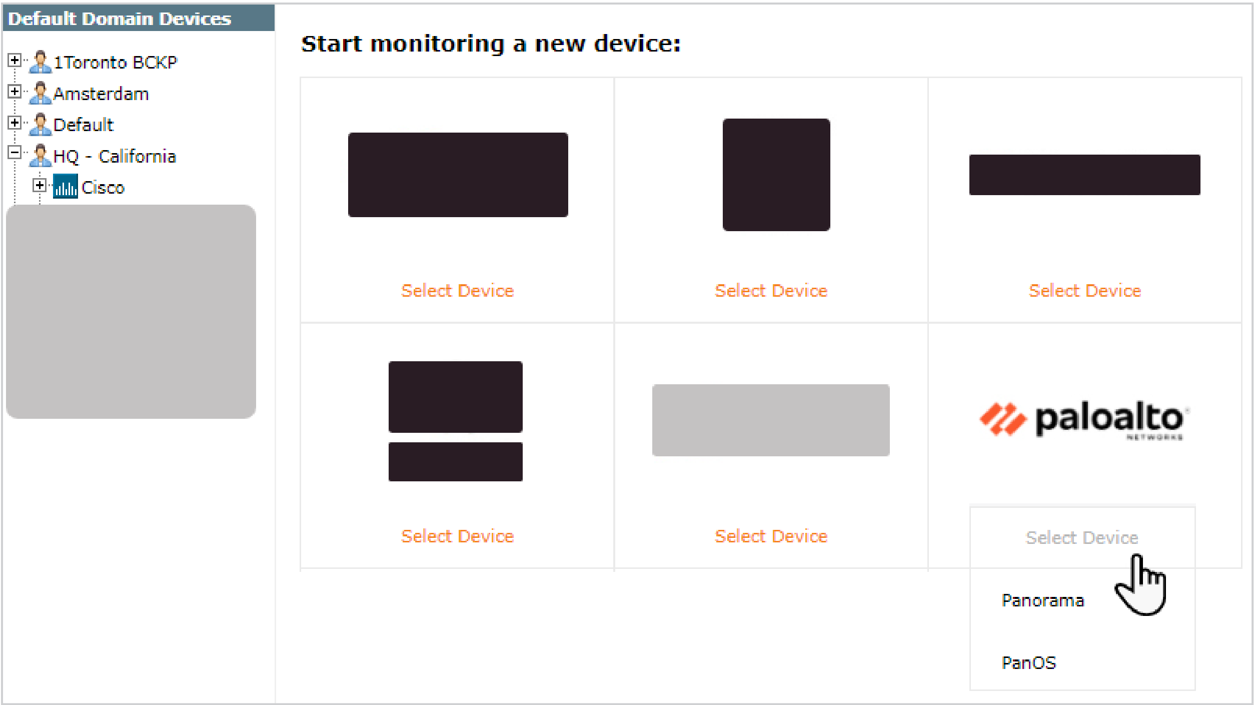
Prerequisites

Monitoring and Provisioning: Create a user with the **Superuser** admin role for the Palo Alto Panorama device.

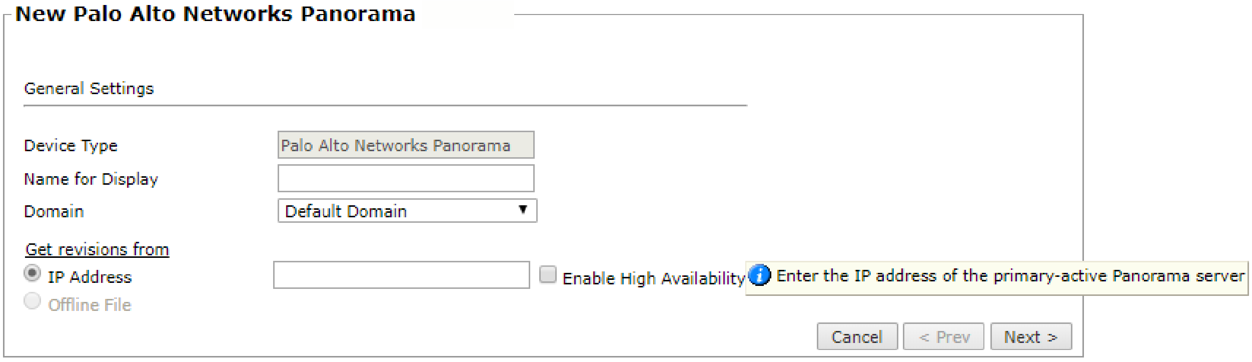
To support FQDN objects in SecureTrack, configure the relevant DNS on your Palo Alto Panorama device. For more information, refer to the Palo Alto documentation.

Adding a Palo Alto Panorama Device

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New Palo Alto Networks Panorama

General Settings

Device Type	Palo Alto Networks Panorama
Name for Display	
Domain	Default Domain ▾

Get revisions from

● IP Address □ Enable High Availability ⓘ Enter the IP address of the primary-active Panorama server

○ Offline File

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- **Get revisions from**: One of the following:
  - **IP Address**: Revisions are retrieved automatically.

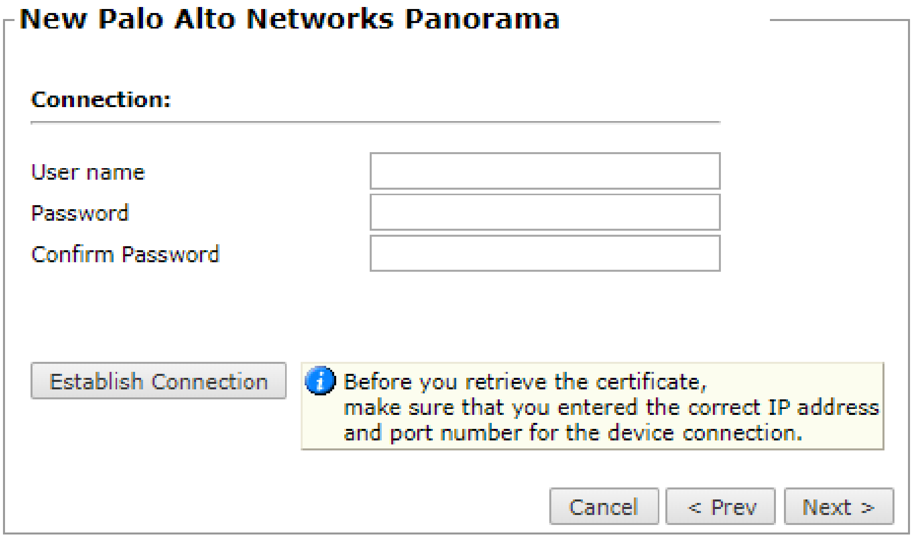
    If your Panorama devices are configured for a High Availability deployment, enter the IP address of the primary (Active) Panorama server
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis

    This option is disabled for Panorama devices.
  - **Enable High Availability**: Select this option if your Panorama devices are configured for a High Availability deployment with a primary (Active) and a secondary (Standby) Panorama server.

    This option is only available in **Advanced management** mode.
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (This field is not displayed in the image)

4. Click **Next**.

5. Configure the TOS Classic connection to the Palo Alto Panorama device, according to the parameters required by the device:



New Palo Alto Networks Panorama

Connection:

User name

Password

Confirm Password

Before you retrieve the certificate,
make sure that you entered the correct IP address
and port number for the device connection.

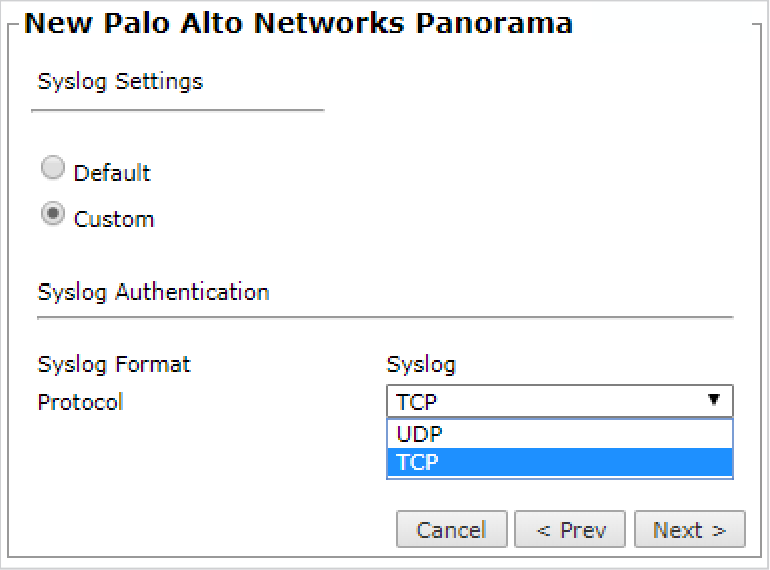
Enter the authentication details needed to connect to the Palo Alto Panorama device.

6. Click **Establish Connection** to retrieve the certificate.
   This is mandatory if you selected **Enable High Availability** when you configured the device settings.

7. Click **Next**.

8. Configure the **Syslog Settings**.

   The default Syslog Authentication protocol option is UDP.



New Palo Alto Networks Panorama

Syslog Settings

○ Default

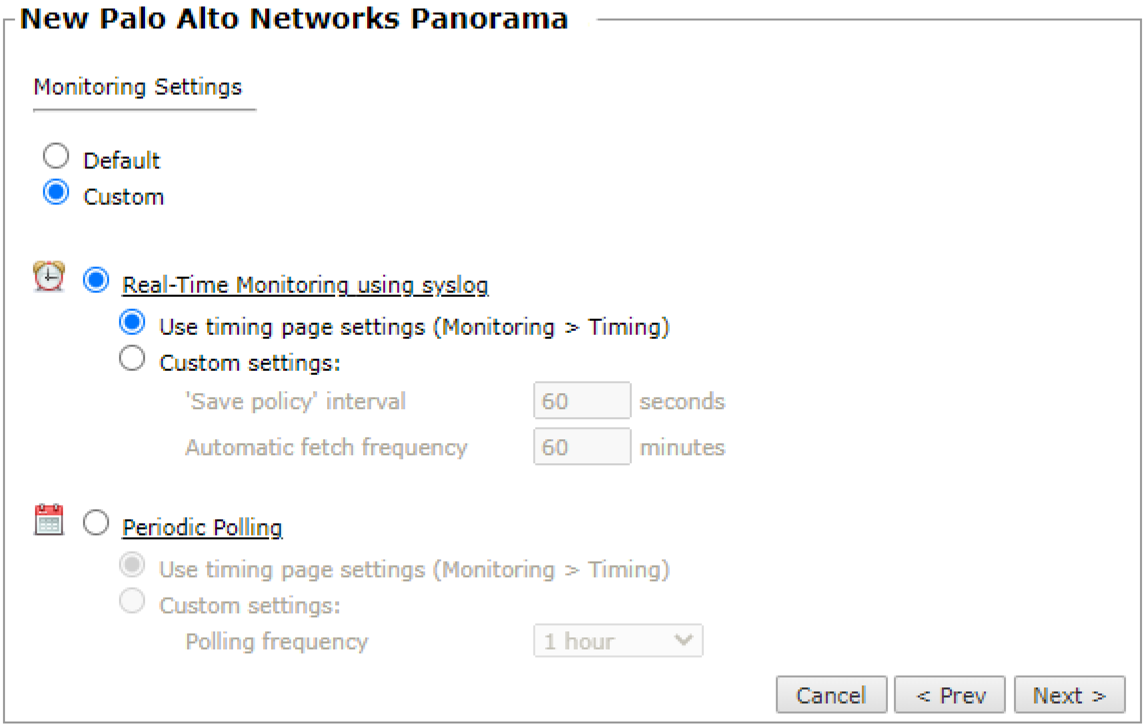
● Custom

Syslog Authentication

Syslog Format: Syslog

Protocol: TCP

9. In **Monitoring Settings**, do one of the following:



New Palo Alto Networks Panorama

Monitoring Settings

○ Default
● Custom

● Real-Time Monitoring using syslog
● Use timing page settings (Monitoring > Timing)
○ Custom settings:
'Save policy' interval 60 seconds
Automatic fetch frequency 60 minutes

○ Periodic Polling
● Use timing page settings (Monitoring > Timing)
○ Custom settings:
Polling frequency 1 hour

- To use real-time monitoring and timing settings from the Timing page, select **Default**.

Otherwise, select **Custom** and configure the monitoring mode and settings.

- **Real-Time Monitoring**: Applies only if syslogs (Configuring Devices to Send Logs) are configured. Select **Custom settings** and configure:
  - **'Save policy' interval**: When a Save Policy event is followed within this time interval by an Install Policy event for the same policy, TOS Classic tries to combine the two events into a single revision. The default value is 60 seconds.
  - **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

  If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.

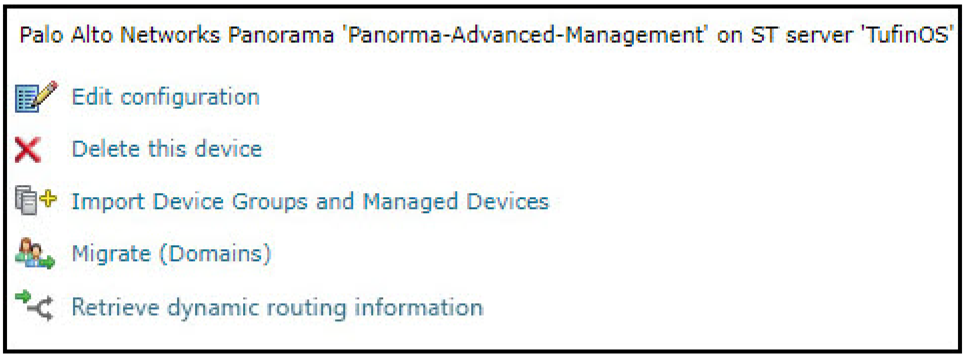
10. Click **Next** and then click **Save**.

    The Palo Alto Panorama device now appears in the **Monitored Devices** tree.

11. To complete the configuration, do one of the following:
    - Click **Done**.
    - Click **Import Managed Devices** (or **Import Administrative Domains and Managed Devices/Import Device Groups and Managed Devices** if available), select all the managed devices to be added, and click **Save** or **Import**.

      To import managed devices later, you can select the device and click **Import Managed Devices** (or **Import Administrative Domains and Managed Devices/Import Device Groups and Managed Devices** if available).

- Add another device.



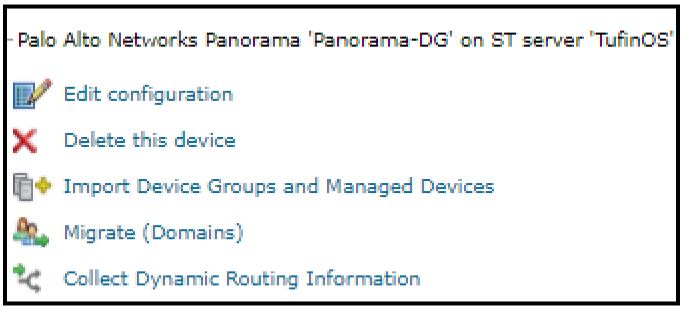
Palo Alto Networks Panorama 'Panorma-Advanced-Management' on ST server 'TufinOS'

Edit configuration
Delete this device
Import Device Groups and Managed Devices
Migrate (Domains)
Retrieve dynamic routing information

Topology options to collect routing information for building the network Interactive Map are configured when you import managed devices.

Importing the Domains or Devices Managed by a Palo Alto Panorama Device

1. Select the Palo Alto Panorama device from the device tree.
2. Click **Import Device Groups and Managed Devices**.



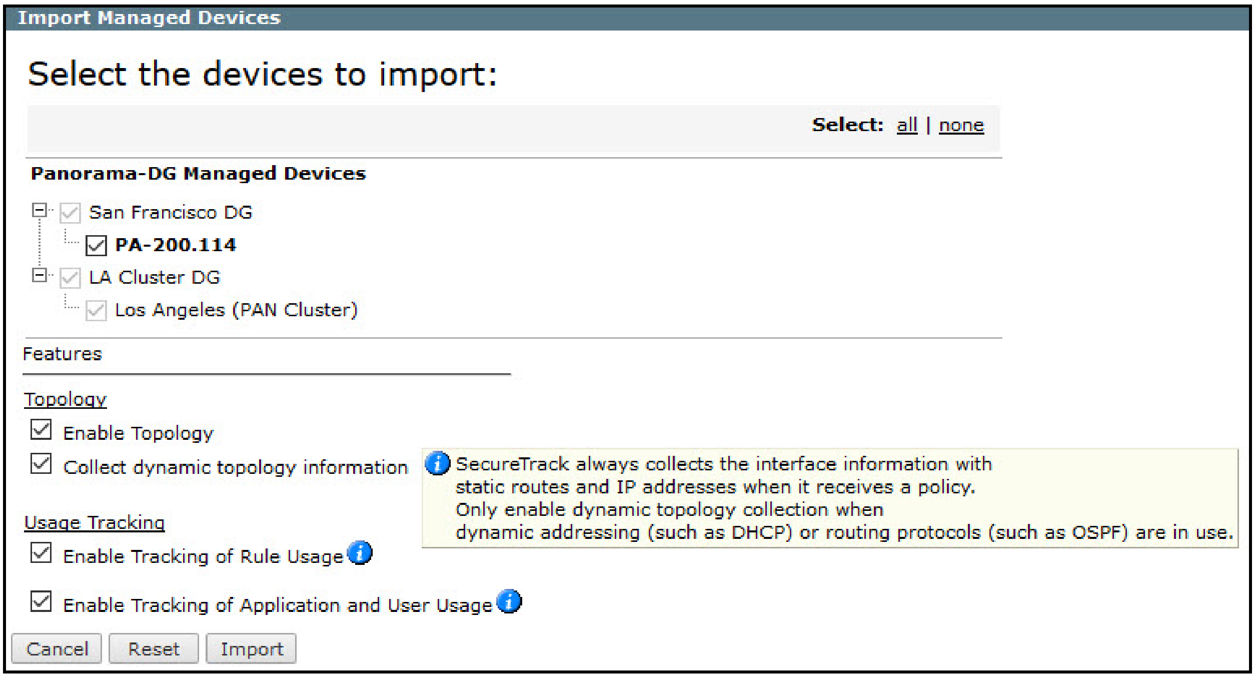
Palo Alto Networks Panorama 'Panorama-DG' on ST server 'TufinOS'

Edit configuration
Delete this device
Import Device Groups and Managed Devices
Migrate (Domains)
Collect Dynamic Routing Information

3. From the list of devices managed by the Palo Alto Panorama device, select the devices to import.
4. Configure the **Topology** options:

   Enable Topology: Collects routing information for building the network Interactive Map.
   Topology options are configured when you import managed devices.

   - **Collect dynamic topology information** when dynamic addressing (DHCP) or routing protocols (OSPF and BGP) are in use.



Import Managed Devices

Select the devices to import:

Select: all | none

Panorama-DG Managed Devices

☑ San Francisco DG
☑ PA-200.114
☑ LA Cluster DG
☑ Los Angeles (PAN Cluster)

Features

Topology

☑ Enable Topology
☑ Collect dynamic topology information

SecureTrack always collects the interface information with static routes and IP addresses when it receives a policy. Only enable dynamic topology collection when dynamic addressing (such as DHCP) or routing protocols (such as OSPF) are in use.

Usage Tracking

☑ Enable Tracking of Rule Usage
☑ Enable Tracking of Application and User Usage

5. Configure the **Usage Tracking** options:

- **Enable Tracking of Rule Usage** - Monitor last hit information for rules in the managed devices being imported.
- **Enable Tracking of Application and User Usage** - Monitor last hit information for applications and users in the managed devices being imported.

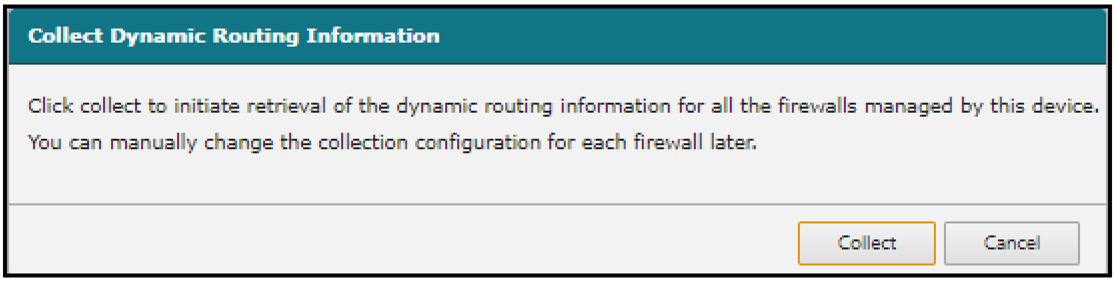
6. Click **Import**.
7. Do one of the following:
   - Click **Reset** to update the list of managed devices.
   - Click **Done** to return to the device tree.

   The managed devices appear under the Palo Alto Panorama device in the device tree.

> If a conflict is detected between the name of a management domain (DG) on the Panorama device, and the name of the DG in SecureTrack, you will have to choose whether to **Update** the name or **Ignore** the conflict.
> After the DG name in SecureTrack is synchronized with the name on the Panorama device, the DG is no longer suggested when you next select devices to import.

Editing the Dynamic Topology Settings for Devices Managed by a Palo Alto Panorama Device

1. Select the Palo Alto Panorama device from the device tree.
2. Click **Collect Dynamic Routing Information** and click **Collect**.



Collect Dynamic Routing Information

Click collect to initiate retrieval of the dynamic routing information for all the firewalls managed by this device.
You can manually change the collection configuration for each firewall later.

Collect dynamic topology information is enabled for all the managed devices.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Configuring Palo Alto Panorama Logging

Introduction

Tufin lets you configure Palo Alto Panorama Advanced Mode logging to occur at the beginning of a session, end of a session, or both the beginning and end of a session.

By default, logging occurs at both the start and end of the session. If session processing is overloaded or backed-up, configure Panorama logging to occur at the end of the session.

The Panorama logging option in StConf affects only the logging for provisioning of new rules for all the Panorama Advanced Mode devices managed in Secure Track.

How do I do it?

To configure the Panorama logging option for provisioning:

We recommend that you backup the stconf table prior to making any changes.

1. Navigate to: `https://<SecureTrack_IP>/securetrack/admin/stcgitest.htm`
2. Navigate to **Edit StConf > Fetch StConf**.
3. In the StConf file, navigate to the `<provisioning>` section and verify that the `<panorama_ng_log_options>` flag is present.
4. If the `<panorama_ng_log_options>` flag is not present, manually insert it into the `<provisioning>` section.
5. In the `<provisioning>` section of the StConf file, set the `<panorama_ng_log_options>` flag to configure logging to occur at the beginning of a session `(log-start`), at the end of a session (`log-end`), or at both the beginning and the end of a session (`both`).

   The logging default is `both`
6. Click **Submit New Conf**.

Sample code

```
<provisioning>
    <panorama_ng_log_option>log-end</panorama_ng_log_options>
            <!--Available values: log-start, log-end, both-->
</provisioning>
```

Adding VMware NSX Cloud Platform

TOS Classic monitors the VMware platform for policy revision changes. For TOS Classic to show full accountability details (who made the policy changes and when the changes were made), you must also configure the platform to send syslogs. To help you organize the information for your devices, you can use the device information worksheet. To see which TOS features are supported for your device, review the feature support table.

Prerequisites

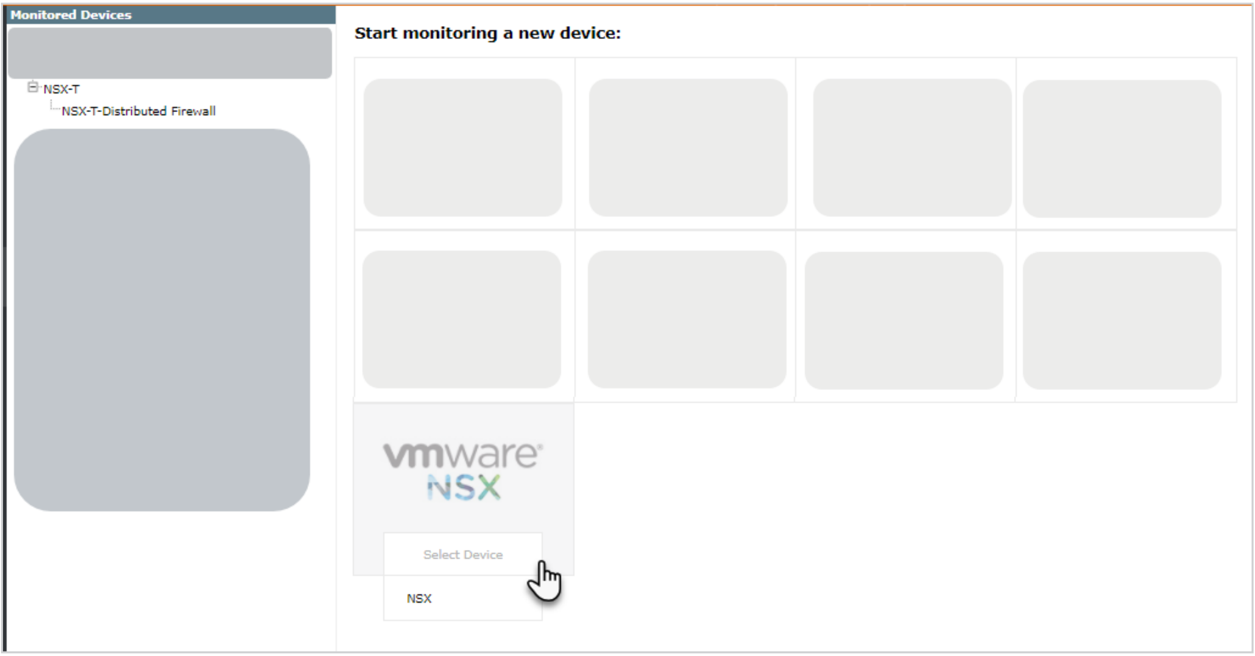
- Monitoring: You must have a user with read-only permissions for the NSX manager and for NSX-V, also a user with at least read-only permissions for the vCenter server. See Creating Read-only accounts for NSX devices for details.
- Provisioning: You must have a user with admin permissions.

By default, changes to unlogged rules do not trigger new revisions on TOS Classic. Therefore, unlogged changes created by tools such as Service Composer will not trigger a TOS Classic revision. See Tracking Unlogged Rules for details.

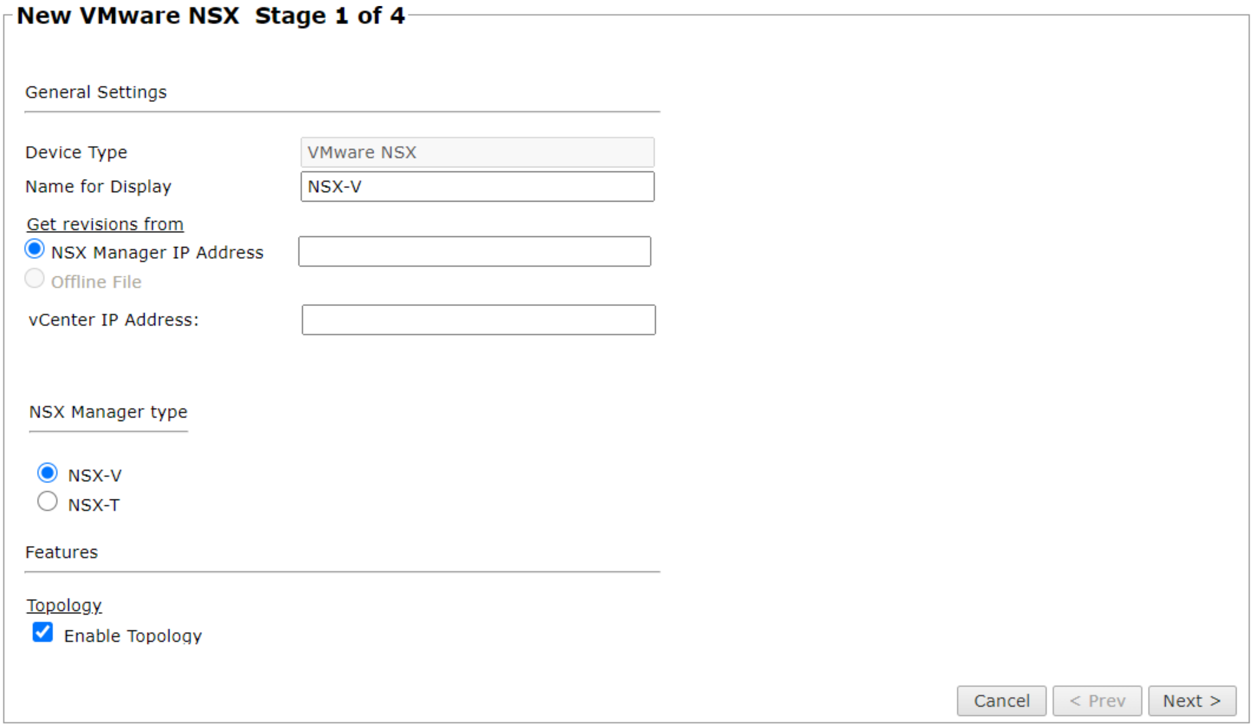
Monitor a VMware Device

To configure TOS Classic to monitor the policy revisions of a VMware device:

1. In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.
2. Select the appropriate device type:



3. Configure the device settings:



New VMware NSX Stage 1 of 4

General Settings

Device Type: VMware NSX

Name for Display: NSX-V

Get revisions from

● NSX Manager IP Address

○ Offline File

vCenter IP Address:

NSX Manager type

● NSX-V

○ NSX-T

Features

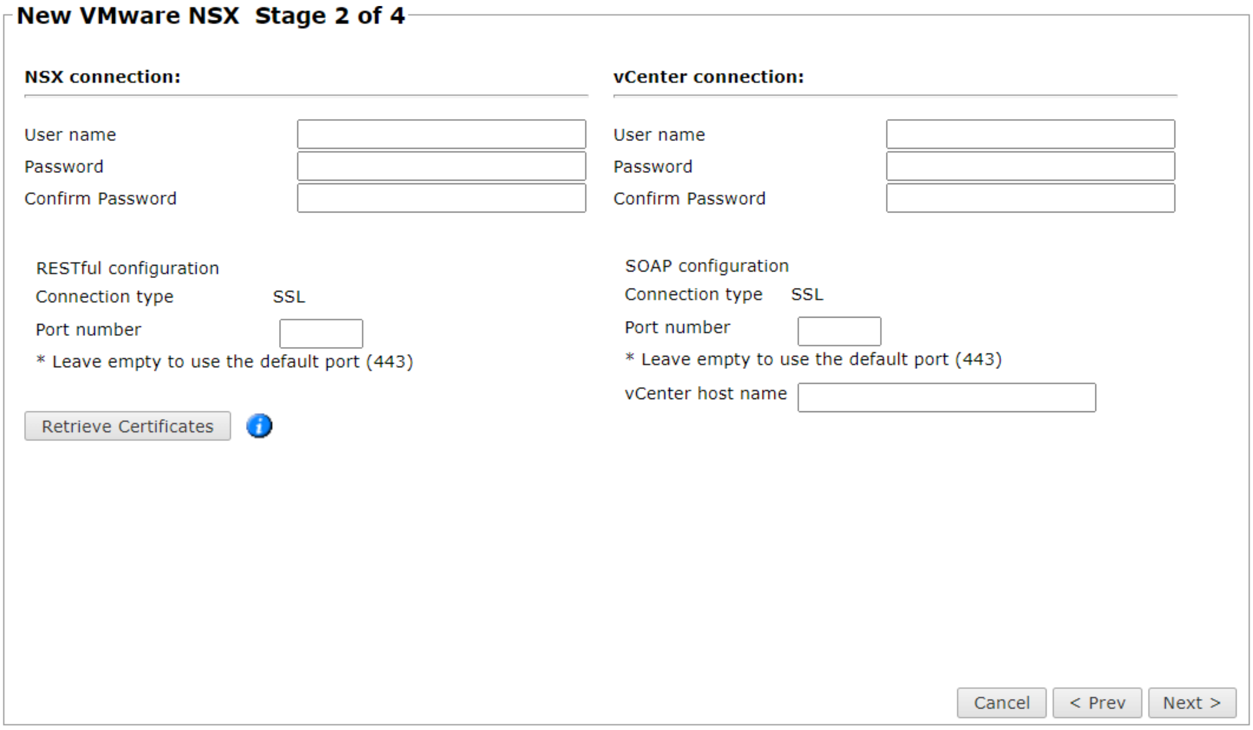
Topology

☑ Enable Topology

- **Name for Display**
- **Domain**: Available only if you have configured your system for managing multi-domains and All Domains is currently selected. Select the domain to which to add the device. The Domain can only be entered when adding a device; to change the Domain, you must migrate the device.
- Get revisions from one of the following:
  - **NSX Manager IP Address**: Enter the IP address of the NSX manager
  - **Offline File**: (If available) Revisions are manually uploaded to TOS Classic for Offline Analysis
  - **vCenter IP Address**: Enter the IP address of the vCenter device. vCenter information is not required for NSX-T devices.
- **NSX Manager Type**: The NSX Manager type (NSX-V or NSX-T).
- **Enable Topology**: Collects routing information for building the network Interactive Map.

  Topology options for **Advanced management** mode are configured when you import managed devices.
- For NSX-T devices, if the device uses dynamic addressing (such as DHCP) or dynamic routing protocols (such as OSPF), select **Collect dynamic topology information**.
- **ST server**: In a distributed deployment, select which TOS Classic server monitors this device (Not shown in image)

4. Click **Next**.
5. Configure the TOS Classic connection to the VMware device, according to the parameters required by the device:



New VMware NSX Stage 2 of 4

NSX connection:

User name	
Password	
Confirm Password	

RESTful configuration

Connection type	SSL
Port number	

* Leave empty to use the default port (443)

vCenter connection:

User name	
Password	
Confirm Password	

SOAP configuration

Connection type	SSL
Port number	

* Leave empty to use the default port (443)

vCenter host name	

- Enter admin credentials for the NSX manager
- Enter appropriate vCenter details. vCenter information is not required for NSX-T devices.
  - Enter credentials for the vCenter server - with at least read-only permissions
  - Enter the **vCenter host name** if configuring an external device for VMware NSX syslogs.
- To use default settings (recommended in most cases), leave the **Port number** blank.

  The device must be configured to use SSH version 2.
- Click **Retrieve Certificate** to setup encrypted communication between TOS Classic and the VMware device.

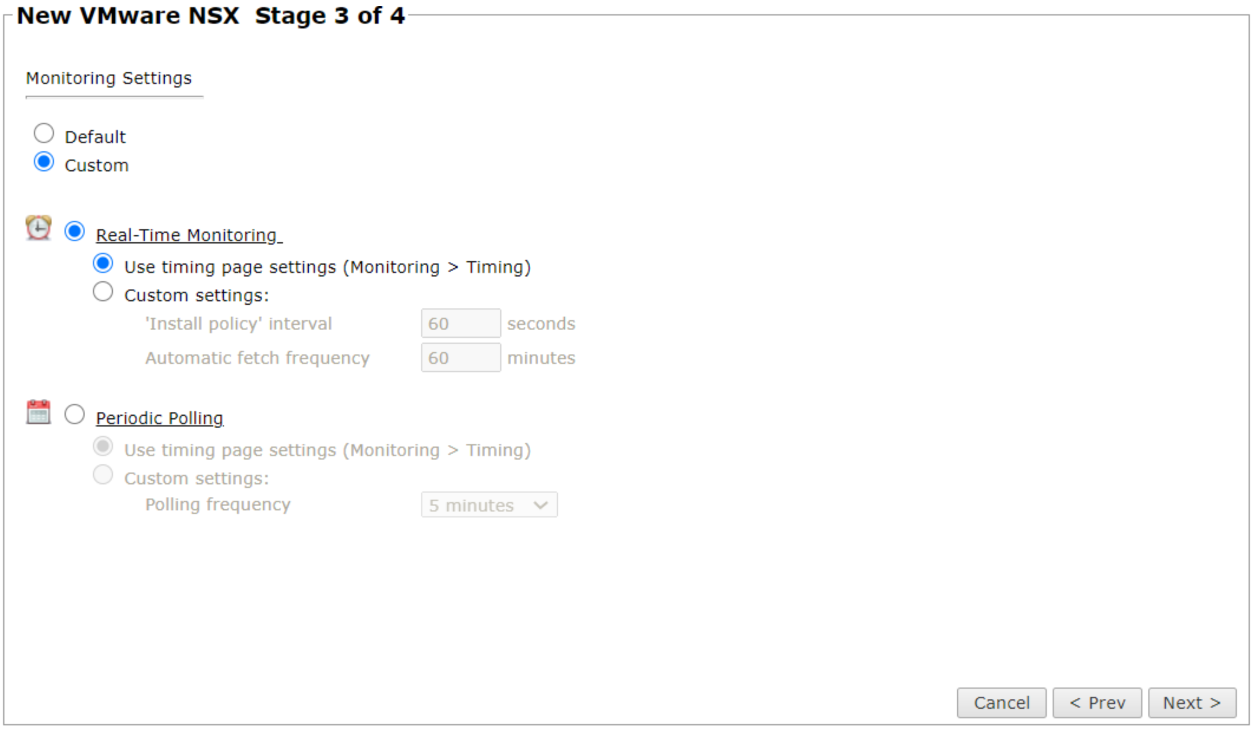
  The certificate appears, and the following message is displayed:

  The certificate was retrieved successfully.

  > The certificate is retrieved from the vCenter over port 8443.

6. Click **Next**.

   The Monitoring Settings page appears:



New VMware NSX Stage 3 of 4

Monitoring Settings

○ Default
● Custom

● Real-Time Monitoring
● Use timing page settings (Monitoring > Timing)
○ Custom settings:
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

○ Periodic Polling
● Use timing page settings (Monitoring > Timing)
○ Custom settings:
Polling frequency 5 minutes

7. To use timing settings from the Timing page, select **Default**. Otherwise, select **Custom** and configure the monitoring mode and settings:
   - **Real-Time Monitoring**: Applies only if syslogs are configured. In **Custom settings**:
     - **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, TOS Classic combines the events into a single Install Policy revision (Default: 60 seconds)
     - **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
   - **Periodic Polling**, select **Custom settings** and configure the **Polling frequency**: How often TOS Classic fetches the configuration from each device.

     If you select **1 day**, you can then select the exact time (hour and minute) for the daily polling.
8. Click **Next**.
9. **Save** the configuration.

   The VMware device now appears in the **Monitored Devices** tree.

How Do I Get Here?

In TOS Classic, go to **Settings** > **Monitoring** > **Manage Devices**.

Tracking Unlogged Rules

By default TOS uses NSX Audit Log to monitor DFW modifications, however modification to rules that are marked non-logged (for example, Service Composer rules) are not published to audit log. If any rules in the monitored NSX are marked with no-log, follow the steps below in order to track any modification in SecureTrack.

Log Service Composer rule changes:

We recommend that you backup the stconf table prior to making any changes.

1. In the browser address bar, after the IP address, add: `/stcgitest.htm`
2. Click **Edit StConf**.
3. Click **Fetch StConf**.
4. Change the value of the `read_audit_logs` tag for nsx to 0.

   ```
   <nsx>
       <read_audit_logs>0</read_audit_logs>
   </nsx>
   ```
5. Click **Submit New Conf**.

Creating Accounts for NSX Devices

NSX-T Devices

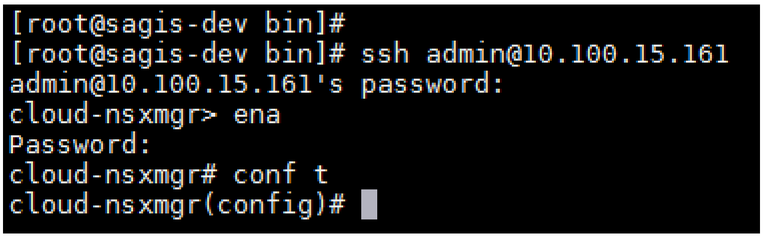
1. In the NSX-T manager go to **System** > **Settings** > **User and Roles**
2. Click on **ADD** and select a role assignment for LDAP
3. Add the LDAP domain
4. Add a User, and select Role “Auditor” for read only or “Enterprise Admin” for read write user , and click on **Save**.

NSX-V Devices

SecureTrack uses the NSX API to monitor NSX-V devices. To retrieve revisions, use NSX Role Based Access Control (RBAC) to create an NSX-CLI user with read-only access to the NSX API as follows:

A: Create an NSX Manager user account with read-only permission for the API.

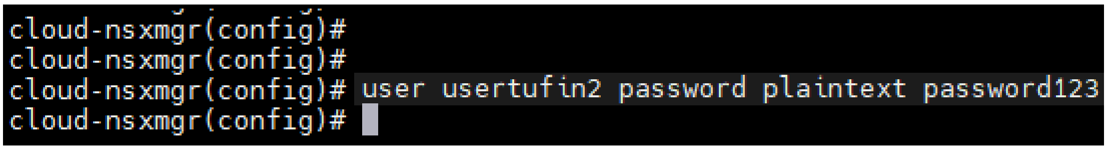
1. Connect to the NSX manager via SSH, switch to enable mode, and enter the configuration terminal.



```
[root@sagis-dev bin]#
[root@sagis-dev bin]# ssh admin@10.100.15.161
admin@10.100.15.161's password:
cloud-nsxmgr> ena
Password:
cloud-nsxmgr# conf t
cloud-nsxmgr(config)#
```

2. From the configuration terminal, create a new user account on the NSX Manager with the following command:

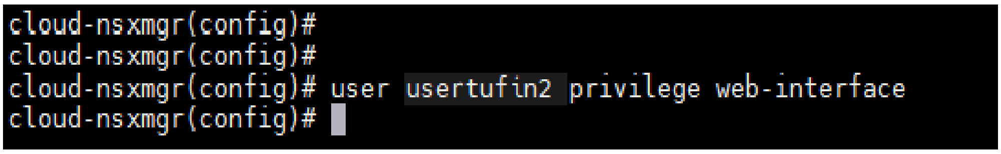
```
user username password (hash | plaintext) password
```



```
cloud-nsxmgr(config)#
cloud-nsxmgr(config)#
cloud-nsxmgr(config)# user usertufin2 password plaintext password123
cloud-nsxmgr(config)#
```

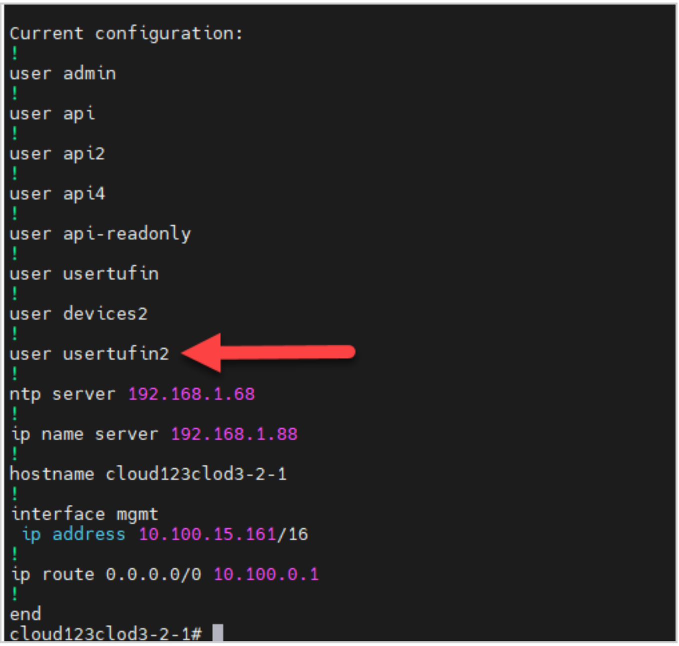
3. After you create the CLI user, use the following command to assign the user web-interface privileges so that it can be authenticated against the NSX Manager web interface:

```
user username privilege web-interface
```



```
cloud-nsxmgr(config)#
cloud-nsxmgr(config)#
cloud-nsxmgr(config)# user usertufin2 privilege web-interface
cloud-nsxmgr(config)#
```

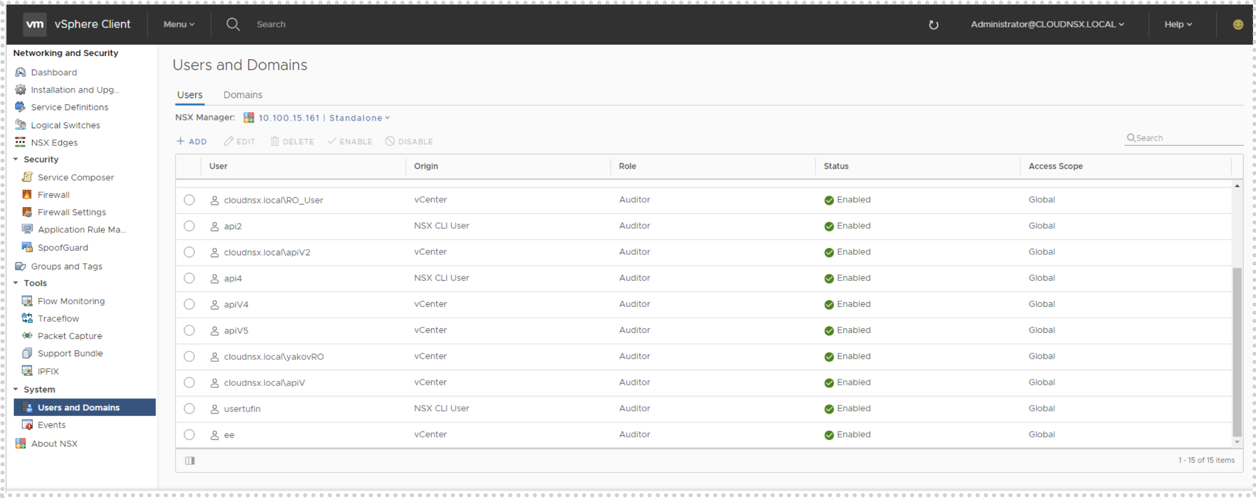
4. Save the configuration.
5. To view the running configuration, enter the following commands:
   1. exit
   2. write memory
   3. show running-config



```
Current configuration:
!
user admin
!
user api
!
user api2
!
user api4
!
user api-readonly
!
user usertufin
!
user devices2
!
user usertufin2
!
ntp server 192.168.1.68
!
ip name server 192.168.1.88
!
hostname cloud123clod3-2-1
!
interface mgmt
 ip address 10.100.15.161/16
!
ip route 0.0.0.0/0 10.100.0.1
!
end
cloud123clod3-2-1#
```

6. In the vSphere Web Client, navigate to **Menu > Networking & Security > Users and Domains > Users tab**.

   In the example below, the new user **usertufin2** is not listed and therefore has no assigned role:



User	Origin	Role	Status	Access Scope
cloudnsx.local\RO_User	vCenter	Auditor	Enabled	Global
api2	NSX CLI User	Auditor	Enabled	Global
cloudnsx.local\apiV2	vCenter	Auditor	Enabled	Global
api4	NSX CLI User	Auditor	Enabled	Global
apiV4	vCenter	Auditor	Enabled	Global
apiV5	vCenter	Auditor	Enabled	Global
cloudnsx.local\yakovRO	vCenter	Auditor	Enabled	Global
cloudnsx.local\apiV	vCenter	Auditor	Enabled	Global
usertufin	NSX CLI User	Auditor	Enabled	Global
ee	vCenter	Auditor	Enabled	Global

1 - 15 of 15 items

7. Create a user using the following REST API POST call, using CURL, Postman, or another REST client:

   `https://<NSX-Manager-IP-Address>/api/2.0/services/usermgmt/role/userId?isCli=true`

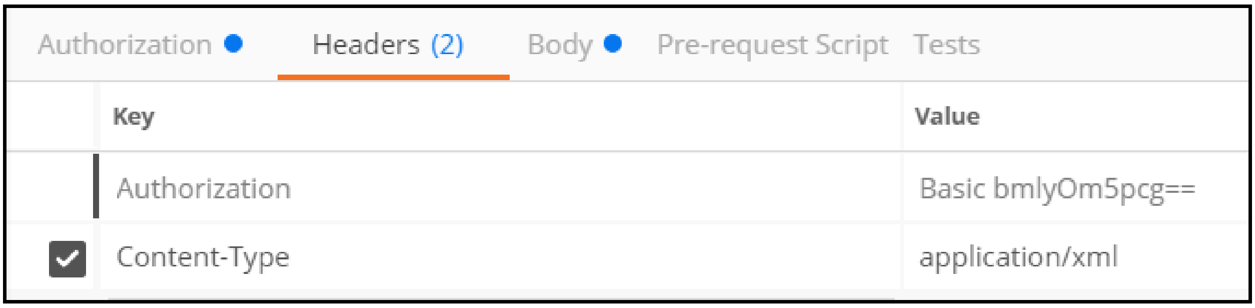
   - **Authorization**

     To authenticate the request, add an Authorization header with the admin user/password for the NSX Manager device.

   - **Headers**

     The REST call must also include the `Authorization` and `Content-Type` headers.

     The example below shows the headers in the Postman client:



	Key	Value
	Authorization	Basic bmlyOm5pcg==
☑	Content-Type	application/xml

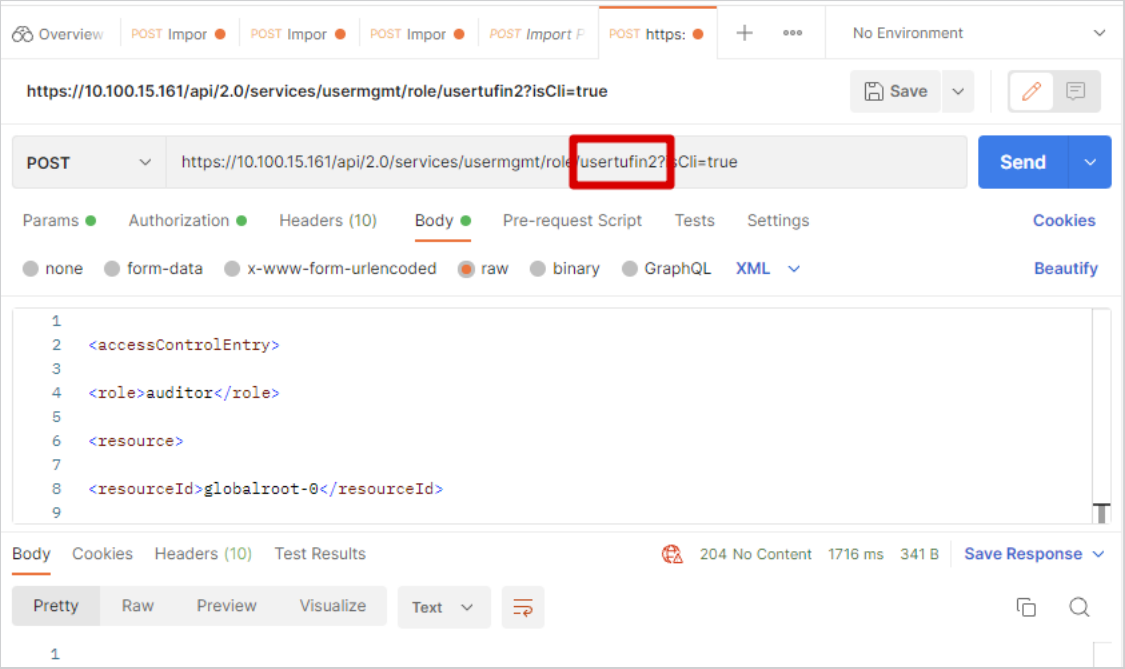
- **Request Body**

```
<accessControlEntry>
 <role>auditor</role>
 <resource>
 <resourceId>globalroot-0</resourceId>
 </resource>
</accessControlEntry>
```

The options for `role` are:

- auditor (Auditor for monitor changes only from ST)
- security_admin (Security Administrator if needed provision changes from SC)

The example below shows the results in the Postman client:



https://10.100.15.161/api/2.0/services/usermgmt/role/usertufin2?isCli=true

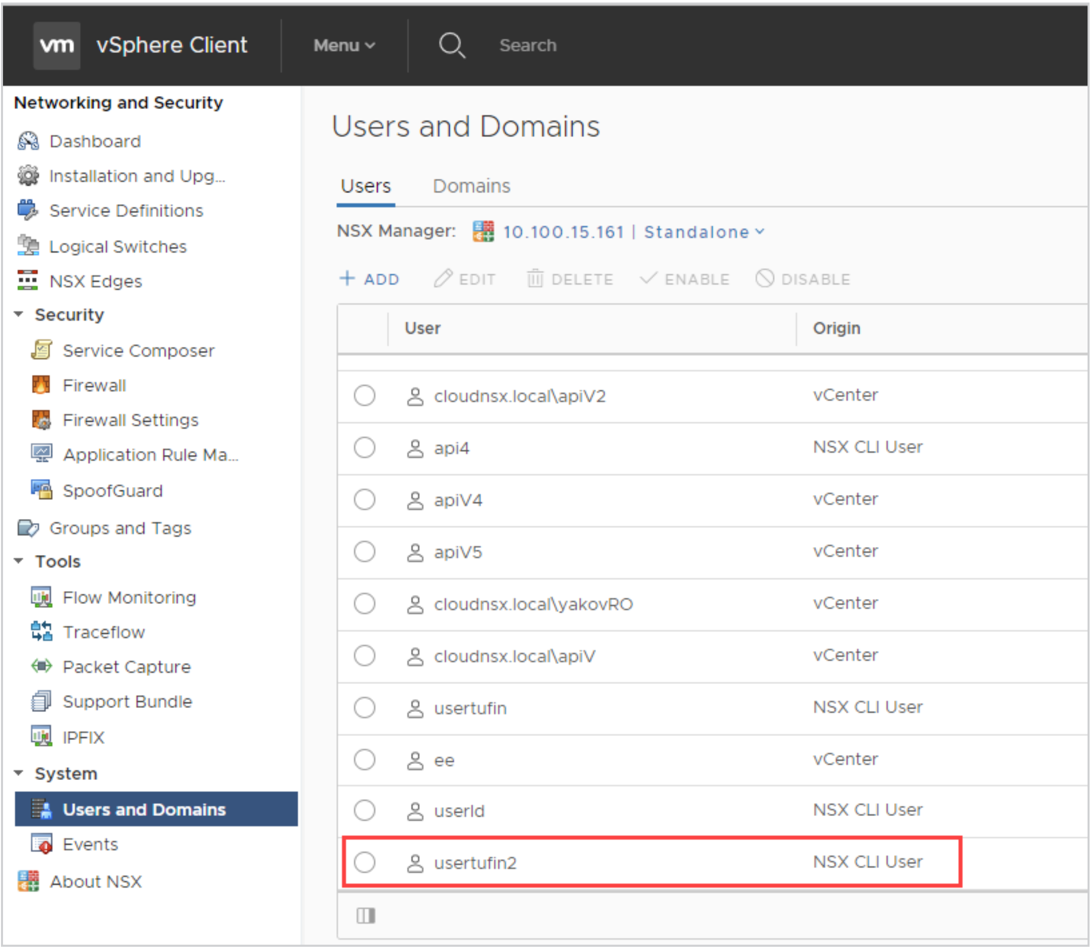
POST https://10.100.15.161/api/2.0/services/usermgmt/role/usertufin2?isCli=true

```

<accessControlEntry>

<role>auditor</role>

<resource>

<resourceId>globalroot-0</resourceId>

```

204 No Content 1716 ms 341 B

8. To verify that the user is created, in the vSphere Web Client navigate to **Menu > Networking & Security > Users and Domains > Users tab**.

   In the example below, the new user **usertufin2** is listed with the role you assigned:



Users and Domains

NSX Manager: 10.100.15.161 | Standalone

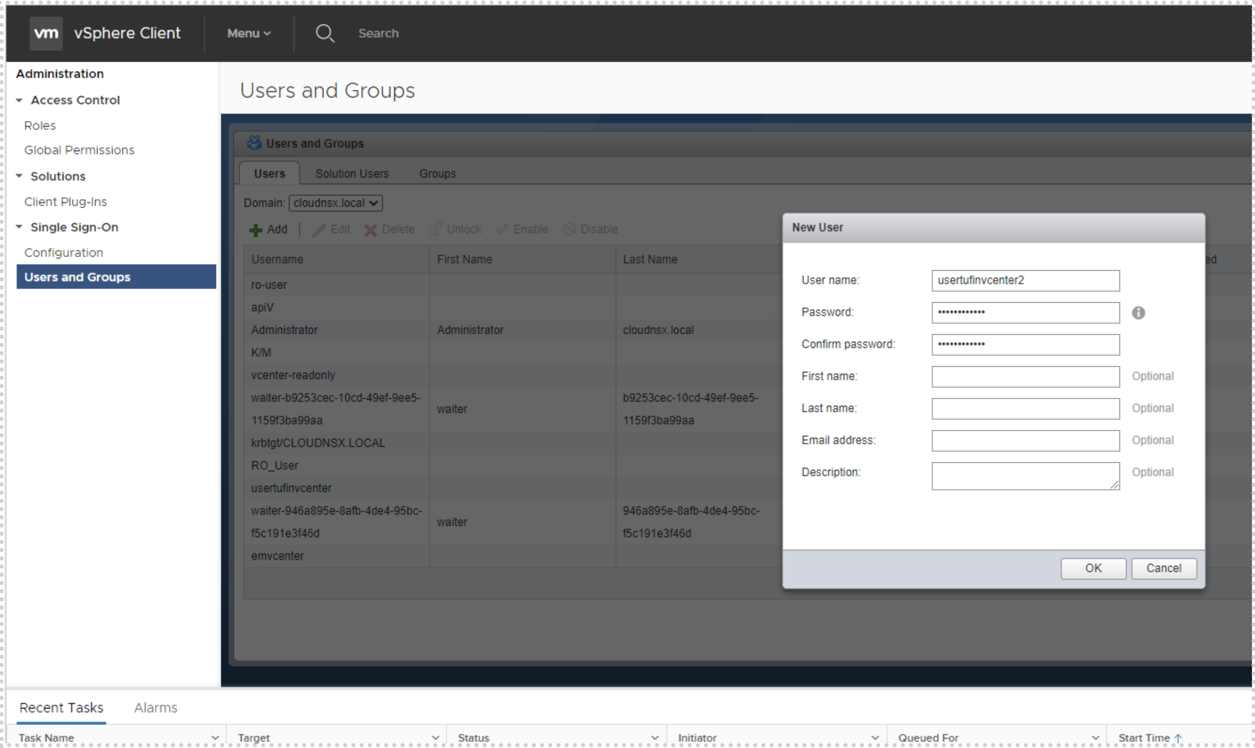
	User	Origin
○	cloudnsx.local\apiV2	vCenter
○	api4	NSX CLI User
○	apiV4	vCenter
○	apiV5	vCenter
○	cloudnsx.local\yakovRO	vCenter
○	cloudnsx.local\apiV	vCenter
○	usertufin	NSX CLI User
○	ee	vCenter
○	userId	NSX CLI User
○	usertufin2	NSX CLI User

For more information, see the Sneaku.com article "How to create a NSX-v API Only User Account".

B: Create a vCenter Single Sign On (SSO) User with the vSphere Web Client

1. Log in to vCenter and browse to **Menu > Administration > Single Sign-On > Users and Groups** in the vSphere Web Client.
2. To add a new user, in the **Users** tab, click ✚.
3. Enter a user name and password for the new user.
   - You cannot change the username after you create a user.
   - The password must meet the password policy requirements for the system.
   - Optional: Enter a first and last name for the user.
   - Optional: Enter an email address for the user.

4. Click **OK**.



Domain: cloudnsx.local

Username	First Name	Last Name
ro-user		
apiV		
Administrator	Administrator	cloudnsx.local
K/M		
vcenter-readonly		
waiter-b9253cec-10cd-49ef-9ee5-1159f3ba99aa	waiter	b9253cec-10cd-49ef-9ee5-1159f3ba99aa
krbtgt/CLOUDNSX.LOCAL		
RO_User		
usertufinvcenter		
waiter-946a895e-8afb-4de4-95bc-f5c191e3f46d	waiter	946a895e-8afb-4de4-95bc-f5c191e3f46d
emvcenter		

User name: usertufinvcenter2

Password: ••••••••••••

Confirm password: ••••••••••••

First name: Optional

Last name: Optional

Email address: Optional

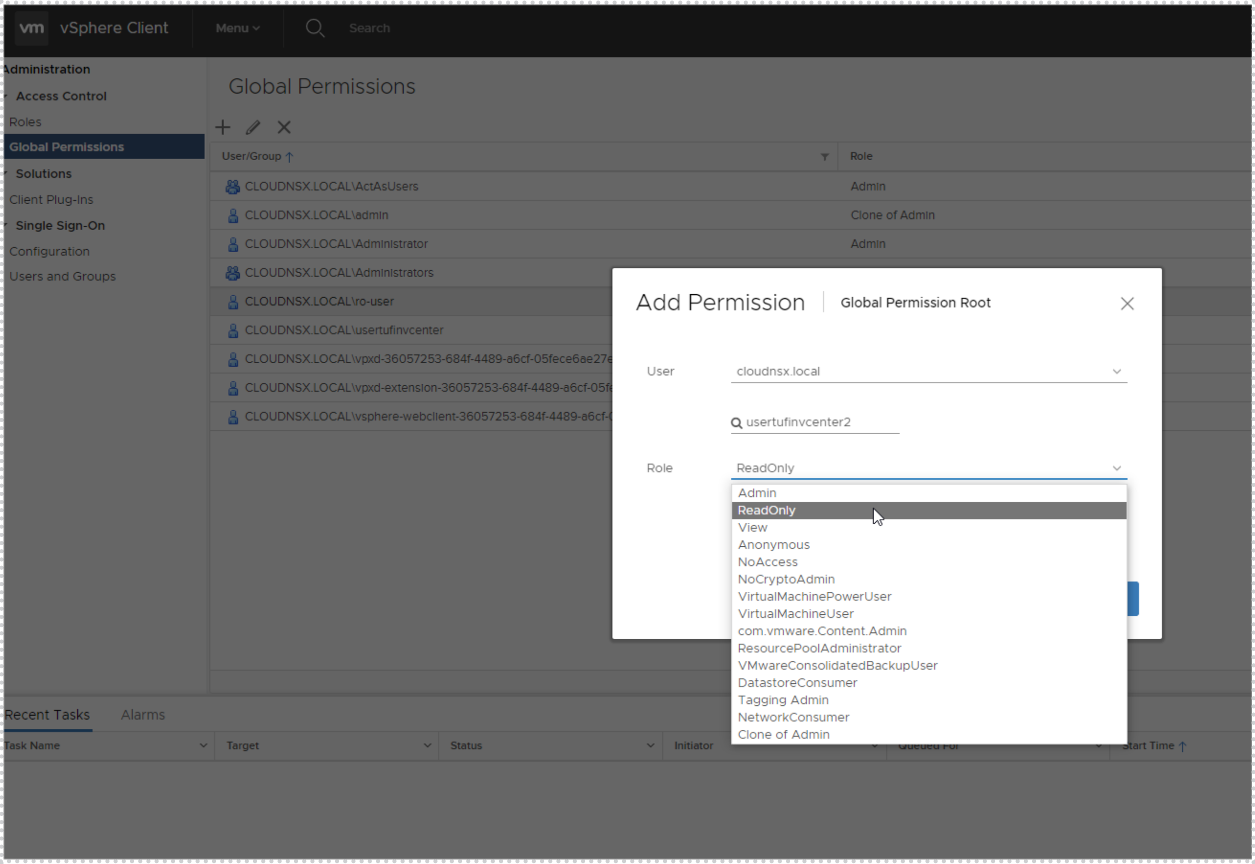
Description: Optional

This user should have access to view DFW policies, with read-only permission. For more information, see the VMware vSphere 5.1 Documentation Center article "Add a vCenter Single Sign On User with the vSphere Web Client".

C: Assign permissions to a vCenter Client user

1. In the vSphere Web Client navigate to **Administration > Access Control > Global Permissions**.
2. Select the user and click + to open the **Add Permission** window.

   In **Assigned Role**, select **Read-only** (or **Administrator** for user provisioning permissions) from the list of roles.



Global Permissions

User/Group	Role
CLOUDNSX.LOCAL\ActAsUsers	Admin
CLOUDNSX.LOCAL\admin	Clone of Admin
CLOUDNSX.LOCAL\Administrator	Admin
CLOUDNSX.LOCAL\Administrators	
CLOUDNSX.LOCAL\ro-user	
CLOUDNSX.LOCAL\usertufinvcenter	
CLOUDNSX.LOCAL\vpxd-36057253-684f-4489-a6cf-05fece6ae27e	
CLOUDNSX.LOCAL\vpxd-extension-36057253-684f-4489-a6cf-05f	
CLOUDNSX.LOCAL\vsphere-webclient-36057253-684f-4489-a6cf-	

Add Permission | Global Permission Root

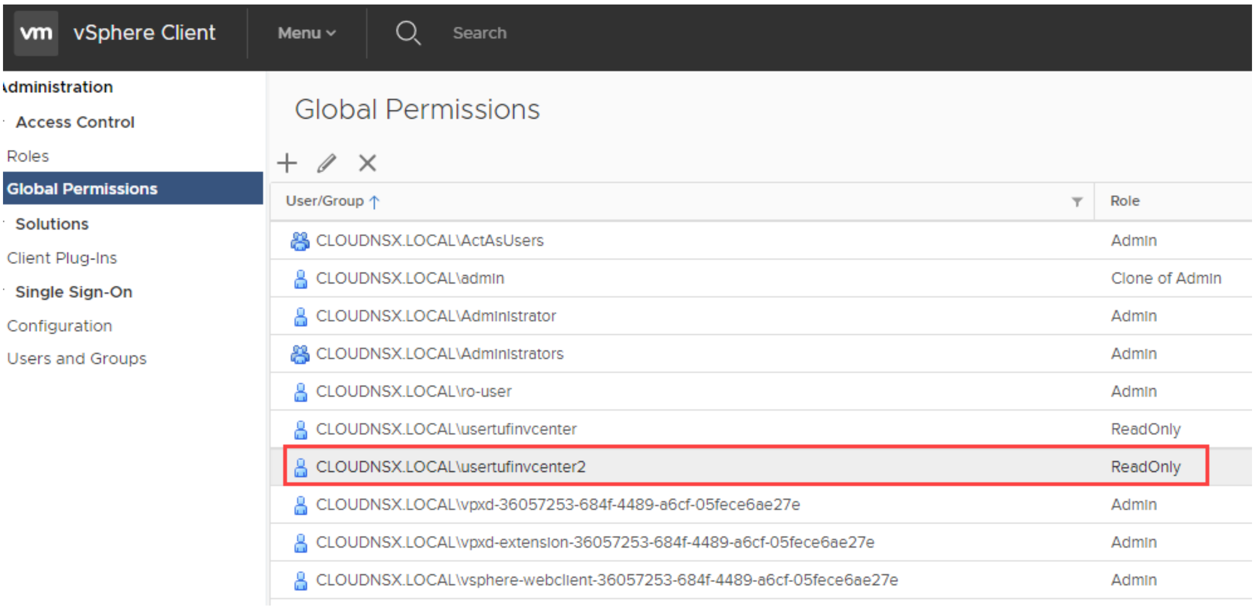
User: cloudnsx.local

usertufinvcenter2

Role: ReadOnly

3. Optional: Select the **Domain** from the list.
4. Click **OK**.

   The user appears in the list with the assigned **Read-only** role.



Global Permissions

User/Group	Role
CLOUDNSX.LOCAL\ActAsUsers	Admin
CLOUDNSX.LOCAL\admin	Clone of Admin
CLOUDNSX.LOCAL\Administrator	Admin
CLOUDNSX.LOCAL\Administrators	Admin
CLOUDNSX.LOCAL\ro-user	Admin
CLOUDNSX.LOCAL\usertufinvcenter	ReadOnly
CLOUDNSX.LOCAL\usertufinvcenter2	ReadOnly
CLOUDNSX.LOCAL\vpxd-36057253-684f-4489-a6cf-05fece6ae27e	Admin
CLOUDNSX.LOCAL\vpxd-extension-36057253-684f-4489-a6cf-05fece6ae27e	Admin
CLOUDNSX.LOCAL\vsphere-webclient-36057253-684f-4489-a6cf-05fece6ae27e	Admin

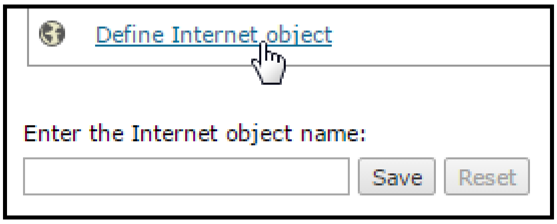
For more information, see the VMware vSphere 5.1 Documentation Center article "Assign Permissions in the vSphere Web Client". In step 6 of the procedure, select the **Auditor** role from the **Assigned Role** menu.

Define Internet Object

By default, TOS uses the ANY object to represent the all IPv4 addresses in the Internet in TOS features, such as SecureChange Designer. For Check Point and Stonesoft devices, the Internet object can be configured to use a custom object name that you define on the device.

To define the device object that represents the Internet:

1. Make sure you receive the first policy revision.
2. Select the device from the device tree.
3. Click **Define Internet object**.



Define Internet object

Enter the Internet object name:

4. Enter the name of the object in the device that represents the Internet (case-sensitive) and click **Save**.

   To change the Internet object back to the ANY object, click **Reset**.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Manage Devices**.

Managing Device Groups

You can organize your devices into groups to represent a logical grouping of your devices, such as grouping devices by network segment or security level.

When you create device groups, the groups are shown in the device tree for the Dashboard and the Risk, Cleanup and Change browsers. When you select a group, the charts and tables show the data for the members of the group.

The options in the ≡ ▾ menu change according to which objects are selected in the tree. If you select more than one type of object, the menu is disabled.

You can:

- **Delete one or more devices**
  1. In either the Vendors or Groups tree, select the devices that you want to delete.
  2. Click ≡ ▾ and click **Delete**.
- **Manage devices in groups**
  - **Create new groups**
  1. In the Groups tree, select the parent group for the new group. If Multi-Domain is implemented, you can add groups under the each domain, but not directly under the All Devices group.
     1. Enter a unique name for the new group in **Group name** and click **Save**.

     Each group directly under the same parent group must have a unique name. If you want to rearrange the groups after they are created, you must delete and re-add the groups that you want to move.
  - **Rename groups**
    1. In the Groups tree, select the group to rename.
    2. Edit the name and click **Save**.
  - **Delete groups**
    1. In the Groups tree, select the group to delete
    2. Click ≡ ▾ and click **Delete**.
  - **Add and remove devices from groups**
    1. In the Groups tree, select a group.
    2. Select the devices to move and use the › and ‹ buttons to move them into or out of the group.

You can also enter text into the search fields and press Enter or click 🔍 to filter the lists of devices.

- **Change the admin credentials for all devices in a group**
  1. In the Groups tree, select a group.
  2. Click ☰ ▾ and click **Change Credentials**.
  3. Enter and confirm any of the new credential details, including username, password or both. If relevant for the device, you can also enter and confirm a new enable password. If you leave fields blank, those details are not updated.
  4. Click **Apply** to save the new credentials for the devices in SecureTrack.

     Note: SecureTrack stops retrieving policies from the devices until you configure the matching credentials on the devices.

The changes to device groups take effect immediately and you can see the new device tree in the Dashboard and Browsers.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Device Groups**

Sending Additional Information via Syslog

Many of your monitored devices can be set up to send additional information to TOS, such as:

- Rule and object usage information that can be seen in SecureTrack, such as the rules that were invoked or 'hit'
- Accountability information that can be seen in SecureTrack, such as the users who made policy changes and the computer used to make the change
- Details of the applications that pass traffic through the device - can be seen in SecureApp
- Notifications to TOS that a security configuration change has occurred, so TOS can fetch the updated policy (revision) from the device immediately, rather than wait for the periodic polling

To get this additional information, you must configure your devices to send syslogs to SecureTrack.

Syslog traffic must be sent to port 514 on the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server), to the IP or host name of the server.

Syslog proxy is supported for specific devices. Only rules that are marked in the device for logging will be included in the syslogs.

For more information on syslog proxy support for supported devices, see the related topics in this section:

- Configuring Check Point Syslogs
- Retrieving the Check Point Audit Log
- Configuring Cisco Syslogs
- Configuring Fortinet Syslogs
- Configuring Juniper Syslogs
- Configuring VMware Syslogs
- Configuring Palo Alto Syslogs

Configuring Check Point Syslogs

What is Syslog for Check Point devices?

The syslog mechanism is used to pass policy change and traffic information from Check Point devices to SecureTrack. See Syslog VIP.

Why Do I Want to Use Syslog for My Check Point Devices?

For Check Point devices, this process lets users set up and use an alternative syslog mechanism for log collection instead of LEA logging.

Prerequisites

- Your company must have an existing root CA and passphrase.
- Before you start:
  - Verify that the machine that sends the logs and the Tufin server that monitors the management device are able to communicate on TCP port 6514.

- Ensure that the Check Point Log Exporter is installed on your management device.

  Create the log_exporter with the `cp_log_export add` command, as described in the **Check Point Support Center**: SecureKnowledge Details > Log Exporter - Check Point Log Export (Solution ID sk122323)

Compatibility issues

This setup is for Check Point R77 and R80 devices.

How do I set up syslog for Check Point?

The following process is required to set up a syslog mechanism for log collection for Check Point devices:

A. Create a Server Certificate for NGINX on the Tufin server.

B. Configure NGINX for mutual TLS authentication.

C. Create a client certificate for log_exporter on the Check Point server.

D. Modify the log_exporter configuration.

Create a Server Certificate for NGINX on the Tufin server

1. To create a private key for the server, run:

   ```
   openssl genrsa -out server.key 2048 chmod 400 server.key
   ```

2. To create a Certificate Signing Request (CSR), run:

   ```
   openssl req -new -key server.key -sha256 -out server.csr
   ```

   - **Common Name** attribute: Provide the IP address or resolvable host name of the Tufin server that will receive the logs. (Can be the Tufin Central Server, Distributed Server or a Remote Collector.)
   - All other attributes: Enter a period (•) to leave all other attributes blank.
   - Challenge password []: <leave empty>

     Do not use a period (•) for this value.

3. To use the root CA to sign the CSR, run:

   ```
   openssl x509 -req -days 365 -sha256 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 1 -out
   server.crt
   ```

   ```
   chmod 444 server.crt
   ```

4. To verify the validity of the certificate, run:

   openssl x509 -noout -text -in server.crt

5. To verify the signature, run:

   openssl verify -CAfile ca.crt server.crt

Configure NGINX for mutual TLS authentication

Configuration Prerequisite

It is assumed that certificate generation occurs on another machine. Before you configure NGINX, transfer the following files to the Tufin machine:

- **server.crt**
- **server.key**
- **ca.crt**

Configuration

Add the following lines to the **stream/server** section of the NIGINX config file `/etc/nginx/nginx.conf:`

```
listen 6514 ssl;

proxy_pass localhost:10514;

ssl_certificate <full path to ceritifcate dir>/server.crt;

ssl_certificate_key <full path to ceritifcate dir>/server.key;

ssl_client_certificate <full path to ceritifcate dir>/ca.crt;

ssl_verify_client on;

ssl_protocols TLSv1.2;
```

Create a client certificate for log_exporter on the Check Point server

This procedure is similar to the procedure for generating a server certificate.

1. To create a private key for the client, run:

   openssl genrsa -out client.key 2048

2. To create a Certificate Signing Request (CSR), run:

   openssl req -new -key client.key -out client.csr

   - **Common Name** attribute: Provide the (CMA/Domain) IP address or resolvable host name of client.
   - All other attributes: Enter a period (•) to leave all other attributes blank.
   - Challenge password []: <leave empty>

     Do not use a period (•) for this value.

3. To use the root CA to sign the CSR, run:

   openssl x509 -req -days 365 -sha256 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 2 -out client.pem

4. To verify the validity of the certificate, run:

   openssl x509 -noout -text -in client.crt

5. To verify the signature, run:

   openssl verify -CAfile ca.crt client.crt

6. To convert the certificate to .p12 format, run:

   openssl pkcs12 -inkey client.key -in client.crt -export -out client.p12

Modify the log_exporter configuration

This procedure describes how to modify the configuration of the existing log-exporter instance for TLS.

Configuration Prerequisites

- Ensure that the Check Point Log Exporter is installed on your management device.

  Create the log_exporter with the `cp_log_export add` command, as described in the **Check Point Support Center**: SecureKnowledge Details > Log Exporter - Check Point Log Export (Solution ID sk122323)

- It is assumed that certificate generation occurs on another machine. Before you configure the log_exporter, transfer the following files to the Check Point machine:

  - **ca.pem**
  - **client.p12**

Configuration

1. Run the following:

   ```
   cp_log_export set name <exporter-name> domain-server <domain-server> ca-cert <path_to_CA_pem>
   client-cert <path_to_p12_certificate> client-secret <challenge_phrase_for _p12>
   ```

2. Restart the log_exporter instance with the command:

   ```
   cp_log_export restart name <exporter-name>
   ```

3. Configure the log_id:

   ```
   edit <exporter-name>/conf/SyslogFormatDefinition.xml
   ```

4. Perform the following change to the existing file:

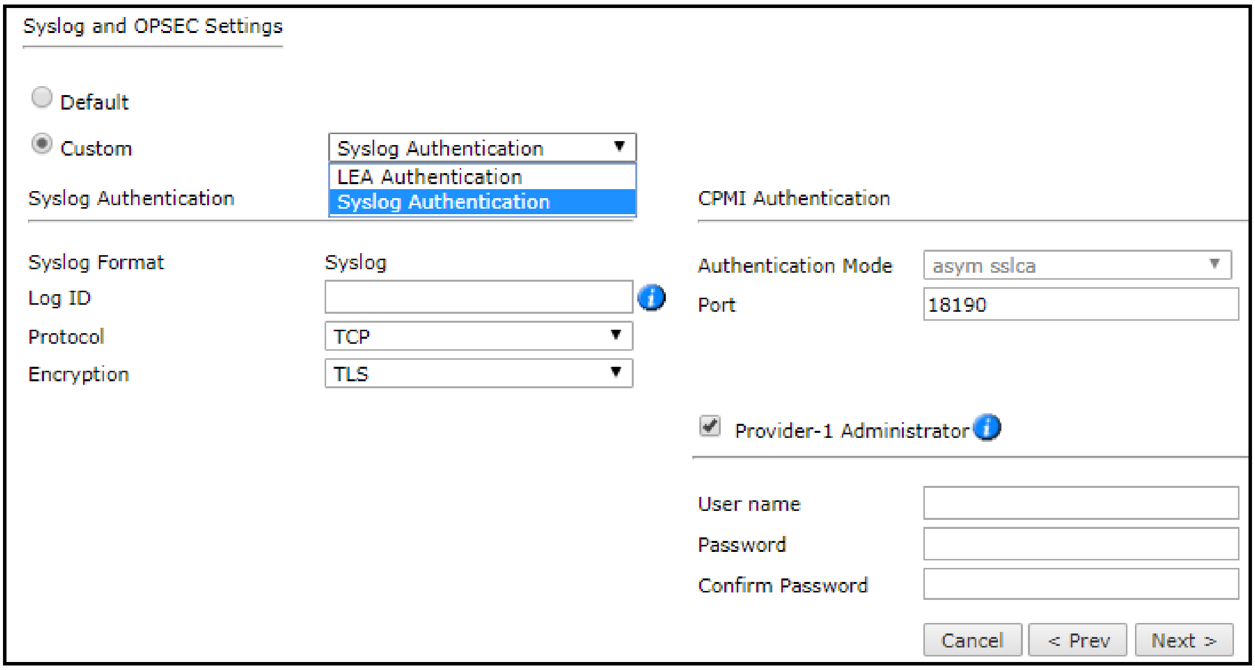
   From:

```
<!-- HOSTNAME-->
  <header>
    <default_value>-</default_value>
    <assign_order>init</assign_order>
      <callback>
        <name>get_host_name_callback</name>
      </callback>
  </header>
```

To:

```
<!-- HOSTNAME-->
  <header>
    <default_value><Desired-Log-ID-Name></default_value>
  </header>
```

The desired-log-id string must be the same as the **Log ID** you configure in Tufin:



Syslog and OPSEC Settings

○ Default

● Custom — Syslog Authentication

Syslog Authentication

Syslog Format: Syslog

Log ID:

Protocol: TCP

Encryption: TLS

CPMI Authentication

Authentication Mode: asym sslca

Port: 18190

☑ Provider-1 Administrator

User name:

Password:

Confirm Password:

5. Restart the log_exporter instance:

```
cp_log_export restart name <exporter-name>
```

Configuration Example

1. Create server key:

   openssl genrsa -out server.key 2048 chmod 400 server.key

   ```
   Generating RSA private key, 2048 bit long modulus
   ...........................................+++
   ..................+++
   e is 65537 (0x10001)
   ```

2. Create server request:

   openssl req -new -key server.key -sha256 -out server.csr

   ```
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   ```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:.
State or Province Name (full name) []:.
Locality Name (eg, city) [Default City]:.
Organization Name (eg, company) [Default Company Ltd]:.
Organizational Unit Name (eg, section) []:.
Common Name (eg, your name or your server's hostname) []:10.100.2.235
Email Address []:.
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:<leave empty>
An optional company name []:.
```

3. Create server certificate:

   ```
   openssl x509 -req -days 365 -sha256 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 1 -out server.crt
   Signature ok
   subject=/CN=10.100.2.235
   Getting CA Private Key
   Enter pass phrase for ca.key:tufin
   ```

4. Give permissions to server certificate file

   ```
   chmod 444 server.crt
   ```

5. Insert the following into `/etc/nginx/nginx.conf`

   ```
   vim /etc/nginx/nginx.conf
   ssl_certificate /root/newCA/server.crt;
   ssl_certificate_key /root/newCA/server.key;
   ssl_client_certificate /root/newCA/ca.crt;
   ssl_verify_client on;
   ```

6. Restart NGINX service:

   ```
   service nginx restart
   ```

7. Create client key:

   ```
   openssl genrsa -out client.key 2048
   Generating RSA private key, 2048 bit long modulus
   .............................+++
   .............+++
   e is 65537 (0x10001)
   ```

8. Create client request:

   ```
   openssl req -new -key client.key -out client.csr
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   ```

```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:.
State or Province Name (full name) []:.
Locality Name (eg, city) [Default City]:.
Organization Name (eg, company) [Default Company Ltd]:.
Organizational Unit Name (eg, section) []:.
Common Name (eg, your name or your server's hostname) []:10.100.110.212
Email Address []:.
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:<leave empty>
An optional company name []:.
```

9. Create client certificate:

   ```
   openssl x509 -req -days 365 -sha256 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 2 -out client.crt
   ```

   ```
   Signature ok
   subject=/CN=10.100.110.212
   Getting CA Private Key
   Enter pass phrase for ca.key:tufin
   ```

10. Convert client certificate to p12 format:

    ```
    openssl pkcs12 -inkey client.key -in client.crt -export -out client.p12
    ```

    ```
    Enter Export Password:tufin
    Verifying - Enter Export Password:tufin
    ```

11. Copy the CA certificate, client.p12 to the Check Point management device (to the `certs` folder under `targets/<syslogname>`).

    ```
    scp ca.crt client.p12 admin@10.100.110.212:/opt/CPmds-R77/customers/CMA_110.212_Management_Server/CPsuite-R77/fw1/log_exporter/targets/syslog235/certs/
    ```

12. In the Check Point CLI, enter the domain environment `mdsenv <ip-of-domain>` and edit the `targetConfiguration.xml` file for Check Point device.

    ```
    vim /opt/CPmds-R77/customers/CMA_110.212_Management_Server/CPsuite-R77/fw1/log_exporter/targets/syslog235/targetConfiguration.xml
    ```

    For example:

    ```
    <transport>
    <security>tls</security>
    <pem_ca_file>/opt/CPmds-R77/customers/CMA_110.212_Management_Server/CPsuite-R77/fw1/log_exporter/targets/syslog235/certs/ca.crt</pem_ca_file>
    <p12_certificate_file>/opt/CPmds-R77/customers/CMA_110.212_Management_Server/CPsuite-R77/fw1/log_exporter/targets/syslog235/certs/client.p12</p12_certificate_file>
    <client_certificate_challenge_phrase>tufin</client_certificate_challenge_phrase>
    </transport>
    ```

13. Restart syslog log_exporter in Check Point

    ```
    cp_log_export restart name syslog235
    ```

14. Verify that syslog is encrypted via tcpdump on tufin service

    ```
    tcpdump -A -c200 -nni eth0 port <port_that_received_syslog>
    ```

    ```
    tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
    ```

```
 listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

d...#.&qka.(.S..........

.ifg]T...\.$w.k..I....B...H.H<j....I.......8x...o...7..p....Z..`..P.j@....Ip.f.W.O....a.m.l.....z..M
d...&Id.J..F..'S../..l..q8)..@.h.2......i.8.1...x..`/..2..l.}4'..K..>+...."..v

...u.v.}/.@.\.....h...,.*D.5...!... a..X<..+...`.Pw@m.%.....7.....%n
(........y.|#.s.@...........+.u.w>+M....(.J........s.h|...m.d......w..HDI...1W...H....l>.$7

17:52:25.931561 IP 10.100.2.235.550 > 10.100.110.10.49955: Flags [.], ack 668, win 1282, options
[nop,nop,TS val 2270172977 ecr 2438094682], length 0


E..4t{@.@.@.

d..
 Dn
```

15. Configure log id:

    vi <target-name>/conf/SyslogFormatDefinition.xml

    Change from existing:

    ```
    <!-- HOSTNAME-->
    <header>
    <default_value>-</default_value>
    <assign_order>init</assign_order>
     <callback>
     <name>get_host_name_callback</name>
     </callback>
    </header>
    ```

    To:

    ```
    <!-- HOSTNAME-->
    <header>
    <default_value><Desired-Log-ID-Name></default_value>
    </header>
    ```

Additional Information

For more information see:

- Introduction to mutual SSL authentication: https://www.codeproject.com/Articles/326574/An-Introduction-to-Mutual-SSL-Authentication
- The main guide for setting up TLS authentication: https://blog.codeship.com/how-to-set-up-mutual-tls-authentication/
- Check Point sk122323 for log exporter which includes TLS configuration: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122323
- Multiple clients in mutual authentication: https://medium.com/@Jenananthan/nginx-mutual-ssl-one-way-ssl-with-multiple-clients-ae87b3de0935
- NGINX as a reverse proxy configuration: https://docs.nginx.com/nginx/admin-guide/load-balancer/tcp-udp-load-balancer/

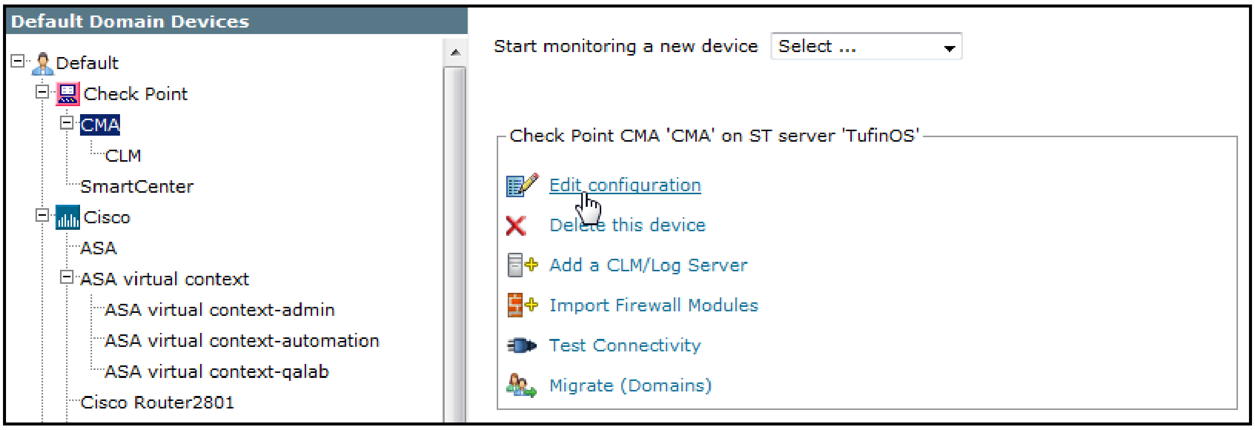
Retrieving the Check Point Audit Log

By default, Check Point management servers (SmartCenters and Provider-1 CMAs) store audit logs that track administrative actions locally, rather than sending them to the Log Server or CLM. SecureTrack retrieves audit logs from the management server, not from the Log Server or CLM. If you configured your management server to send audit logs to the Log Server or CLM, you must configure SecureTrack to retrieve them from there.

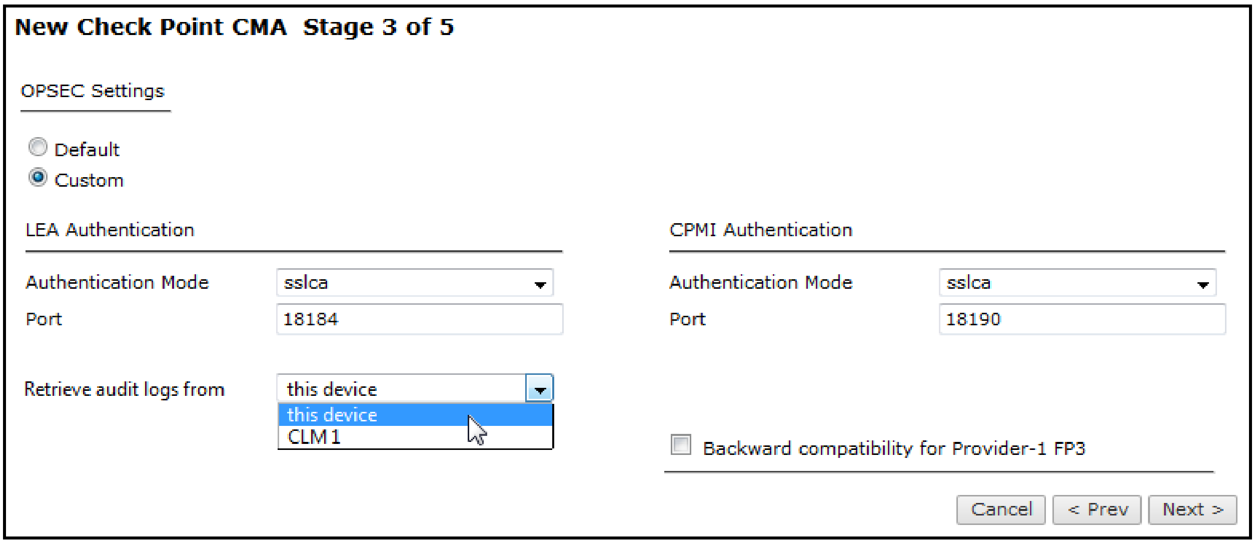
To configure SecureTrack to retrieve audit logs from the Log Server or CLM:

1. Add to SecureTrack the first management server and its associated Log Server or CLM.
2. In the **Device Configuration** list, select the relevant management server (not the log server).

3. Click **Edit configuration**:



4. Click **Next** and **Next**.
5. In the **stage 3** page, select **Custom**.
6. By **Retrieve audit logs from**, select the appropriate CLM/Log Server:



New Check Point CMA Stage 3 of 5

OPSEC Settings

○ Default
● Custom

LEA Authentication

Authentication Mode: sslca
Port: 18184

Retrieve audit logs from: this device

CPMI Authentication

Authentication Mode: sslca
Port: 18190

□ Backward compatibility for Provider-1 FP3

7. Click **Next**, and then **Save**.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Device Groups**

Configuring Cisco Syslogs

To monitor with full accountability, your Cisco devices must send syslogs to SecureTrack. To do this, define SecureTrack as a syslog server for each monitored Cisco switch, router, and firewall.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Certain devices can also use syslogs to collect traffic information that you can use for the Automatic Policy Generator (APG).

The firewalls in the organization must be configured to allow the relevant traffic.

For switches, SecureTrack associates syslogs with their source device only by IP address. Therefore, accountability information for switches will be incorrect if the syslogs are sent from an IP address other than the one monitored by SecureTrack.

For Cisco devices, a logging string is used to map a syslog message to a Device ID. If the logging string is not mapped, there is a fallback mechanism that maps the log message to the source IP of the packet. This mechanism does not work if the log message is sent via a syslog server because the syslog source-IP would be that of the syslog server and not that of the monitored device.

If the logging string is changed from “A” to “B”, SecureTrack cannot recognize logs by their contents until a new revision is received. During the period of time before the new revision arrives, the source-IP fallback allows SecureTrack to correctly recognize the device that sent the logs, provided that the syslog server is not used.

To use syslog server forwarding, ensure the following:

- The syslog server does not modify the message content
- The device is configured with the logging host
- A revision has been received by the current logging host

Configuring a Cisco ASA to Send Syslogs

To configure Cisco ASA or virtual context syslogs to be sent, configure either from the CLI or from ADSM according to the instructions below.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

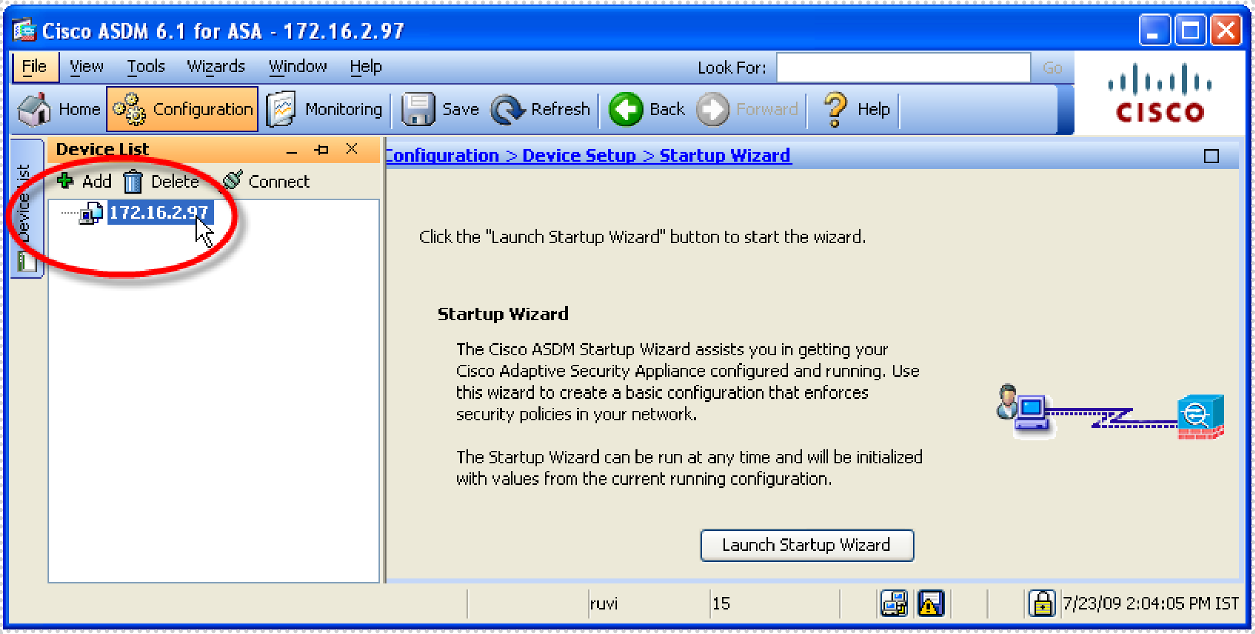
CLI Commands

Configure the device to send syslog messages	logging enable
Set that the timestamp is included in the syslog message	logging timestamp
Set the level of events for which syslog messages are sent	logging facility 23
Set the device-id that is included in the syslog message	logging device-id hostname
Set the device-id that is included in the syslog message with a virtual context	logging device-id context-name
Set to send events to SecureTrack for full accountability	logging list securetrack message 111008
Set to send events for SecureTrack APG and SecureApp discovery	logging list securetrack message 106100
Set to send events for SecureTrack APG and SecureApp discovery	logging list securetrack message 106023
Set the level of severity of the messages that you want to receive	• logging message 111008 level notifications • logging message 106100 level notifications • logging message 106023 level notifications
Set the trap message list name for the syslog messages	logging trap securetrack
Set the SecureTrack server to send the syslog messages to: • ip_address - The IP address of the SecureTrack server. • interface_name - The interface that the SecureTrack server is behind.	logging host <interface_name> <ip_address>

ASDM Configuration

1. Log into the ASDM and enter the syslog configuration for the ASA device:

   a. Log into the ASDM, and select the device from the Device List.


Cisco ASDM 6.1 for ASA - 172.16.2.97
File View Tools Wizards Window Help
Look For: Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Add Delete Connect
172.16.2.97
Configuration > Device Setup > Startup Wizard
Launch Startup Wizard
ruvi 15
7/23/09 2:04:05 PM IST

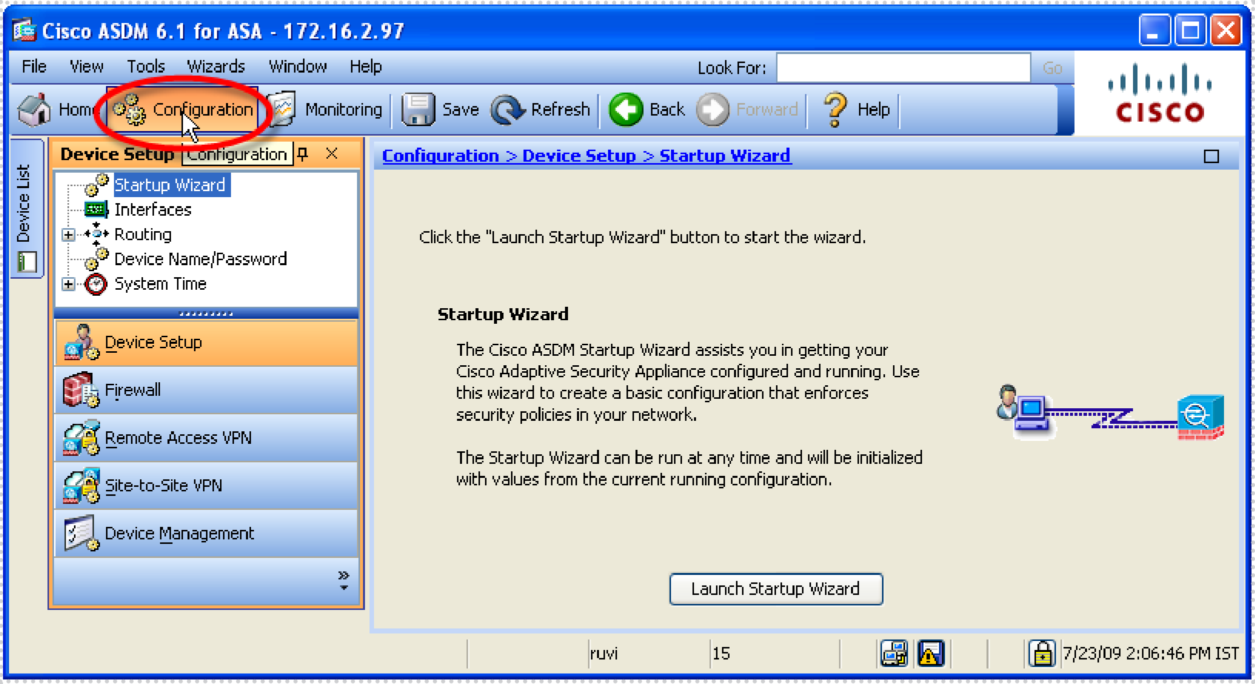
Click the "Launch Startup Wizard" button to start the wizard.

Startup Wizard

The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.

The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

   b. Click **Configuration**.



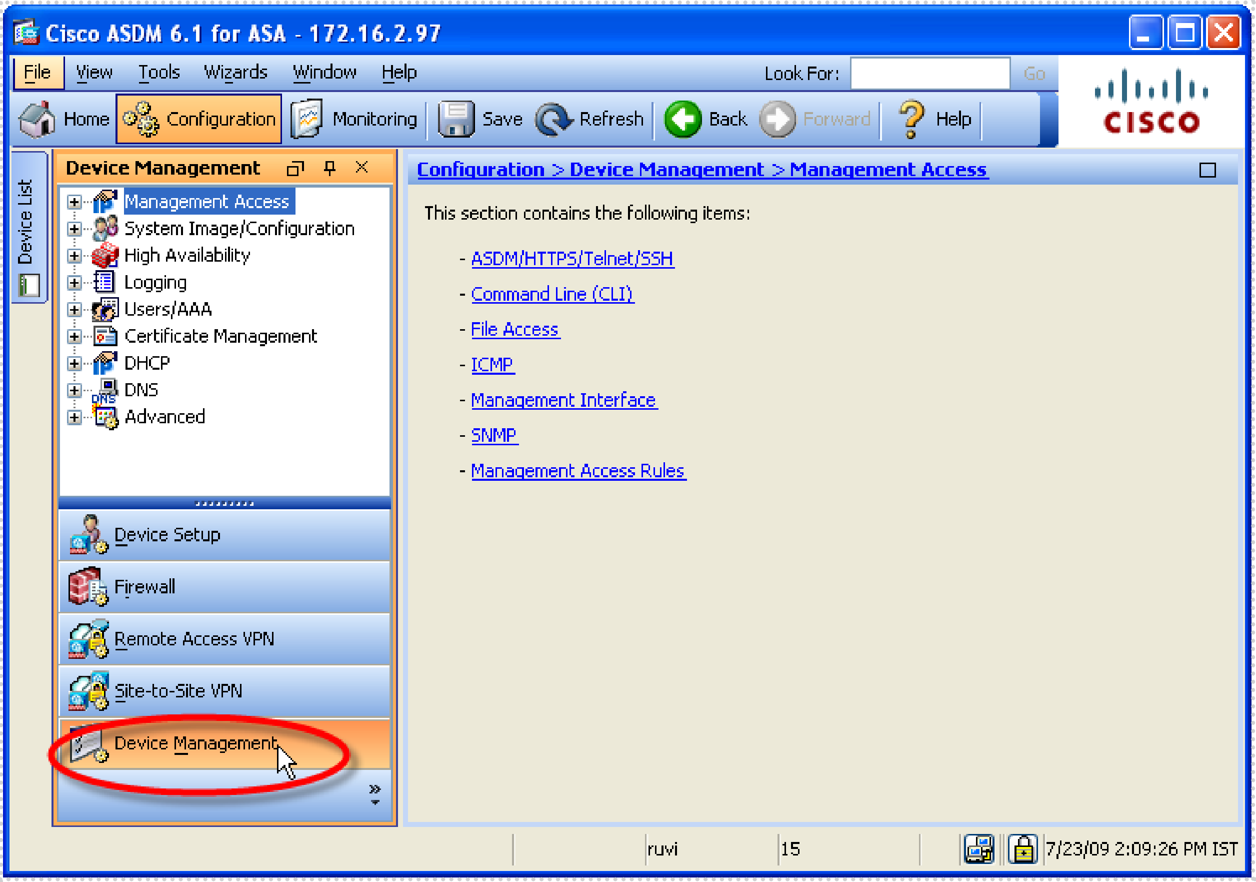
Click the "Launch Startup Wizard" button to start the wizard.

Startup Wizard

The Cisco ASDM Startup Wizard assists you in getting your Cisco Adaptive Security Appliance configured and running. Use this wizard to create a basic configuration that enforces security policies in your network.

The Startup Wizard can be run at any time and will be initialized with values from the current running configuration.

c. Click **Device Management**.

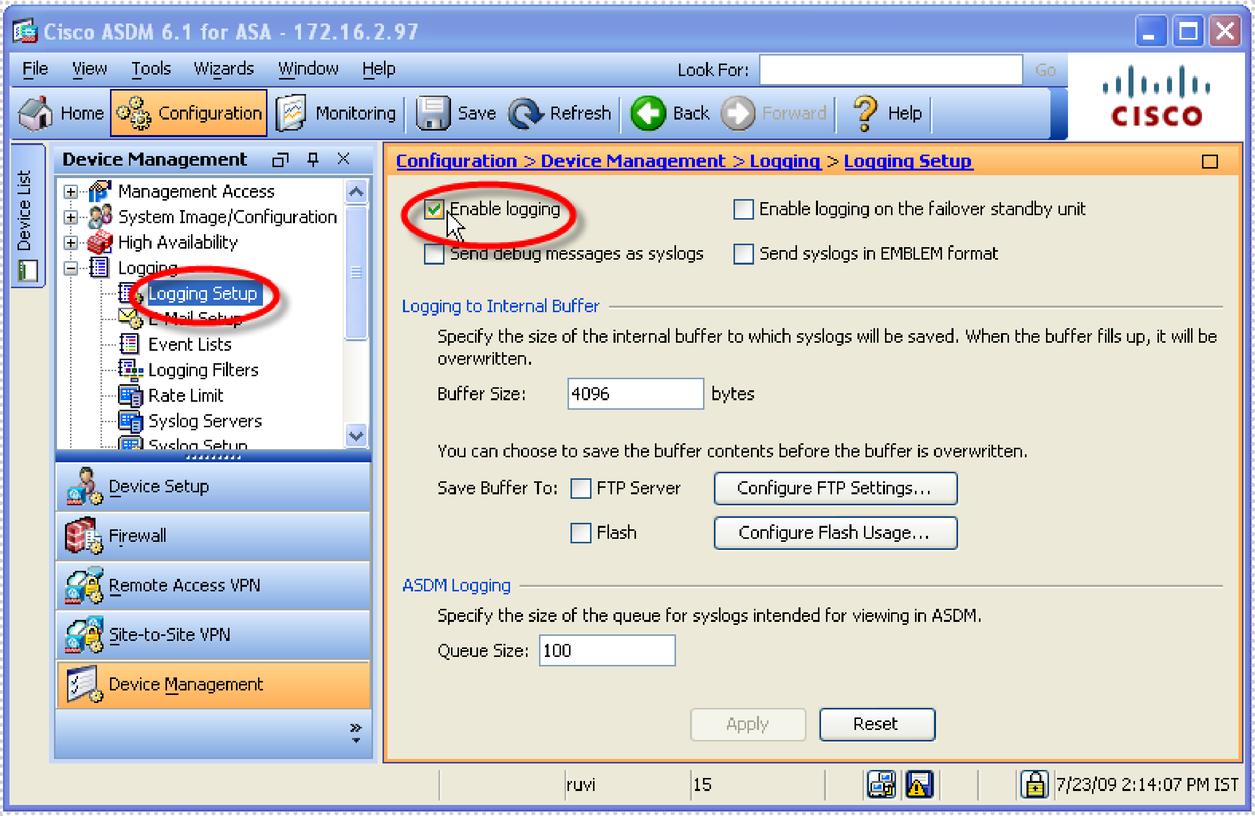


This section contains the following items:

- ASDM/HTTPS/Telnet/SSH
- Command Line (CLI)
- File Access
- ICMP
- Management Interface
- SNMP
- Management Access Rules

2. Enable logging on the ASA device:

- In **Logging** > **Logging Setup**, select **Enable logging**.



Configuration > Device Management > Logging > Logging Setup

☑ Enable logging ☐ Enable logging on the failover standby unit

☐ Send debug messages as syslogs ☐ Send syslogs in EMBLEM format

Logging to Internal Buffer

Specify the size of the internal buffer to which syslogs will be saved. When the buffer fills up, it will be overwritten.

Buffer Size: 4096 bytes

You can choose to save the buffer contents before the buffer is overwritten.

Save Buffer To: ☐ FTP Server [Configure FTP Settings...]

☐ Flash [Configure Flash Usage...]

ASDM Logging

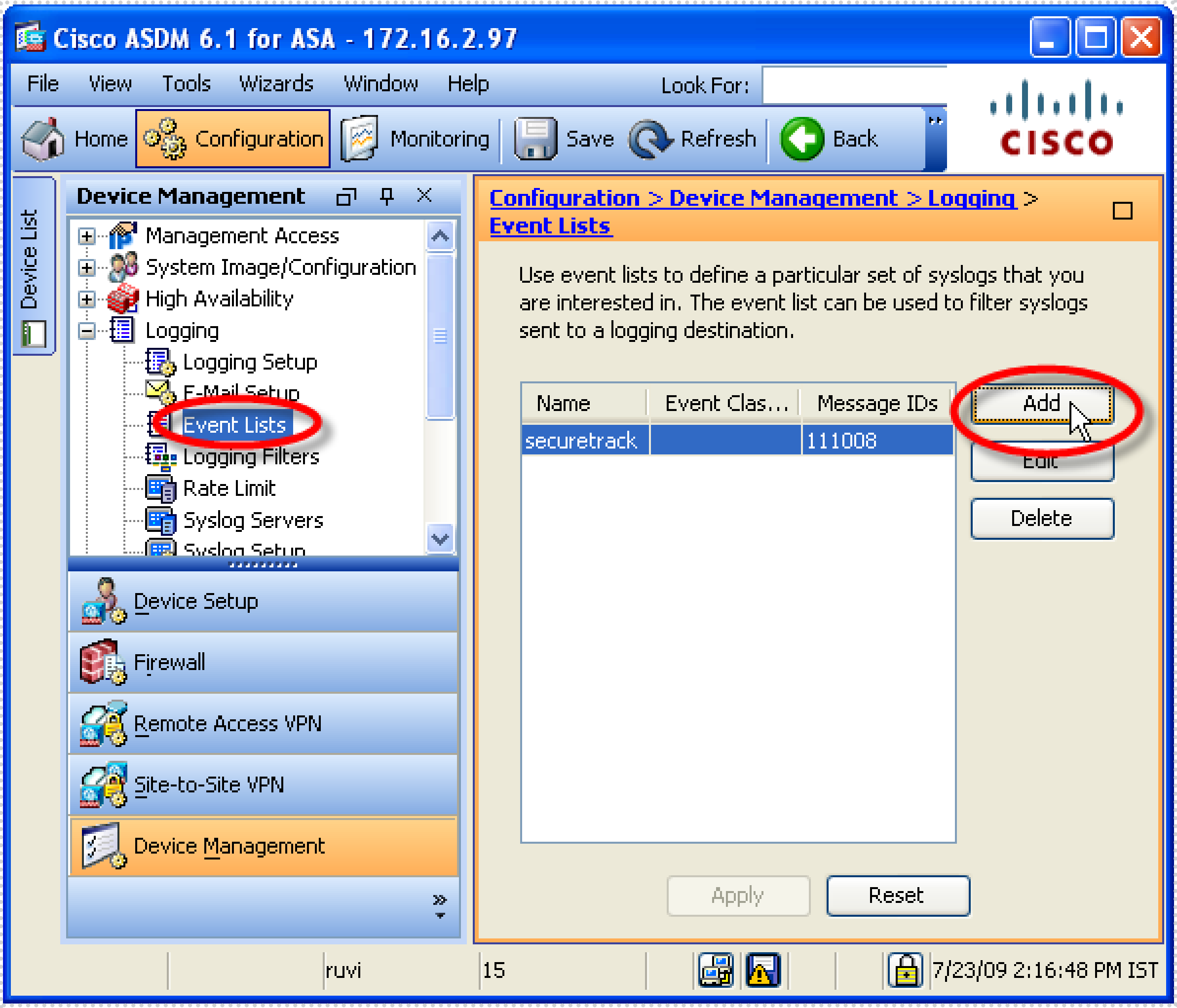
Specify the size of the queue for syslogs intended for viewing in ASDM.

Queue Size: 100

[Apply] [Reset]

3. Add the event IDs that you want to the ASA device to send:

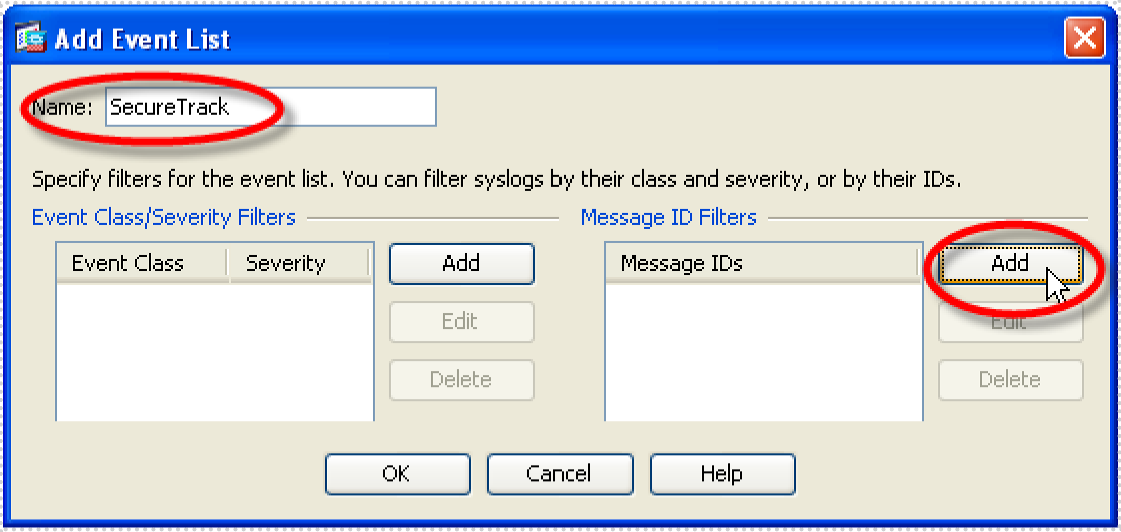
a. Select **Event Lists**, and click **Add**.



Use event lists to define a particular set of syslogs that you are interested in. The event list can be used to filter syslogs sent to a logging destination.

Name	Event Clas...	Message IDs
securetrack		111008

b. In the **Add Event List** window, type a **Name**, and under **Message ID Filters**, click **Add**.



Name: SecureTrack

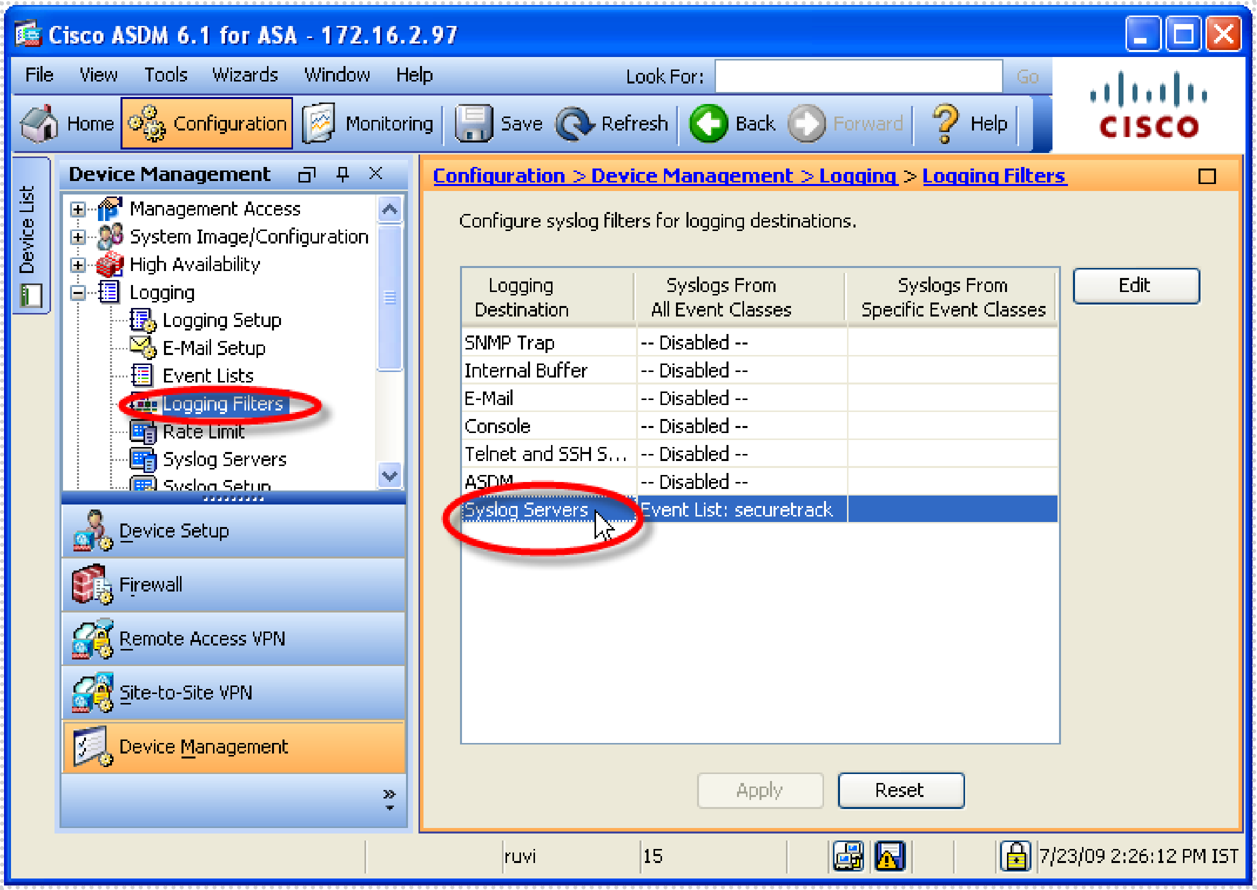
Specify filters for the event list. You can filter syslogs by their class and severity, or by their IDs.

c. Enter a syslog ID and click **OK**.

Syslog ID	Purpose	Notes
111008	Full accountability	
106023 106100	SecureTrack APG and SecureApp connection discovery	- Syslog ID 106100 only sends syslogs for logged rules. - For APG, you can use either of the syslog IDs or both IDs 1. Click OK to close the Add Event List window.

4. Configure the logging filters to use the specified event IDs:

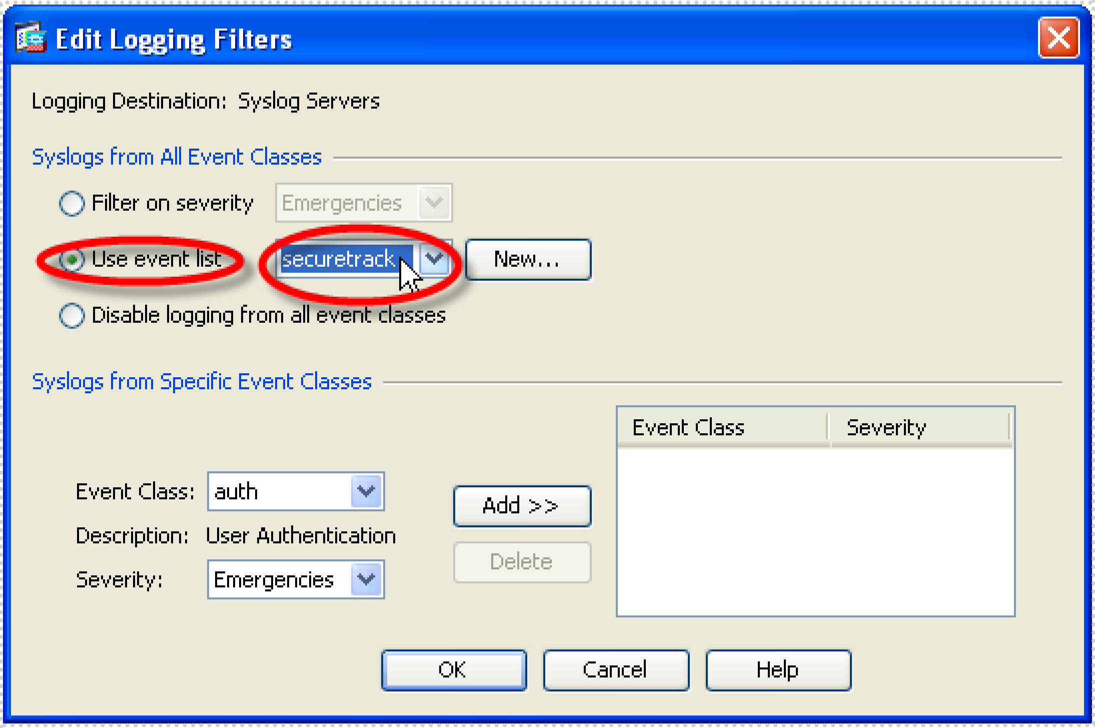
   a. Select **Logging Filters**, and double-click **Syslog Servers**.



Configure syslog filters for logging destinations.

Logging Destination	Syslogs From All Event Classes	Syslogs From Specific Event Classes
SNMP Trap	-- Disabled --	
Internal Buffer	-- Disabled --	
E-Mail	-- Disabled --	
Console	-- Disabled --	
Telnet and SSH S...	-- Disabled --	
ASDM	-- Disabled --	
Syslog Servers	Event List: securetrack	

b. In the **Edit Logging Filters** window, select **Use event list** and select the event list configured above.



Edit Logging Filters

Logging Destination: Syslog Servers

Syslogs from All Event Classes

○ Filter on severity: Emergencies

● Use event list: securetrack

○ Disable logging from all event classes

Syslogs from Specific Event Classes

Event Class: auth

Description: User Authentication

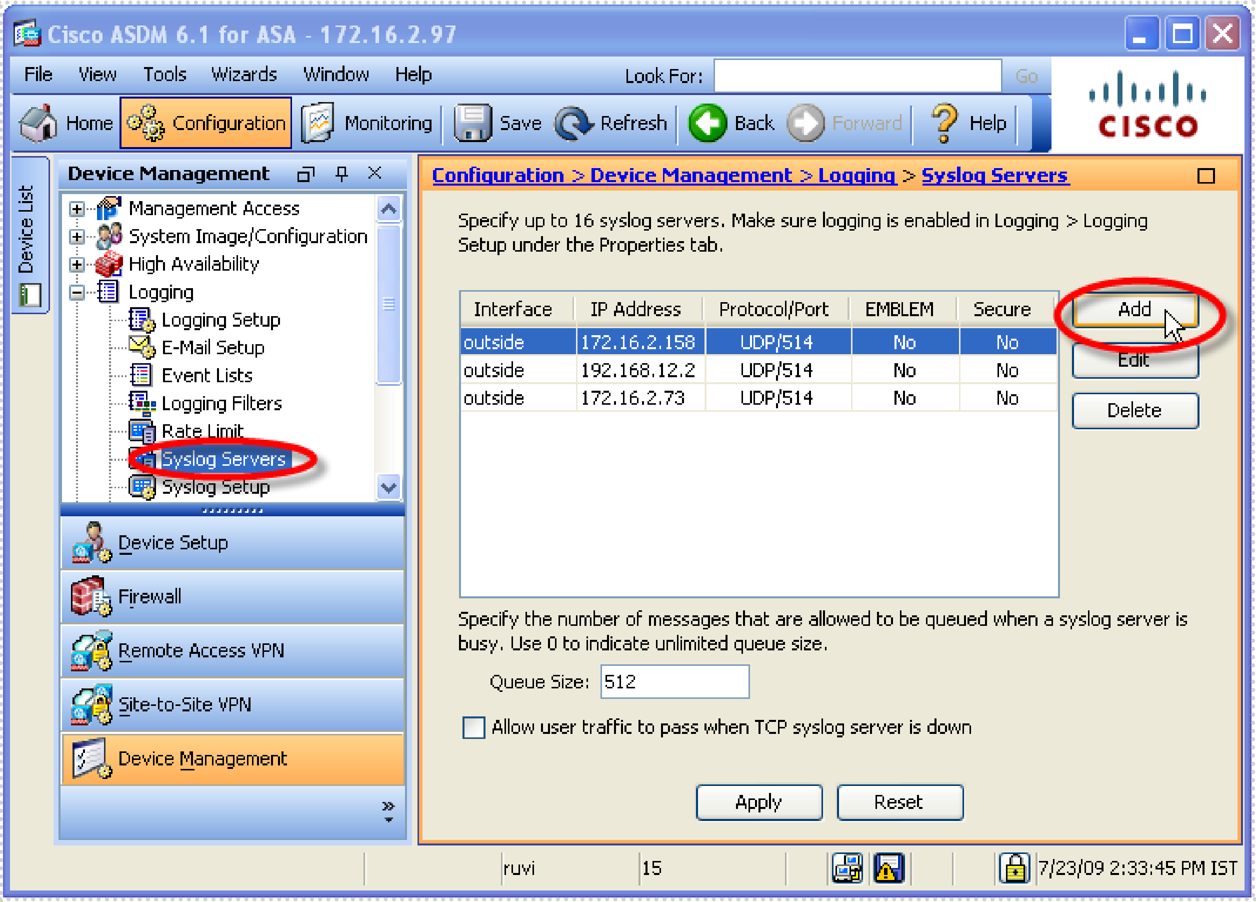
Severity: Emergencies

Event Class	Severity

c. Click **OK**.

5. Configure SecureTrack as a syslog server:

a. Select **Syslog Servers**, and click **Add**.



Configuration > Device Management > Logging > Syslog Servers

Specify up to 16 syslog servers. Make sure logging is enabled in Logging > Logging Setup under the Properties tab.

Interface	IP Address	Protocol/Port	EMBLEM	Secure
outside	172.16.2.158	UDP/514	No	No
outside	192.168.12.2	UDP/514	No	No
outside	172.16.2.73	UDP/514	No	No

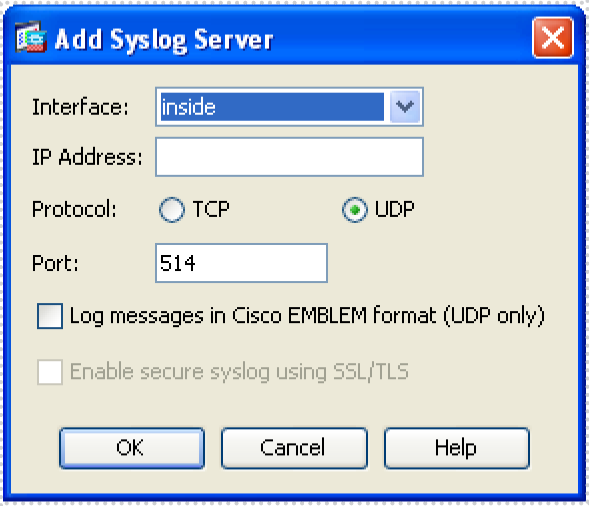
Specify the number of messages that are allowed to be queued when a syslog server is busy. Use 0 to indicate unlimited queue size.

Queue Size: 512

□ Allow user traffic to pass when TCP syslog server is down

b. In the Add Syslog Server window, select the interface used to access SecureTrack, and enter the IP address of the SecureTrack server, remote collector or distribution server that is managing the device.

c. Select **UDP**, **Port**: `514` , and clear **Log messages in Cisco EMBLEM format**.



Interface: inside

IP Address:

Protocol: ○ TCP ● UDP

Port: 514

□ Log messages in Cisco EMBLEM format (UDP only)

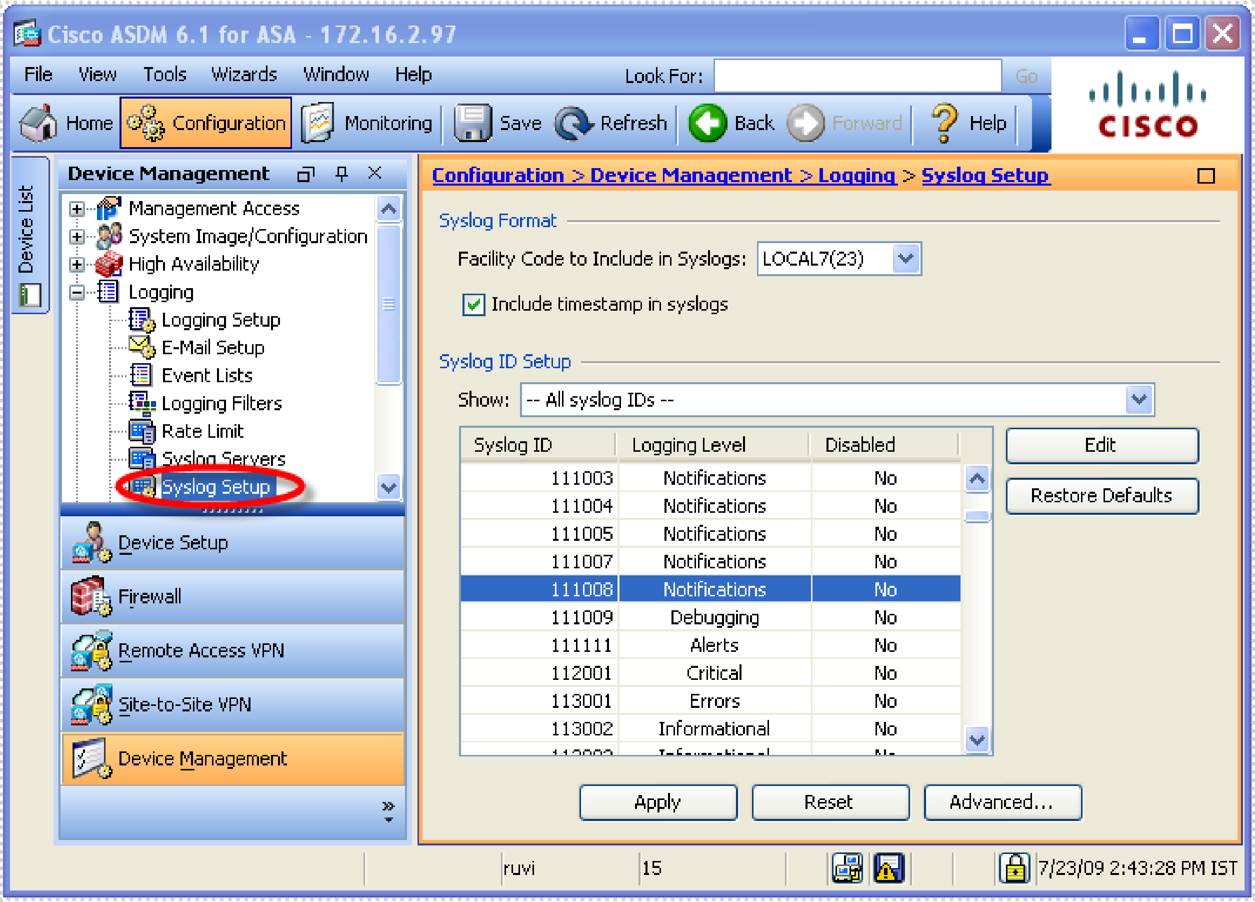
□ Enable secure syslog using SSL/TLS

d.

e. Click **OK**.

6. Configure the format for the syslogs:

a. Select **Syslog Setup**.



Facility Code to Include in Syslogs: LOCAL7(23)

☑ Include timestamp in syslogs

Show: -- All syslog IDs --

Syslog ID	Logging Level	Disabled
111003	Notifications	No
111004	Notifications	No
111005	Notifications	No
111007	Notifications	No
111008	Notifications	No
111009	Debugging	No
111111	Alerts	No
112001	Critical	No
113001	Errors	No
113002	Informational	No

b. Select **Include timestamp in syslogs**.

c. By **Facility Code to Include in Syslogs**, select **LOCAL7(23)**.

To use a different facility, you must configure SecureTrack as described in this tech note: Configuring SecureTrack for Non-Default Syslogs

d. Scroll down and double-click entry **111008**. Set its **Logging Level** to **Notifications**, and click **OK**.

e. Click **Apply**.

f. Still in the Syslog Setup page, click **Advanced** and select **Enable syslog device ID**.

If the device is not in context mode, you must enable the syslog device ID from the device's CLI with this command: `logging device-id string <Enter the ID>`

g. Configure a unique logging ID by selecting one of the following. No other device, including virtual contexts even on other devices, may have the same ID:

- **Hostname**
- **Context name** (in a Virtual Context)
- **IP address** (select an interface)
- **String** (type the desired ID)

h. Click **OK**, and **Apply**.

For virtual contexts, configure a logging ID for each context.

Configuring a Cisco IOS Router or Switch to Send Syslogs

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

To configure sending syslogs from a Cisco router or switch (for accountability):

1. Open a command line to the device, and run the following commands:

   ```
   configure terminal
   logging on
   logging facility local7
   logging trap notifications
   logging host <ST_IP>
   ```

   where <ST_IP> is the IP address of the SecureTrack server, remote collector or distribution server that is managing the device.

2. For routers only (not switches), configure a unique logging ID in one of the following ways. No other device or virtual context may have the same ID:

   - To set the logging ID to the hostname, run:

     ```
     logging origin-id hostname
     ```

   - To set the logging ID to another name, run:

     ```
     logging origin-id string <name>
     ```

     where <name> is the new unique logging ID.

     To use a non-default facility, see the Tech Note to configure SecureTrack for non-default syslogs.

Configuring a Cisco Nexus Switch to Send Syslogs

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

To configure sending syslogs from a Cisco Nexus switch (for Full Accountability):

- Open a command line to the device, and run the these commands:

  configure terminal

  logging server <ST_IP>

  where <ST_IP> is the IP address of the SecureTrack server, remote collector or distribution server that is managing the device.

  If you need to use a non-default facility, you can, in which case you'll also need to configure SecureTrack as described in this tech note.

Configuring a Cisco Firewall Management Center (FMC) to Send Syslogs

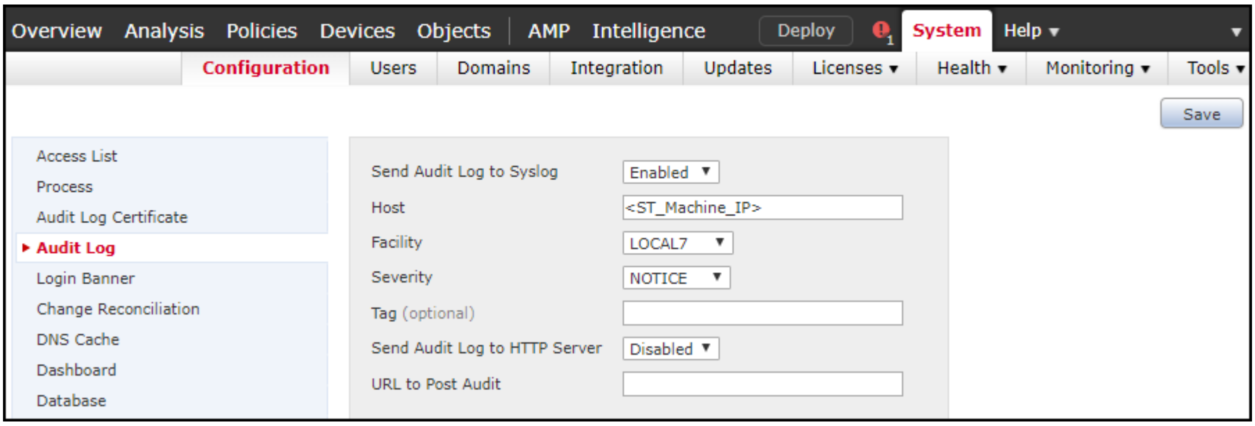
If you want to collect usage from Cisco Firewall Threat Defense (FTD) devices managed by an FMC, you can configure a policy in the FMC to send syslogs to SecureTrack. This configuration will apply to all the policy's rules that send syslogs to SecureTrack.

Configuring the FMC comprises the following stages:

1. "Enable Syslog in FMC (Accountability)" on the next page
2. "Enable a Syslog Device ID on the FTDs (Data Usage)" on the next page
3. "Create a new Syslog alert" on page 259
4. "Edit an FMC policy to send syslogs using the new alert" on page 260

Enable Syslog in FMC (Accountability)

1. In the FMC, navigate to the **System > Configuration** tab.
2. Select **Audit Log**.



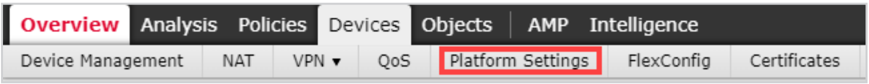
Send Audit Log to Syslog	Enabled ▼
Host	<ST_Machine_IP>
Facility	LOCAL7 ▼
Severity	NOTICE ▼
Tag (optional)	
Send Audit Log to HTTP Server	Disabled ▼
URL to Post Audit	

3. Configure the following parameters:
   - Set **Send Audit Log to Syslog** to Enabled.
   - In the **Host** field, enter the IP address of the SecureTrack servef
   - Set **Facility** to LOCAL7.
   - Set **Severity** to NOTICE.
   - In the **Tag** field, enter the Log Tag defined in the Syslog Authentication window (Stage 3 of 5) when the device was configured. This tag will be used in SecureTrack under “Syslog Authentication” as the Tag ID. The tag must be unique per FMC device.
4. Click **Save.**

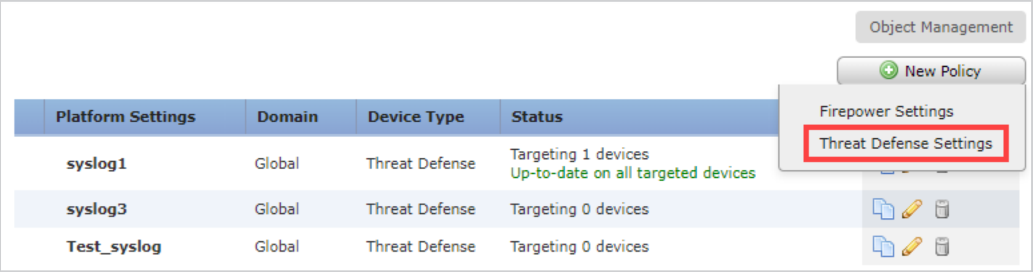
Enable a Syslog Device ID on the FTDs (Data Usage)

After the FMC device is configured, in SecureTrack, you can configure the device to collect usage data.

1. In the FMC, navigate to the **Devices > Platform Settings** tab.

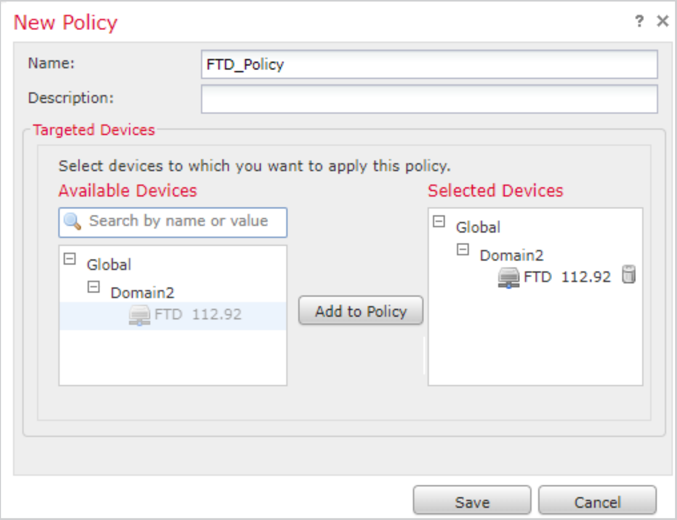


2. To create a new policy: (If you are configuring an existing policy, skip to step 3)
   a. Click **New Policy** > **Threat Defense Settings**.



Platform Settings	Domain	Device Type	Status
syslog1	Global	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices
syslog3	Global	Threat Defense	Targeting 0 devices
Test_syslog	Global	Threat Defense	Targeting 0 devices

The **New Policy** dialog box appears.



New Policy

Name: FTD_Policy

Description:

Targeted Devices

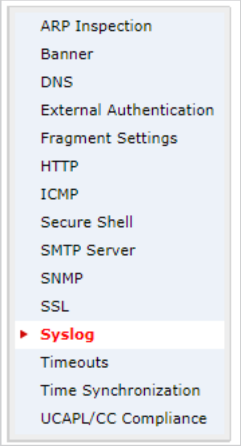
Select devices to which you want to apply this policy.

b. In the **Name** field, enter a name for the new policy.

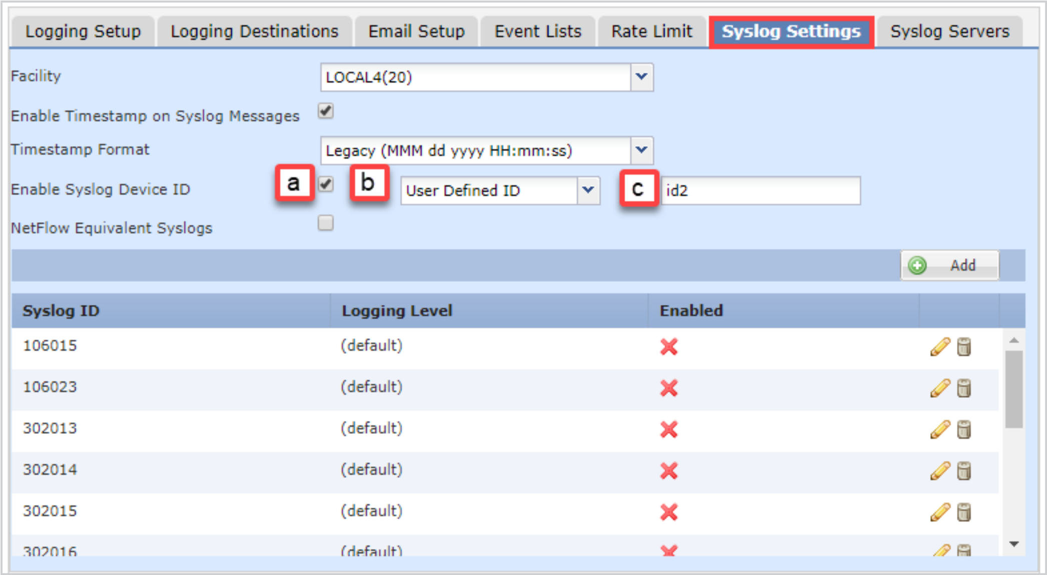
c. Select an FTD device to add to the policy, and click **Add to Policy**.

d. Click **Save**.

3. In the row of the policy you want to configure, click the **Edit**( ) button.
4. In the navigation pane, select **Syslog**.



5. Select the **Syslog Settings** tab.



Facility: LOCAL4(20)

Enable Timestamp on Syslog Messages ☑

Timestamp Format: Legacy (MMM dd yyyy HH:mm:ss)

Enable Syslog Device ID ☑ User Defined ID id2

NetFlow Equivalent Syslogs □

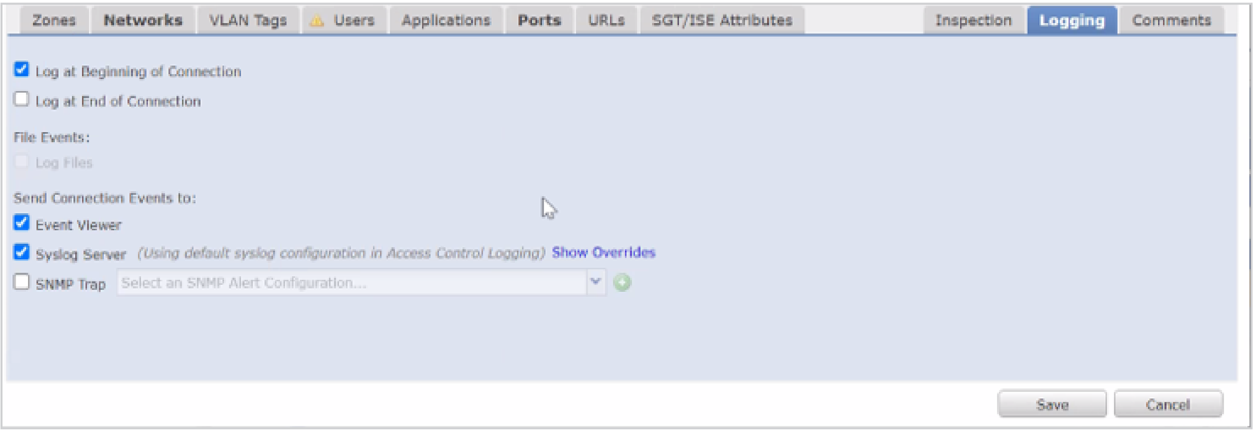
Syslog ID	Logging Level	Enabled
106015	(default)	✗
106023	(default)	✗
302013	(default)	✗
302014	(default)	✗
302015	(default)	✗
302016	(default)	✗

a. Select the **Enable Syslog Device ID** option.

b. From the drop-down menu, select **User Defined ID**.

c. Enter an ID for the device syslogs. This ID will be used when configuring the device in SecureTrack.

6. In the FMC for the required domain, navigate to the **Policies > Access Control > RULE_IN_THE_POLICY > Logging** tab.



☑ Log at Beginning of Connection

□ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

☑ Syslog Server *(Using default syslog configuration in Access Control Logging)* Show Overrides

□ SNMP Trap Select an SNMP Alert Configuration...

a. Select one of these options:

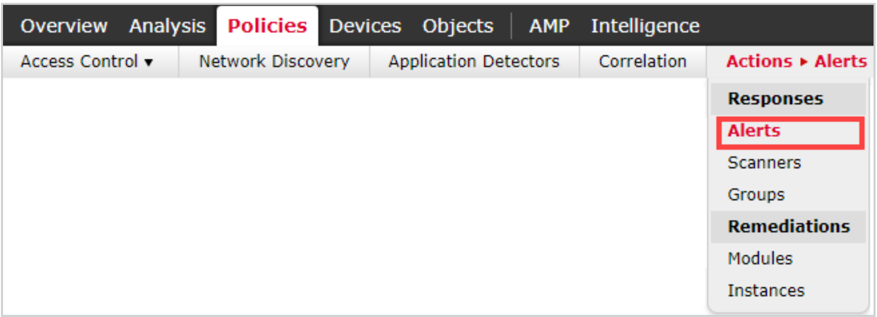
- **Log at Beginning of Connection**
- **Log at End of Connection**

b. Select **Syslog Server**.

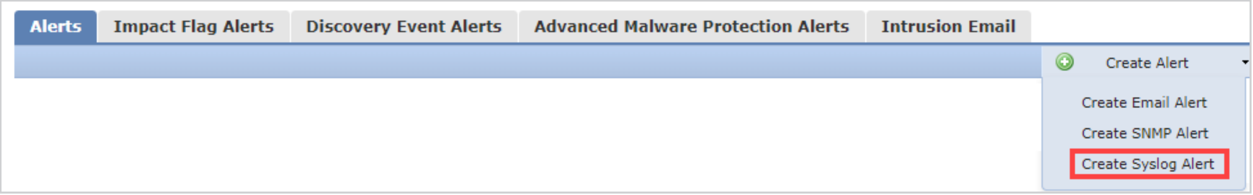
7. Click **Save**.

Create a new Syslog alert

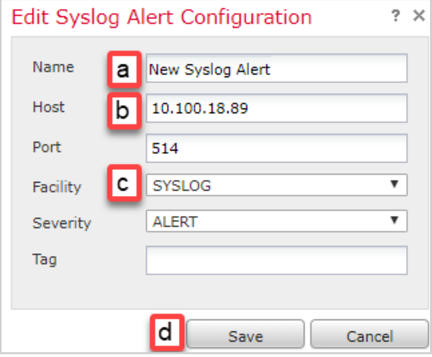
1. In the FMC, navigate to **Policies** > **Actions** > **Alerts**.



2. Click **Create Alert** > **Create Syslog Alert**.



The **Edit Syslog Configuration** dialog box appears.



Name	New Syslog Alert
Host	10.100.18.89
Port	514
Facility	SYSLOG
Severity	ALERT
Tag	

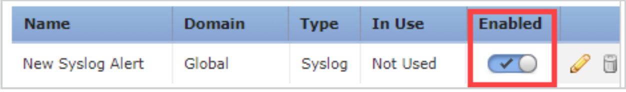
a. In the **Name** field, enter a name for the new alert.

b. In the **Host** field, enter the SecureTrack IP address.

c. In the **Facility** field, select **Syslog**.

d. Click **Save**.

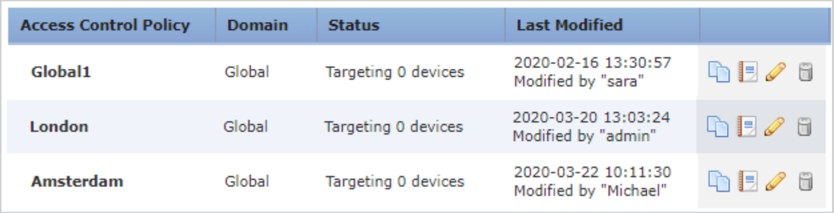
3. In the **Enable** column, enable the alert.



Name	Domain	Type	In Use	Enabled	
New Syslog Alert	Global	Syslog	Not Used	✓	

Edit an FMC policy to send syslogs using the new alert

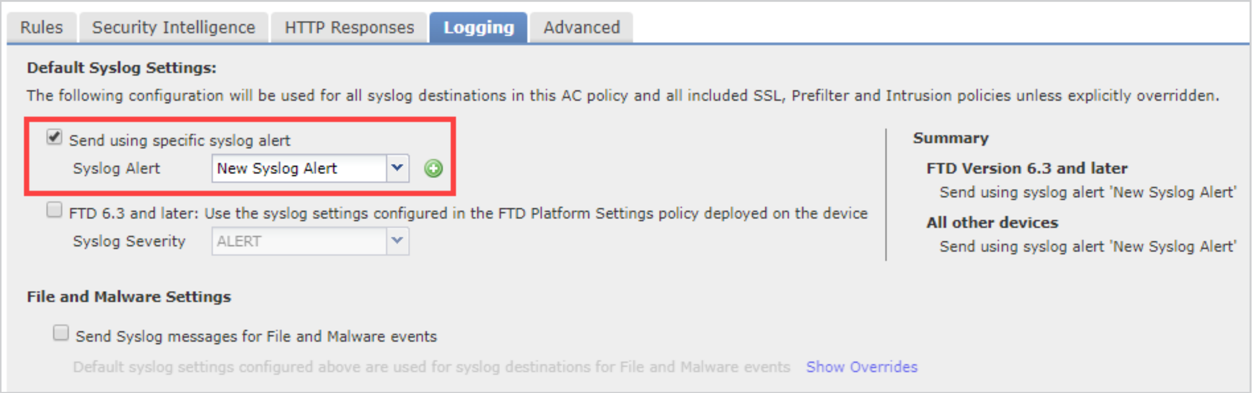
1. In the FMC, navigate to **Policies**.



Access Control Policy	Domain	Status	Last Modified	
Global1	Global	Targeting 0 devices	2020-02-16 13:30:57 Modified by "sara"	
London	Global	Targeting 0 devices	2020-03-20 13:03:24 Modified by "admin"	
Amsterdam	Global	Targeting 0 devices	2020-03-22 10:11:30 Modified by "Michael"	

2. In the row of the policy which you want to use to send syslog alerts to SecureTrack, click the **Edit** (✎) button.

3. Go to the **Logging** tab.



Default Syslog Settings:

The following configuration will be used for all syslog destinations in this AC policy and all included SSL, Prefilter and Intrusion policies unless explicitly overridden.

☑ Send using specific syslog alert

Syslog Alert: New Syslog Alert

□ FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device

Syslog Severity: ALERT

Summary

FTD Version 6.3 and later

Send using syslog alert 'New Syslog Alert'

All other devices

Send using syslog alert 'New Syslog Alert'

File and Malware Settings

□ Send Syslog messages for File and Malware events

Default syslog settings configured above are used for syslog destinations for File and Malware events Show Overrides

4. Select **Send using specific syslog alert**.
5. In the **Syslog alert** field, select the new syslog alert you created.
6. Click **Save**.

Configuring Fortinet Syslogs

To get full accountability details (i.e. who made policy changes and when) and to utilize rule and object usage reporting, you must get your Fortinet devices to send syslogs to SecureTrack by defining SecureTrack as a syslog server on each device. FortiManager devices cannot be configured to send syslog traffic. Therefore, you must configure either the gateway or FortiAnalyzer.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

The firewalls in the organization must be configured to allow the relevant traffic.

Configuring a Fortinet Firewall to Send Syslogs

To monitor with full accountability and get rule and object usage reporting, your Fortinet devices must send syslogs to TOS Classic. To do this, define TOS Classic as a syslog server for each monitored Fortinet devices.

The firewalls in the organization must be configured to allow relevant traffic.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

To define TOS Classic as a syslog server on a FortiOS 5.x device:

Run the following commands:

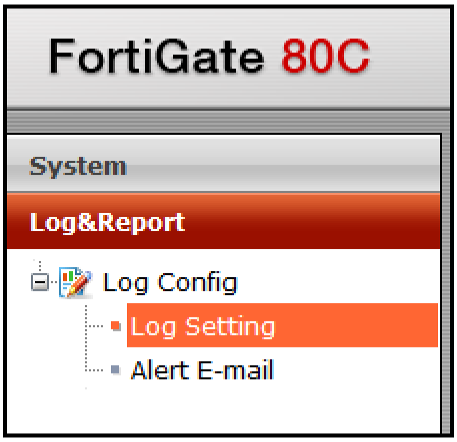
```
Config global
config log syslogd setting
set csv disable
set facility local7
set source-ip <Fortinet_Ip>
set port 514
set server <st_ip_address>
set status enable
end
config log syslogd filter
set severity information
end
end
```

FortiGate supports multiple active syslog server destinations.

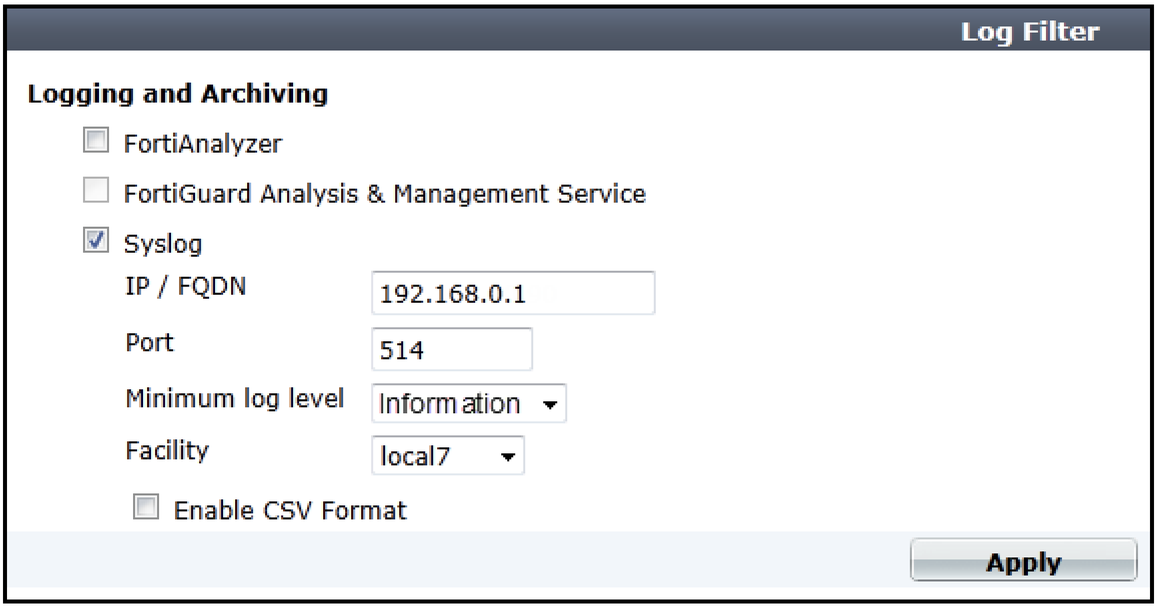
We recommend that you verify how many syslog servers your FortiGate device version supports, and then use `syslogd, syslogd2,syslog3,…syslog<n>` to configure the desired syslog server setting.

To define TOS Classic as a syslog server on a FortiOS 4.x device:

1. Log into the device's web interface. Under **Log & Report**, click **Log Config**:



2. In the **Log Setting** tab, select **Syslog**:



Logging and Archiving

□ FortiAnalyzer

□ FortiGuard Analysis & Management Service

☑ Syslog

IP / FQDN 192.168.0.1

Port 514

Minimum log level Information

Facility local7

□ Enable CSV Format

3. Configure the following settings:
   - **Name/IP**: A resolvable hostname or the IP address of the TOS Classic server, remote collector or distribution server that is managing the device
   - **Port**: 514
   - **Minimum log level**: Information or higher
   - **Facility**: local7

   > If you need to use a lower facility, configure TOS Classic as described in this tech note.

   - **Enable CSV Format**: Not selected

Configuring a Fortinet FortiManager to Send Syslogs

To monitor with full accountability and get rule and object usage reporting, your Fortinet devices must send syslogs to TOS Classic. To do this, define TOS Classic as a syslog server for each monitored Fortinet FortiManager device.

The firewalls in the organization must be configured to allow relevant traffic.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

To add TOS Classic as a syslog server:

1. Run these commands to create a SysLog Server address:
   1. `config system syslog`
   2. `edit New_syslog_server`
   3. `set ip <securetrack_server_ip_address>`
   4. `end`
2. Run these commands to configure the syslog server setting and to enable it:
   1. `config system locallog syslogd3 setting`
   2. `set severity information`
   3. `set syslog-name New_syslog_server`
   4. `set status enable`
   5. `end`

FortiManager supports multiple active syslog server destinations.

We recommend that you verify how many firewalls your FortiManager device version supports, and then use `syslogd, syslogd2,syslog3,…syslog`<n> to configure the desired syslog server setting.

Configuring Juniper Syslogs

To monitor with full accountability and get rule and object usage reporting, either the NSM or each Juniper device must send syslogs to SecureTrack. To do this, define SecureTrack as a syslog server for each Netscreen device and each JunOS device, or for the NSM.

The firewalls in the organization must be configured to allow the relevant traffic.

Configuring a Juniper Netscreen device to Send Syslogs

For SecureTrack to be able to associate syslogs with their respective firewalls, each Netscreen device that sends syslogs to SecureTrack must have a unique hostname.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

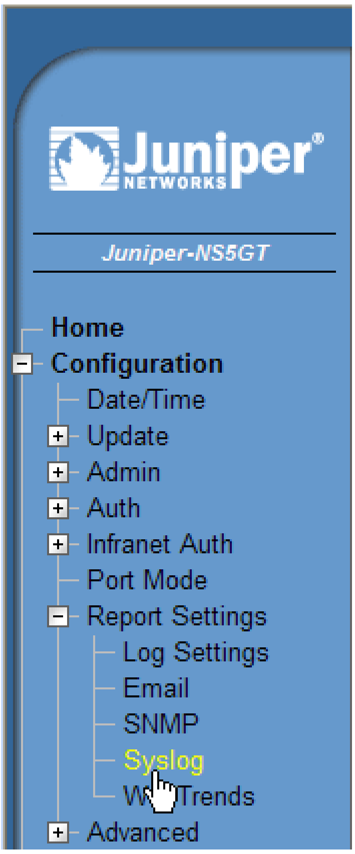
For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs (Configuring Devices to Send Logs).

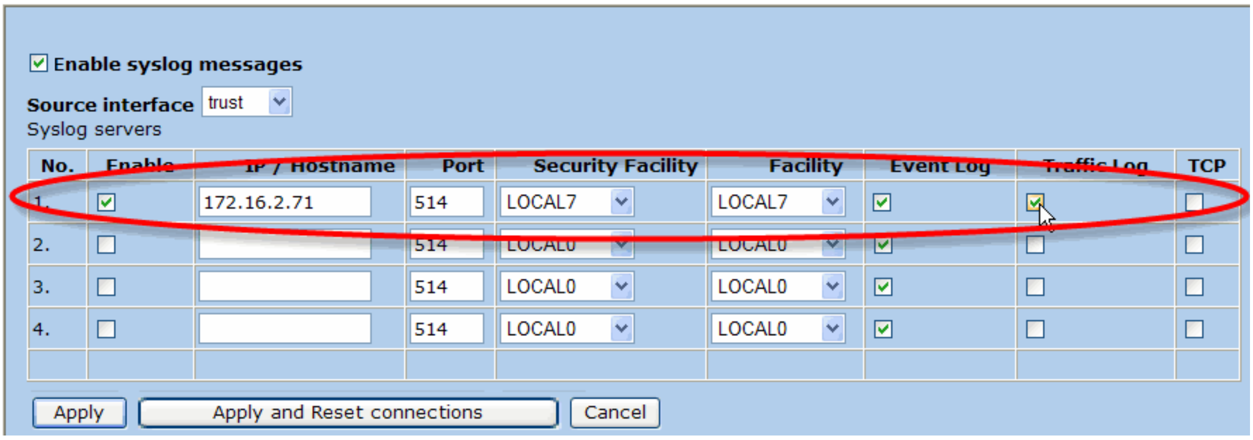
Only rules that are marked for logging in the device are included in the syslogs.

To define SecureTrack as a syslog server on a Netscreen device:

1. Log into the firewall's web interface.
2. In the navigation pane, under **Configuration** > **Report Settings**, select **Syslog**:



3. Configure a row with the following settings:



☑ Enable syslog messages

Source interface trust

Syslog servers

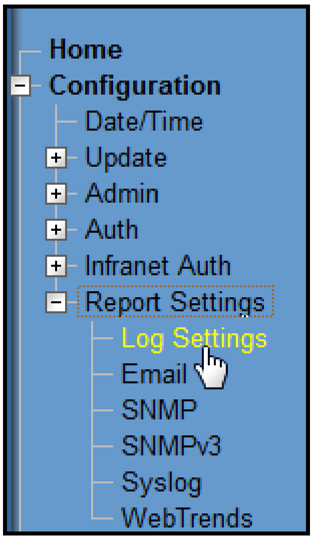
No.	Enable	IP / Hostname	Port	Security Facility	Facility	Event Log	Traffic Log	TCP
1.	☑	172.16.2.71	514	LOCAL7	LOCAL7	☑	☑	☐
2.	☐		514	LOCAL0	LOCAL0	☑	☐	☐
3.	☐		514	LOCAL0	LOCAL0	☑	☐	☐
4.	☐		514	LOCAL0	LOCAL0	☑	☐	☐

- **Enable**: Selected
- **IP/Hostname**: the IP address of the SecureTrack server, remote collector or distribution server that is managing the device
- **Port**: 514
- **Security Facility**: LOCAL7
- **Facility**: LOCAL7

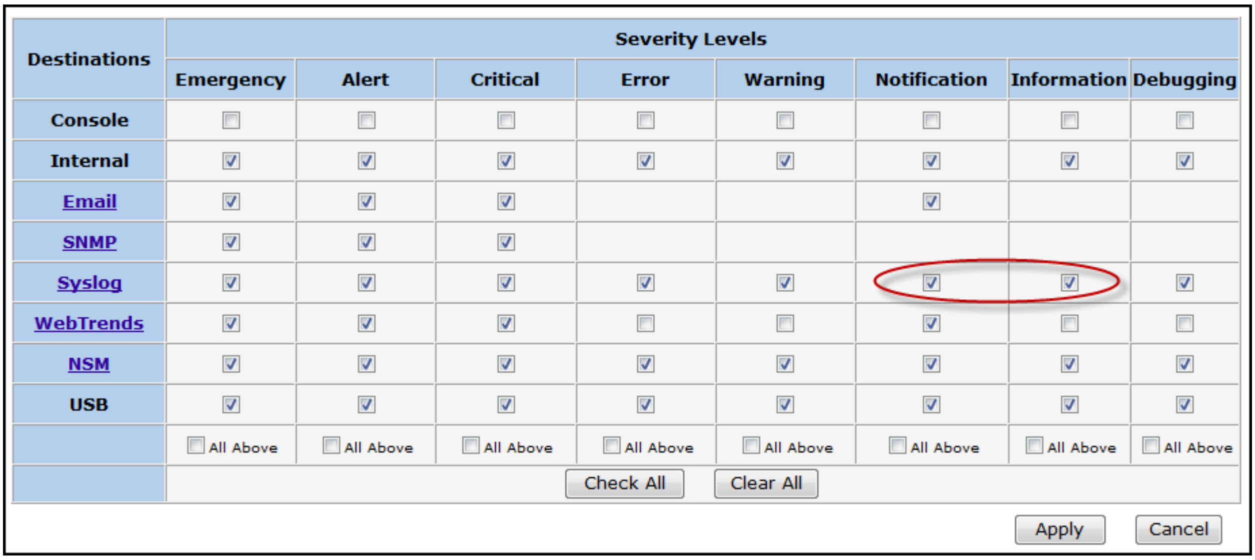
  If you need to use a different facility, you can, in which case you'll also need to configure SecureTrack as described in this tech note.
- **Event Log**: To enable identification of users who made policy changes and the time of those policy changes, **Event Log** must be selected.
- **Traffic Log**: To enable Usage reporting, **Traffic Log** must be selected.
- **TCP**: Cleared.

4. Click **Apply**.

5. In the navigation pane, click **Log Settings**:



6. Make sure that in the **Syslog** row, **Notification** and **Information** are selected:



Destinations	Severity Levels							
	Emergency	Alert	Critical	Error	Warning	Notification	Information	Debugging
Console	□	□	□	□	□	□	□	□
Internal	☑	☑	☑	☑	☑	☑	☑	☑
Email	☑	☑	☑			☑		
SNMP	☑	☑	☑					
Syslog	☑	☑	☑	☑	☑	☑	☑	☑
WebTrends	☑	☑	☑	□	□	☑	□	□
NSM	☑	☑	☑	☑	☑	☑	☑	☑
USB	☑	☑	☑	☑	☑	☑	☑	☑
	□ All Above	□ All Above	□ All Above	□ All Above	□ All Above	□ All Above	□ All Above	□ All Above

7. Click **Apply**.

Configuring a Juniper JunOS device to Send Syslogs

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

Define SecureTrack as a Syslog Server on each JunOS device

1. Open a command line to the device.
2. Run these commands:

```
cli (Only if you login with the root user)
configure
set system syslog host <ST_IP> user info
set system syslog host <ST_IP> change-log notice
set system syslog host <ST_IP> interactive-commands notice
set system syslog host <ST_IP> match
"(UI_COMMIT:)|(UI_COMMIT_AT_COMPLETED)|(FLOW_SESSION_CREATE)|(FLOW_SESSION_DENY)|(FLOW_SESSION_
CLOSE)"
set system syslog host <ST_IP> log-prefix <ID>
commit
```

Where:

- `<ST_IP>` - the IP address of the SecureTrack server, remote collector or distribution server that is managing the device
- `<ID>` - a unique ID string for each JunOS device that must begin with: `SecureTrack_`

  To get usage reporting for JunOS devices, you must also configure policy rules logging for session-init, session-close, or both. If you want to use a non-default facility level, you must configure SecureTrack as described in this tech note.

  For **Juniper SRX devices running JunOS**, if you configure the data plane to send syslogs, you must use sd-syslog format and add these lines before the `commit` command:

  ```
  set security log mode stream
  set security log source-address <SRX_IP>
  set security log stream tufin format sd-syslog
  set security log stream tufin host <ST_IP>
  ```

Configure Syslogs for Logical Systems

For Juniper SRX R22-1R1 devices (Supported from R21-3 HF4 and above) you need to configure syslogs for logical systems.

1. Open a command line to the device.
2. Run these commands:

```
set logical-systems <lsys_name> syslog host <ST_IP> user info
set logical-systems <lsys_name> syslog host <ST_IP> change-log notice
set logical-systems <lsys_name> syslog host <ST_IP> interactive-commands notice
set logical-systems <lsys_name> syslog host <ST_IP> match "(UI_COMMIT:)|(UI_COMMIT_AT_
COMPLETED)|(FLOW_SESSION_CREATE)|(FLOW_SESSION_DENY)|(FLOW_SESSION_CLOSE)"
set logical-systems <lsys_name> syslog host <ST_IP> log-prefix <ST_ID>
```

Where:

- `<lsys_name>` - The name of the logical system.
- `<ST_IP>` - The IP address of the SecureTrack server, remote collector or distribution server that is managing the device.
- `<ST_ID>` - The SecureTrack ID used to identify the device.

Configuring the NSM to Send Syslogs

Syslog traffic must be configured to arrive to SecureTrack from the IP and/or host name of the device.

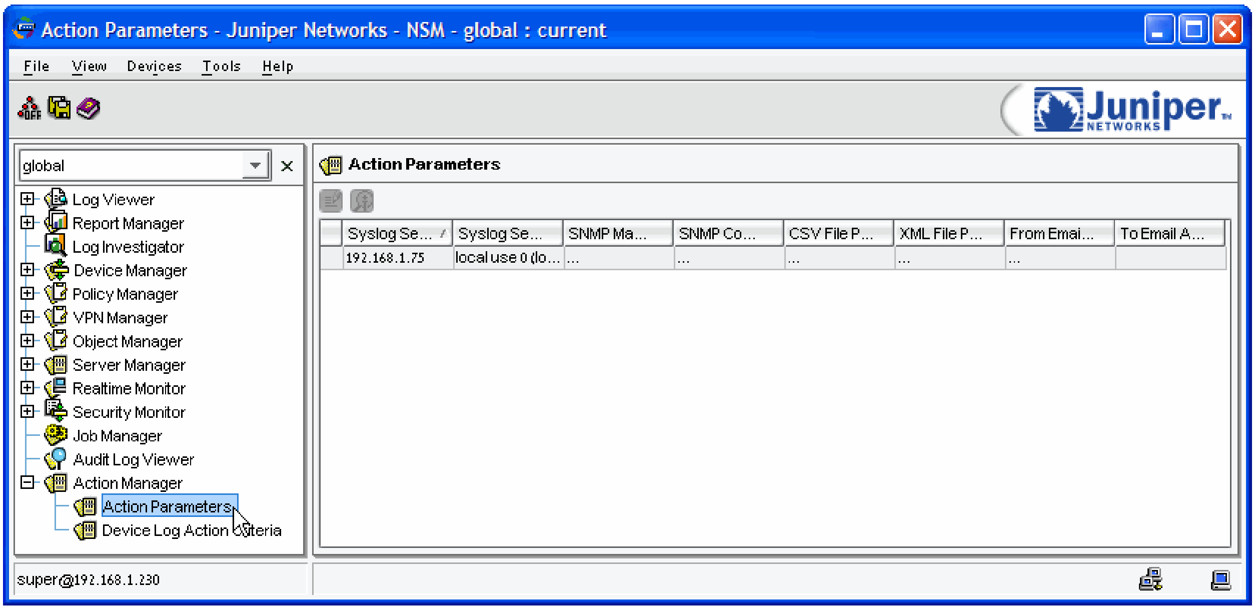
Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

To define SecureTrack as a syslog server on the NSM:

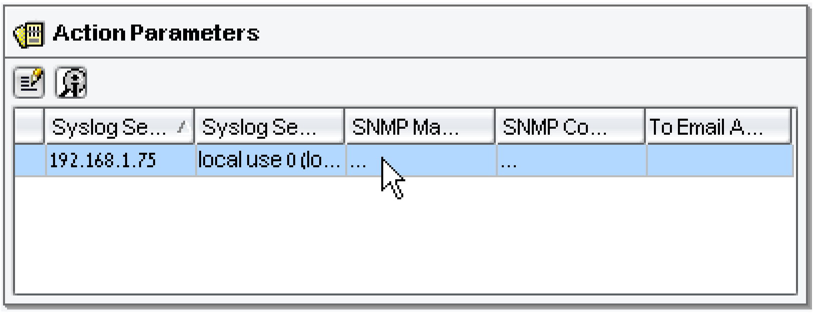
1. Make sure that the IP address of each Juniper NetScreen device is configured identically on both SecureTrack and on the NSM.

   For JunOS devices, you must configure each device to send syslogs directly to SecureTrack.
2. Log into the NSM.
3. In the navigation pane, under **Action Manager**, select **Action Parameters**:



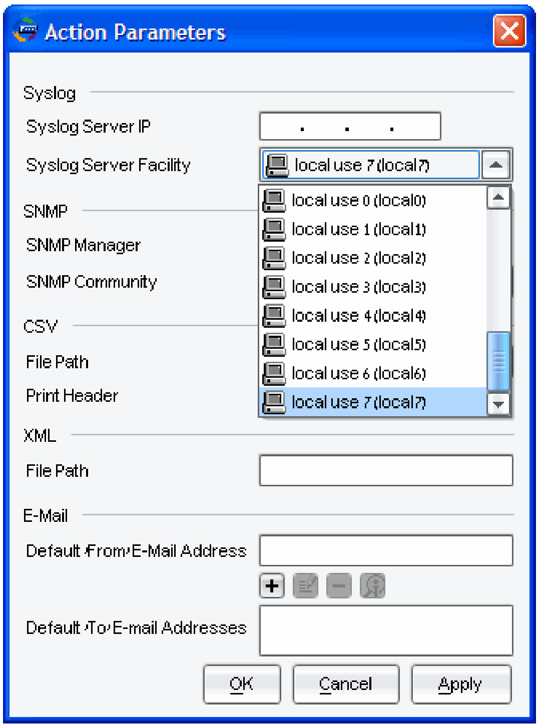
Syslog Se...	Syslog Se...	SNMP Ma...	SNMP Co...	CSV File P...	XML File P...	From Emai...	To Email A...
192.168.1.75	local use 0 (lo...	...	...	...	...	...	

4. In the **Action Parameters** pane, double-click the entry row:



Syslog Se...	Syslog Se...	SNMP Ma...	SNMP Co...	To Email A...
192.168.1.75	local use 0 (lo...	...	...	

5. In the **Action Parameters** window, enter the following:

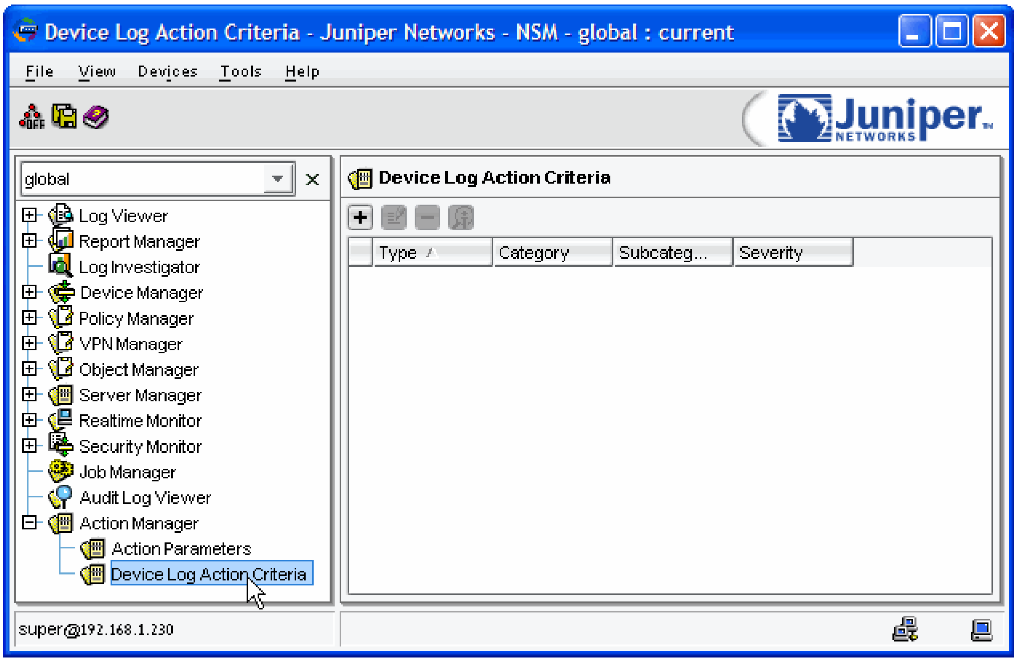


- **Syslog Server IP**: the IP address of the SecureTrack server, remote collector or distribution server that is managing the device
- **Syslog Server Facility**: Select **local use 7 (local7)**

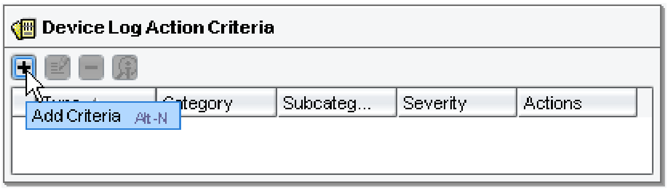
  If you need to use a different facility, you can, in which case you'll also need to configure SecureTrack as described in this tech note.

Click **OK**.

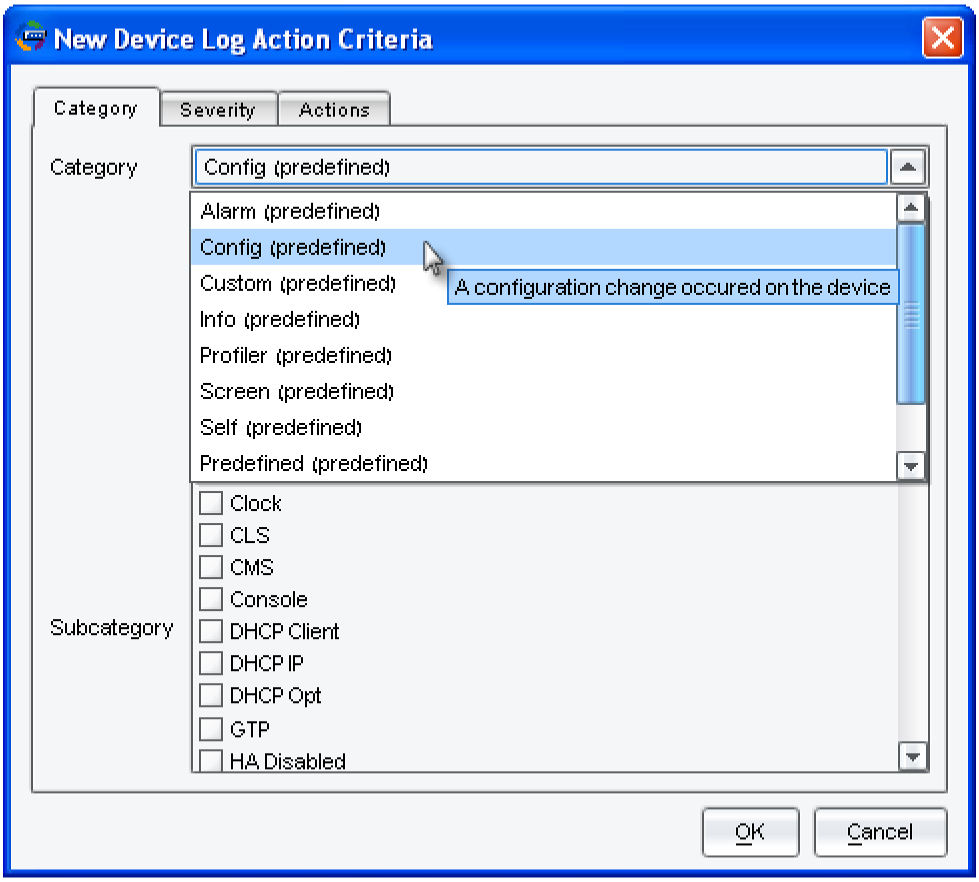
6. In the navigation pane, under **Action Manager**, select **Device Log Action Criteria**:



7. To enable identification of users who made policy changes and the time of those policy changes, do the following:
   a. Click the plus sign:



   b. By **Category**, select **Config (predefined)**:



New Device Log Action Criteria

Category | Severity | Actions

Category: Config (predefined)

- Alarm (predefined)
- Config (predefined)
- Custom (predefined)
- Info (predefined)
- Profiler (predefined)
- Screen (predefined)
- Self (predefined)
- Predefined (predefined)

A configuration change occured on the device

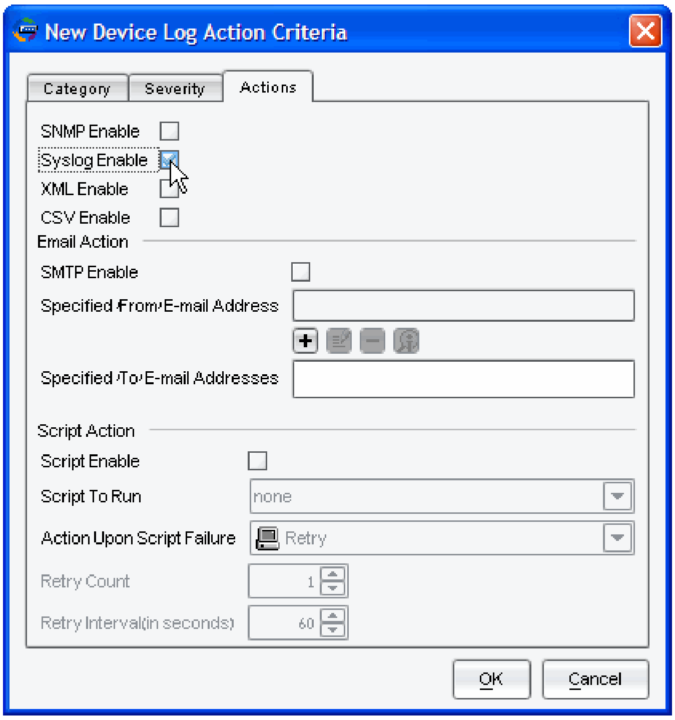
Subcategory:

- □ Clock
- □ CLS
- □ CMS
- □ Console
- □ DHCP Client
- □ DHCP IP
- □ DHCP Opt
- □ GTP
- □ HA Disabled

OK | Cancel

No Subcategory should be selected.

c. In the **Actions** tab, select **Syslog Enable**:



New Device Log Action Criteria

Category | Severity | Actions

SNMP Enable □
Syslog Enable ☑
XML Enable □
CSV Enable □

Email Action

SMTP Enable □
Specified 'From' E-mail Address
Specified 'To' E-mail Addresses

Script Action

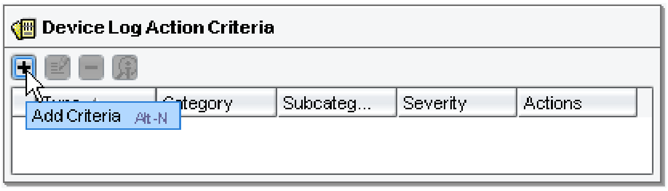
Script Enable □
Script To Run: none
Action Upon Script Failure: Retry
Retry Count: 1
Retry Interval(in seconds): 60

OK | Cancel

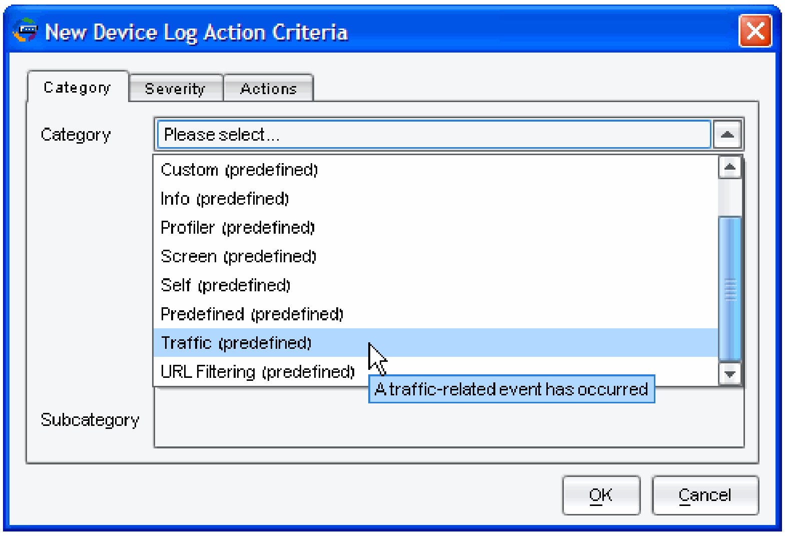
d. Click **OK**.

8. To enable Usage reporting, do the following:

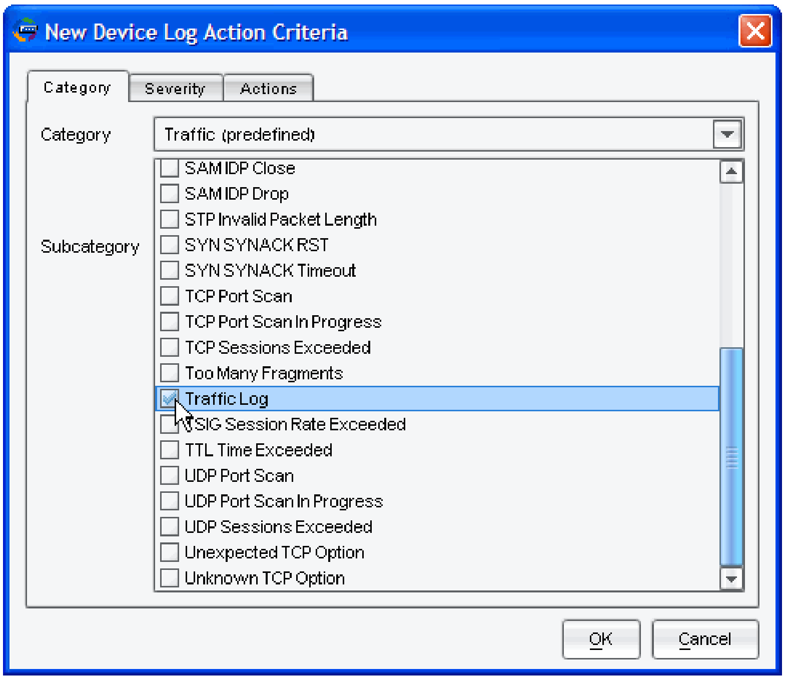
a. Click the plus sign:



b. By **Category**, select **Traffic (predefined)**:



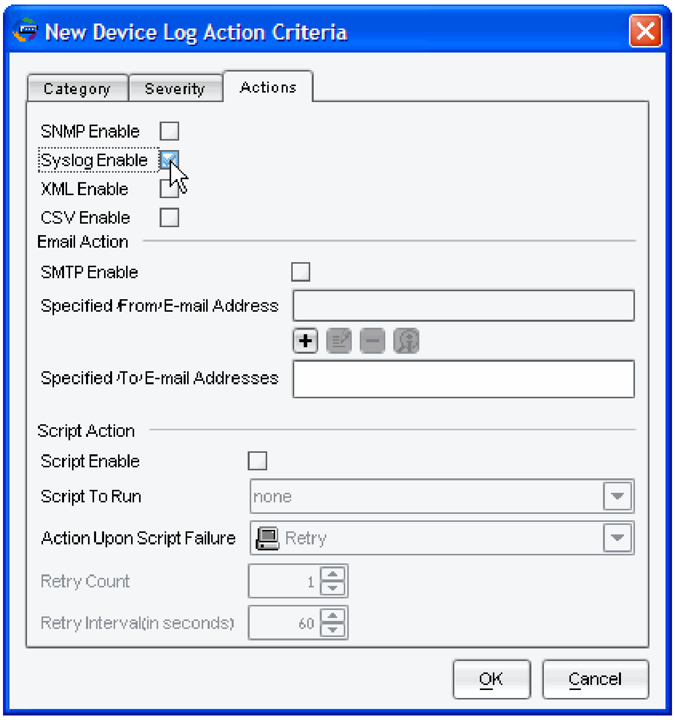
c. For **Subcategory**, select **Traffic Log**:


Category: Traffic (predefined)

Subcategory:

- □ SAM IDP Close
- □ SAM IDP Drop
- □ STP Invalid Packet Length
- □ SYN SYNACK RST
- □ SYN SYNACK Timeout
- □ TCP Port Scan
- □ TCP Port Scan In Progress
- □ TCP Sessions Exceeded
- □ Too Many Fragments
- ☑ Traffic Log
- □ TSIG Session Rate Exceeded
- □ TTL Time Exceeded
- □ UDP Port Scan
- □ UDP Port Scan In Progress
- □ UDP Sessions Exceeded
- □ Unexpected TCP Option
- □ Unknown TCP Option

d. In the **Actions** tab, select **Syslog Enable**:



New Device Log Action Criteria

SNMP Enable □

Syslog Enable ☑

XML Enable □

CSV Enable □

Email Action

SMTP Enable □

Specified 'From' E-mail Address

Specified 'To' E-mail Addresses

Script Action

Script Enable □

Script To Run: none

Action Upon Script Failure: Retry

Retry Count: 1

Retry Interval(in seconds): 60

e. Click **OK**.

Configuring VMware Syslogs

To monitor with full accountability, your VMware devices must send syslogs to SecureTrack. To do this, define SecureTrack as a syslog server for each monitored VMware device.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs. For NSX-T devices that work with declarative APIs, real time monitoring (accountability) is supported only for syslogs which were received with the default `messageid`.

Configuring a VMware NSX-V Device to Send Syslogs

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

To define SecureTrack as a syslog server on a VMware NSX device:

1. From the vSphere Client or the vSphere Web Admin, login to either the vCenter server or directly to the relevant ESXi server.
2. Select the ESXi server and select the **Configuration** tab.
3. Under the Software heading, select **Advanced Settings**.
4. From the list of settings, select **Syslog** > **Global**.
5. In the **Syslog.global.logHost** field, enter the connection information for SecureTrack in the syntax: `udp://<ip_address>:514`

   For example: `udp://192.168.0.1:514`
6. Make sure the Distributed Firewall rules are configured with the Log option. (VMware NSX documentation)
7. (Optional) To configure the NSX Manager to send change logs to SecureTrack to receive revisions when firewall rules are changed:

a. Login to the NSX Manager.

b. Click **Manage Appliance Settings**.

c. In the Settings > General section, in the Syslog Server section click **Edit**.

d. Enter the SecureTrack server details:

  - Syslog server - Enter the IP address of the SecureTrack server
  - Port - Enter **514**
  - Protocol - Select **UDP**
  - Click **OK**.

Configuring a VMware NSX-T Device to Send Syslogs

Configure the NSX Manager to send change logs to SecureTrack to receive revisions when firewall rules are changed.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

To define SecureTrack as a syslog server on a VMware NSX-T device

1. Login to the NSX Manager CLI
2. Run the command:

```
set logging-server <host>:514 proto udp level info messageid <messageid> [structured-data
update="true"]
```

   where,

   <host> is the host name or IP address,

   <messageid> is "FIREWALL" for imperative APIs or the dash character "-" for declarative APIs,

   the structured-data parameter is optional but recommended for in-depth filtering

For more information, see official VMware documentation - Configure Remote Logging and Log Message IDs

Configuring an External Device for VMware NSX-V Syslogs

If you are using an external log manager (for example, vRealize Log Insight) with your NSX-V device:

1. Ensure that you entered the vCenter host name when adding or editing the NSX device.
2. Configure the external log manager to send the syslog information to SecureTrack.

   Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

   For more information see Sending Additional Information via Syslog.

Configuring Palo Alto Syslogs

To show revision accountability and report on rule and object usage, each of your Palo Alto firewall devices must send syslogs to SecureTrack.

The firewalls in the organization must be configured to allow relevant traffic.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

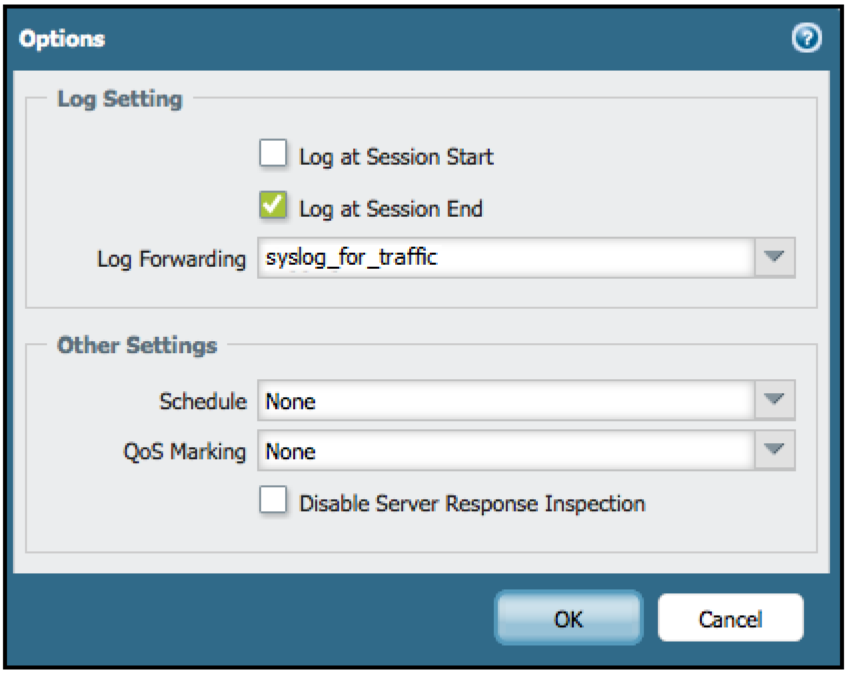
For more information see Sending Additional Information via Syslog.

Syslog proxy is supported for specific devices. For more information on syslog proxy support for supported devices, see Configuring Devices to Send Logs.

Only rules that are marked for logging in the device are included in the syslogs.

Configure a Palo Alto Device to Send Traffic Syslogs to SecureTrack for a Rule That Is Tracked

1. View the security policy and click on the **Options** column of the rule.



Options

Log Setting

☐ Log at Session Start

☑ Log at Session End

Log Forwarding: syslog_for_traffic

Other Settings

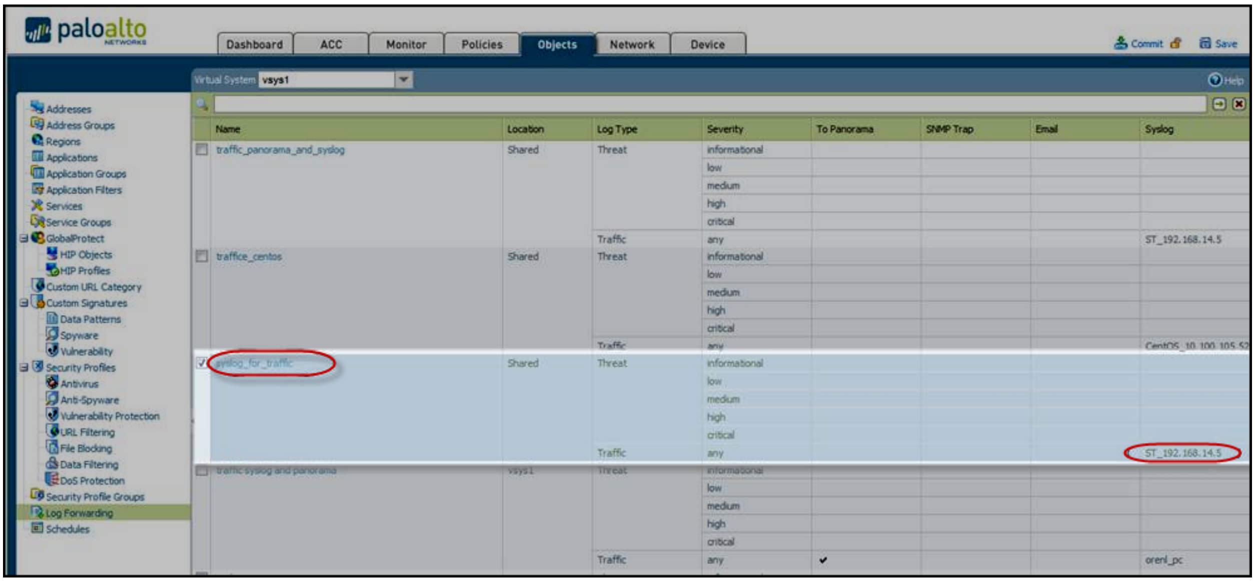
Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

Notice the name of the Log Forwarding profile. At least one of the **Log At** options must be checked. We recommend that you select only **Log at Session End**, to better manage the traffic load.

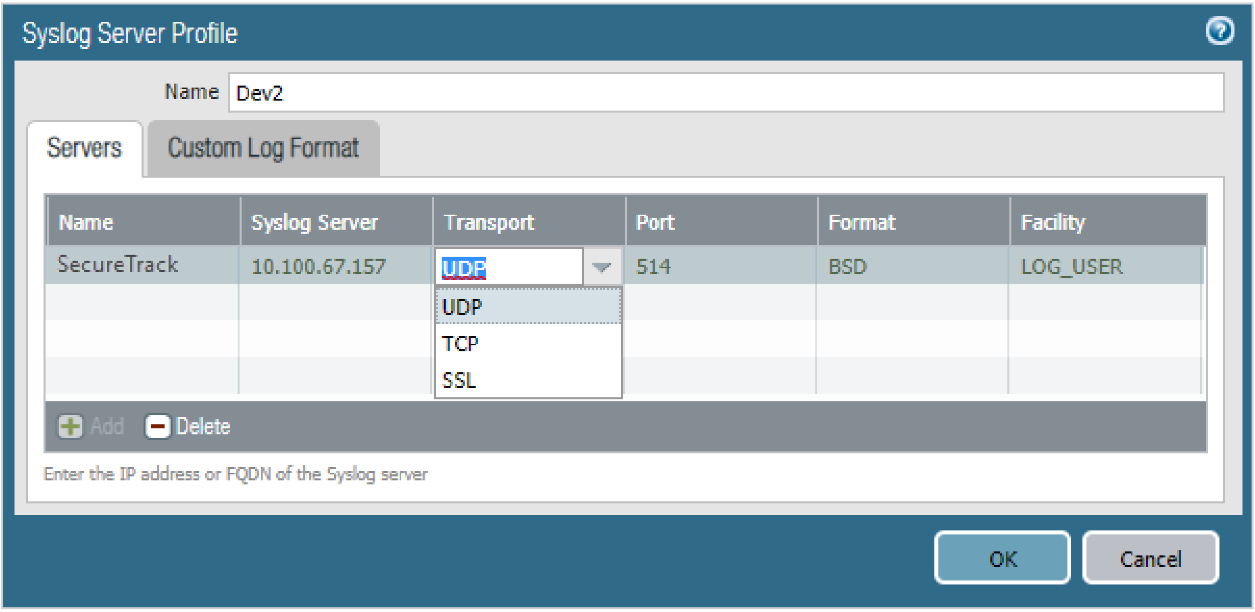
2. Go to **Objects** > **Log Forwarding** and select the profile used in the rule. Note the name of the syslog profile.



Virtual System: vsys1

	Name	Location	Log Type	Severity	To Panorama	SNMP Trap	Email	Syslog
☐	traffic_panorama_and_syslog	Shared	Threat	informational				
				low				
				medium				
				high				
				critical				
			Traffic	any				ST_192.168.14.5
☐	traffice_centos	Shared	Threat	informational				
				low				
				medium				
				high				
				critical				
			Traffic	any				CentOS_10.100.105.52
☑	syslog_for_traffic	Shared	Threat	informational				
				low				
				medium				
				high				
				critical				
			Traffic	any				ST_192.168.14.5
☐	traffic syslog and panorama	vsys1	Threat	informational				
				low				
				medium				
				high				
				critical				
			Traffic	any	✓			orenl_pc

3. Go to **Device** > **Server Profiles** > **Syslog**, and add the SecureTrack server to the profile:



Syslog Server Profile

Name: Dev2

Name	Syslog Server	Transport	Port	Format	Facility
SecureTrack	10.100.67.157	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

Use port 514 (for UDP) or port 6514 (for TCP) and any facility. You must use the default log format for traffic.

To configure a Palo Alto device to send traffic syslogs to SecureTrack for a rule that is not tracked, perform the steps in reverse order.

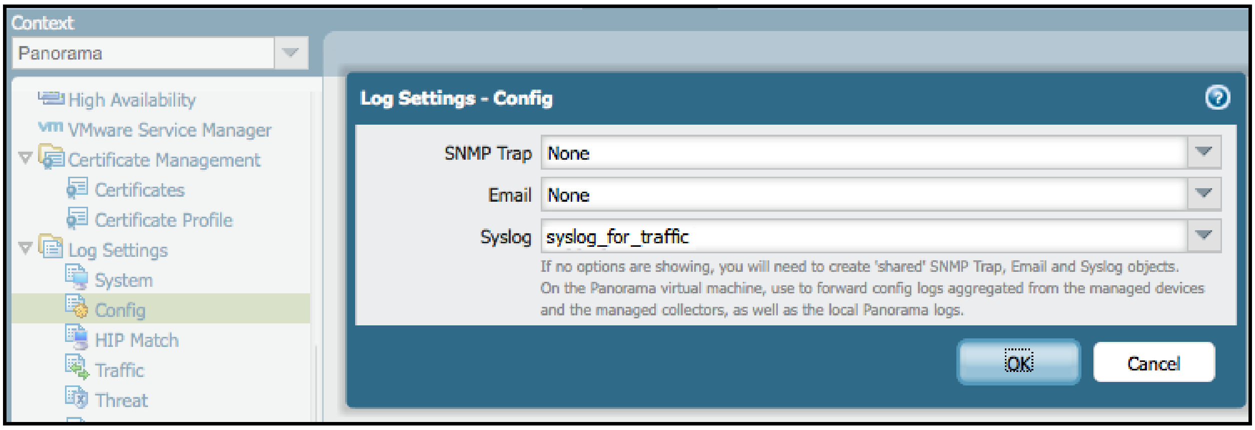
a. Add a new syslog server profile with the IP address of the SecureTrack server, remote collector or distribution server that is managing the device.

b. Add the syslog profile to a new Log Forwarding profile.

c. For the rule that you want to track, select the new log forwarding profile in the rule **Options** field and mark either **Send at session** start or **Send at session end**.

Configure a Palo Alto Device to Send Accountability Syslogs to SecureTrack

1. Go to: **Device** > **Log Settings** > **Config**
2. Configure the syslogs to be sent to the SecureTrack server.



Log Settings - Config

SNMP Trap: None

Email: None

Syslog: syslog_for_traffic

If no options are showing, you will need to create 'shared' SNMP Trap, Email and Syslog objects. On the Panorama virtual machine, use to forward config logs aggregated from the managed devices and the managed collectors, as well as the local Panorama logs.

3. In SecureTrack, make sure that the Palo Alto device is monitored in real-time.
   a. Go to: **Settings** > **Monitoring** > **Manage Devices**
   b. Select the device and click **Edit configuration**.
   c. To go to the monitoring settings, click **Next** and **Next**.
   d. Click **Custom** and review the monitoring settings.

Panorama 8.x, 9.x, or 10.x Log Forwarding and Accountability

Panorama log forwarding requires you to:

- **Forward traffic logs to Panorama** - If the firewall was imported via Panorama, SecureTrack will not recognize logs sent directly by the firewall. The logs must be sent by the firewall to Panorama, and then Panorama forwards the traffic logs to SecureTrack
- **Enable accountability** - Enabling accountability ensures that firewall changes made by SecureChange and manual firewall changes made via Panorama are seen by SecureTrack.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

For more information see Sending Additional Information via Syslog.

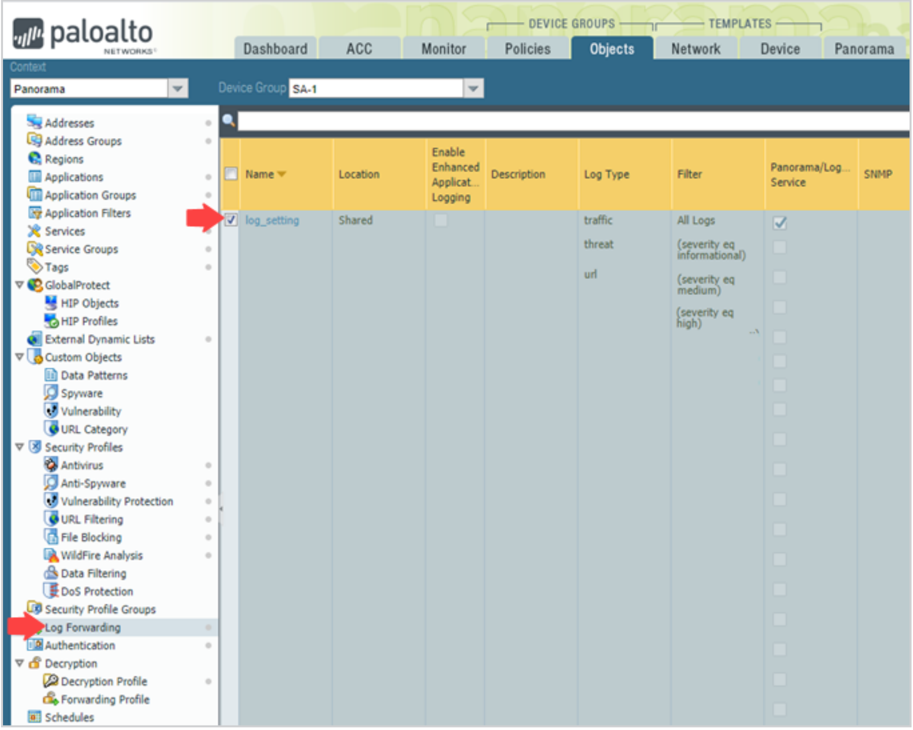
For more information, see the Palo Alto Networks technical documentation site:

- **PanOS 8:** Configure Log Forwarding and Device > Server Profiles > Syslog
- **For PanOS 9:** Configure Log Forwarding and Device > Server Profiles > Syslog
- **For PanOS 10**: Configure Log Forwarding and Device > Server Profiles > Syslog

Forwarding Traffic Logs to Panorama

These steps will explain how to send the firewall traffic logs to a Panorama device (for Panorama version 8.x or 9.x), and then configure the Panorama to forward the logs to SecureTrack.

1. Log into the Panorama device.
2. Modify a log forwarding profile to enable the log forwarding for the Panorama device.
   a. In the **Objects** tab, navigate to **Log Forwarding**.
   b. Click on the link of the log forwarding profile.

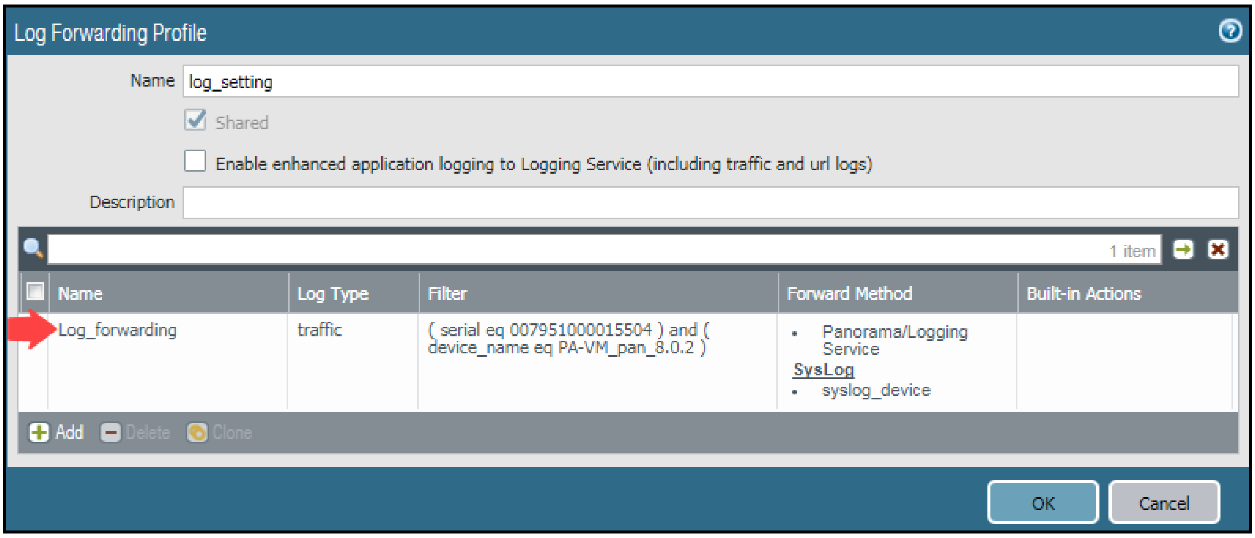


Context: Panorama

Device Group: SA-1

☐	Name	Location	Enable Enhanced Applicat... Logging	Description	Log Type	Filter	Panorama/Log... Service	SNMP
☑	log_setting	Shared	☐		traffic threat url	All Logs (severity eq informational) (severity eq medium) (severity eq high)	☑ ☐ ☐ ☐	

The **Log Forwarding Profile** dialog box is displayed.



Log Forwarding Profile

Name: log_setting

☑ Shared

☐ Enable enhanced application logging to Logging Service (including traffic and url logs)

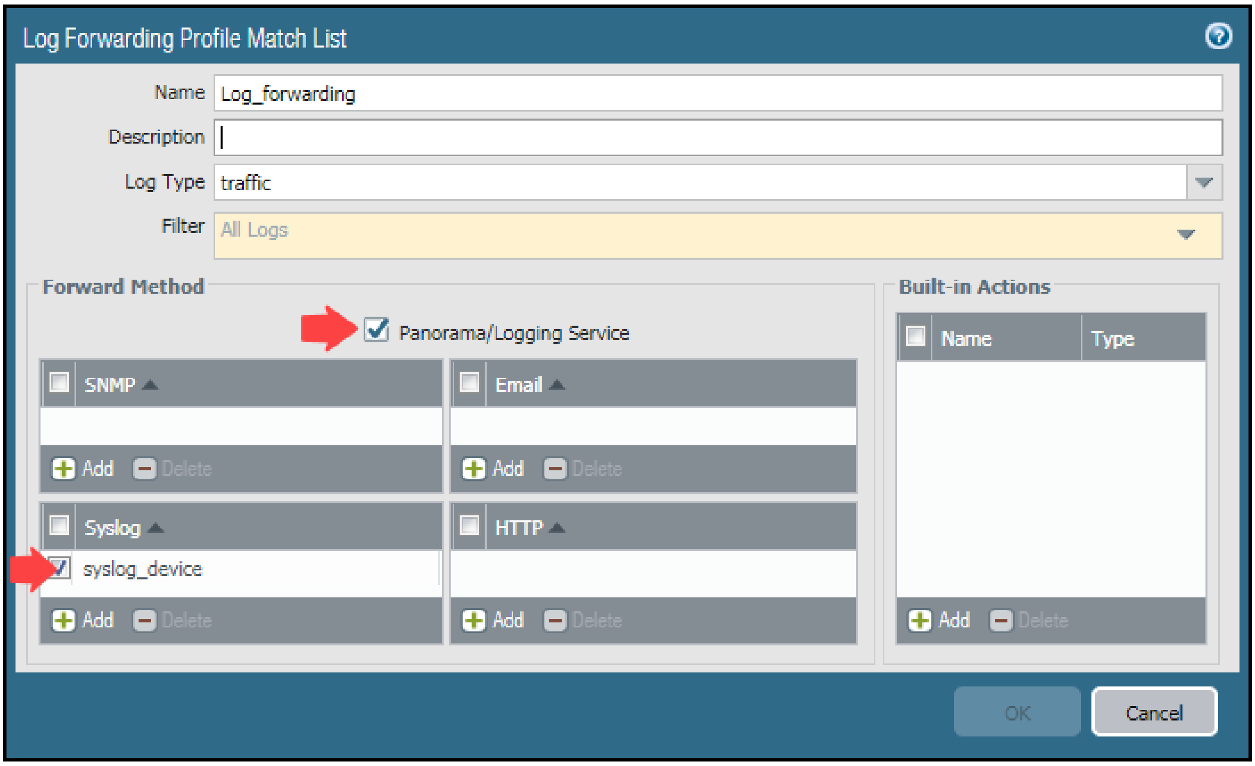
Description:

1 item

☐	Name	Log Type	Filter	Forward Method	Built-in Actions
	Log_forwarding	traffic	(serial eq 007951000015504) and (device_name eq PA-VM_pan_8.0.2)	• Panorama/Logging Service SysLog • syslog_device	

c. Click on a log forwarding profile match list link.

The **Log Forwarding Profile Match List** dialog box is displayed.



Log Forwarding Profile Match List

Name: Log_forwarding

Description:

Log Type: traffic

Filter: All Logs

Forward Method

☑ Panorama/Logging Service

☐	SNMP

☐	Email

☐	Syslog
☑	syslog_device

☐	HTTP

Built-in Actions

☐	Name	Type

d. Select **Panorama/Logging Service**.

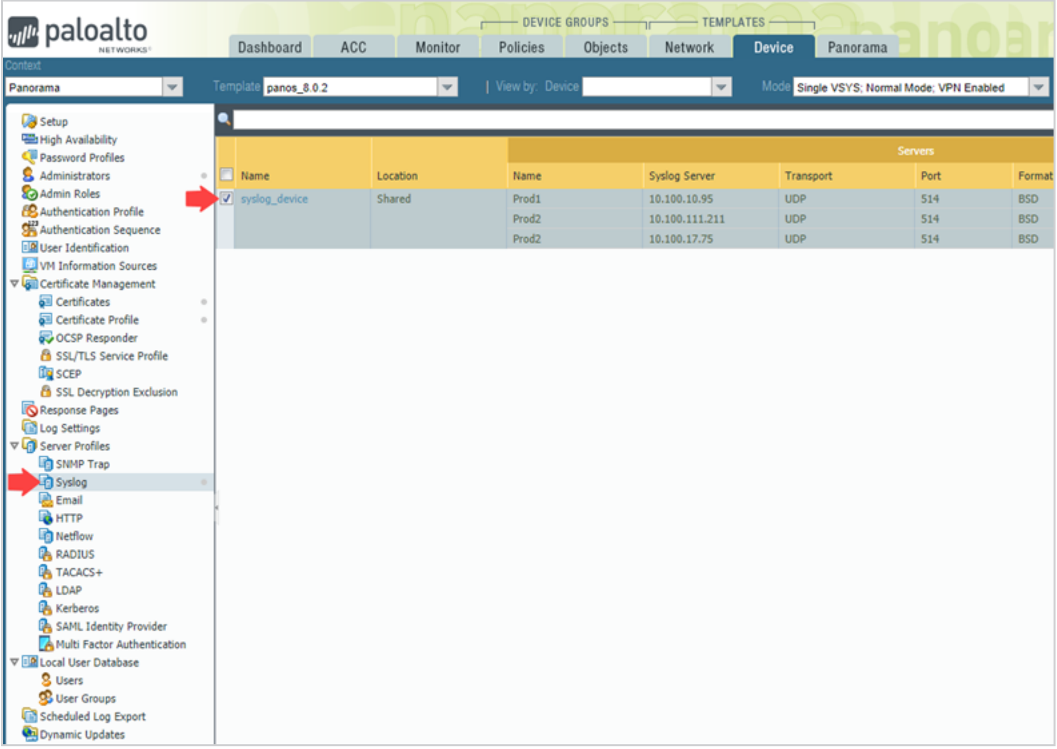
e. In the **Syslog** area, select an existing syslog profile or click **Add** to create a syslog profile.

f. Click **OK** and **OK.**

3. Add SecureTrack to the syslog server profile to ensure that the Panorama forwards the logs to SecureTrack.

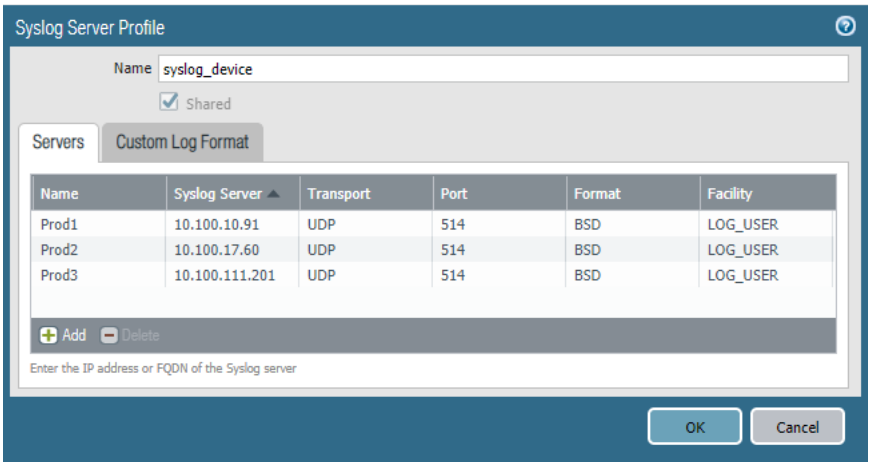
   a. In the **Devices** tab, navigate to **Syslog** (under **Server Profiles**).

   b. Click on the link of the syslog server profile to which you want to add SecureTrack.



			Servers				
☐	Name	Location	Name	Syslog Server	Transport	Port	Format
☑	syslog_device	Shared	Prod1	10.100.10.95	UDP	514	BSD
			Prod2	10.100.111.211	UDP	514	BSD
			Prod2	10.100.17.75	UDP	514	BSD

The **Syslog Server Profile** dialog box is displayed.



Name syslog_device

☑ Shared

Name	Syslog Server	Transport	Port	Format	Facility
Prod1	10.100.10.91	UDP	514	BSD	LOG_USER
Prod2	10.100.17.60	UDP	514	BSD	LOG_USER
Prod3	10.100.111.201	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

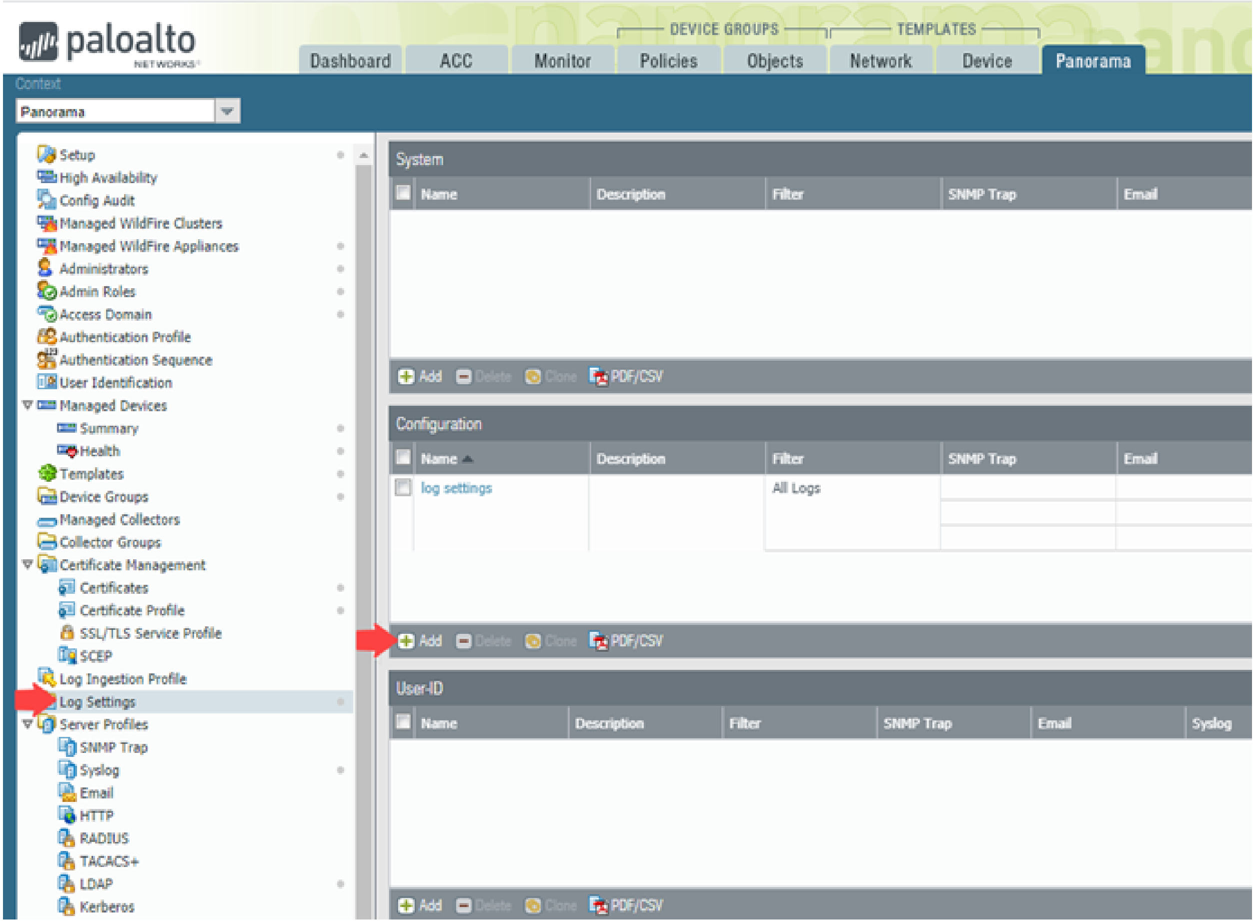
c. Click the **Add** button, and enter the details of the SecureTrack server.

- **Name:** The name of the SecureTrack server.
- **Syslog Server:** The IP address of the syslog server
- **Facility:**
    - For Basic firewall management mode, use the **LOG_USER** facility.
    - For Advanced management mode, use the **LOG_LOCAL7** facility.

4. Click **OK**.

Enabling Accountability

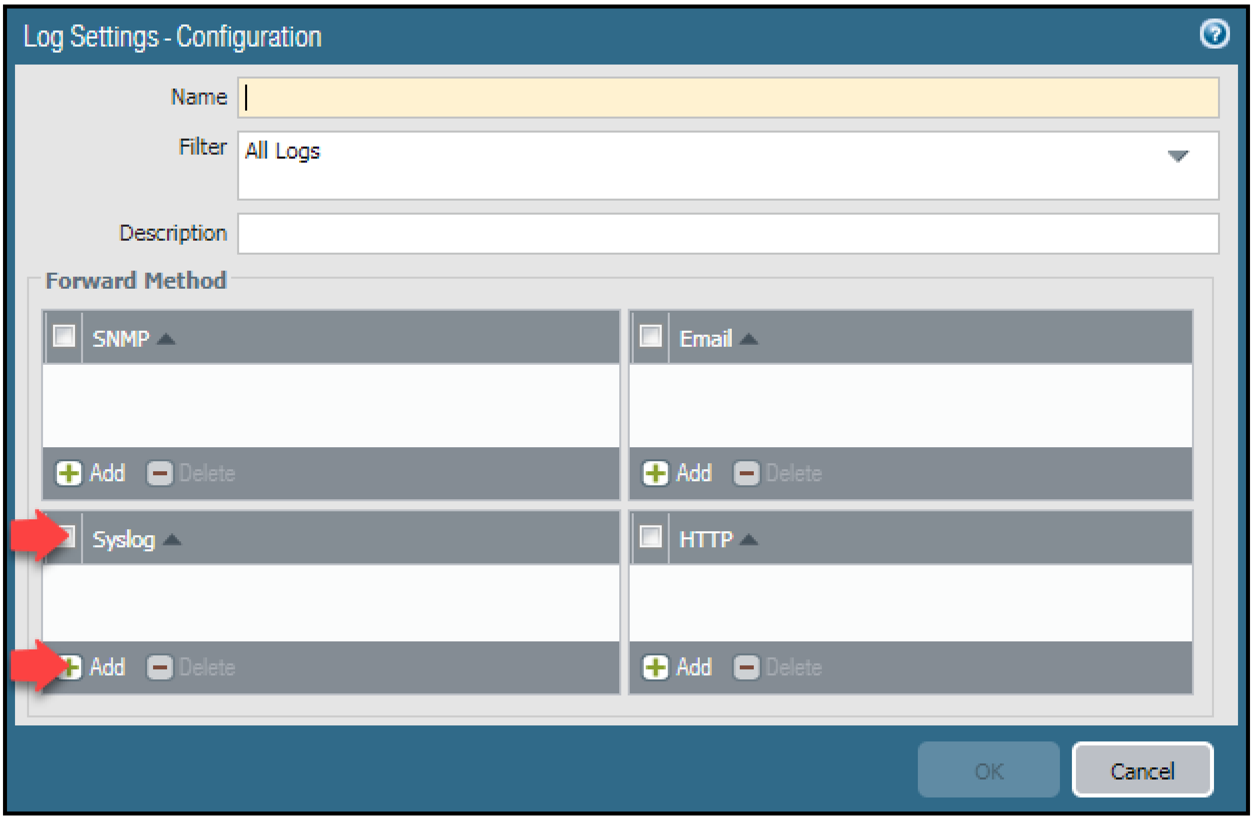
1. In the **Panorama** tab, navigate to **Log Settings.**
2. In the **Configuration** table, click the **Add** button to configure a new log.



Configuration

Name	Description	Filter	SNMP Trap	Email
log settings		All Logs		

The **Log Settings - Configuration** dialog box is displayed.



Name

Filter: All Logs

Description

3. In the **Forward Method** table:
   a. Select **Syslog**
   b. Click the **Add** button, and select the **Syslog Server Profile** you created in the previous section.
4. Click **OK**.

Panorama 6.x-7.x Log Forwarding and Accountability

Panorama log forwarding requires you to:

- **Forward traffic logs to Panorama** - If the firewall was imported via Panorama, SecureTrack will not recognize logs sent directly by the firewall. The logs must be sent by the firewall to Panorama, and then Panorama forwards the traffic logs to SecureTrack
- **Enable accountability** - Enabling accountability ensures that firewall changes made by SecureChange and manual firewall changes made via Panorama are seen by SecureTrack.

Syslog traffic must be configured to arrive to the SecureTrack server that monitors the device (Central Server, Distribution Server or Remote Collector Server) from the IP and/or host name of the device.

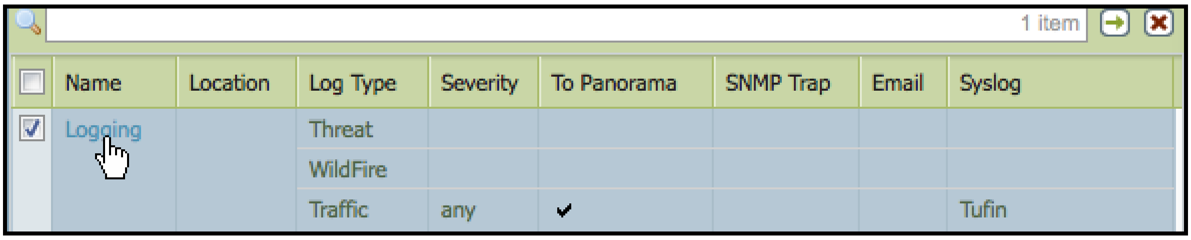
For more information see Sending Additional Information via Syslog.

Forward Traffic Logs to Panorama

These steps will send the firewall traffic logs to Panorama (for Panorama versions 6.x-7.x), and then configure the Panorama to forward the logs to SecureTrack.

To configure Panorama log forwarding

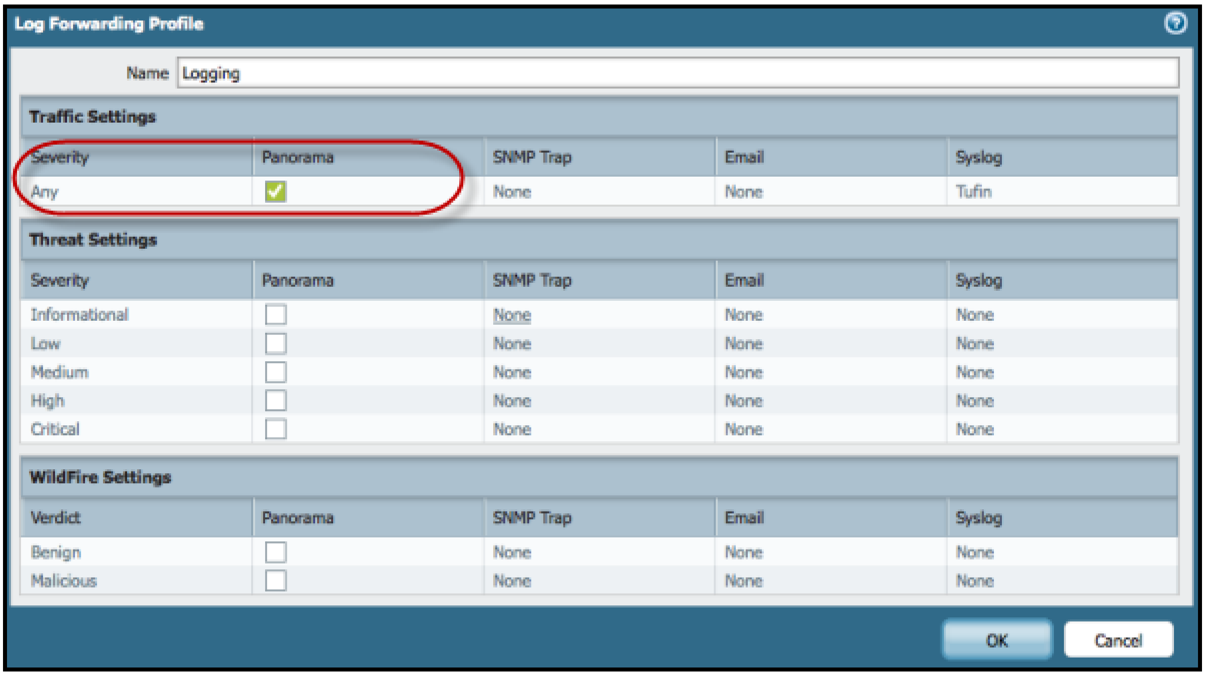
1. On the Panorama device go to **Objects** > **Log Forwarding**, to modify a template to enable log forwarding.
2. Select the **Logging** object.



1 item

□	Name	Location	Log Type	Severity	To Panorama	SNMP Trap	Email	Syslog
☑	Logging		Threat					
			WildFire					
			Traffic	any	✓			Tufin

3. Add a check mark to **Any** under Panorama for the traffic logs.



Log Forwarding Profile

Name Logging

Traffic Settings

Severity	Panorama	SNMP Trap	Email	Syslog
Any	☑	None	None	Tufin

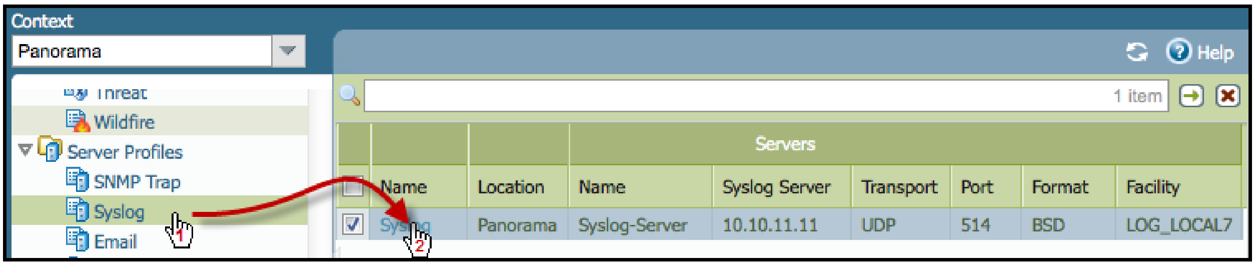
Threat Settings

Severity	Panorama	SNMP Trap	Email	Syslog
Informational	□	None	None	None
Low	□	None	None	None
Medium	□	None	None	None
High	□	None	None	None
Critical	□	None	None	None

WildFire Settings

Verdict	Panorama	SNMP Trap	Email	Syslog
Benign	□	None	None	None
Malicious	□	None	None	None

4. Go to **Device** > **Server Profiles** > **Syslog**.

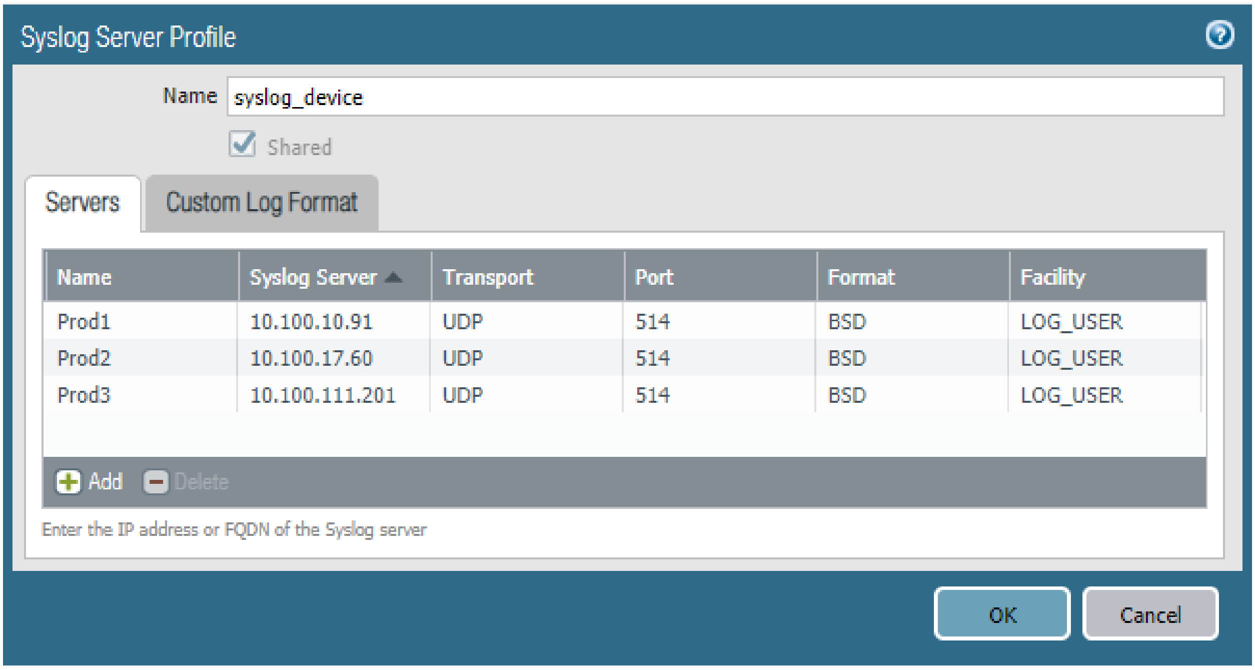


		Servers				
Name	Location	Name	Syslog Server	Transport	Port	Format	Facility
☑ Syslog	Panorama	Syslog-Server	10.10.11.11	UDP	514	BSD	LOG_LOCAL7

5. Add SecureTrack to the syslog server profile, so that Panorama will forward the logs SecureTrack.

   For Basic firewall management mode, use the **LOG_USER** facility.

   For Advanced management mode, use the **LOG_LOCAL7** facility.



Name syslog_device

☑ Shared

Name	Syslog Server ▲	Transport	Port	Format	Facility
Prod1	10.100.10.91	UDP	514	BSD	LOG_USER
Prod2	10.100.17.60	UDP	514	BSD	LOG_USER
Prod3	10.100.111.201	UDP	514	BSD	LOG_USER

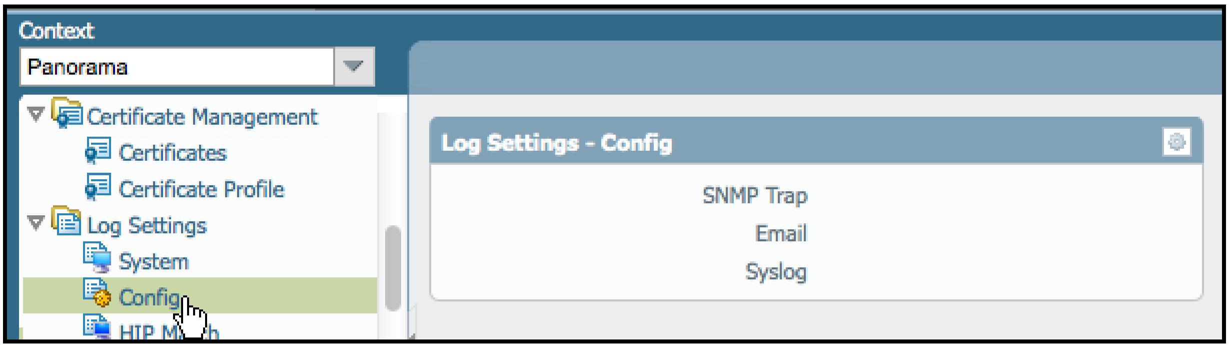
Enter the IP address or FQDN of the Syslog server

6. Commit the template to the firewalls.

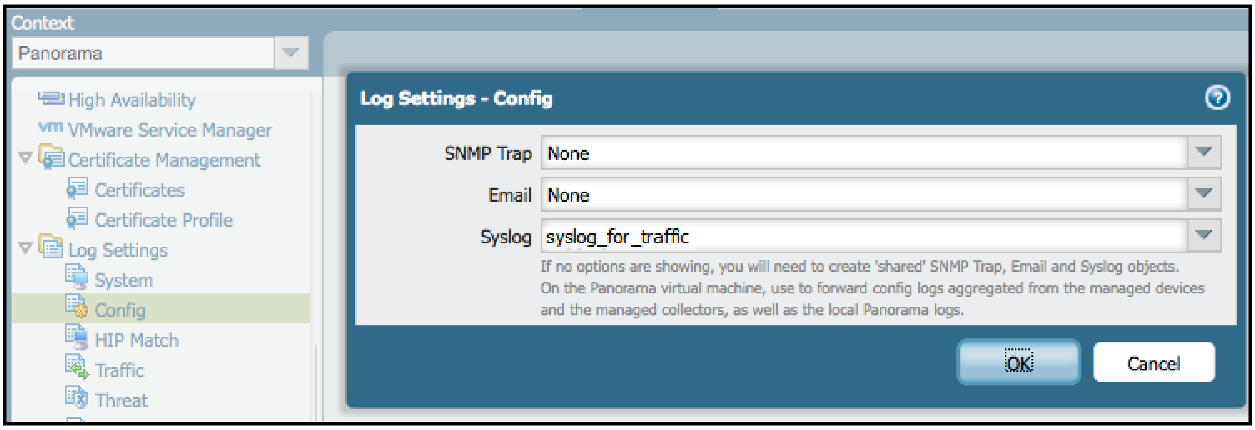
Enable Accountability

To enable accountability:

1. Go to the Panorama tab.
2. Go to **Log Settings** > **Config**.



3. Configure the syslog to be sent to SecureTrack.



Log Settings - Config

SNMP Trap: None

Email: None

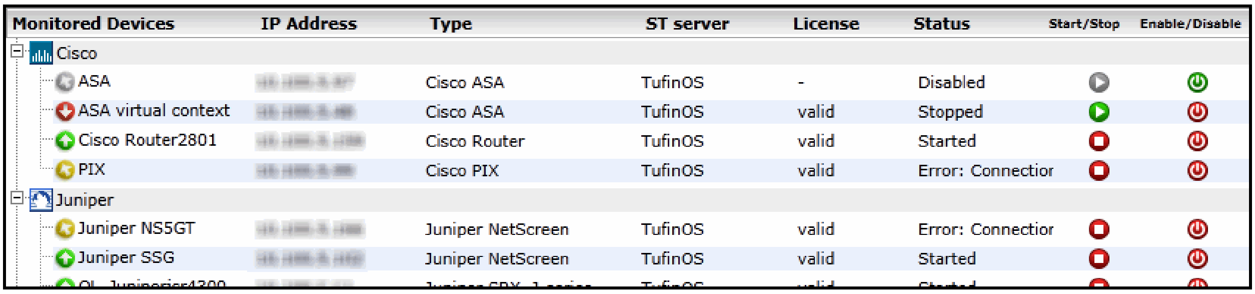
Syslog: syslog_for_traffic

If no options are showing, you will need to create 'shared' SNMP Trap, Email and Syslog objects. On the Panorama virtual machine, use to forward config logs aggregated from the managed devices and the managed collectors, as well as the local Panorama logs.

4. Commit the changes to Panorama.

Verifying Communication

To confirm that monitored devices are communicating successfully with SecureTrack, see Status. The status icons are also shown for each device in also appear in **Compare**. The SecureTrack process for each device is shown with a status icon.



Monitored Devices	IP Address	Type	ST server	License	Status	Start/Stop	Enable/Disable
Cisco							
ASA	[redacted]	Cisco ASA	TufinOS	-	Disabled	▶	⏻
ASA virtual context	[redacted]	Cisco ASA	TufinOS	valid	Stopped	▶	⏻
Cisco Router2801	[redacted]	Cisco Router	TufinOS	valid	Started	■	⏻
PIX	[redacted]	Cisco PIX	TufinOS	valid	Error: Connectior	■	⏻
Juniper							
Juniper NS5GT	[redacted]	Juniper NetScreen	TufinOS	valid	Error: Connectior	■	⏻
Juniper SSG	[redacted]	Juniper NetScreen	TufinOS	valid	Started	■	⏻

The status icons are:

- Monitoring is running successfully.
- Monitoring is enabled and started but SecureTrack cannot communicate with the device. For example, the IP address of the device is not correct or there is a routing problem.
- Monitoring is disabled.
- Monitoring is stopped.
- Device is offline.

If the device reports that usage data is not being collected, make sure that the device is configured to send syslog messages (Configuring Devices to Send Logs) to SecureTrack and that there are hits on the rules on the device.

You can also:

- **Start/Stop** monitoring a device without deleting the device from SecureTrack
- **Enable/Disable** the device in order to use the device's SecureTrack license for another device

To see the revisions for the new device:

1. Go to **Compare**.
2. In the **Monitored Devices** list, select the new device.

   You should see the automatically fetched first policy revision for the device.

In a new installation (not upgrade), if SecureTrack does not fetch the first policy revision within 10 minutes, check that the time set on the device and SecureTrack are synchronized. If you still do not see the first revision, review Troubleshooting SecureTrack.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Administration** > **Status**.

Offline Analysis

You can manually upload policy configurations to SecureTrack, for offline analysis, auditing, and compliance. All SecureTrack features that don't require real-time monitoring or usage analysis are available.

This has two main uses:

- **Offline monitoring**: When there can be no connectivity between SecureTrack and the actual firewalls and management servers, you can periodically export the firewall policy from the device as a file, and then import the file into SecureTrack. Each time you import an updated file, SecureTrack records a policy revision.
- **What If analysis** (non-Check Point only): You can edit a firewall policy in text format, and then upload it to SecureTrack to analyze its effects, without having to actually deploy it on a device.

Offline Analysis needs to be enabled for the specific device. To record a policy revision, first obtain a policy configuration file from the device and then upload it to SecureTrack.

Offline Analysis is supported for all devices that can be monitored by SecureTrack, except for Check Point MDS (log server and CLM), and Palo Alto Panorama devices.
Offline Analysis is not supported for child-level devices (that is devices managed by other devices).

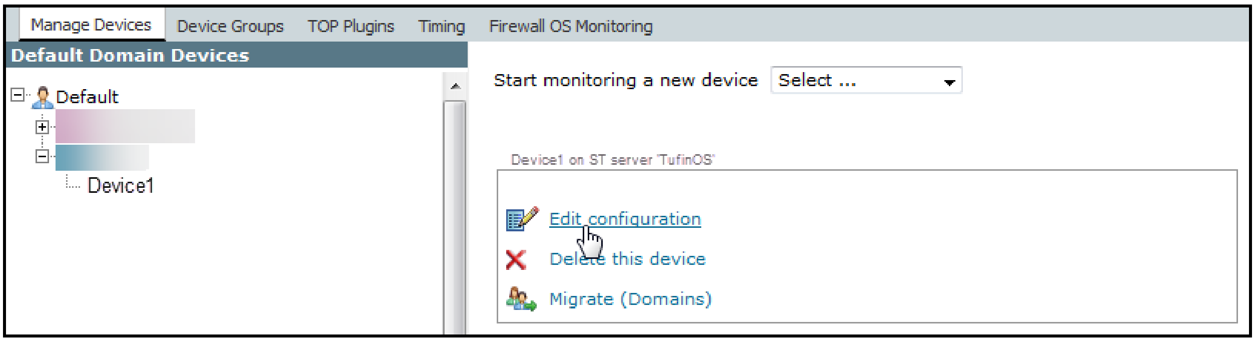
When using Offline Analysis, these features are NOT available:

All Devices	Check Point Devices
• Real time alerts for revisions and compliance policies • Accountability • Rule and object usage • Dynamic routes considered for topology (topology based only on static routes)	• Performance alerts • Topology

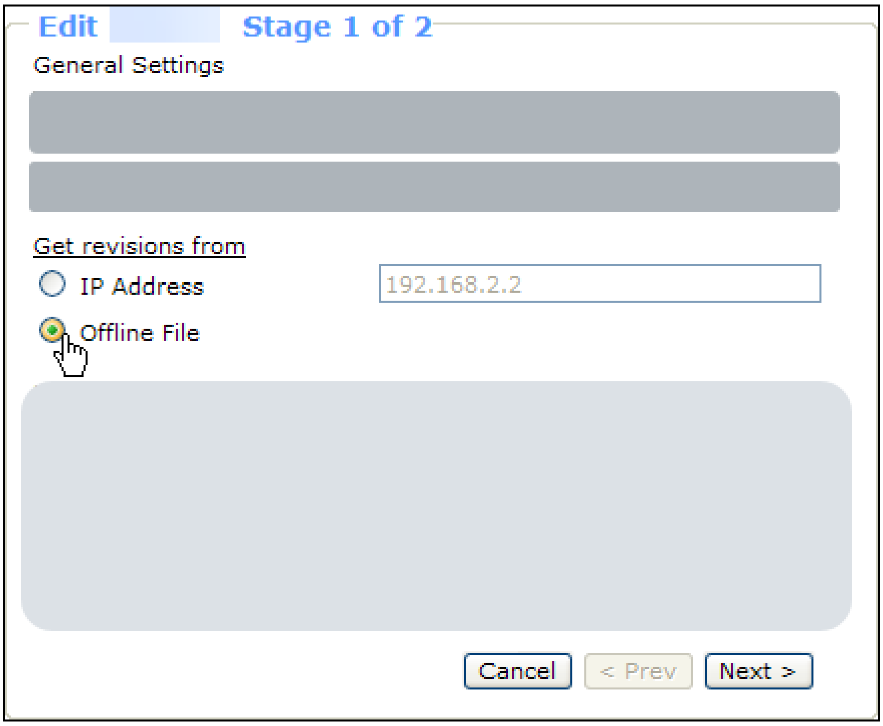
Configuring a Device for Offline Analysis

Before you can manually upload policy configuration files to a device, the device needs to be configured in SecureTrack for Offline Analysis. This can be done in one of two ways:

- As part of the process of adding the device to SecureTrack.
- For a device already configured in SecureTrack for online monitoring, configure Offline Analysis as follows:
  1. Go to Manage Devices.
  2. In the device tree, select the relevant device. Click **Edit Configuration**:



3. Select **Offline File**:



Edit Stage 1 of 2

General Settings

Get revisions from

○ IP Address 192.168.2.2

● Offline File

4. Click **Next**, and **Save**.

Getting a Policy Configuration File for Offline Analysis

You can use these commands to get policy configuration files for offline analysis.

Check Point

Offline configuration is not supported for Check Point R80 and above.

To get a Check Point policy configuration file:

1. Download the R70 tool archive, and extract the contents to any location on the SmartDashboard host.
2. On the SmartDashboard host, open a Windows command line, navigate to the tool's saved location, and run:

```
st_cpmi_pull_win.exe <file> <ip>
```

   Where:

   `<file>` - a name for the output file

   `<ip>` - the IP address of the relevant offline Check Point management server
3. When prompted, type the username and password of a user authorized for the Check Point management server (can be read-only).

Fortinet

To get an offline configuration from Fortigate firewalls:

1. Open a command line to the device.

   For a virtual device, make sure to connect directly to the virtual device (not through the parent device).
2. Run these commands:

- For a VDOM-enabled Fortigate device:

  a. Run these commands:

```
config global
config system console
set output standard
end
end
```

  b. Print the configuration:

```
config vdom
edit VDOM_NAME
show
get system status
show full-configuration firewall service custom
show full-configuration firewall service group
show full-configuration firewall address
show full-configuration firewall addrgrp
show full-configuration firewall schedule onetime
show full-configuration firewall schedule recurring
show full-configuration firewall vip
show full-configuration firewall vipgrp
show full-configuration firewall policy
show full-configuration router static
show full-configuration system interface
show full-configuration system zone
```

  (where `VDOM_NAME` is the name of the desired VDOM)

  c. Copy the configuration output to a text file.

In a Fortinet Virtual Domain, you may receive some error messages, which can be safely ignored. The configuration output may be provided one page at a time.

Each virtual domain collected should be imported as a standalone Fortigate Firewall.

The license required is for a Firewall (and not a Virtual Firewall).

Shared router configurations will not be imported.

- For other Fortigate devices:
  a. Run these commands:

```
config system console
set output standard
end
```

  b. Print the configuration:

```
show
show
get system status
show full-configuration firewall service custom
show full-configuration firewall service group
show full-configuration firewall address
show full-configuration firewall addrgrp
show full-configuration firewall schedule onetime
show full-configuration firewall schedule recurring
show full-configuration firewall vip
show full-configuration firewall vipgrp
show full-configuration firewall policy
show full-configuration router static
show full-configuration system interface
show full-configuration system zone
```

  c. Copy the configuration output to a text file.

Forcepoint

1. Open a command line to the device.
2. Run these commands:

```
srole
cf -J interface query
cf -J subnet query
cf -J netgroup query
cf -J iprange query
cf -J ipaddr query
cf -J domain query
cf -JK name,description,download_path geolocation query | grep -v
download_path
cf -JK name,description host query
cf -JK name,description netmap query
cf appdb version
cf -J externalgroup query
cf -J application query
cf -J appgroup query
cf appdb list verbose=on
cf -J zone query
cf -J zonegroup query
cf -J route query
cf -J udb query
cf -J externalgroup query
cf -J usergroup query
cf -JK table,name,action,disable,source_zones,dest_
zones,source,dest,application,ssl_ports,tcp_ports,udp_
ports,authgroups,description  policy query
exit
exit
```

3. Copy the configuration output to a text file.

Palo Alto

To get an offline configuration from Palo Alto firewalls:

1. Make sure you have network connectivity between SecureTrack and the Palo Alto firewall.
2. Run the commands:

```
cd /usr/local/st
```

```
./st_paloalto_fw_login.pl ssl <ip> <user> <timeout> 443 <vsys>
offline > <offline_file>
```

Where:

`<ip>` - IP address of the firewall

`<user>` - a user with the superuser Admin Role for the firewall

`<timeout>` - seconds to wait for a response from the device (recommended: at least 120)

`<vsys>` - the ID of the vsys, such as vsys1; you can find the vsys ID in the device web interface in **Device** > **Virtual Systems**

For devices that do not support vsys or for devices that do not yet contain vsys, we recommend that you change the run script from `<vsys>` to `vsys1`.
Note that certain versions of Palo Alto do not have Virtual Systems listed under Devices.

3. When prompted, enter the password of the user account.

Other Devices

To get a policy configuration file from other devices:

1. Open a command line to the device.

   For a virtual device, make sure to connect directly to the virtual device (not through the parent device).

2. Run these commands:

   - On **Cisco** firewalls:

     ```
     show running-config
     ```

   - On **Netscreen** firewalls:

     ```
     get config
     get zone all
     ```

     For each zone run: `get zone id <zone id> | include "(Zone name)|(interface)"`

   - On **JunOS** devices:

     ```
     show configuration | display set | no-more
     show configuration | display inheritance defaults | display xml
     | no-more
     show configuration | display detail | display xml | display omit
     | no-more
     show configuration policy-options | display inheritance | no-
     more
     ```

   - On **IPtables** firewalls:

     ```
     iptables-save
     ```

     Copy the output except for the first line (`# Generated by...`) and last line (`# Completed on...`).

- On **F5** devices: (For the Common partition only)

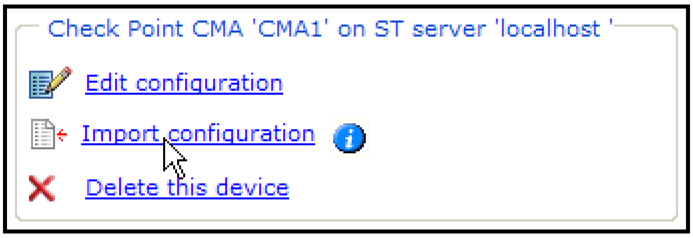
```
show running config
```

3. Copy the configuration output to a text file.

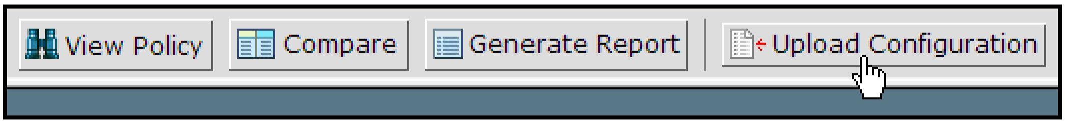
Uploading a Policy Configuration for Offline Analysis

Once you have obtained a policy configuration file, you can upload it to SecureTrack, as a revision for a device configured for Offline Analysis, as follows:

1. Do one of the following:
   - Go to Manage Devices. In the device tree, select the relevant device. Click **Import configuration**:



   - In **Compare** view, in the device tree, select the relevant device. Click **Upload Configuration**:



2. Navigate to the policy configuration file, and click **Open**.

The revision will appear after a few minutes in **Compare** view.

Alternatively, you can upload a policy configuration file to SecureTrack via CLI, as follows:

1. Get the ID of the offline device:

```
# st stat
```

2. Copy the policy configuration file to the SecureTrack host, to:

   /usr/local/st/offline_analysis/offline_<id>

   where `<id>` is the ID# from step 2.

3. Run:

```
st restart <id>
```

   where `<id>` is the ID# from step 2.

The revision will appear after a few minutes in the **Compare** view.

Dashboard and Browsers

In **Home**, SecureTrack includes a dynamic dashboard with charts for key indicators, as well as browsers that let you drill-down into the data that SecureTrack collects from the monitored devices. The dashboard tabs give you a central location to monitor the security of your environment and to see at a glance where you can improve your security stance.

Each of these tabs includes the device tree with:

- An automatic device tree with devices grouped by vendor and domain
- A customizable device tree that lets you group together devices of similar location or function

You can quickly understand the security status of the grouped devices to help you focus on the areas that require your attention.

SecureTrack Dashboard

The SecureTrack Dashboard is the central location for you to see the current status of security in your environment. In the dashboard you can:

- Pivot the data for the indicators to highlight specific data points
- View the data points over time to see data trends

Each dashboard section focuses on a key indicator and offers a variety of charts to help you view your security status. When you click on an element in a chart, you can drill-down and see more detail in the risk, change and cleanup browsers.

How Do I Get Here?

In SecureTrack, go to: **Home** >**Dashboard** ▭.

Risk Charts

The risk charts in the **Dashboard**, let you quickly understand the network security risks in your environment. Risk is summarized with: **Security Score**, and **Risks by Severity** or **Type**.

When you click on a section of a chart, SecureTrack opens the risk browser with the relevant data shown.

Security Score

SecureTrack calculates the security score based on the number and severity of the risks found in the specified device. The security score is on a scale of 0-100, where 100 represents that no risks are found. Each risk in a device lowers the score, but the number of times a risk is found in a policy does not impact the score.

More specifically, the security score is determined by multiplying each risk found in the specified device by its severity (for example, Low=1 and Critical=4) and dividing it by the total number of risks multiplied by their severities. The result is subtracted from 100 to produce a score on a scale of 0-100, where 100 represents that no risks are found. For example, if SecureTrack checks a policy for 10 risks in each severity level (10*1+10*2+10*3+10*4 = 100) and finds two high (2*3) and one critical (1*4) risks, the calculation is [100-(2*3+1*4)] = 90%, or a security score of 90.

SecureTrack calculates the security score for every new revision that it receives. When you select a device from the device tree, you see the security score for the current policy on the device and an arrow that indicates that the security score improved ▲, decreased ▼ or did not change ▭▭ since the previous score calculation. The security score for a group is the average of the scores of all of the devices in that group, including devices that are in subgroups.

The charts for security score are:

- Security score - the security score for the selected device or group
- Security score by member - the security scores for each of the direct members of the selected group
- Security score trend - the security score of the device or group at the end of each of the previous days, weeks, or months; the last point in the trend is the current security score

Risks by Severity or Type

You can see the number of risks in the latest revision on a device or group of devices shown according to the risk severity levels or risk types.

Each risk is part of a category of risks, or **risk types**. The risk types are:

- Risky rules - Rules that include services with source and destination that are likely to not be secure
- Weak rules - Rules that are not configured according to basic networking principles or industry best practices
- Weak policies - Policies that are not configured according to basic networking principles or industry best practices

Each risk is also assigned a **severity** level to help you identify the priority for risk remediation. The severity levels are: Critical, High, Medium, and Low. You can change the severity of a risk in risk configuration.

The charts for risks are:

- Risks by type - For the selected device or group, the number of risks in each risk type
- Risks by severity - For the selected device or group, the number of risks in each severity level
- Risks of members by severity - For each device or group that is a direct member of the selected group, the number of risks in each severity level
- Risks of devices by severity - For each device that is a member of the selected group or its subgroups, the number of risks in each severity level

Viewing Security Score and Risk Charts

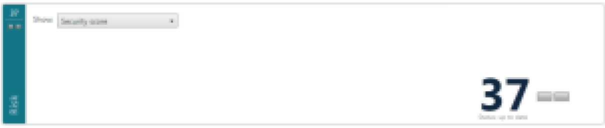
The security score shows you the security of your network and how the security changes over time. The risk charts show you where the critical risks are in your network.

To see security score and risk charts:

1. From the Dashboard, select a device or group from the device tree.
2. Select one of the charts:

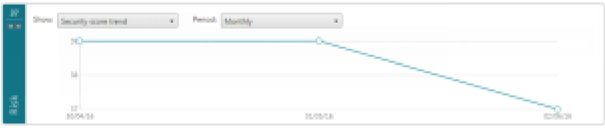
   - To see the security score of the selected device or group, select **Security score**.

     The arrow next to the score tells you if the current score is higher, lower or the same as the previous security score.

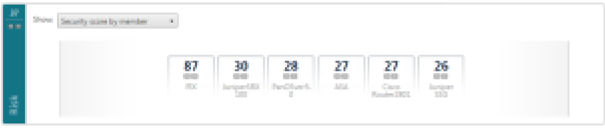
   - To see how the security score changed over time, select **Security score trend** and the **Daily**, **Weekly** or **Monthly** range.

     The chart shows the previous security scores. You can see when the score has improved or decreased over time.

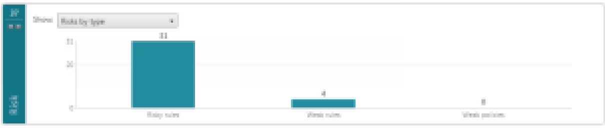
   - To see the security scores of each member of a group, select **Security score by member**.

     The chart shows the current security score for up to 10 devices or groups, from lowest to highest score. The arrow below each score tells you if the current score is higher, lower or the same as the previous security score.

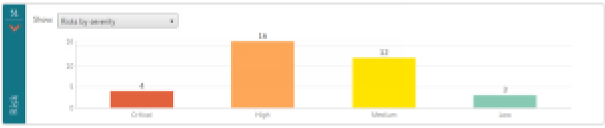
   - To see the number of risks in each risk type for a device or group, select **Risks by type**.

     The chart shows the types of risks and the number of risks the device has in each risk type.

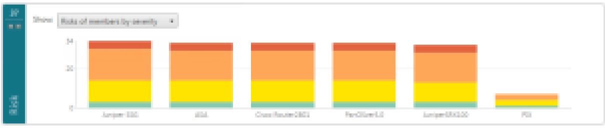
   - To see the number of risks in each severity level for a device or group, select **Risks by severity**.

     The chart shows the severities and the number of risks the device has in each severity level.

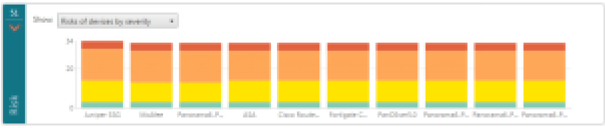
   - To see the number of risks in each severity level for each member of a group, select **Risks of members by severity**.

     The chart shows the number of risks for each member of the group and shows the number of risks each member has in each severity level, for up to 10 devices or groups and from highest to lowest number of risks.

   - To see the number of risks in each severity level for each device in the group and its subgroups, select the **Risks of devices by severity**.

     The chart shows the number of risks for each device that is in the group, even if the device is not directly a member of the group. It also shows the number of the risks each device has in each severity level, for up to 10 devices or groups and from highest to lowest number of risks.

Change Charts

The **Change Chart**, in the **Dashboard**,shows you at-a-glance the most recent revision changes in your network. You can select a device to show the revisions for that device, or you can select a group of devices from the tree to show the recent revisions for all of the devices in the group.

The revisions are shown in a table that you can sort by column headers, including by device name, policy name, date the policy was changed on the device, or the date the policy was received by SecureTrack.

You can filter the revisions for the last day, week or month so that you can focus on a specific time period, or you can filter for the last 20, 100, or 200 revisions.

Revision Authorization

In the Change chart, you can quickly see that revisions are made as a result of requests in your ticketing system. If you manage your access requests in SecureChange and SecureChange is connected to SecureTrack (in SecureChange **Settings** > **SecureTrack**), you can configure SecureTrack to monitor authorized revisions so that:

- When a policy is changed to allow traffic that was previously blocked by the policy, SecureTrack searches for SecureChange tickets that match the newly allowed traffic. If it finds matching tickets, the tickets are associated with the revision and listed in the Change chart.
- When a policy is changed to block traffic that was previously allowed by the policy, SecureTrack searches for SecureChange tickets that match the newly blocked traffic. If it finds matching tickets, the tickets are associated with the revision and listed in the Change chart.

  Traffic can be blocked by adding it to a drop rule or removing it from an allow rule.
- If all of the changed traffic is associated with tickets, the revision is marked **Authorized**. If not, the revision is marked **Unauthorized**.
- You can manually change the authorization status. A tooltip shows the name of the administrator that changed the authorization status and when the status was changed.

SecureTrack automatically associates a SecureChange ticket with the revision if:

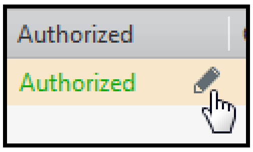
- The ticket has an access request that at least partially matches the traffic changes in the revision
- The target of the access request is **Any** with Topology disabled, or the same as the device from which the revision was received
- The ticket is open (You can also configure authorization to include tickets that were closed within the last 3, 6, 9 or 12 months.)
- The ticket is authorized, meaning that it either:
  - Has at least one step with the Approve/Decline field and the final step with this field is Approved
  - Does not have any steps with the Approve/Decline field but the ticket has passed to the last step of the workflow

SecureTrack automatically marks each revision as, either:

- **Authorized** without tickets - There are no rule changes in the revision or there is a rule change that does not impact network traffic, such as a change to a rule comment
- **Authorized** with tickets - All of the changed traffic matches at least one associated SecureChange ticket
- **Unauthorized** with tickets - Tickets are associated with the revision, but not all of the changed traffic matches at least one associated SecureChange ticket
- **Unauthorized** without tickets - No tickets are associated with the changed traffic in the revision

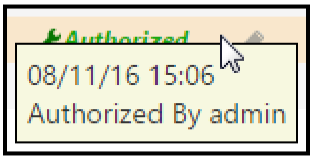
To change the authorization status for a revision:

1. In the Change chart, hover over the revision.
2. In the Authorized column, click on the Edit icon.

3. Select **Authorized** or **Unauthorized**.
4. Click **Confirm**.

   The revision is marked with the new Authorization status with a Configured icon ( ) and a tooltip that shows who changed the authorization last and when it was changed:

   
   Authorized

   08/11/16 15:06
   Authorized By admin

Cleanup Charts

> This is a Legacy Feature. We recommend you consider using the "Cleanup Browser" on page 296.

The cleanup charts, in the **Dashboard**, let you quickly understand the ways that you can simplify your policies by removing unnecessary rules and objects.Cleanup is summarized with two indicators: **Optimization Score**, and **Cleanups by Type**.

When you click on a section of a chart, SecureTrack opens the cleanup browser with the results shown.

IPv6 is not supported for this TOS feature. (Except for NSM IPv6 objects which are shown in unused objects.)

Optimization Score

SecureTrack calculates the optimization score based on the number and priority of the cleanups found in the specified device.The optimization score is on a scale of 0-100, where 100 represents optimal efficiency.Each cleanup in a device lowers the score.

SecureTrack calculates the optimization score for every new revision that it receives.When you select a device from the device tree, you see the optimization score for the current policy on the device and an arrow that indicates that the optimization score improved ▲, decreased ▼ or did not change ▭▭ since the previous score.

The optimization score for a group is the average of the scores of all of the devices in that group, including devices that are in subgroups.

The charts for optimization score are:

- Optimization score - the optimization score for the selected device or group
- Optimization score by member - the optimization scores for each of the direct members of the selected group

Cleanups by Type

You can see the number of cleanups in the latest revision on a device or group of devices shown according to the cleanup types.

Each cleanup is part of a category of cleanups, or **cleanup types**.The cleanup types are:

- Disabled rules - Rules that never have hits from traffic because they are disabled
- Duplicate network objects - Network objects (including networks, hosts and ranges) are reported as matching when they have the same IP address and netmask (or start and end IP addresses for ranges) and the same zone.

  Groups of network objects are reported as matching when they have the same group members.
- Duplicate services - Services are reported as matching when they are not pre-defined and when they have the same values for:
  - Protocol - TCP or UDP
  - Port - Destination port
  - Source port - If specified in the object's properties
  - Timeout setting - Either session timeout (Check Point) or inactivity timeout (Juniper)
  - Match for Any - Check Point only

    The duplicate service cleanup does not compare source port and timeout in Palo Alto, service timeout in Juniper Netscreen, or protocol type in Check Point.

  Groups of services are reported as matching when they have the same group members and at least one of the group members is not a pre-defined service.
- Empty groups (`C08`) - Group objects that do not have any members
- Fully shadowed and redundant rules (`C01`) - Rules that never have hits from traffic because rules above them in the policy handle the traffic.
  - Shadowed - For rules that are marked as fully shadowed, you can click on **Details** to see the rules that shadow it.
- Unattached network objects (`C06`) - Objects that are not used in any firewall rules, group objects.Objects used in other forms of management, such as NAT rules or VPN connections, may appear as unattached in the security policy.Verify the use of unattached objects across the relevant device management tools.
- Unused network objects (`C15`) - Network objects and network object groups that are not in use across the security policy and have no hits in the policy traffic log during the time period configured in Cleanup Configuration.These can be unattached objects, or objects that appear in access rules and object groups but are not being hit within those rules and groups.

  Notes:

  - The unused objects cleanup is disabled by default. When you enable it in Cleanup Configuration, you must also select the time period (days, weeks or months) of the usage data. Objects that have no hits during the usage period are listed as unused.
  - Make sure that the cleanup settings in maintenance are set for a longer period than the usage period for the cleanup.

- The cleanup is shown in the Dashboard only if the amount of time configured for the usage period has passed since the upgrade to R13-4 or higher.
- The cleanup is shown only if there are hits for every day in the usage period, such that an object is not shown as unused when there was a connectivity problem that resulted in at least one day without any traffic hits.
- The cleanup does not include:
  - Objects used in VPN rules
  - Addresses in Cisco configurations that are not associated with defined objects
  - Traffic hits from the current day because the results are calculated nightly
  - Rules that were changed during the period and the objects that are used in the rules
  - Rules without logs
  - IPv6 objects in devices other than Juniper NSM
  - Predefined, implicit and NAT objects

Each cleanup is defined with a name, severity, and description.You can change the name and definition to fit the terminology and structure of your organization.You can also change the severity to indicate how important the cleanup is to your organization.You can change the severity of a risk in Cleanup Configuration.

The chart for cleanups is:

- Cleanups by type - For the selected device or group, the number of cleanups in each cleanup type

Viewing Optimization Score and Cleanup Charts

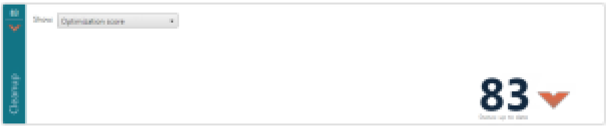
> This is a Legacy Feature. We recommend you consider using the "Cleanup Browser" on page 296.

The optimization score shows you where you can remove unused rules and objects to improve the efficiency of your policies. The cleanup charts show you where the cleanups are in your network.

To see optimization score and cleanup charts:

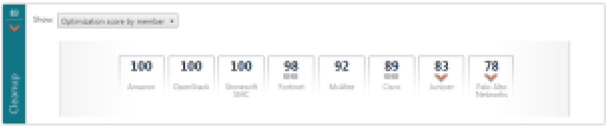
1. From the Dashboard, select a device or group from the device tree.
2. Select one of the charts:
   - To see the optimization score of the selected device or group, select **Optimization score**.

     The arrow next to the score tells you if the current score is higher, lower or the same as the previous security score.

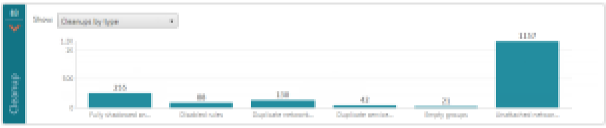
   - To see the optimization scores of each member of a group, select **Optimization score by member**.

     The chart shows the current optimization score for up to 10 devices or groups, from lowest to highest score. The arrow below each score tells you if the current score is higher, lower or the same as the previous security score.

   - To see the number of cleanups in each cleanup type for a device or group, select **Cleanups by type**.

     The chart shows the types of cleanups and the number of cleanups the device has in each type.

Risk Browser

The risk browser, in **Home** > **Risk**, lets you drill-down into the risks in your network to see exactly in which policies and rules the risks exist. Each risk has an ID that is colored according to its severity and is shown on each policy or rule where the risk exists.

You can also configure which risks are used in the risk calculations.

For each risk you can see:

- Instances - the specific rules and policies where the risk exists in the current policy revisions for the selected device or group, shown by device.

- Information - General information about the risk, including the risk description

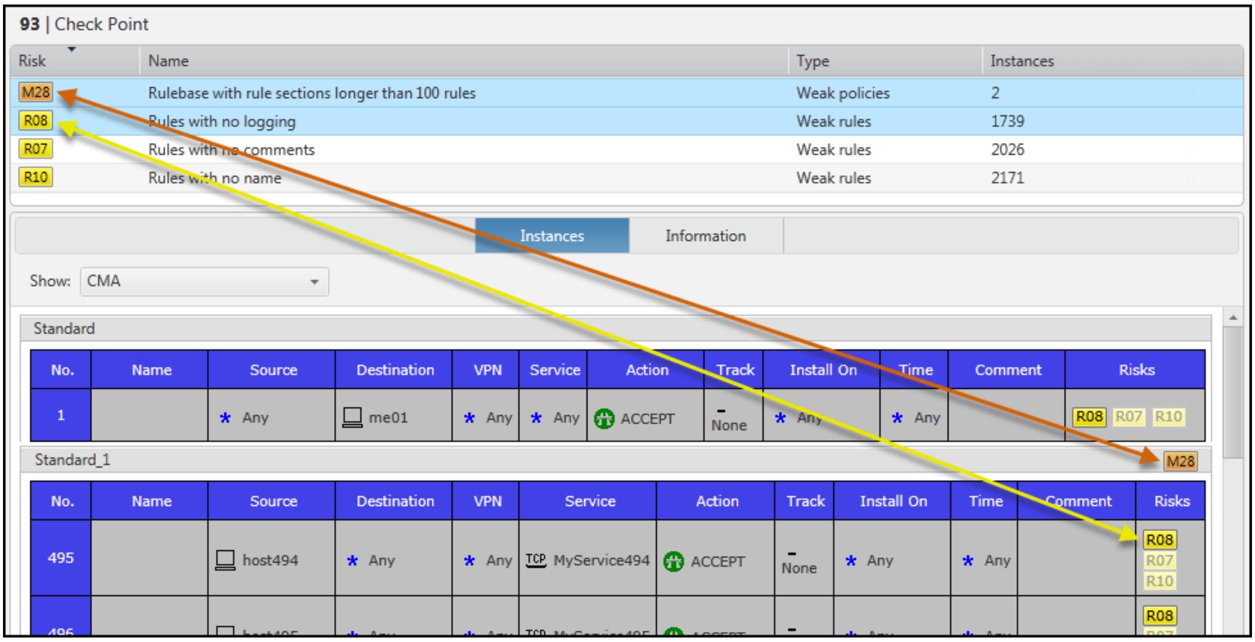
To find a risk instance:

1. Go to **Home** > **Risk**.
2. Select a device or group from the device tree.

   The risks in the specified device or group are listed and sorted according to severity.
3. To select risks, click on one or more risks from the list of risks.

   For the specified device or group, the risk browser shows where the specified risks exist in the current policies, shown in the vendor's format.

   The instances are listed with all of the risks that apply to them. The risk IDs for the selected risks are highlighted and the risks that are not currently selected are dimmed.



93 | Check Point

Risk	Name	Type	Instances
M28	Rulebase with rule sections longer than 100 rules	Weak policies	2
R08	Rules with no logging	Weak rules	1739
R07	Rules with no comments	Weak rules	2026
R10	Rules with no name	Weak rules	2171

Show: CMA

Standard

No.	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment	Risks
1		* Any	me01	* Any	* Any	ACCEPT	- None	* Any	* Any		R08 R07 R10

Standard_1 M28

No.	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment	Risks
495		host494	* Any	* Any	TCP MyService494	ACCEPT	- None	* Any	* Any		R08 R07 R10
496		host495	* Any	* Any	TCP MyService495	ACCEPT	-	* Any	* Any		R08

Risk Configuration

SecureTrack comes with a defined set of risks. SecureTrack produces the security score and risk instances in the risk charts and risk browser based on the risks that are selected in the risks configuration.

These risks are divided into these risk types:

- Risky rules - Rules that include services with source and destination that are likely to not be secure
- Weak rules - Rules that are not configured according to basic networking principles or industry best practices
- Weak policies - Policies that are not configured according to basic networking principles or industry best practices

Each risk is defined with a name, severity, description and access, if applicable. You can change the name and definition to fit the terminology and structure of your organization. You can also change the severity to indicate how important the risk is to your organization.

How Do I Get Here?

In SecureTrack, go to: **Settings** > **Configuration** > **Risk**.

Removing Risks

You can remove a risk from the risk configuration so that it is not used in security score and risk calculations.

To remove a risk:

1. Go to Risk.
2. Select the risk type.
3. Clear the checkbox for a risk.
4. Click **Save**.

Editing Risks

Each risk is defined with a name, severity, description and access, if applicable. You can change the name and definition to fit the terminology and structure of your organization. You can also change the severity to indicate how important the risk is to your organization.

To edit a risk:

1. Go to Risk.
2. Select the risk type.
3. Click on the name of the risk.
4. Edit the name, description or severity of the risk.
5. Click **Save**.

Setting Network Types for Risky Rules

The risks in Risky Rules are defined by source and destination network-types. For example, if a rule allows HTTP or HTTPS from the DMZ to the internal network, it is labeled as a risky rule.

SecureTrack can either use Topology Intelligence to calculate what networks are Internal, DMZ or External automatically for these risks, or you can specify zones that are Internal, DMZ or External. In order to specify zones, you must first create zones (in **Network** > **Zones**) and add subnets to the zones.

To change the definition of Internal, DMZ or External network types for Risky Rules:

1. Go to Risk.
2. From the menu, select **General**.
3. Under **Risky Rules**, select either:
   - **Topology** to let SecureTrack define the network types based on topology intelligence
   - **Zones** to manually define the network types using zones, and select a zone for each of the network types: Internal, DMZ, External
4. Click **Save**.

Change Browser

The Change browser shows you at-a-glance the most recent revision changes in your network.You can select a device to show the revisions for that device, or you can select a group of devices from the tree to show the recent revisions for all of the devices in the group.

The revisions are shown in a table that you can sort by column headers, including by device name, policy name, date the policy was changed on the device, or the date the policy was received by SecureTrack.

IPv6 is not supported for this TOS feature.

Revision Authorization

In the Change chart, you can quickly see that revisions are made as a result of requests in your ticketing system. If you manage your access requests in SecureChange, you can configure SecureTrack to monitor authorized revisions so that:

- When a policy is changed to allow traffic that was previously blocked by the policy, SecureTrack searches for SecureChange tickets that match the newly allowed traffic. If it finds matching tickets, the tickets are associated with the revision and listed in the Change chart.
- When a policy is changed to block traffic that was previously allowed by the policy, SecureTrack searches for SecureChange tickets that match the newly blocked traffic. If it finds matching tickets, the tickets are associated with the revision and listed in the Change chart.

  Traffic can be blocked by adding it to a drop rule or removing it from an allow rule.
- If all of the changed traffic is associated with tickets, the revision is marked **Authorized**. If not, the revision is marked **Unauthorized**.
- You can manually change the authorization status. A tooltip shows the name of the administrator that changed the authorization status and when the status was changed.

SecureTrack automatically associates a SecureChange ticket with the revision if:

- The ticket has an access request that at least partially matches the traffic changes in the revision
- The target of the access request is **Any** with Topology disabled, or the same as the device from which the revision was received
- The ticket is open (You can also configure authorization to include tickets that were closed within the last 3, 6, 9 or 12 months.)
- The ticket is authorized, meaning that it either:
  - Has at least one step with the Approve/Decline field and the final step with this field is Approved
  - Does not have any steps with the Approve/Decline field but the ticket has passed to the last step of the workflow

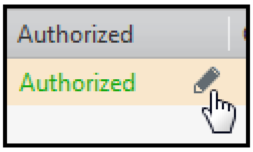
SecureTrack automatically marks each revision as, either:

- **Authorized** without tickets - There are no rule changes in the revision or there is a rule change that does not impact network traffic, such as a change to a rule comment
- **Authorized** with tickets - All of the changed traffic matches at least one associated SecureChange ticket
- **Unauthorized** with tickets - Tickets are associated with the revision, but not all of the changed traffic matches at least one associated SecureChange ticket
- **Unauthorized** without tickets - No tickets are associated with the changed traffic in the revision

To change the authorization status for a revision

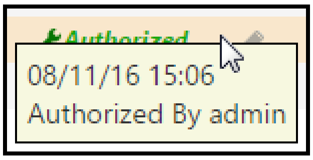
This procedure can only be performed by a Multi-Domain Administrator or by a Super Administrator.

1. In the **Change** chart, hover over the revision.
2. In the **Authorized** column, click on the **Edit** icon.



3. Select **Authorized** or **Unauthorized**.
4. Click **Confirm**.

The revision is marked with the new Authorization status with a Configured icon ( ) and a tooltip that shows who changed the authorization last and when it was changed:


Authorized

08/11/16 15:06
Authorized By admin

How Do I Get Here?

In SecureTrack, go to **Home** > **Change**.

Cleanup Browser

Overview

The Cleanup Browser, lets you drill-down into the cleanups in your network to see exactly in which policies and rules the cleanups exist. Each cleanup has an ID that is colored according to its priority and is shown on each policy or object where the cleanup exists.

For devices that support VIP (Virtual IP) objects, if the cleanup rule contains a VIP object then the rule must be global for the cleanup browser to match the cleanup rule.

IPv6 is not supported for this TOS feature. (Except for NSM IPv6 objects which are shown in unused objects.)

You can export the instances to a CSV file that you can use to automate the process of removing the duplicate objects. For Cisco devices, you can view the rules in textual format and click **Export** to save the ACLs as a CSV file. To properly view the CSV file, open it with a text editor.

Cleanups by Type

You can see the number of cleanups in the latest revision on a device or group of devices shown according to the cleanup types.

Each cleanup is part of a category of cleanups, or **cleanup types**. The cleanup types are:

- **Disabled rules** - Rules that never have hits from traffic because they are disabled
- **Duplicate services** - Services are reported as matching when they are not pre-defined and when they have the same values for:
  - Protocol - TCP or UDP
  - Port - Destination port
  - Source port - If specified in the object's properties
  - Timeout setting - Either session timeout (Check Point) or inactivity timeout (Juniper)
  - Match for Any - Check Point only

The duplicate service cleanup does not compare source port and timeout in Palo Alto, service timeout in Juniper Netscreen, or protocol type in Check Point.

Groups of services are reported as matching when they have the same group members and at least one of the group members is not a pre-defined service.

- **Empty groups (C08)** - Group objects that do not have any members
- **Fully shadowed and redundant rules (C01)** - Rules that never have hits from traffic because rules above them in the policy handle the traffic.
    - Shadowed - For rules that are marked as fully shadowed, you can click on **Details** to see the rules that shadow it.

  Note that layer 7 rule information such as application-related criteria is not currently taken into account when determining if a rule is shadowed and so, in some cases, non-shadowed rules may show up as shadowed. All rules marked as fully shadowed should be therefore be checked for the existence of layer 7 criteria before deciding whether to remove them.
- **Unattached network objects (C06)** - Objects that are not used in any firewall rules, group objects. Objects used in other forms of management, such as NAT rules or VPN connections, may appear as unattached in the security policy. Verify the use of unattached objects across the relevant device management tools.
- **Unused network objects (C15)** - Network objects and network object groups that are not in use across the security policy and have no hits in the policy traffic log during the time period configured in **Settings** > **Configuration** > **Cleanup**.These can be unattached objects, or objects that appear in access rules and object groups but are not being hit within those rules and groups.

  Notes:
    - The unused objects cleanup is disabled by default. When you enable it in **Settings** > **Configuration** > **Cleanup**, you must also select the time period (days, weeks or months) of the usage data. Objects that have no hits during the usage period are listed as unused.
    - Make sure that the cleanup settings in **Settings** > **Administration** > **Maintenance** are set for a longer period than the usage period for the cleanup.
    - The cleanup is shown only if there are hits for every day in the usage period, such that an object is not shown as unused when there was a connectivity problem that resulted in at least one day without any traffic hits.
    - The cleanup does not include:
        - Objects used in VPN rules
        - Addresses in Cisco configurations that are not associated with defined objects
        - Traffic hits from the current day because the results are calculated nightly
        - Rules that were changed during the period and the objects that are used in the rules
        - Rules without logs
        - IPv6 objects in devices other than Juniper NSM
        - Predefined, implicit and NAT objects

Each cleanup is defined with a name, severity, and description. You can change the name and definition to fit the terminology and structure of your organization. You can also change the severity to indicate how important the cleanup is to your organization. You can change the severity of a risk in **Settings** > **Configuration** > **Cleanup**.

For each cleanup you can see:

- Instances - the specific rules and objects where the cleanup exists in the current policy revisions and group objects for the selected device or group
- Information - General information about the cleanup including the cleanup description

What Can I Do Here?

Finding and Exporting Cleanup Instances

1. Go to **Home** > **Cleanups**.
2. Select a device or group from the device tree.

   The cleanups are listed and sorted according to priority.
3. Select a cleanup type.

   If you selected a group of devices, you can select from the **Show** list to see the instances for each device in the group.

For the specified device, the cleanup browser shows where the specified cleanups exist in the current policies, shown in the vendor's format. The instances are listed with all of the cleanups that apply to them. The IDs for the selected cleanups are highlighted and the cleanups that are not currently selected are dimmed.

4. Click to save all of the cleanup instances to a CSV file you can open from the Reports Repository.

   If you selected a group of devices, the CSV file contains the cleanup instances for all of the devices in the group. To export only the instances for one device, select that device from the device tree and click .

How Do I Get Here?

In SecureTrack, go to **Home** > **Cleanups**.

CSV Format for Cleanup Instances

When you select a cleanup type in the cleanup browser and click **Export**, you are prompted to download a CSV file with the details of the instances of the selected cleanup for all of the selected devices. The filename includes cleanup type, and the date and time of the export. The first few lines of the file include commented text that you can set a parser to ignore.

To properly view the CSV file, open it with a text editor.

The file includes file header, device header and instance sections:

- **File header** - The 3 lines at the beginning of the file that identify the:
  - Version of the export engine - "# version <VERSION NUMBER>"
  - Cleanup type name - "# cleanup type:","<NAME>"
  - Cleanup type code - "# cleanup code:","<CODE>" where the code has one letter and two digits, such as C05
- **Device header** - The 3 lines before the instances from each device that identify the:
  - Device name - "# device:","<DEVICE NAME>"
  - Device vendor name - "# type:","<VENDOR NAME>"
  - Instance format - The format for the instances for the cleanup type and vendor (see below)
- **Instance** - Each rule or object that matches the criteria for the cleanup

For each cleanup type and vendor, the instance format is:

Disabled Rules

Check Point	"POLICY PACKAGE","RULE NUMBER","CHECK POINT UID","RULE NAME","RULE COMMENT"
Cisco	"ACL NAME","ACE COMMENT"
Fortinet	"ZONE2ZONE","RULE NUMBER","RULE UID","RULE NAME","RULE COMMENT"
Juniper	"ZONE2ZONE","POLICY ID","POLICY NAME","POLICY COMMENT"
Palo Alto	"ZONE2ZONE","RULE NUMBER","RULE UID","RULE NAME","RULE COMMENT"

Duplicate Network Objects

The two lines before each set of duplicates are:

All vendors	**Number of duplicates and their matched properties** "DUPLICATE_<OBJECT TYPE>:<NUMBER OF DUPLICATES>","IP:<IP_ADDRESS>","MASK:<NETMASK>","<COMMENT>" For example: "DUPLICATE_NETWORKS:2","IP:1.1.1.0","MASK:255.255.255.0","" * For Juniper devices, the object's zone is added to the end of the instance. **Instance format** "OBJECT TYPE","OBJECT NAME","IP","COMMENT" Where "OBJECT TYPE" is either: Host, Network For example: "Network","LAN","1.1.1.0/255.255.255.0",""

Duplicate Services

The two lines before each set of duplicates are:

All vendors	**Number of duplicates and their matched properties** "DUPLICATE_<OBJECT TYPE>:<NUMBER OF DUPLICATES>","PROTOCOL:<PROTOCOL NUMBER>","Port:<PORT NUMBER>","SrcPort:<PORT NUMBER>","Timeout:<TIMEOUT VALUE>"

	For example: `"DUPLICATE_SERVICES: 4","PROTOCOL: 6","Port: 5060","","Timeout: 0"` **Instance format** `"OBJECT TYPE","OBJECT NAME","IP","COMMENT"` Where `"OBJECT TYPE"` is: Service For example: "Service","sip-tcp","6","5060","Session Initiation Protocol over TCP"

Empty Groups

All vendors	`"OBJECT TYPE","OBJECT NAME",,"COMMENT"` Where `"OBJECT TYPE"` is either: Network group, Service Group For example: "Network group","Group1","","Internal Group"

Fully Shadowed and Redundant Rules

Check Point	`"POLICY PACKAGE","RULE NUMBER","CHECK POINT UID","RULE NAME","RULE COMMENT"`
Cisco	`"ACL NAME","ACE COMMENT"`
Fortinet	`"ZONE2ZONE","RULE NUMBER","RULE UID","RULE NAME","RULE COMMENT"`
Juniper	`"ZONE2ZONE","JUNIPER POLICY ID","RULE NAME","RULE COMMENT"`
Palo Alto	`"ZONE2ZONE","RULE NUMBER","RULE UID","RULE NAME","RULE COMMENT"`

Unattached Objects

All vendors	`"OBJECT TYPE","OBJECT NAME","IP","COMMENT"` Where `"OBJECT TYPE"` is either: Host, Network, Network group For example: "Network","Network_2_IPV6","2001:400:1:1::100/64",""

Unused Objects

All vendors	`"OBJECT TYPE","OBJECT NAME","IP","COMMENT"` Where `"OBJECT TYPE"` is either: Host, Network, Network group For example: "Network","Network_2_IPV6","2001:400:1:1::100/64",""

Cleanup Configuration

SecureTrack comes with a defined set of cleanups. SecureTrack produces the security score and cleanup instances in the cleanup charts and cleanup browser based on the cleanups that are selected in the cleanup configuration.

These cleanups are divided into cleanup types:

- Disabled rules - Rules that never have hits from traffic because they are disabled
- Duplicate network objects - Network objects (including networks, hosts and ranges) are reported as matching when they have the same IP address and netmask (or start and end IP addresses for ranges) and the same zone.

  Groups of network objects are reported as matching when they have the same group members.
- Duplicate services - Services are reported as matching when they are not pre-defined and when they have the same values for:
  - Protocol - TCP or UDP
  - Port - Destination port
  - Source port - If specified in the object's properties
  - Timeout setting - Either session timeout (Check Point) or inactivity timeout (Juniper)
  - Match for Any - Check Point only

    The duplicate service cleanup does not compare source port and timeout in Palo Alto, service timeout in Juniper Netscreen, or protocol type in Check Point.

  Groups of services are reported as matching when they have the same group members and at least one of the group members is not a pre-defined service.
- Empty groups (`C08`) - Group objects that do not have any members

- Fully shadowed and redundant rules (`C01`) - Rules that never have hits from traffic because rules above them in the policy handle the traffic.
    - Shadowed - For rules that are marked as fully shadowed, you can click on **Details** to see the rules that shadow it.
- Unattached network objects (`C06`) - Objects that are not used in any firewall rules, group objects. Objects used in other forms of management, such as NAT rules or VPN connections, may appear as unattached in the security policy. Verify the use of unattached objects across the relevant device management tools.
- Unused network objects (`C15`) - Network objects and network object groups that are not in use across the security policy and have no hits in the policy traffic log during the time period configured. These can be unattached objects, or objects that appear in access rules and object groups but are not being hit within those rules and groups.

  Notes:

    - The unused objects cleanup is disabled by default. When you enable it, you must also select the time period (days, weeks or months) of the usage data. Objects that have no hits during the usage period are listed as unused.
    - Make sure that the cleanup settings in **Settings > Administration** > **Maintenance** are set for a longer period than the usage period for the cleanup.
    - The cleanup is shown only if there are hits for every day in the usage period, such that an object is not shown as unused when there was a connectivity problem that resulted in at least one day without any traffic hits.
    - The cleanup does not include:
        - Objects used in VPN rules
        - Addresses in Cisco configurations that are not associated with defined objects
        - Traffic hits from the current day because the results are calculated nightly
        - Rules that were changed during the period and the objects that are used in the rules
        - Rules without logs
        - IPv6 objects in devices other than Juniper NSM
        - Predefined, implicit and NAT objects

Each cleanup is defined with a name, severity, and description. You can change the name and definition to fit the terminology and structure of your organization. You can also change the severity to indicate how important the cleanup is to your organization.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration** > **Cleanup**.

Removing Cleanups

You can remove a cleanup from the cleanup configuration so that it is not used in optimization score and cleanup calculations.

To remove a cleanup:

1. Go to **Settings > Configuration** > **Cleanup**.
2. Select the cleanup type.
3. Clear the checkbox for a cleanup.
4. Click **Save**.

Editing Cleanups

Each cleanup is defined with a name, severity, and description. You can change the name and definition to fit the terminology and structure of your organization. You can also change the severity to indicate how important the cleanup is to your organization.

To edit a cleanup:

1. Go to **Settings > Configuration**> **Cleanup**.
2. Select the cleanup type.
3. Click on the name of the cleanup.
4. Edit the name, description or severity of the cleanup.
5. Click **Save**.

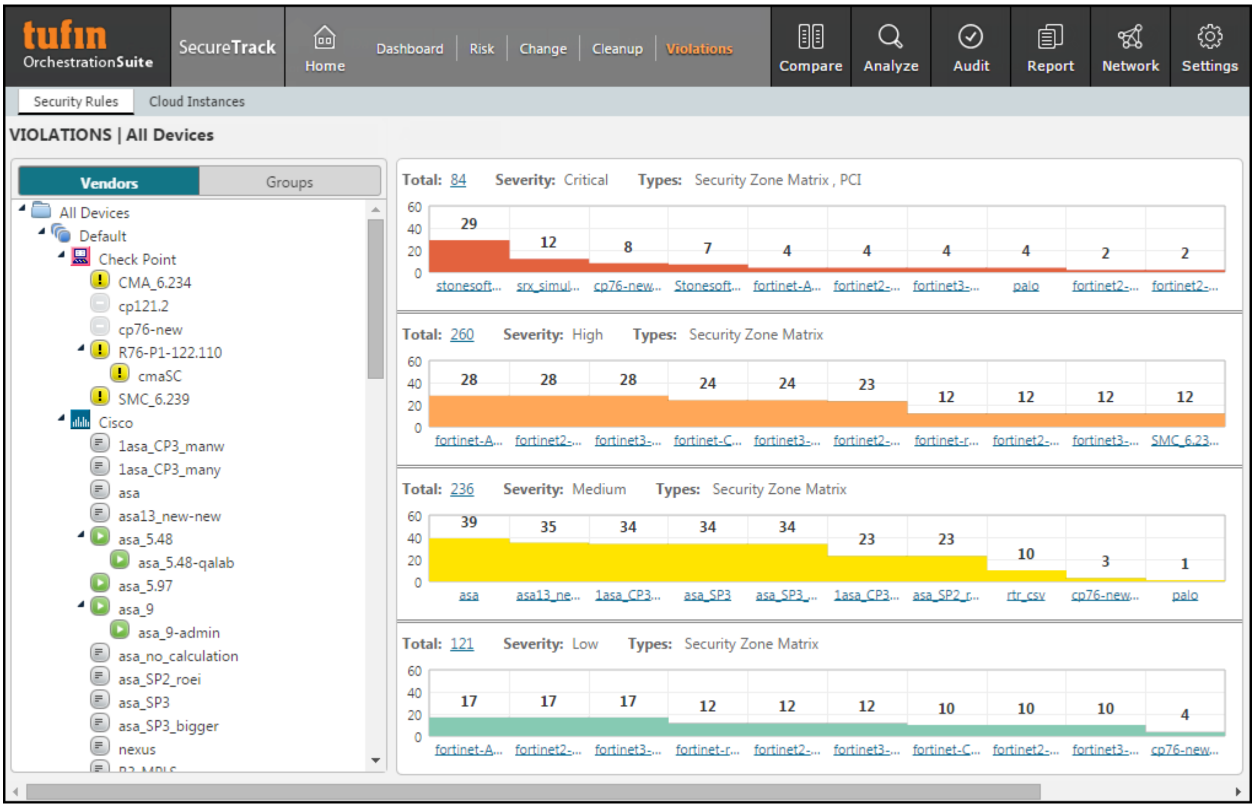
Violations Browser

The Violations browser lets you see at-a-glance the security compliance violations in your network by device.You can drill-down to see the exact rules that cause the violations, as well as suggested ways to remediate the violations.For management platform devices, the violations are shown at the level in the hierarchy in which the violation can be resolved.

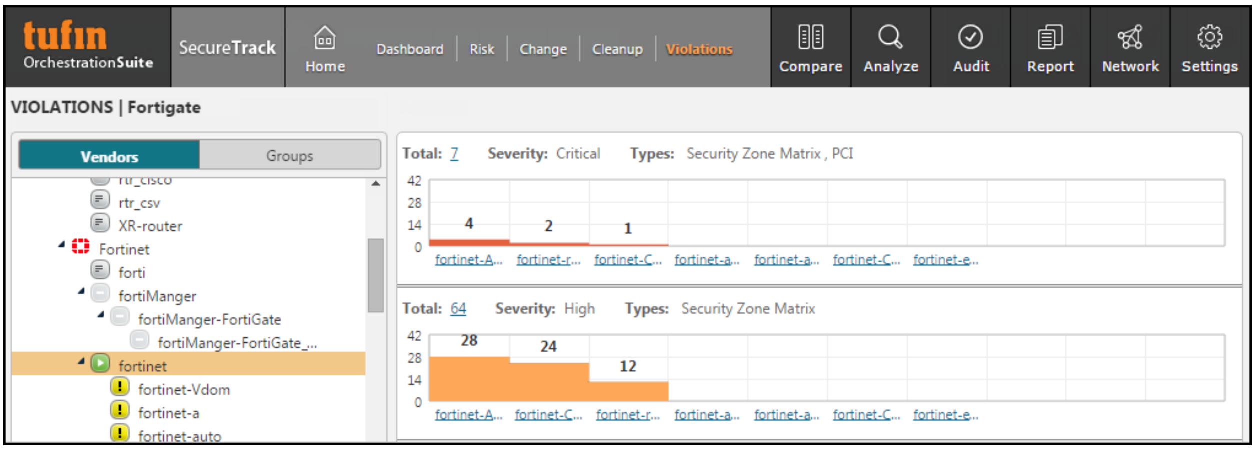
Violations are calculated when the USP or PCI policy is changed, when devices in the USP or PCI policy are changed, or when the Interactive Map is synchronized, either automatically or manually.

SecureTrack uses these compliance requirements to determine the violations:

- Security Rules
  - Security zone matrix requirements configured in **Audit** > **Compliance** > Unified Security Policy
  - PCI DSS policies configured in **Settings** > **Configuration** > Regulations(Only critical violations)
- Cloud Instances
  - Cloud tag policy requirements configured in **Audit** > **Compliance** > Unified Security Policy (Only critical violations)


tufin OrchestrationSuite
SecureTrack
Home
Dashboard
Risk
Change
Cleanup
Violations
Compare
Analyze
Audit
Report
Network
Settings
Security Rules
Cloud Instances
VIOLATIONS | All Devices
Vendors
Groups
All Devices
Default
Check Point
CMA_6.234
cp121.2
cp76-new
R76-P1-122.110
cmaSC
SMC_6.239
Cisco
1asa_CP3_manw
1asa_CP3_many
asa
asa13_new-new
asa_5.48
asa_5.48-qalab
asa_5.97
asa_9
asa_9-admin
asa_no_calculation
asa_SP2_roei
asa_SP3
asa_SP3_bigger
nexus
Total: 84 Severity: Critical Types: Security Zone Matrix , PCI
29 12 8 7 4 4 4 4 2 2
stonesoft... srx_simul... cp76-new... Stonesoft... fortinet-A... fortinet2-... fortinet3-... palo fortinet2-... fortinet2-...
Total: 260 Severity: High Types: Security Zone Matrix
28 28 28 24 24 23 12 12 12 12
fortinet-A... fortinet2-... fortinet3-... fortinet-C... fortinet3-... fortinet2-... fortinet-r... fortinet2-... fortinet3-... SMC_6.23...
Total: 236 Severity: Medium Types: Security Zone Matrix
39 35 34 34 34 23 23 10 3 1
asa asa13_ne... 1asa_CP3... asa_SP3 asa_SP3_... 1asa_CP3... asa_SP2_r... rtr_csv cp76-new... palo
Total: 121 Severity: Low Types: Security Zone Matrix
17 17 17 12 12 12 10 10 10 4
fortinet-A... fortinet2-... fortinet3-... fortinet-r... fortinet2-... fortinet3-... fortinet-C... fortinet2-... fortinet3-... cp76-new...
60 40 20 0

You can select a single device to show the revisions for that device, or you can select a group of devices from the tree to show the recent revisions for all of the devices in the group.


tufin OrchestrationSuite
SecureTrack
Home
Dashboard
Risk
Change
Cleanup
Violations
Compare
Analyze
Audit
Report
Network
Settings
VIOLATIONS | Fortigate
Vendors
Groups
rtr_cisco
rtr_csv
XR-router
Fortinet
forti
fortiManger
fortiManger-FortiGate
fortiManger-FortiGate_...
fortinet
fortinet-Vdom
fortinet-a
fortinet-auto
Total: 7 Severity: Critical Types: Security Zone Matrix , PCI
42 28 14 0
4 2 1
fortinet-A... fortinet-r... fortinet-C... fortinet-a... fortinet-a... fortinet-C... fortinet-e...
Total: 64 Severity: High Types: Security Zone Matrix
28 24 12
fortinet-A... fortinet-C... fortinet-r... fortinet-a... fortinet-a... fortinet-C... fortinet-e...

IPv6 is not supported for this TOS feature.

Note: Security Groups are currently not displayed in the Violations Browser.

What can I do on this page?

- Violations Browser Summary - Click on violations total to view a summary of all violations.
- Violating Rules - Click on the device name or violations bar of a device to view the violating rules of that specific device.

How Do I Get Here?

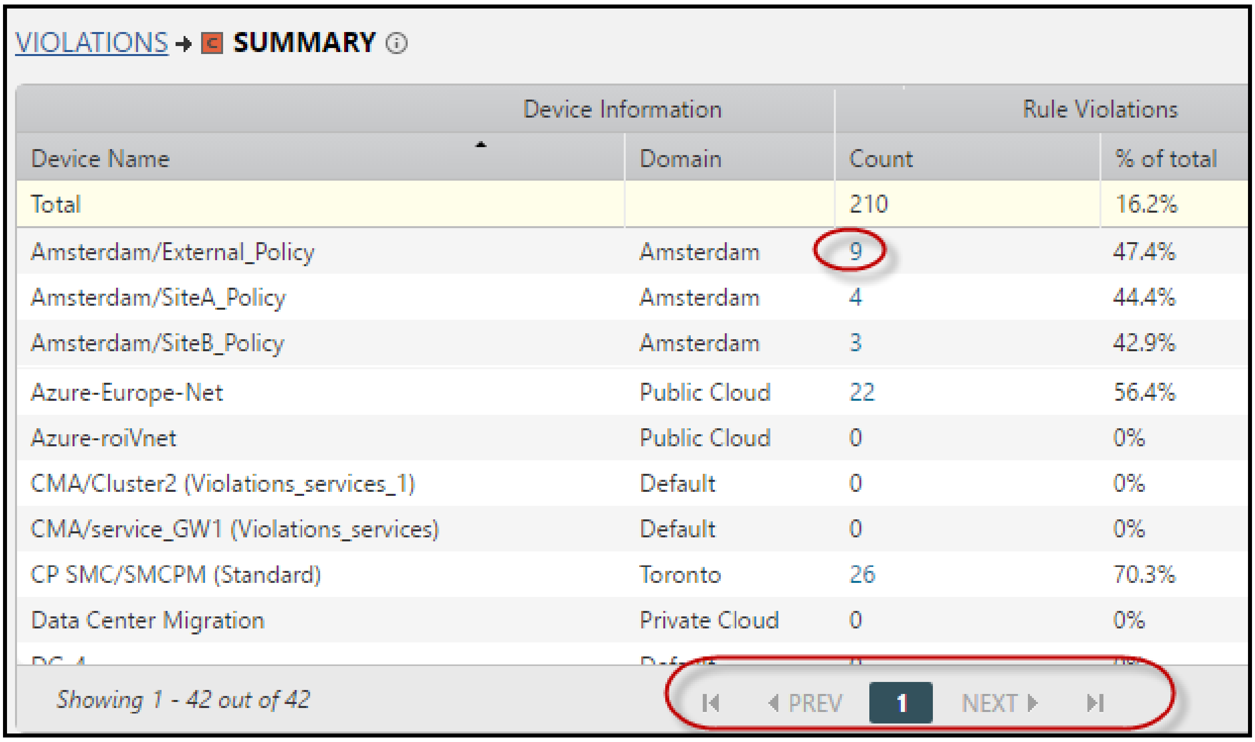
To view the Violations Browser:

1. In SecureTrack, click **Home** > **Violations**.

Violations Browser Summary

The Violations browser summary lets you see a summary of all security compliance violations in your network. For any device listed, you can drill-down to see the exact rules that cause the the violations and suggested ways to remediate the violations.

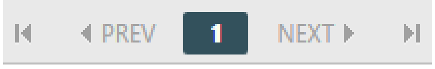
For each device, review the number of violations in the device, the device domain, the rule violation count, and the percentage of the total number of rules that contain violations.



VIOLATIONS → SUMMARY

Device Information		Rule Violations	
Device Name	Domain	Count	% of total
Total		210	16.2%
Amsterdam/External_Policy	Amsterdam	9	47.4%
Amsterdam/SiteA_Policy	Amsterdam	4	44.4%
Amsterdam/SiteB_Policy	Amsterdam	3	42.9%
Azure-Europe-Net	Public Cloud	22	56.4%
Azure-roiVnet	Public Cloud	0	0%
CMA/Cluster2 (Violations_services_1)	Default	0	0%
CMA/service_GW1 (Violations_services)	Default	0	0%
CP SMC/SMCPM (Standard)	Toronto	26	70.3%
Data Center Migration	Private Cloud	0	0%
DC 4	Default	0	0%

Showing 1 - 42 out of 42

Use the navigation controls  to view additional pages in the summary, as needed.

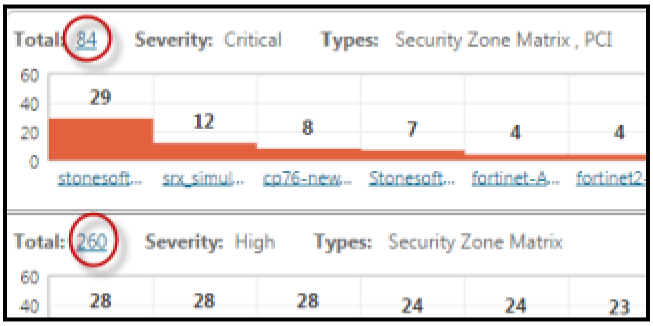
What can I do on this page?

- View Violating Rules - Click a number in the count column to show the violating rules for the specified device.

How Do I Get Here?

To view the Violations Browser Summary:

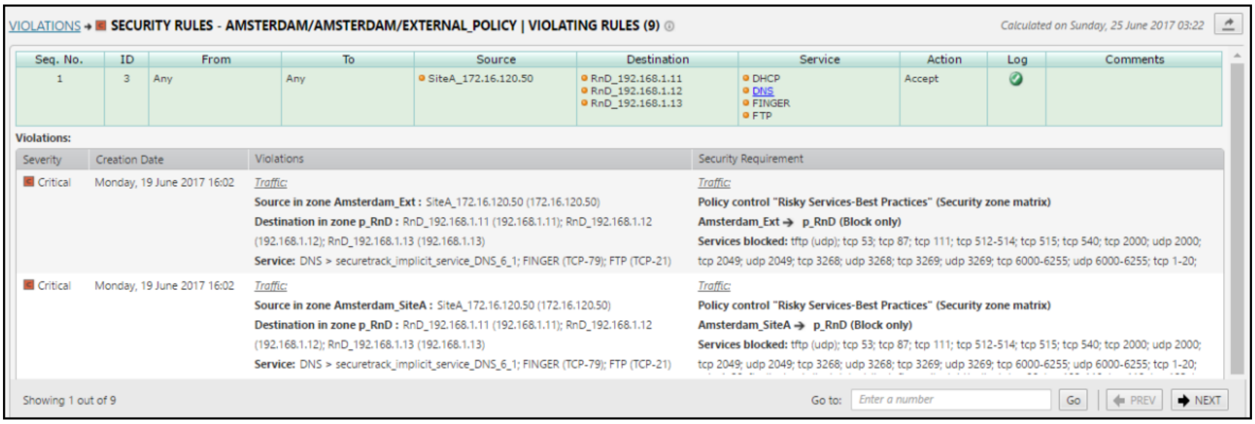
1. Navigate to the Violations Browser.
2. Click on the violations total.



The violations for the selected group of devices are shown.

Violating Rules

Violating Rules shows all of the violations that apply to a specified rule. The violations are shown along with the severity, the creation date of the violation, the security requirement that causes the violation, and the recommended action to mitigate the violation where available.



VIOLATIONS → SECURITY RULES - AMSTERDAM/AMSTERDAM/EXTERNAL_POLICY | VIOLATING RULES (9)

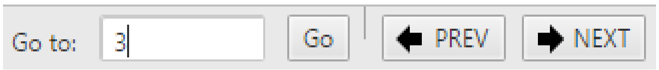
Calculated on Sunday, 25 June 2017 03:22

Seq. No.	ID	From	To	Source	Destination	Service	Action	Log	Comments
1	3	Any	Any	SiteA_172.16.120.50	RnD_192.168.1.11 RnD_192.168.1.12 RnD_192.168.1.13	DHCP DNS FINGER FTP	Accept	✓	

Violations:

Severity	Creation Date	Violations	Security Requirement
Critical	Monday, 19 June 2017 16:02	*Traffic:* **Source in zone Amsterdam_Ext :** SiteA_172.16.120.50 (172.16.120.50) **Destination in zone p_RnD :** RnD_192.168.1.11 (192.168.1.11); RnD_192.168.1.12 (192.168.1.12); RnD_192.168.1.13 (192.168.1.13) **Service:** DNS > securetrack_implicit_service_DNS_6_1; FINGER (TCP-79); FTP (TCP-21)	*Traffic:* **Policy control "Risky Services-Best Practices" (Security zone matrix)** **Amsterdam_Ext → p_RnD (Block only)** **Services blocked:** tftp (udp); tcp 53; tcp 87; tcp 111; tcp 512-514; tcp 515; tcp 540; tcp 2000; udp 2000; tcp 2049; udp 2049; tcp 3268; udp 3268; tcp 3269; udp 3269; tcp 6000-6255; udp 6000-6255; tcp 1-20;
Critical	Monday, 19 June 2017 16:02	*Traffic:* **Source in zone Amsterdam_SiteA :** SiteA_172.16.120.50 (172.16.120.50) **Destination in zone p_RnD :** RnD_192.168.1.11 (192.168.1.11); RnD_192.168.1.12 (192.168.1.12); RnD_192.168.1.13 (192.168.1.13) **Service:** DNS > securetrack_implicit_service_DNS_6_1; FINGER (TCP-79); FTP (TCP-21)	*Traffic:* **Policy control "Risky Services-Best Practices" (Security zone matrix)** **Amsterdam_SiteA → p_RnD (Block only)** **Services blocked:** tftp (udp); tcp 53; tcp 87; tcp 111; tcp 512-514; tcp 515; tcp 540; tcp 2000; udp 2000; tcp 2049; udp 2049; tcp 3268; udp 3268; tcp 3269; udp 3269; tcp 6000-6255; udp 6000-6255; tcp 1-20;

Showing 1 out of 9

Use the navigation controls  to review the rules one at a time with all of the violations that apply to the rule.

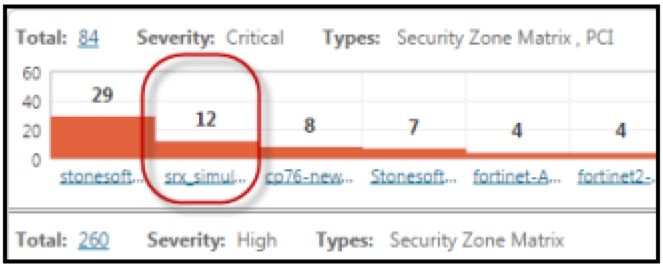
What can I do on this page?

- Export violating rules - Click to create a report of violating rules that is saved in the report repository.

How Do I Get Here?

To view the violations browser summary:

1. Go to the Violations Browser.
2. Click on total number of rules with violations.



NavigateTo Violations Browser

To view the Violations Browser:

1. In SecureTrack, click **Home** > **Violations**.

Policy Browser

SecureTrack can include editable details about policy rules so you can manage rule ownership, expiration and recertification. You can use this information for reporting on documentation and ownership management of security, such as for periodic recertification projects and network security audits, including PCI-DSS.

When new policy revisions are received, they undergo multiple processing steps. New policy revisions appear in the Policy Browser search results after TOS processing is completed.

You can save policy details, or metadata, in SecureTrack for each rule in the most recent policy revision for each device. In the **Compare** tab, the 📝 icon next to a rule indicates that the rule has documentation details.

The rule metadata includes the information categories listed below.

Rule Statistics

Rule statistics includes the following information:

- Permissiveness level (high/medium/low) – An indication of how widely a rule is defined, for example:
    - A rule with one source host, one destination host and one service is low permissiveness
    - A rule with Source "ANY", Destination "ANY" and Protocol "ANY" is high permissiveness

  Rules with high permissiveness can be a security risk because they allow too much access through the firewall. N/A indicates that the platform is not supported for permissiveness calculations.
- Violations - The number of PCI DSS and Unified Security Policy violations caused by the rule
- Last Hit - The last time traffic that passed through the device matched either the rule, user, or application identities details
- Last Modified - The last time a revision showed that the source, destination or service changed in the rule, including changes group members.

  After you upgrade to R16-4 or higher, SecureTrack analyzes the revisions to identify the last time any part of the rule was changed, for example source, destination, service, log, or comment. Rules are labeled with the last modified date of yesterday, 3 months ago, 6 months ago, 12 months ago, or longer, whichever is the most recent change. This process can take up to a few days to complete.
- Shadowing Status - For rules that are marked as fully shadowed, you can click on **Details** to see the rules that shadow it.

Metadata per rule

The metadata per rule includes the following information:

- Technical owner - One of the SecureTrack admin users: Typically, the firewall administrator who is responsible for the technical accuracy of the rule.
- Rule description - A useful description stored in SecureTrack
- Advanced options:
    - Legacy rule - When a rule is marked as legacy, SecureChange Designer will treat a rule marked as legacy as a shadowed rule when making recommendations, and SecureChange Verifier will ignore a rule marked as legacy when verifying access.

      Marking rules as legacy can be used to let you methodically replace overly permissive rules over a period of time. Only rules that have an Allow action will be considered by Designer as legacy.

      When the traffic in an access request is fully or partially implemented by traffic that is handled by legacy rules, Designer locates the recommended rules above the related legacy rule with the highest position in the policy.
    - Stealth rule – When a rule as is marked as stealth, SecureChange Designer recommendations will place any new rules recommended for an access request below the stealth section of the policy. Only rules that have a Deny action will be considered by Designer as stealth.

      The stealth section is comprised of all rules above and including the last rule marked as stealth in the device policy and is therefore always the top section in the device policy. Stealth rules can be used to protect a firewall device from attack by denying unwanted access to specific firewalls.

  For devices that support hierarchical structures and management of grouped entities, Policy Browser does not display propagated Legacy or Stealth Rules for the devices that are lower in the hierarchy.

  To determine whether a device that is lower in the hierarchy includes a Legacy or Stealth Rule propagated from higher up, SecureTrack users should search for the level at which the Legacy or Stealth Rule was defined. The level of each rule is displayed in the Policy Browser, in the Rule Location column.

Designer takes the propagated Legacy or Stealth Rules into account for the managed devices that are lower in the hierarchy when suggesting changes and when provisioning. With Legacy rules, Designer will not create new rules on lower level entities that intersect with the legacy rule.

Record sets for each workflow ticket associated with the rule

This category includes the following information:

- Ticket ID - Entered manually or matched automatically with SecureChange authorized tickets that allow new traffic.

  For tickets marked as **SecureChange Ticket ID**, the **Ticket ID** column is populated when a change triggers a revision on a rule. Rules are mapped to a ticket when active rules intersect with another ticket’s traffic, whether or not a policy change has occurred within an Access Request.

  In Policy Browser, click on the ticket ID to go to the SecureChange ticket in Tasks (Requires permission to view the ticket). In the rule documentation report, you can see the expiration date of the ticket, if one is configured.

- Business owner name and email - The user who opens the ticket

  Assigned automatically

- Expiration date - Entered manually or matched automatically with SecureChange ticket expiration

SecureApp Connection Details

This category includes the application details for SecureApp application connections that match firewall rules:

- Application name
- Application owner

This information is automatically updated when new revisions are retrieved, when a connection change is saved in SecureApp or when there is a change in the Topology.

Also, rules marked with application information are selected based on the potential traffic for each device in the path as defined in the rule, and not based on the effective traffic that passes through the device which may be blocked by another device or changed by NAT rules before reaching the device.

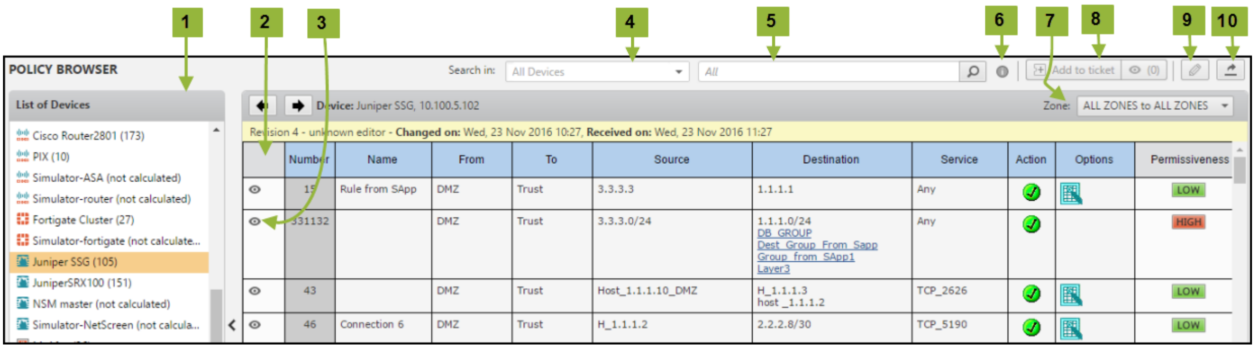
To help you manage, track, and recertify ownership and expiration, you can:

- View and export the details
- Search for matching rules
- Edit the details

  When rules are results of SecureChange Access Requests, you can also manage expiration and recertification using the ticket expiration date in SecureChange.

Viewing Policy Browser

When you click on Policy Browser you can either click on 🔍 to search for all rules or enter search parameters to return rules that meet your search criteria. The results show the list of devices with the number of matching rules and all of the rules that match the search criteria. When you select a device from the list of devices, you can see the graphical view of the last revision retrieved from the devices listing all the rules that match the search criteria.



List of Devices

- Cisco Router2801 (173)
- PIX (10)
- Simulator-ASA (not calculated)
- Simulator-router (not calculated)
- Fortigate Cluster (27)
- Simulator-fortigate (not calculate...
- Juniper SSG (105)
- JuniperSRX100 (151)
- NSM master (not calculated)
- Simulator-NetScreen (not calcula...

Device: Juniper SSG, 10.100.5.102

Revision 4 - unknown editor - **Changed on:** Wed, 23 Nov 2016 10:27, **Received on:** Wed, 23 Nov 2016 11:27

	Number	Name	From	To	Source	Destination	Service	Action	Options	Permissiveness
👁	15	Rule from SApp	DMZ	Trust	3.3.3.3	1.1.1.1	Any	✓	▦	LOW
👁	331132		DMZ	Trust	3.3.3.0/24	1.1.1.0/24 DB_GROUP Dest_Group_From_Sapp Group_from_SApp1 Layer3	Any	✓		HIGH
👁	43		DMZ	Trust	Host_1.1.1.10_DMZ	H_1.1.1.3 host _1.1.1.2	TCP_2626	✓	▦	LOW
👁	46	Connection 6	DMZ	Trust	H_1.1.1.2	2.2.2.8/30	TCP_5190	✓	▦	LOW

What can I do on this page?

1. **View Devices** - Displays a listing of all the devices that have policies that contain rules that match the search criteria, and the number of matching rules. Rule that have an open ticket will display the ticket icon 🎫. Click on the icon to view the ticket in SecureChange.

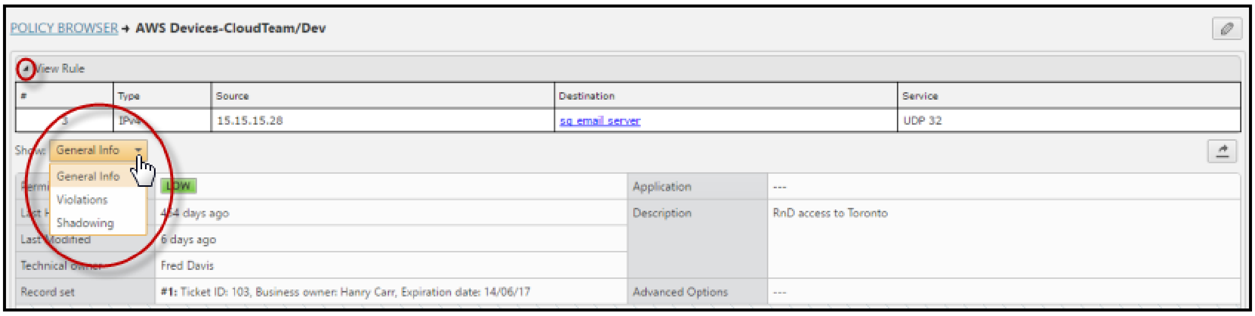
2. **View Policy and Documentation** - Displays the policy rules and their metadata of the last revision of the selected device. Above the rules you can see the date the policy was changed on the device and the date that the policy was received by SecureTrack.
3. **View Rule Details** (👁) - View additional information about a rule, including:
   - The last time the specified rule was hit
   - The last time the source destination or service of the specified rule was edited, including group members
   - The violations caused by the specified rule
   - The rules that shadow the specified rule
4. **Search by Device** - Select a device from the list or enter the name of a device.
5. **Search by Field Contents** - Search in the metadata and rule fields by specified search criteria.
6. **View Syntax for Search Criteria** (ℹ) - Review the syntax to use in the search bar.
7. **Filter** - Filter the items displayed by the device-specific category, for example Security Group, Interface, Zone.
8. **Rule Decommission** - Select rules and click [+ Add to ticket | 👁 (3)] to decommission rules. See Decommission Rules.
9. **Edit Metadata** (✎) - Edit the rule details for the rule that you select.
10. **Export Results** (⇪) - Export the Policy Browser data shown to a CSV or PDF file that is downloaded to your local computer.

How Do I Get Here?

To view the Policy Browser:

1. In SecureTrack, click **Home** > **Policy Browser**.

Viewing General, Violation and Shadowing Information



POLICY BROWSER → **AWS Devices-CloudTeam/Dev**

View Rule

#	Type	Source	Destination	Service
3	IPv4	15.15.15.28	sg email server	UDP 32

Show: General Info

Permi	LOW	Application	---
Last H	454 days ago	Description	RnD access to Toronto
Last Modified	6 days ago		
Technical owner	Fred Davis		
Record set	#1: Ticket ID: 103, Business owner: Hanry Carr, Expiration date: 14/06/17	Advanced Options	---

When you click on the rule details (👁) for a rule in Policy Browser you can see a more detailed view of any rule. The rule is shown at the top of the page.

Below the rule is a menu that shows the following three groups of information you can view:

- **General** - In this section you can see:
  - Permissiveness level (high/medium/low) - An indication of how widely a rule is defined, for example:
    - A rule with one source host, one destination host and one service is low permissiveness
    - A rule with Source "ANY", Destination "ANY" and Protocol "ANY" is high permissiveness

    Rules with high permissiveness can be a security risk because they allow too much access through the firewall. N/A indicates that the platform is not supported for permissiveness calculations.
  - Last hit for rule - How many days ago the device received traffic that matched the rule
    - Policies need to have unique names. If there are multiple policies that share the same name, rule hits will not be mapped correctly to these policies.
  - Last hit for users (Palo Alto only) - How many days ago the device received traffic that matched a user that is specified in the rule
  - Last hit for application identities (Palo Alto only) - How many days ago the device received traffic that matched an application identity that is specified in the rule
  - Last Modified - The last time a revision showed that the source, destination or service changed in the rule, including changes group members

    After you upgrade to R16-4 or higher, SecureTrack analyzes the revisions to identify the last time any part of the rule was changed, for example source, destination, service, log, or comment. Rules are labeled with the last modified date of yesterday, 3 months ago, 6 months ago, 12 months ago, or longer, whichever is the most recent change. This process can take up to a few days to complete.

  - Technical owner - Typically, the firewall administrator who is responsible for the technical accuracy of the rule
  - Record sets - The business details of the rule including the business owner (person responsible for the business needs for the rule), email address of the business owner, ticket IDs associated with the rule, the expiration date when the business need for the rule is no longer valid
  - Application - The application in SecureApp that is associated with the rule

    If the rule is IPv4 only, it is associated with an application when the topology of the SecureApp connection matches the rule. If the rule uses IPv6 addresses, it is associated with an application when the target selected for the SecureChange ticket created from the connection matches the rule.

  - Rule description - The description of the rule entered into Policy Browser

- **Violations** - In this section you can see the violations caused by the rule as they are shown in the Violations browser:
  - Severity - The level of severity of the violation as defined by the severity of the security requirement
  - Creation Date - The date and time the violation first occurred
  - Violations - The traffic allowed by the rule that violates the security requirement
  - Security Requirement - The requirement that governs the traffic allowed by the rule
- **Shadowing** - In this section you can see any rules that shadow the selected rule

What can I do on this page?

- **Hide the rule** - Click ◢ to hide the rule details, which gives more space for the additional information thta may be available.
- **Export** - Click ⇪ to export the details of each group to a supported format, such as PDF or CSV.
- **Edit the Metadata** - Click ✎ to edit the metadata for this rule.

How Do I Get Here?

To view the additional information about a specific policy:

1. In SecureTrack, click **Home** > **Policy Browser**.
2. Click 👁 on the desired rule.

Searching in Policy Browser

Overview

Policy Browser lets you search for rules in the device policies according to device and according to policy and policy documentation metadata. You can then view the results and edit the metadata. You can export the results to a PDF or schedule a report of rules in the Rule Documentation Report.

The search applies to the display of rules for all matching devices, so that when you select a different device you only see the rules that match the filter.

Searches in the source and destination fields will return all rules that contain the specified host within contained groups and subnets. For example, searching in the source field for the host 1.1.1.1 will return all rules that have the following the source field:

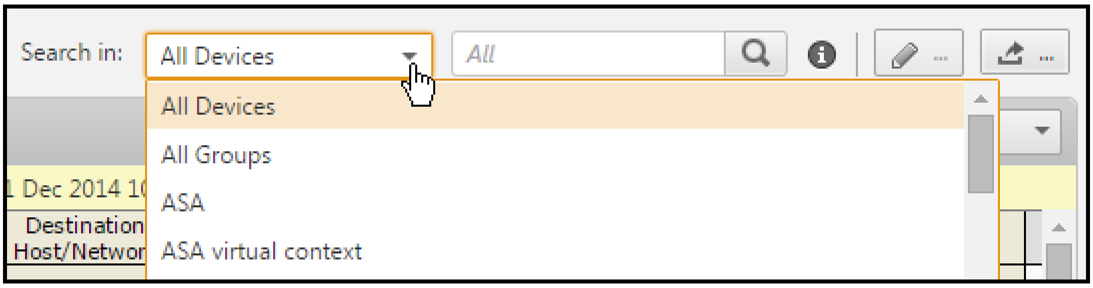
- 1.1.1.1
- 1.1.1.0/24
- ANY
- a group that contains either 1.1.1.1, 1.1.1.0/24, or ANY

Note the following search limitations:

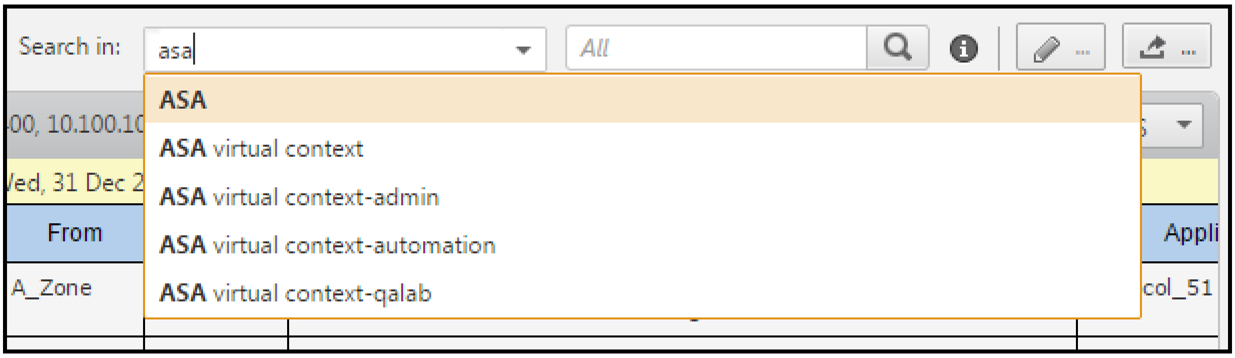
- IPv6 objects are shown for all devices; use the text search to find IPv6 addresses in the source and destination (IPv6 is not supported for F5)
- If a search match includes an IP address, and the same address is negated in a separate rule, the search results will include the IP address.
- You cannot search for non-continuous IP addresses

Defining a search

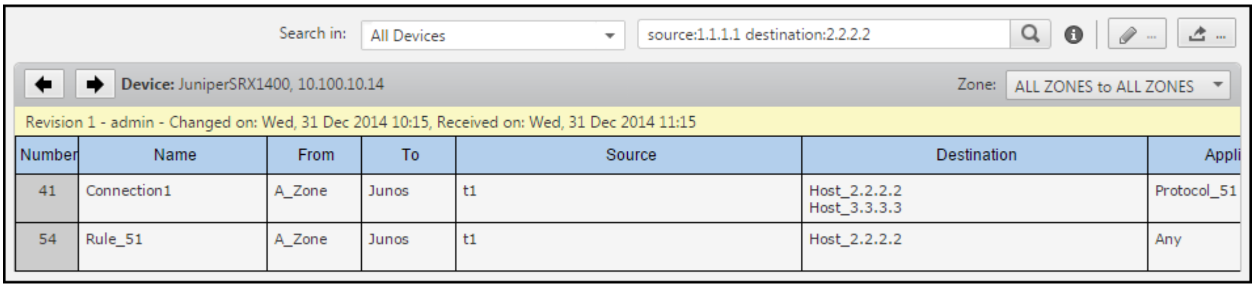
1. Select the devices to search in with:
   - Select from dropdown list - Click on the down arrow of the search box to see all available devices, and select the device to search in.



   - Enter text of a device name - You can enter text in the device field to filter the list of devices and select a device.



2. Enter the search criteria that defines the rules to show.



source:1.1.1.1 destination:2.2.2.2

Device: JuniperSRX1400, 10.100.10.14

Revision 1 - admin - Changed on: Wed, 31 Dec 2014 10:15, Received on: Wed, 31 Dec 2014 11:15

Number	Name	From	To	Source	Destination	Appli
41	Connection1	A_Zone	Junos	t1	Host_2.2.2.2 Host_3.3.3.3	Protocol_51
54	Rule_51	A_Zone	Junos	t1	Host_2.2.2.2	Any

Enter one or more words to search for in rule or metadata details:

- `text1 text2` - Returns rules where text1 is found in the rule or metadata fields and text2 is found in the rule or metadata fields. (Not case-sensitive)
- `" "` - Returns rules with the exact phrase in one of the rule or metadata fields, for example, `"web server"`
- `<fieldname>:<text>` - Returns rules with the text in the specified field, for example: `source: 192.168.1.1`

  The rule field names are: name, rulenumber, source, destination, log, service, action (reject, deny, drop, refuse, discard; or allow, accept, permit), comment/description, fromzone, tozone, application, user, priority

  For Cisco ACI, the name field returns Contracts, the source and destination field returns Consumers or Providers, and the service field returns Filters.

  For Palo Alto, the following additional rule field names are available: tags, profile. For Palo Alto Panorama, the tags field also returns rules that contain Dynamic Groups based on Panorama tags in the match criteria.

  The metadata field names are: violations, technicalowner, ticketid, businessowner, expirationdate (requires the format: YYYYMMDD), businessowneremail, applicationname, applicationowner, ruledescription, advancedoptions, certificationstatus, certificationdate, certificationexpirationdate

  If you specify more than one field in the search, only rules with both field values are shown.

- `<fieldname>.isempty:<true/false>` Returns all rules where the specified <fieldname> is empty (true) or filled (false), for example: comment.isempty:true

  Supported fields are: advancedoptions, applicationname, applicationowner, businessowner, businessowneremail, comment, expirationdate, log, profile, ruledescription, tags, technicalowner, ticketid, violations, certificationdate, certificationexpirationdate, and certificationstatus
- `service:<text>` - Returns rules with either the name of a service or the protocol/port number of a predefined service
- `protocol:<number>` - Returns rules with the specified protocol number (0-255) in the rule service
- `port:<number>` - Returns rules with the specified port number (0-65535) in the rule service
- `Rule.isdisabled:<true/false>` - Returns all rules that are disabled (true) or are enabled (false)
- `rulelocation:<text>` - Returns rules where the rule location field matches (for example, `rulelocation:“mydevice”`) or contains the specified text (for example, `rulelocation:mydevice`)
- `shadowed:<true/false>` - Returns rules that are shadowed (true) or are not shadowed (false), for example: `shadowed:true`
- `lasthitgreater:<number>` - Returns rules with last hit greater than the specified (non-negative) number of days before the current day
- `lastmodifiedgreater:<number>` - Returns rules with last modification date greater than the specified (non-negative) number of days before the current day
- `applasthitgreater:<number>` - Returns rules where the last hit for an application is greater than the specified number of days before the current day (Click on the rule to see usage information)
- `userlasthitgreater:<number>` - Returns rules where the last hit for a user is greater than the specified number of days before the current day (Click on the rule to see usage information)
- `violationcreationdategreater:<date>` - Returns rules where the violation creation date is after than the date specified, required format: YYYYMMDD (Click on the rule to see usage information)
- `certificationstatus:<certified/decertified>` - Returns all rules where the specified certification status is certified or decertified, for example, `certificationstatus:certified`
- `certificationstatus.isempty:<true/false>` - Returns all rules where the specified certification status is empty (true) or filled (false), for example, `certificationstatus.isempty:true`
- `certificationdate:<date>` - Returns rules where the certification date is before the specified date, required format: YYYYMMDD
- `certificationdate.isempty:<true/false>` - Returns all rules where the specified certification date is empty (true) or filled (false), for example, `certificationdate.isempty:true`
- `certificationexpirationdate:<date>` - Returns rules where the certification expiration date is before the specified date, required format: YYYYMMDD
- `certificationexpirationdate.isempty:<true/false>` - Returns all rules where the specified certification expiration date is empty (true) or filled (false), for example, `certificationexpirationdate.isempty:true`
- tags:<text> - Returns all rules that contain the specified text as part of the tag (Not case-sensitive)
- `profile.<profiletype>:<text>` - Returns all rules that specify a profile of type <profile type> which contains the specified text in its name (Not case-sensitive)

  Recognized profile types for <profiletype> are: antivirus, antispyware, vulnerabilityprotection, urlfiltering, datafiltering, fileblocking, wildfireanalysis, securitygroup, logforwarding

  Note: If a Security Profile Group contains a profile of type <profiletype> which contains the specified text in its name, then rules containing the Security Profile Group will also be returned.
- `permissiveness.level:<high/medium/low>` - Returns rules with the specified permissiveness level indicating how much traffic is allowed by the rule.
- `inprogressticketid:<number>` - Returns all rules that have a ticket in progress (for actions such as Rule Decommission) matching the specified ticket ID, for example, `nprogressticketid:769`

Recertifying Rules

SecureTrack lets you select rules that you want to recertify from the Policy Browser and add them to a ticket to create a SecureChange rule recertification request that includes the selected rules.

Add to ticket

may be disabled for the following reasons: the selected device is not licensed in SecureChange or is excluded from SecureChange; there is no SecureChange user with the same username as the SecureTrack user; you do not have access to the domain in SecureChange; or SecureChange is not installed.

Rule recertification is used to document and verify the need for a rule, often for standards compliance and auditing. In a typical recertification process, the security system administrator reviews rules periodically and certifies rules that are required and have a business justification, and decertifies rules that are obsolete.

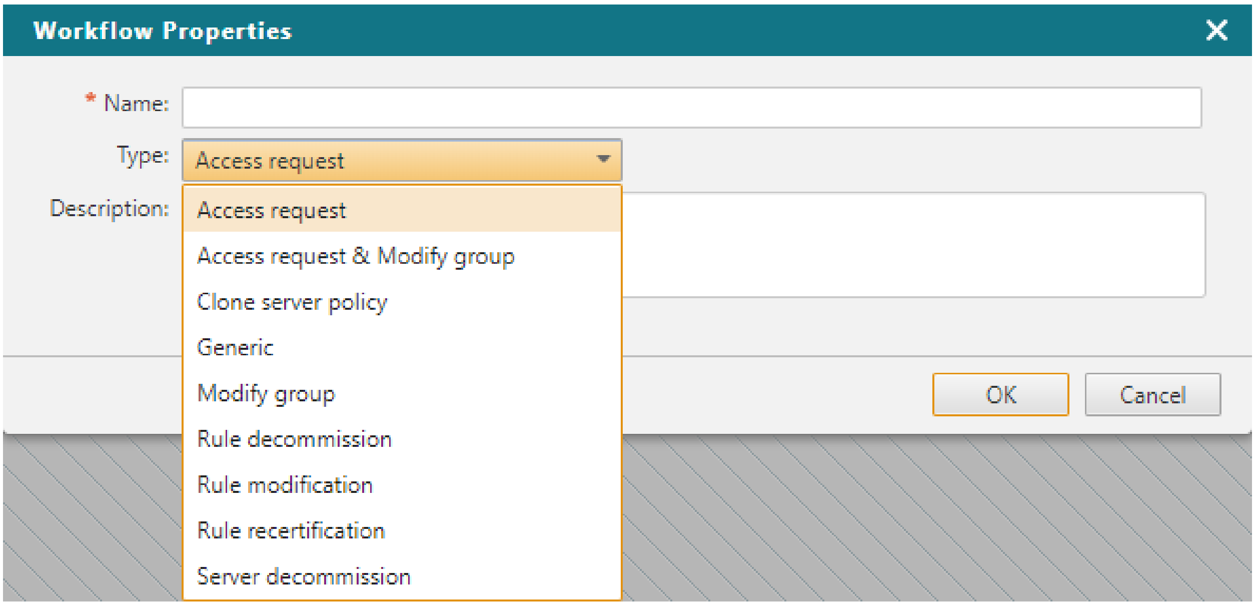
Rules that are active in another ticket (identified with the ticket icon in the Policy Browser) cannot be added to the ticket rules list. Each ticket must include rules from a single device only. To work with rules for multiple devices, create a separate ticket request for each device. Rule recertification is not supported for shared or global rules.

For supported devices, the following Policy Browser metadata fields are populated by rule recertification in SecureChange when you run the Update metadata tool in the SecureChange ticket:

- **Certification Status** - The status of the rule (certify, decertify, or blank)
- **Certification Date** - The date that the certification decision was implemented
- **Certification ExpirationDate** - The date the rule certification expires, after which, it must be reviewed and recertified

Prerequisites

- The SecureChange administrator must create a new workflow in SecureChange using the Rule Recertification field.



Workflow Properties

* Name:

Type: Access request

Description:

- The user must exist with the same username in both SecureTrack and SecureChange.
- The user must have **Create change requests and view 'My Requests' tab** permission in SecureChange. This permission is enabled by default for the Requester role.

How do I create a Rule Recertification ticket request?

1. In **Policy Browser**, search for, and select the desired rules.

   Use the <CTRL> and <SHIFT> keys while clicking to select the multiple rules.

2. Click Add to ticket (9) to add the selected rules to the ticket's list of rules.

   This button is disabled if no rules are selected.

3. Click Add to ticket (9) to review the selected rules.

   The **Selected Rules** window is displayed.

4. Review the selected rules and select or fill in the required fields (**Action**, **Ticket Name**, **Select WorkFlow**).
5. Select and remove rules that you do not want to include in the ticket request.
6. Click Continue > to launch SecureChange and to submit the ticket request using the selected workflow and the list of rules.

   The SecureChange ticket request appears in the **My Requests** window, using the workflow and rules that you selected.

   Once you submit the ticket, the list of selected rules in SecureTrack is cleared.

7. Review the ticket request in SecureChange, and click Submit.

How Do I Get Here?

To view the Policy Browser:

- In SecureTrack, click **Home** > **Policy Browser**.

Decommissioning Rules

SecureTrack lets you select rules that you want to decommission from the Policy Browser, and then create a SecureChange rule decommission request that includes the selected rules. You can either disable or remove the selected rules.

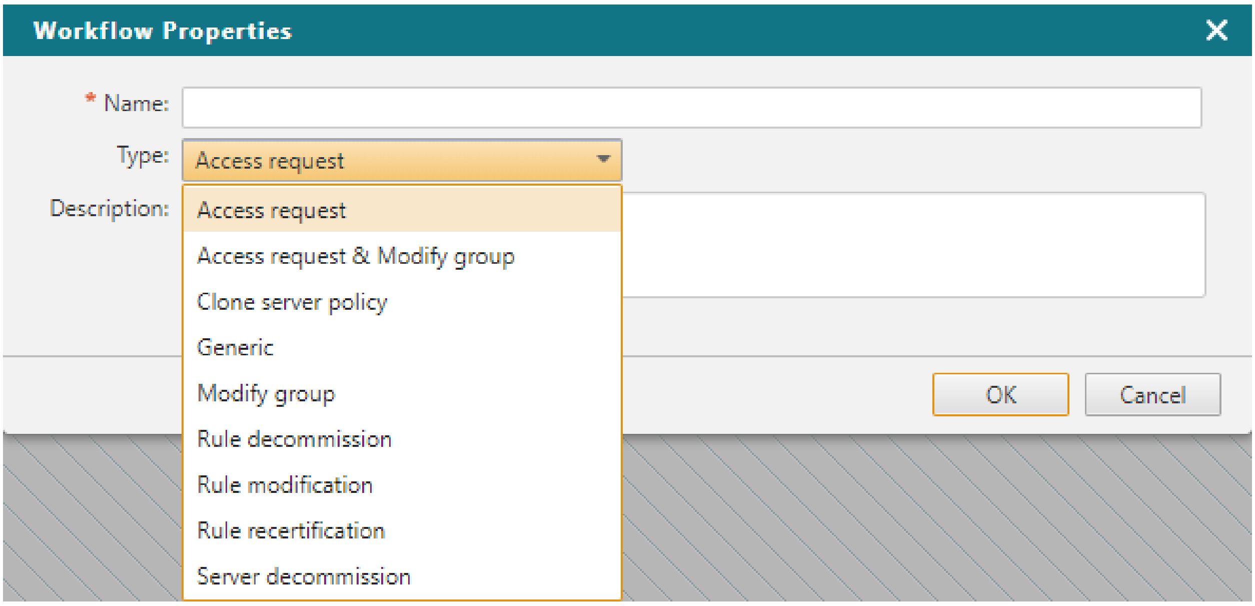
Rules that are active in another ticket (identified with the ticket icon 🎫 in the Policy Browser) cannot be added to the ticket rules list. Each ticket must include rules from a single device only. To work with rules for multiple devices, create a separate ticket request for each device.

For supported devices, you can run SecureChange Designer and Verifier to provision the changes. If you configure revision authorization, you can see the changes in the authorized revisions in the Change browser. You cannot decommission shared or global rules.

Add to ticket ⊞ Add to ticket 👁 (3) is disabled if: the selected device is not licensed in SecureChange or is excluded from SecureChange; if there is no SecureChange user with the same username as the SecureTrack user; if you do not have access to the domain in SecureChange; or if SecureChange is not installed.

Prerequisites

- The SecureChange administrator must create a new workflow in SecureChange using the Rule Decommission field.



Workflow Properties

* Name:

Type: Access request

Description:

The workflow takes the **Disable rules** or **Remove rules** action from the **Rule decommission** request in SecureTrack.

- The user must exist with the same username in both SecureTrack and SecureChange.
- The user must have **Create change requests and view 'My Requests' tab** permission in SecureChange. This permission is enabled by default for the Requester role.

How do I create a Rule Decommission ticket request?

1. In **Policy Browser**, search for, and select the desired rules.

   Use the <CTRL> and <SHIFT> keys while clicking to select the multiple rules.

2. Click ⊞ Add to ticket 👁 (9) to add the selected rules to the ticket's list of rules.

   This button is disabled if no rules are selected.

3. Click ⊞ Add to ticket 👁 (9) to review the selected rules.

   The **Selected Rules** window is displayed.

4. Review the selected rules and select or fill in the required fields (**Action**, **Ticket Name**, **Select WorkFlow**).
5. Select and remove rules that you do not want to include in the ticket request.

6. Click [Continue >] to launch SecureChange and to submit the ticket request using the selected workflow and the list of rules.

   The SecureChange ticket request appears in the **My Requests** window, using the workflow and rules that you selected.

   Once you submit the ticket, the list of selected rules in SecureTrack is cleared.

7. Review the ticket request in SecureChange, and click [Submit].

How Do I Get Here?

To view the Policy Browser:

- In SecureTrack, click **Home** > **Policy Browser**.

Modifying Rules

SecureTrack lets you select rules that you want to modify from the Policy Browser, and then create a SecureChange rule modification request that includes the selected rules. You can add or clear network objects or services within the selected rules.

Rules that are active in another ticket (identified with the ticket icon in the Policy Browser) cannot be added to the ticket rules list. Each ticket must include rules from a single device only. To work with rules for multiple devices, create a separate ticket request for each device.

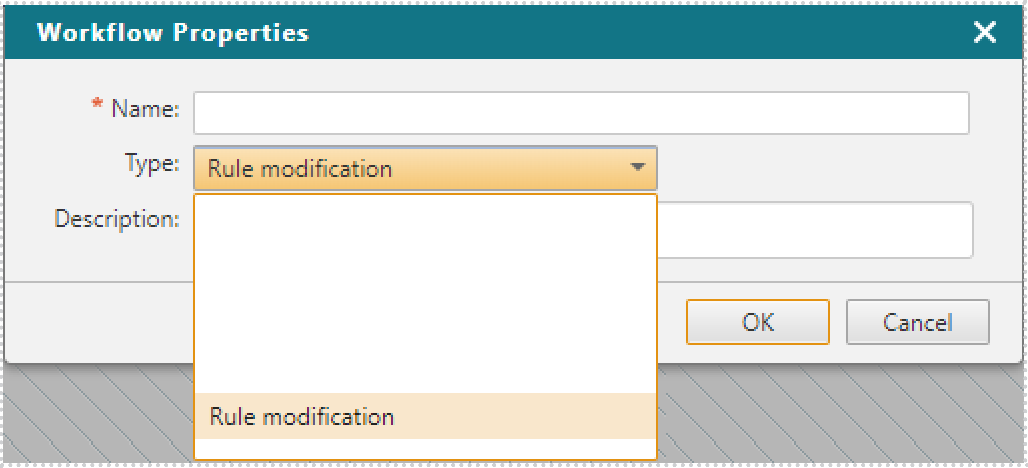
For supported devices, you can run SecureChange Designer to provision the changes.

Add to ticket [Add to ticket | (3)] is disabled if:

- There is no SecureChange user with the same username as the SecureTrack user.
- When the user does not have permission to request SecureChange tickets or when there is no relevant workflow for this user.
- SecureChange is set with segregated domains mode and you do not have access to the domain.
- SecureChange is not installed.

Prerequisites

- The user must exist with the same username in both SecureTrack and SecureChange.
- The user must have **Create change requests and view 'My Requests' tab** permission in SecureChange. This permission is enabled by default for the Requester role.
- To ensure that the relevant workflow is mapped to the **Modify rules** action from the **Rule modification** request in SecureTrack, the SecureChange administrator must create a new workflow in SecureChange with the Rule Modification property, and include the Rule modification field in the relevant steps.



Workflow Properties

* Name:

Type: Rule modification

Description:

How do I create a Rule Modification ticket request?

1. In **Policy Browser**, search for, and select the desired rules.

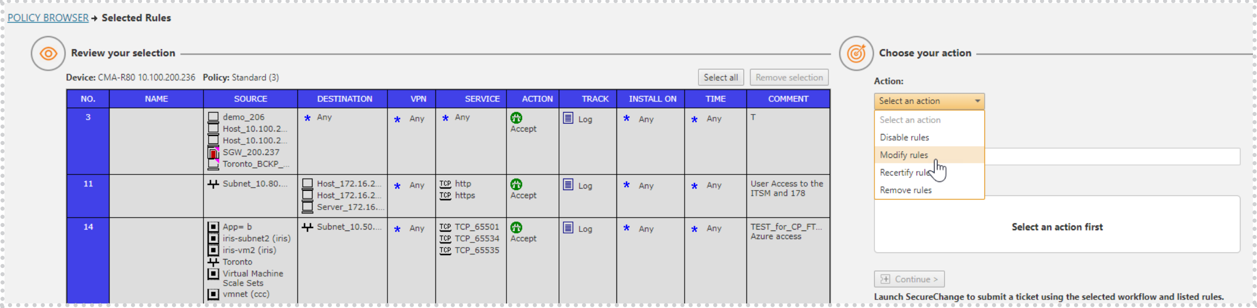
   Use the <CTRL> and <SHIFT> keys to select multiple rules.

2. Click [Add to ticket | (9)] to add the selected rules to the ticket's list of rules.

   This button is disabled if no rules are selected.

3. Click [+ Add to ticket | (9)] to review the selected rules.

   The **Selected Rules** window is displayed.

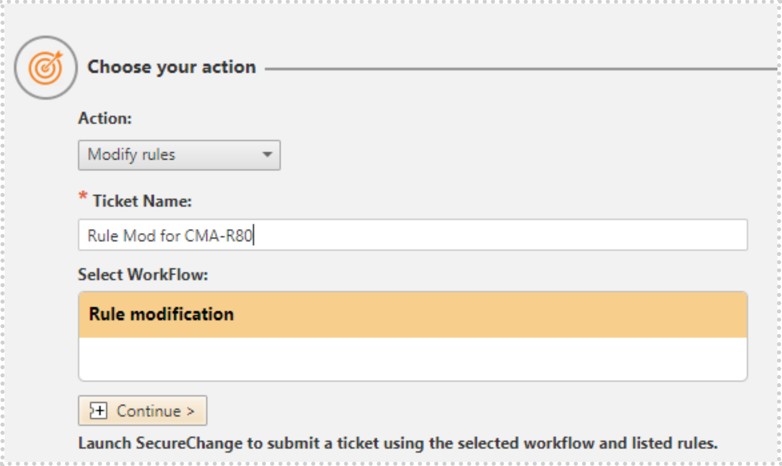


Device: CMA-R80 10.100.200.236 **Policy:** Standard (3)

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
3		demo_206 Host_10.100.2... Host_10.100.2... SGW_200.237 Toronto_BCKP_...	* Any	* Any	* Any	Accept	Log	* Any	* Any	T
11		Subnet_10.80....	Host_172.16.2... Host_172.16.2... Server_172.16....	* Any	TCP http TCP https	Accept	Log	* Any	* Any	User Access to the ITSM and 178
14		App= b iris-subnet2 (iris) iris-vm2 (iris) Toronto Virtual Machine Scale Sets vmnet (ccc)	Subnet_10.50....	* Any	TCP TCP_65501 TCP TCP_65534 TCP TCP_65535	Accept	Log	* Any	* Any	TEST_for_CP_FT... Azure access

Launch SecureChange to submit a ticket using the selected workflow and listed rules.

4. Review the selected rules and select or fill in the required fields (**Action**, **Ticket Name**, **Select WorkFlow**).



Action: Modify rules

* Ticket Name: Rule Mod for CMA-R80

Select WorkFlow: Rule modification

Launch SecureChange to submit a ticket using the selected workflow and listed rules.

5. Select and remove rules that you do not want to include in the ticket request.

6. Click [+ Continue >] to launch SecureChange and to submit the ticket request using the selected workflow and the list of rules.

   The SecureChange ticket request appears in the **My Requests** window, with the workflow and rules that you selected.

   Once you submit the ticket, the list of selected rules in SecureTrack is cleared.

7. Review the ticket request in SecureChange, and click [Submit].

Rule Modification Tips

Use the Rule Modification action to create tickets for quick remediation:

- To enable firewall administrators to edit "allow" rules, and add or remove objects that are "known" to Tufin in the source or destination fields.
- To update a rule as:
  - Part of an access decommission. For example, a user wants to remove an object from the source to decommission an access.
  - Remediation for a cleanup. For example, as part of normal cleanup processes, a user searches for rules with unused devices or services, finds the rules and determines that the remediation action is to update the rule and remove the unused objects.
  - Remediation for APG update
  - Remediation for Policy Violations. For example, a user is looking at rules which violate the USP Policy and determines that the remediation action is to edit the rule by removing a device or service.

How Do I Get Here?

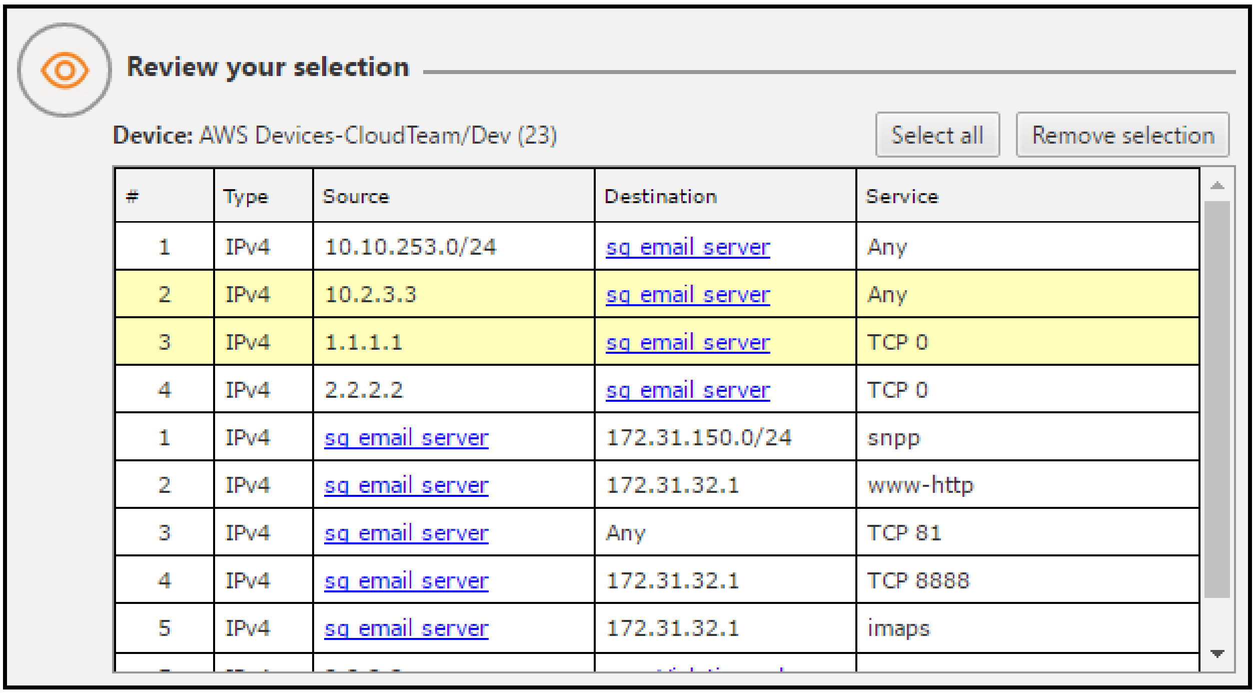
To view the Policy Browser:

- In SecureTrack, click **Home** > **Policy Browser**.

Reviewing Selected Rules

Review the rules that were selected from the Policy Browser, and create a SecureChange ticket request . (See Decommissioning Rules or Recertifying Rules for the prerequisites.) The window is divided into two sections:

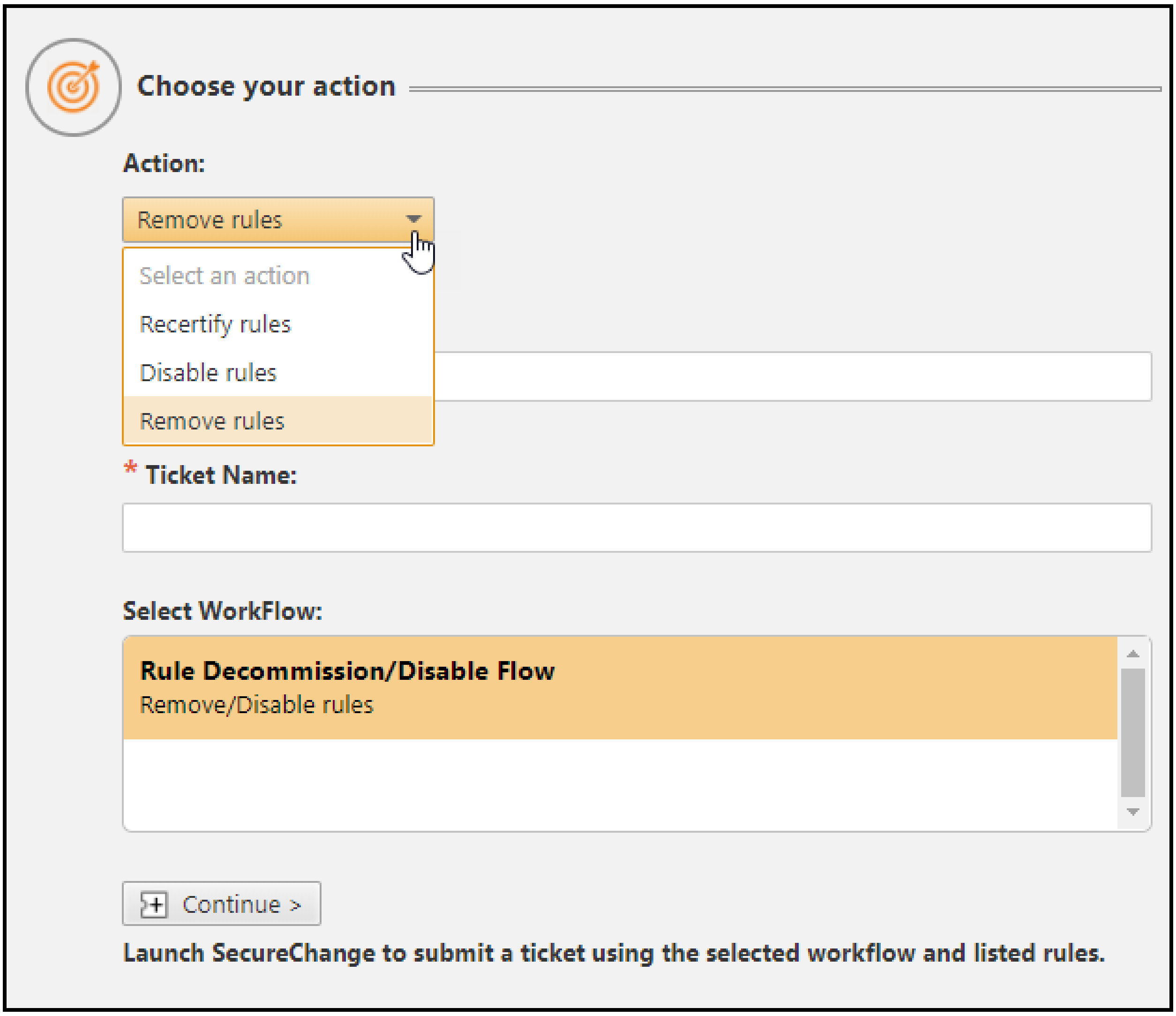
1. **Review your selection** - Review the list of rules to make sure it only contains the rules to which you want to apply the action in the ticket request to.



Device: AWS Devices-CloudTeam/Dev (23)

#	Type	Source	Destination	Service
1	IPv4	10.10.253.0/24	sg email server	Any
2	IPv4	10.2.3.3	sg email server	Any
3	IPv4	1.1.1.1	sg email server	TCP 0
4	IPv4	2.2.2.2	sg email server	TCP 0
1	IPv4	sg email server	172.31.150.0/24	snpp
2	IPv4	sg email server	172.31.32.1	www-http
3	IPv4	sg email server	Any	TCP 81
4	IPv4	sg email server	172.31.32.1	TCP 8888
5	IPv4	sg email server	172.31.32.1	imaps

2. **Choose your action** - Select or fill in **Action**, **Ticket Name**, **Select WorkFlow**, and create the SecureChange ticket.


Choose your action

Action:

Remove rules

- Select an action
- Recertify rules
- Disable rules
- Remove rules

* Ticket Name:

Select WorkFlow:

Rule Decommission/Disable Flow
Remove/Disable rules

Continue >

Launch SecureChange to submit a ticket using the selected workflow and listed rules.

a. **Action** - The user can specify whether to:

- Recertify rules - Recertify the selected rules.
- Disable rules - Disable the selected rules.
- Remove rules - Remove the selected rules.

b. **Ticket Name** - Enter the name to be used for the ticket request in SecureChange.

c. **Select Workflow** - Select the desired workflow to use for the SecureChange ticket.

The SecureChange administrator must create at least one active Rule Recertification or Rule Decommission workflow type, otherwise this section will be empty.

What can I do?

- **Select rules** - Click and select rules to delete them from the Selected Rules list.

  Use the <CTRL> and <SHIFT> keys while clicking to select multiple rules.

  Click Select all to select all the listed rules.

- **Remove Rules** - Click Remove selection to remove the selected rules.

- **Create a request ticket** - Click Continue > to launch SecureChange with the selected workflow and rules.

How do I create a ticket request?

1. In **Policy Browser**, search for, and select the desired rules.

   Use the <CTRL> and <SHIFT> keys while clicking to select the multiple rules.

2. Click Add to ticket 👁 (9) to add the selected rules to the ticket's list of rules.

   This button is disabled if no rules are selected.

3. Click Add to ticket 👁 (9) to review the selected rules.

   The **Selected Rules** window is displayed.

4. Review the selected rules and select or fill in the required fields (**Action**, **Ticket Name**, **Select WorkFlow**).
5. Select and remove rules that you do not want to include in the ticket request.
6. Click Continue > to launch SecureChange and to submit the ticket request using the selected workflow and the list of rules.

   The SecureChange ticket request appears in the **My Requests** window, using the workflow and rules that you selected.

   Once you submit the ticket, the list of selected rules in SecureTrack is cleared.

7. Review the ticket request in SecureChange, and click Submit.

How Do I Get Here?

To view the Policy Browser Selected Rules page:

1. In SecureTrack, click **Home** > **Policy Browser**.
2. Click Add to ticket 👁 (9).

   This button is disabled if no rules have been added to the ticket request.

Editing Rule Metadata

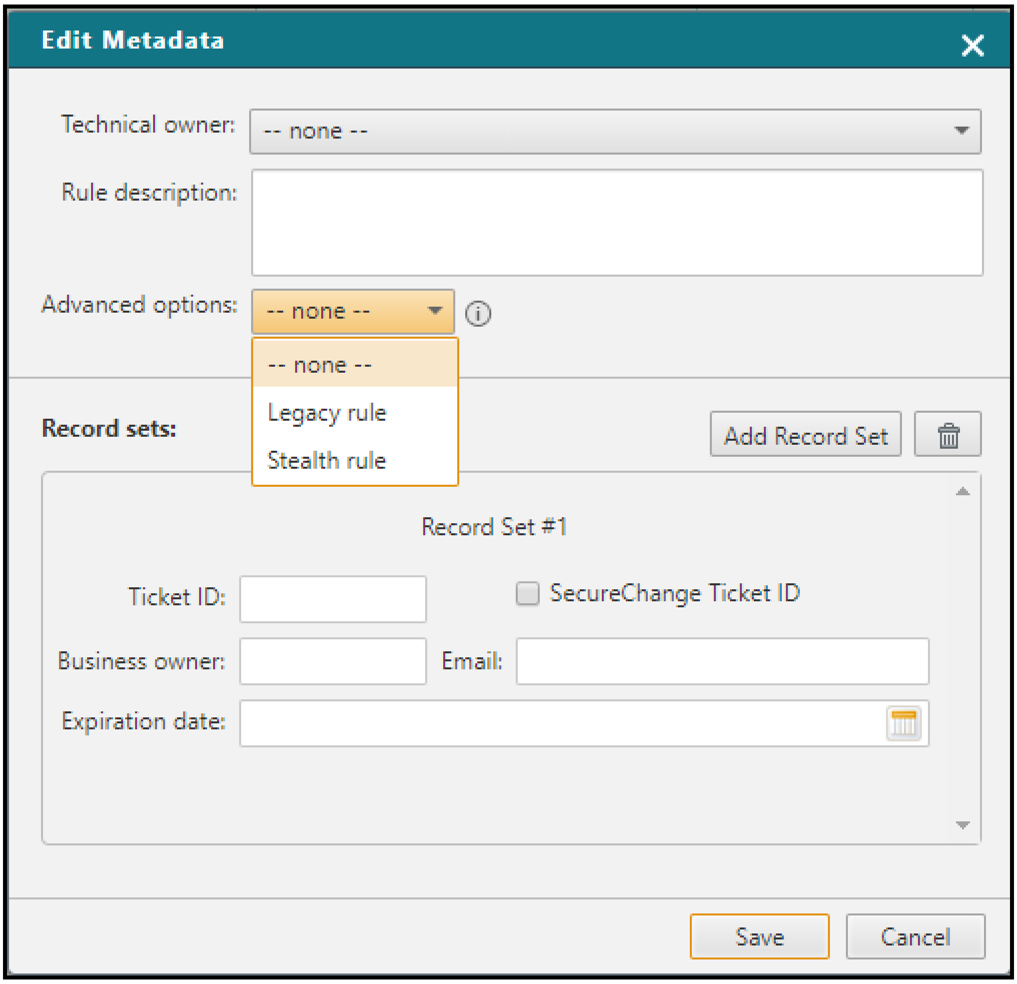
You can edit the details, or metadata, of rules in Policy Browser.

To edit the details of one or more rules:

1. Select the device and enter the search criteria to see matching rules.
2. Click on the rule or rules you want to edit.

   You can also select a rule and click 👁 to see the rule details.

3. Click ✏ to edit the rule metadata, and enter the following:



Edit Metadata

Technical owner: -- none --

Rule description:

Advanced options: -- none --

Record sets:

Record Set #1

Ticket ID:

□ SecureChange Ticket ID

Business owner:

Email:

Expiration date:

a. **Technical Owner** and **Rule Description**:

   If you are a SecureTrack administrator, you can select a SecureTrack user from the list. If more than one rule is being edited, this will be disabled.

b. **Advanced options**:

   - Legacy rule - When a rule is marked as legacy, SecureChange Designer will treat a rule marked as legacy as a shadowed rule when making recommendations, and SecureChange Verifier will ignore a rule marked as legacy when verifying access.

     Marking rules as legacy can be used to let you methodically replace overly permissive rules over a period of time. Only rules that have an Allow action will be considered by Designer as legacy.

     When the traffic in an access request is fully or partially implemented by traffic that is handled by legacy rules, Designer locates the recommended rules above the related legacy rule with the highest position in the policy.

   - Stealth rule - When a rule as is marked as stealth, SecureChange Designer recommendations will place any new rules recommended for an access request below the stealth section of the policy. Only rules that have a Deny action will be considered by Designer as stealth.

     The stealth section is comprised of all rules above and including the last rule marked as stealth in the device policy and is therefore always the top section in the device policy. Stealth rules can be used to protect a firewall device from attack by denying unwanted access to specific firewalls.

For devices that support hierarchical structures and management of grouped entities, Policy Browser does not display propagated Legacy or Stealth Rules for the devices that are lower in the hierarchy.

To determine whether a device that is lower in the hierarchy includes a Legacy or Stealth Rule propagated from higher up, SecureTrack users should search for the level at which the Legacy or Stealth Rule was defined. The level of each rule is displayed in the Policy Browser, in the Rule Location column.

Designer takes the propagated Legacy or Stealth Rules into account for the managed devices that are lower in the hierarchy when suggesting changes and when provisioning. With Legacy rules, Designer will not create new rules on lower level entities that intersect with the legacy rule.

c. **Ticket ID**, **SecureChange Ticket ID**, **Business Owner**, **Email**, **Expiration Date**: Enter the Ticket ID to associate with the rule. Select **SecureChange Ticket ID** if the Ticket ID is from SecureChange, and the ID will display in the Policy Browser as a hyperlink to the specified ticket.

d.

: Click **Add Record Set** to additional Ticket IDs to this rule.

4. Click **Save**.

Comparing Revisions

TOS Classic receives policy revisions in real-time, whenever a policy change is made. In **Compare**, SecureTrack shows you:

- the rules and objects defined in the policy revision
- the details of the revision, including who made the revision and when (Full Accountability)
- a color-coded comparison between any two revisions so you can easily see the changes

Note: IPv6 is supported for this feature, as follows: IPv6 objects are shown for all devices except for F5 and Fortinet.

Compare View

In **Compare** view, the left-hand pane lists all the devices monitored by SecureTrack in this hierarchy:

- In a multi-domain deployment, all domains are listed with their devices.
- Within the domains, devices are divided according to device vendor.
- Management devices, such as Cisco CSM or Juniper NSM, are shown with the devices that they manage.

  Check Point gateways are shown only when Firewall OS Monitoring (FOM) is enabled.

The icon next to each device indicates the status of the connection between it and SecureTrack. The possible statuses are:

🟢 SecureTrack is connected to the device.

🟡 The SecureTrack process monitoring this device is running, but cannot connect to the device.

🔴 The SecureTrack process monitoring this device is not running.

⚪ Monitoring has been disabled for this device.

⚫ Monitoring for this device has been stopped due to a licensing problem, or this device cannot be monitored because it has no policy

📄 The device is configured for Offline Analysis.

You can hover over the status icon to see an explanation for any connectivity problems.

Monitored devices can also be managed in Status.

Viewing the Revision History

You can select a specific device from the monitored devices and see the list of recent revisions for that device. SecureTrack can send email, syslog, or SNMP notifications whenever a new revision is available. You can also filter the list of revisions.

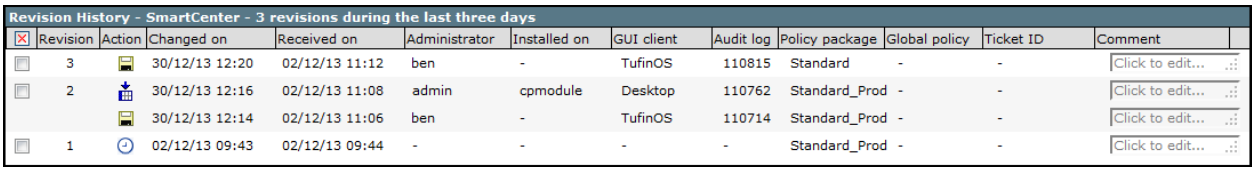
SecureTrack receives the policy every time there is an action, and shows a new revision every time that there is a policy or configuration change. For Check Point and FortiManager policies, consecutive save and install actions are usually combined by SecureTrack as a single revision. For example, if a user creates a new rule and saves the changes at the management level, and then installs the policy with the new rule on the Firewalls, SecureTrack will show two versions in a single revision: one for the rule creation (saved) and one for the policy installation (installed).

When a global policy change is made for Check Point Provider-1, SecureTrack shows **Assigned to** instead of **Installed on** and lists the Provider-1 Customers that the global policy was assigned to.

SecureTrack shows new revisions for Check Point gateways with OS monitoring when relevant configuration changes are made.

Understanding Revisions

By default, SecureTrack shows the revisions created in the past 72 hours. You can see the number of recent revisions next to each device in the list of monitored devices. If SecureTrack receives a new revision while you are in the **Compare** view, a "New Revision" message appears next to the Filter button. To show the new revisions in the revision history, click the alert. You can also click on the device to always to refresh the revision history.



Revision History - SmartCenter - 3 revisions during the last three days

☒	Revision	Action	Changed on	Received on	Administrator	Installed on	GUI client	Audit log	Policy package	Global policy	Ticket ID	Comment
□	3	💾	30/12/13 12:20	02/12/13 11:12	ben	-	TufinOS	110815	Standard	-	-	Click to edit...
□	2	⬇	30/12/13 12:16	02/12/13 11:08	admin	cpmodule	Desktop	110762	Standard_Prod	-	-	Click to edit...
		💾	30/12/13 12:14	02/12/13 11:06	ben	-	TufinOS	110714	Standard_Prod	-	-	Click to edit...
□	1	🕘	02/12/13 09:43	02/12/13 09:44	-	-	-	-	Standard_Prod	-	-	Click to edit...

SecureTrack shows each revision with these details:

- **Revision**: The revision number assigned by SecureTrack.
- **Action**: The operation on the device that generated the new revision. The list of actions includes:

  Note that some actions are available only for specific devices

🕒	Automatic revision Based on the periodic polling frequency setting
⬇▦	Policy was installed on the device
💾	Policy was saved
☰	Policy was restored (For Check Point only)
G	Provider-1 Global Policy was assigned (For Check Point only)
⬇G	Provider-1 Global Policy was assigned and Last Policy installed (For Check Point only)
G	Provider-1 Global Policy was removed (For Check Point only)

- **Date**: The date the revision was created.
- **Time**: The time the revision was created and saved in the SecureTrack database.
- **Administrator**: The device administrator that performed the operation.
  - For Cisco, Fortinet, Juniper and Palo Alto Networks devices, you can only see the administrator if you configure monitoring with syslogs.
- **GUI Client** : The name or IP address of the host used to make the revision.
  - For Cisco and Juniper, you can only see this if you configure monitoring with syslogs.
  - For Check Point Provider-1, when you assign a Global Policy this field shows the Customer that the policy was assigned to.
- **Ticket ID**: The Ticket ID used in the Comment or Description field of a rule or object. You can configure the Ticket ID to link to actual tickets in a third-party Change Management system.
- **Comment**: SecureTrack Administrators can add and edit a comment to the revision here. This information is saved in SecureTrack's database and can subsequently be used as a filter criterion (see below).

For Check Point only:

- **Installed On**: The gateways which the policy was installed on.
- **Audit Log**: The audit log number that relates to the revision.
- **Policy Package**: The name of the policy package that was most recently open in SmartDashboard before the change was made. In most cases, this means that a change was made to this policy package.
- **Global Policy**: The name of the assigned Provider-1 Global Policy.

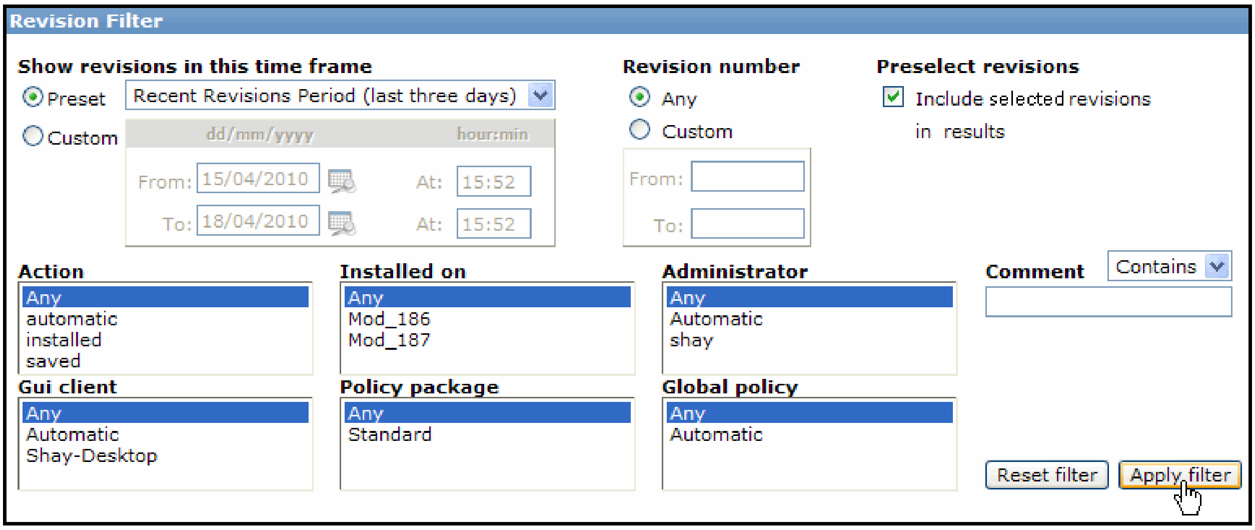
Filtering for Revisions

You can filter the revisions to see only the revisions that are important for you.

To filter the revisions:

1. Click **Filter** below the revision history.

   The Filter settings are shown.



Revision Filter

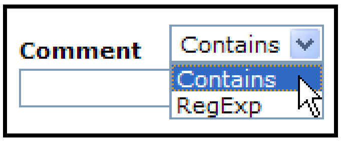
Show revisions in this time frame
● Preset: Recent Revisions Period (last three days)
○ Custom: From: 15/04/2010 At: 15:52 To: 18/04/2010 At: 15:52

Revision number
● Any
○ Custom From: To:

Preselect revisions
☑ Include selected revisions in results

Action: Any, automatic, installed, saved
Installed on: Any, Mod_186, Mod_187
Administrator: Any, Automatic, shay
Comment: Contains
Gui client: Any, Automatic, Shay-Desktop
Policy package: Any, Standard
Global policy: Any, Automatic

2. Configure the filter based on any of the revision details.
   - To include specified revisions that do not match the filter criteria, select **Include selected revisions in results**.
   - To filter for revisions that contain specific text or that match a regular expression, select either **Contains** or **RegExp**:

   - To change the timeframe back to the default, click **Reset filter**. You can configure the default timeframe in My Settings.
3. Click **Apply filter**.

   The revisions list is filtered.

Viewing Policies

> This is a Legacy Feature. We recommend you consider using the "Object Lookup" on page 334 feature.

You can view the details of any policy revision. SecureTrack shows the device's security rules and other information, depending on the device vendor.

If a Check Point rulebase uses a non-English character set in section headings, rule names, and comments, you must configure SecureTrack to support that character set.

To view a single policy revision:

1. In **Compare** View, in the left-hand pane, select the relevant monitored device.
2. In the revisions table, select the desired policy revision, and click **View Policy**.

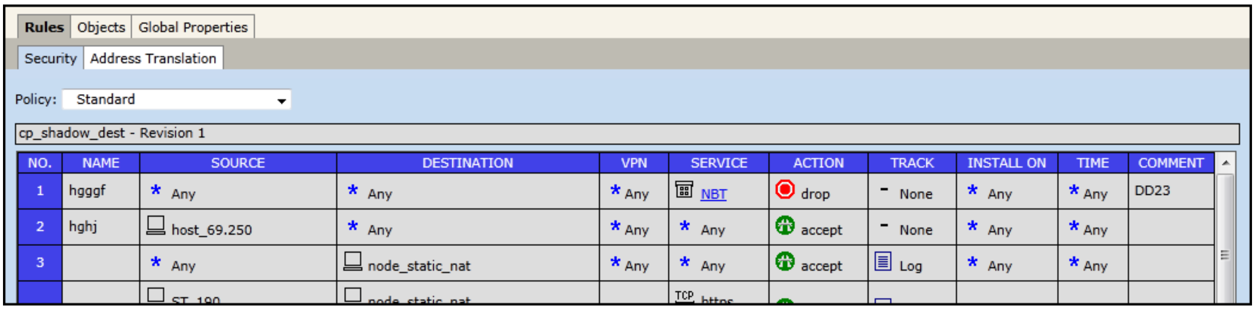
   For devices that have policies that are divided into sections, you can select a section to only see those rules.
   - Check Point - a revision can include multiple policy packages. You can select a policy package from the list. Packages are arranged according to installation targets.
   - Cisco, Juniper, Fortinet and Palo Alto - a revision can include rules for specific zones or interfaces. You can select the zones or interfaces to view. You can also select to show the global rules in the list of rules.

Understanding Policies

> This is a Legacy Feature. We recommend you consider using the "Object Lookup" on page 334 feature.

SecureTrack includes these features to help you understand the device's policy quickly and export them to other formats:

- **Policy sections** - Depending on device type, the policy view can include:
  - Security Rules (Graphical)
  - Check Point NAT rules (Manual and Automatic)
  - Objects configured on the monitored device: Network objects, Services, Resources, Servers, OPSEC applications, Users, VPN communities, and Applications, Application Groups and Filters
  - Check Point Global Properties
  - Running Config / Device Config (Textual)
  - Device interfaces
  - Routing tables
- **Graphical Policy** - SecureTrack shows policies as they are shown in the vendor's management software. For example, a security policy from a Check Point management server looks the same as it does in SmartDashboard.



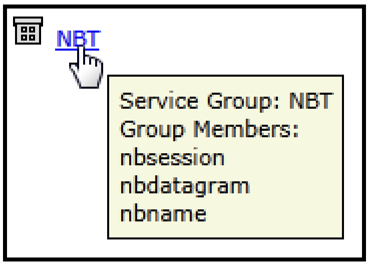
Policy: Standard

cp_shadow_dest - Revision 1

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	hgggf	* Any	* Any	* Any	NBT	drop	- None	* Any	* Any	DD23
2	hghj	host_69.250	* Any	* Any	* Any	accept	- None	* Any	* Any	
3		* Any	node_static_nat	* Any	* Any	accept	Log	* Any	* Any	
		ST_190	node_static_nat		TCP https					

In a non-Check Point policy, you can select zones or interfaces from the drop-down list. In a Check Point policy that contains multiple Policy Packages, you can select a package from the drop-down list, where the packages are arranged according to installation target.

- **Group Object Details** - Group objects appear as links. You can click on a link or point to it to view group members:



Service Group: NBT
Group Members:
nbsession
nbdatagram
nbname

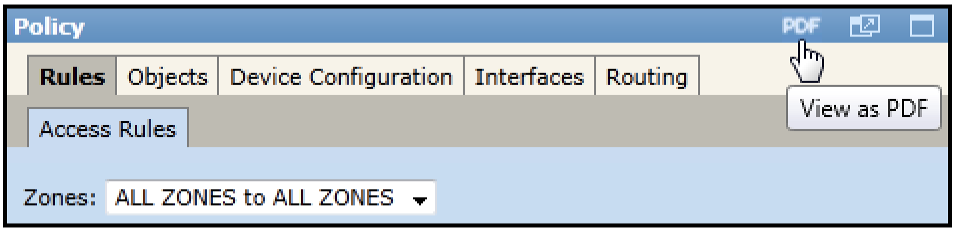
- **Links to Tickets** - When integration with a change management or ticketing system is configured, you can click on the ticket ID in the rule's comment field to open the ticket pages of the change management system.

Exporting Policies

> This is a Legacy Feature. We recommend you consider using the "Object Lookup" on page 334 feature.

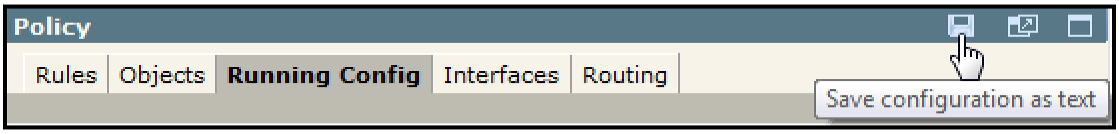
You can export the list of rules with:

- **Export Graphical Policy to PDF** - You can convert the Rules view to a PDF. In the upper-right corner, click PDF:



Zones: ALL ZONES to ALL ZONES

- **Export Config to Text** - You can export the Running Config / Device Config as a text file.



Cisco Router and Switch Monitoring Overview

> This is a Legacy Feature. We recommend you consider using the "Object Lookup" on page 334 feature.

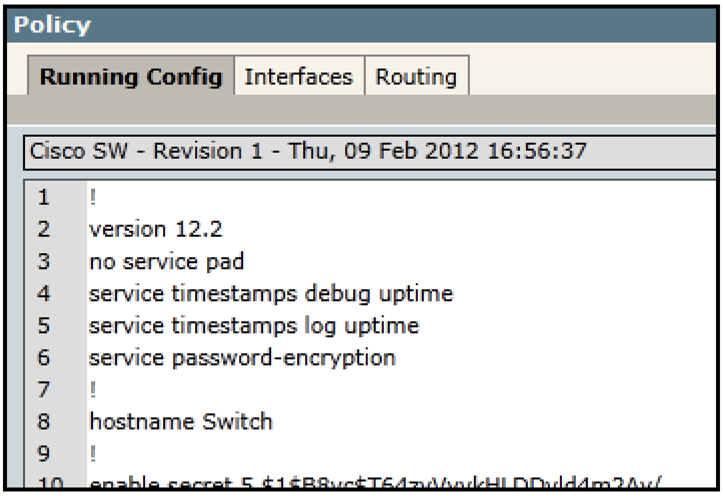
SecureTrack can monitor Cisco routers, including layer 3 switches that have been added to SecureTrack as routers, for access lists, and configuration and routing information. SecureTrack can monitor other Cisco switches for configuration and routing information.

For Cisco routers (including layer 3 switches as above), you can do Policy Management, Policy Analysis, Compliance Policies, and all Reports.

Cisco switch configuration revisions can be viewed or compared, and New Revision Reports can be configured for them. Other auditing and reporting features are currently not supported for switches.

For switches, the information is displayed in **Compare** view:

- **Running Config**
- **Routing Information** (for switches that support routing)



Cisco SW - Revision 1 - Thu, 09 Feb 2012 16:56:37

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Switch
!
enable secret 5 $1$B8vc$T64zvVvvkHLDDvld4m2Av/
```

Using Cisco Switch Monitoring

> This is a Legacy Feature. We recommend you consider using the "Object Lookup" on page 334 feature.

To view a revision of IOS-level configuration data:

1. In **Compare** view, in the left-hand pane, select the relevant Cisco router or switch.
2. In the revisions list, select a revision.
3. Click **View Policy**.

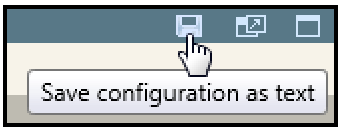
The configuration data is displayed.

To compare two revisions:

1. In **Compare** view, in the left-hand pane, select the relevant device.
2. In the revisions list, select two revisions.
3. Click **Compare**.

   When a change is detected, a "New Revision Report" is sent to SecureTrack users who are configured to receive them.

When viewing a single revision, you can export the policy as a text file:



Comparing Policy Revisions

In some cases a newly-installed policy can cause unforeseen problems, such as network downtime, leading to business downtime. The ability to easily compare the new policy to an older known working policy can significantly improve network and system uptime.

You can either view a side-by-side graphical diff, or generate a report listing the differences.

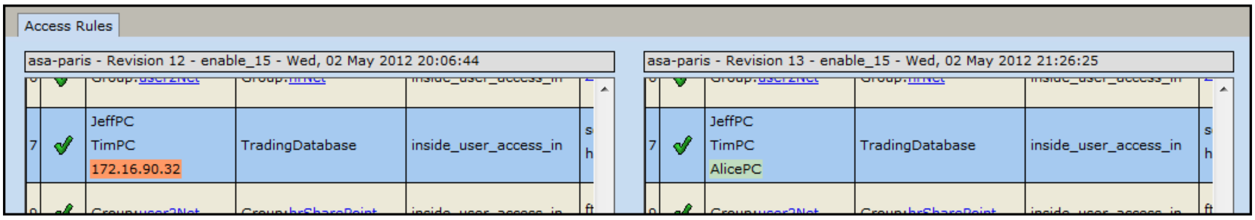
To locate the user who performed a known change, where the exact revision number is not known, use the Advanced Change Report. The Advanced Change Report lists all the changes between two points in time, with the user that performed each change.

Side-by-Side Comparison

To graphically compare two firewall policy revisions side-by-side:

1. In **Compare** View, in the left-hand pane, select the relevant monitored device.
2. In the revisions table, select the two policy revisions to be compared.
3. Click **Compare**.

SecureTrack analyzes the differences between the revisions, and displays a side-by-side graphical comparison.



asa-paris - Revision 12 - enable_15 - Wed, 02 May 2012 20:06:44

7	✓	JeffPC TimPC 172.16.90.32	TradingDatabase	inside_user_access_in	s h

asa-paris - Revision 13 - enable_15 - Wed, 02 May 2012 21:26:25

7	✓	JeffPC TimPC AlicePC	TradingDatabase	inside_user_access_in	s h

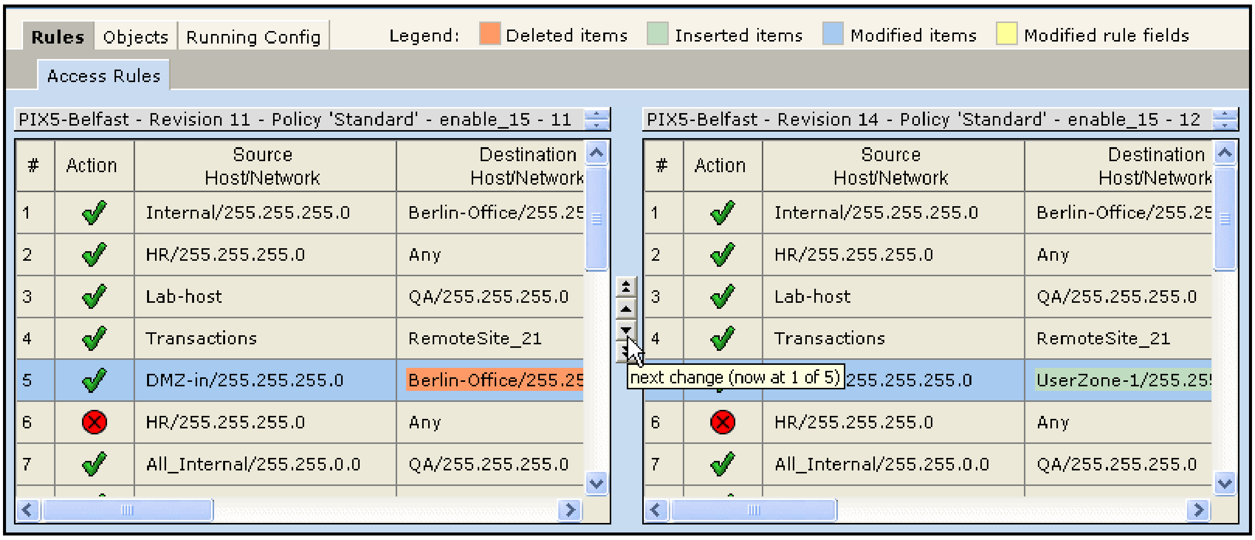
Any configuration changes that were made between the two revisions are highlighted.

Policies containing thousands of rules may take a long time or fail to be compared. For comparison of large policies, it is recommended to use **Generate Report** rather than **Compare**.

Policies are arranged in a similar fashion as when viewing a single policy revision.

Moving between policies and tabs, and scrolling, affects both revisions, so you are always viewing the same part of both revisions.

You can quickly move between changes by using the navigation arrows, located in the space between the two policies:



PIX5-Belfast - Revision 11 - Policy 'Standard' - enable_15 - 11

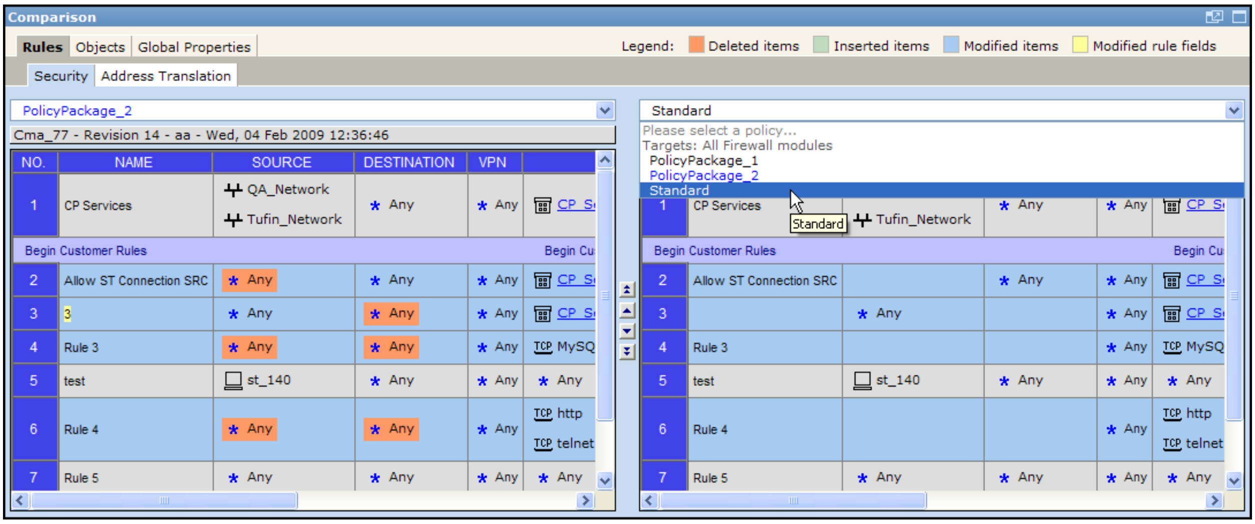
#	Action	Source Host/Network	Destination Host/Network
1	✓	Internal/255.255.255.0	Berlin-Office/255.25
2	✓	HR/255.255.255.0	Any
3	✓	Lab-host	QA/255.255.255.0
4	✓	Transactions	RemoteSite_21
5	✓	DMZ-in/255.255.255.0	Berlin-Office/255.25
6	✗	HR/255.255.255.0	Any
7	✓	All_Internal/255.255.0.0	QA/255.255.255.0

PIX5-Belfast - Revision 14 - Policy 'Standard' - enable_15 - 12

#	Action	Source Host/Network	Destination Host/Network
1	✓	Internal/255.255.255.0	Berlin-Office/255.25
2	✓	HR/255.255.255.0	Any
3	✓	Lab-host	QA/255.255.255.0
4	✓	Transactions	RemoteSite_21
		255.255.255.0	UserZone-1/255.25!
6	✗	HR/255.255.255.0	Any
7	✓	All_Internal/255.255.0.0	QA/255.255.255.0

By default, in the **Objects** tab, only modified objects are shown. This behavior can be changed.

In a Check Point policy that contains multiple Policy Packages, you can select a package from the drop-down list, where the packages are arranged according to installation target. For meaningful results, select on both sides packages intended for the same installation targets. Modified packages are colored blue:



Comparison

Rules | Objects | Global Properties
Security | Address Translation

Legend: 🟧 Deleted items 🟩 Inserted items 🟦 Modified items 🟨 Modified rule fields

PolicyPackage_2

Cma_77 - Revision 14 - aa - Wed, 04 Feb 2009 12:36:46

NO.	NAME	SOURCE	DESTINATION	VPN	
1	CP Services	QA_Network Tufin_Network	Any	Any	CP_S
Begin Customer Rules					Begin Cu
2	Allow ST Connection SRC	Any	Any	Any	CP_S
3	3	Any	Any	Any	CP_S
4	Rule 3	Any	Any	Any	MySQ
5	test	st_140	Any	Any	Any
6	Rule 4	Any	Any	Any	http telnet
7	Rule 5	Any	Any	Any	Any

Standard

Please select a policy...
Targets: All Firewall modules
PolicyPackage_1
PolicyPackage_2
Standard

1	CP Services	Tufin_Network	Any	Any	CP_S
Begin Customer Rules					Begin Cu
2	Allow ST Connection SRC		Any	Any	CP_S
3		Any		Any	CP_S
4	Rule 3			Any	MySQ
5	test	st_140	Any	Any	Any
6	Rule 4			Any	http telnet
7	Rule 5	Any	Any	Any	Any

In Cisco, Fortinet, and Juniper policies, you can view textual differences in the Running Config / Device Configuration tab.

In Fortinet policies, if one or both of the policies contains one or more Global rules, the display is in Global view. If neither policy contains Global rules, Section view is used.

Side-by-side comparison of a Fortinet policy revision containing a Global rule to a Fortinet policy revision that was received by SecureTrack previous to version 5.1 is not supported.

Generating a Comparison Report

To generate a report listing the differences between two firewall policy revisions:

1. In **Compare** View, in the left-hand pane, select the relevant monitored device.
2. In the revisions table, select the two policy revisions to be compared.
3. Click **Generate Report.**

If multiple Policy Packages are used in a Check Point device, the report will show a rulebase comparison for one modified package per gateway installation target group. If there are multiple policy packages defined for the same gateway installation targets, then for each gateway installation target group SecureTrack displays a comparison for one modified policy package.

As in the graphical comparison, the Comparison Report highlights the specific rule field contents that were changed. Some Check Point objects that are not displayed in the Graphical Comparison are captured and displayed in the Comparison Report. These objects include the following:

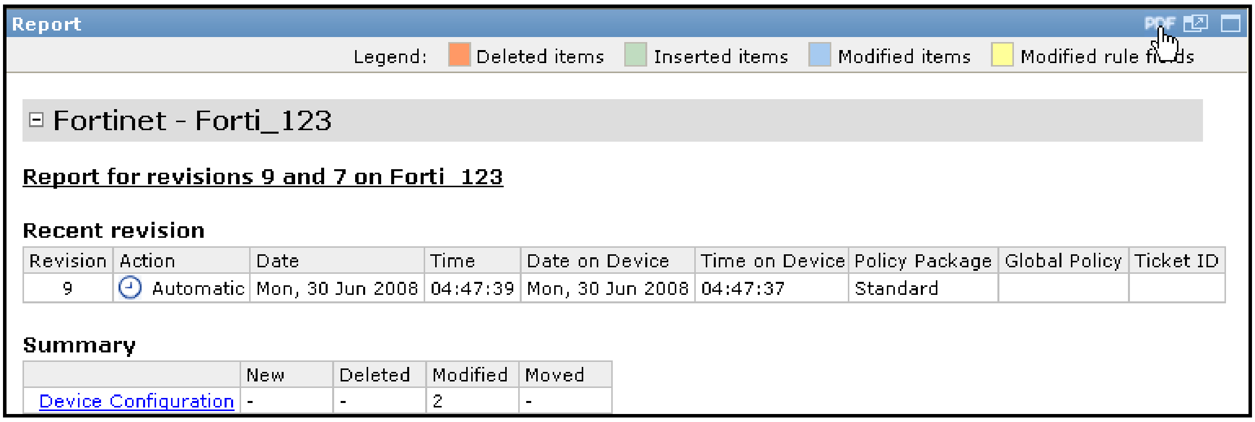
- Desktop Security Policies
- SmartDefense™ and Web Intelligence™ settings
- Provider-1 administrators, licenses, and other objects

When a network or service object is modified, SecureTrack will show all the groups and rules that include that object, either directly or indirectly, through a group. Where a Group object appears, you can click it to view its members.

The comparison report is identical to the automatic report sent to each SecureTrack user that has Detailed Notifications enabled.

In non-Check Point firewalls comparison reports, the graphical rule changes are displayed, along with the underlying textual configuration changes, to suit the preferences of different users.

You can convert the Comparison Report to a PDF. In the upper-right corner, click PDF:



Report

Legend: 🟧 Deleted items 🟩 Inserted items 🟦 Modified items 🟨 Modified rule fields

⊟ Fortinet - Forti_123

Report for revisions 9 and 7 on Forti_123

Recent revision

Revision	Action	Date	Time	Date on Device	Time on Device	Policy Package	Global Policy	Ticket ID
9	Automatic	Mon, 30 Jun 2008	04:47:39	Mon, 30 Jun 2008	04:47:37	Standard		

Summary

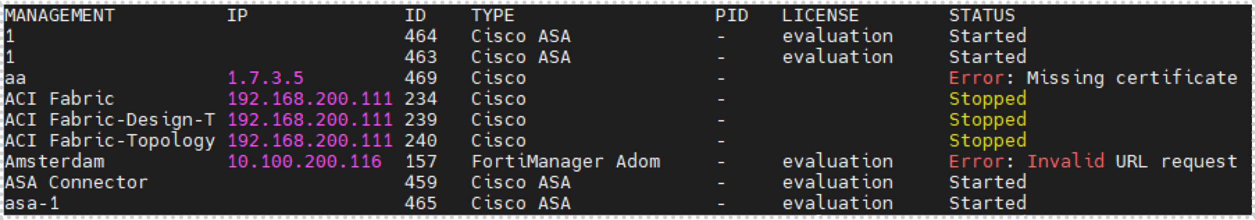
	New	Deleted	Modified	Moved
Device Configuration	-	-	2	-

Identifying the SecureTrack Device ID

You can see the SecureTrack device ID in one of the following ways:

Method 1: Use the `st stat` Command

In the output of the `st stat` command, the ID column lists the device ID.



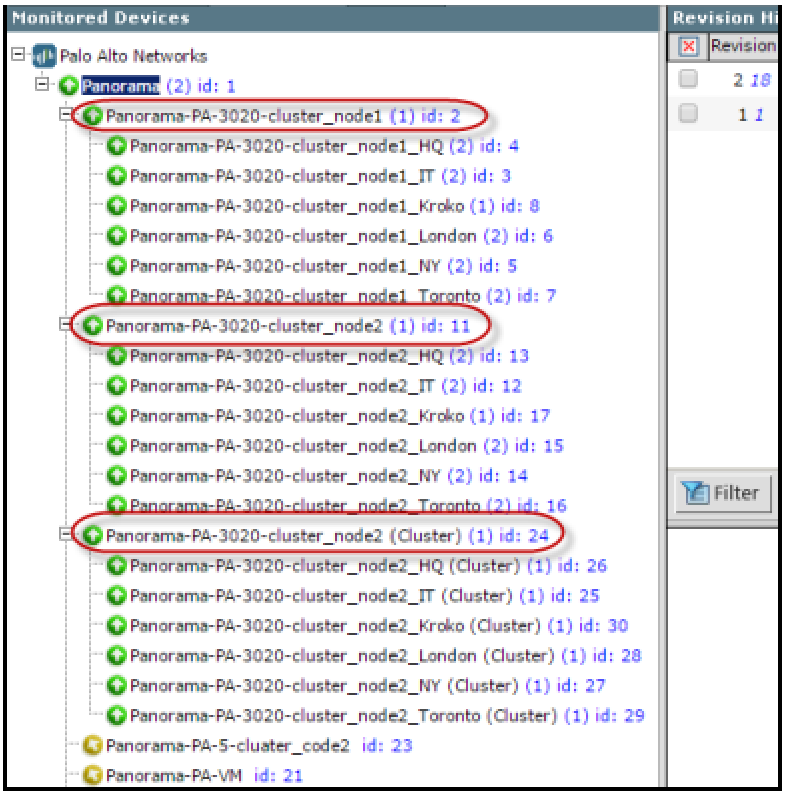
```
MANAGEMENT          IP              ID    TYPE                 PID   LICENSE        STATUS
1                                   464   Cisco ASA             -    evaluation     Started
1                                   463   Cisco ASA             -    evaluation     Started
aa                  1.7.3.5         469   Cisco                 -                   Error: Missing certificate
ACI Fabric          192.168.200.111 234   Cisco                 -                   Stopped
ACI Fabric-Design-T 192.168.200.111 239   Cisco                 -                   Stopped
ACI Fabric-Topology 192.168.200.111 240   Cisco                 -                   Stopped
Amsterdam           10.100.200.116  157   FortiManager Adom     -    evaluation     Error: Invalid URL request
ASA Connector                       459   Cisco ASA             -    evaluation     Started
asa-1                               465   Cisco ASA             -    evaluation     Started
```

1. Open a command line session.
2. Run `st stat`.

Method 2: Use the Compare Revisions Feature

1. Navigate to **Compare** > **Compare Revisions**.
2. Click a device in the device tree.
3. Type the letter "**t**".

The ID for every device appears.



```
Monitored Devices
⊟ Palo Alto Networks
  ⊟ Panorama (2) id: 1
    ⊟ Panorama-PA-3020-cluster_node1 (1) id: 2
        Panorama-PA-3020-cluster_node1_HQ (2) id: 4
        Panorama-PA-3020-cluster_node1_IT (2) id: 3
        Panorama-PA-3020-cluster_node1_Kroko (1) id: 8
        Panorama-PA-3020-cluster_node1_London (2) id: 6
        Panorama-PA-3020-cluster_node1_NY (2) id: 5
        Panorama-PA-3020-cluster_node1_Toronto (2) id: 7
    ⊟ Panorama-PA-3020-cluster_node2 (1) id: 11
        Panorama-PA-3020-cluster_node2_HQ (2) id: 13
        Panorama-PA-3020-cluster_node2_IT (2) id: 12
        Panorama-PA-3020-cluster_node2_Kroko (1) id: 17
        Panorama-PA-3020-cluster_node2_London (2) id: 15
        Panorama-PA-3020-cluster_node2_NY (2) id: 14
        Panorama-PA-3020-cluster_node2_Toronto (2) id: 16
    ⊟ Panorama-PA-3020-cluster_node2 (Cluster) (1) id: 24
        Panorama-PA-3020-cluster_node2_HQ (Cluster) (1) id: 26
        Panorama-PA-3020-cluster_node2_IT (Cluster) (1) id: 25
        Panorama-PA-3020-cluster_node2_Kroko (Cluster) (1) id: 30
        Panorama-PA-3020-cluster_node2_London (Cluster) (1) id: 28
        Panorama-PA-3020-cluster_node2_NY (Cluster) (1) id: 27
        Panorama-PA-3020-cluster_node2_Toronto (Cluster) (1) id: 29
      Panorama-PA-5-cluater_code2 id: 23
      Panorama-PA-VM id: 21
```

☒	Revision
□	2 *18*
□	1 *1*

Analyzing Policies

Policy Analysis

For new installations (from TOS 19-1 and above), **Policy Analysis** will be disabled and removed from the SecureTrack menu of the Tufin Orchestration Suite (TOS R19-1).

From TOS 19-1 and above, many of the **Policy Analysis** features and capabilities are also available via **Policy Browser** and via the **Interactive Map > SEARCH PATHS** queries.

Policy Analysis is also available in the Tufin Marketplace SecureTrack Reporting Essentials application > **Policy Analysis report**. The report displays all data related to handling the traffic defined in the query, including relevant devices, interfaces, and rules, as well as a diagram that presents one or more paths for the specified traffic.

If required, you may contact Tufin Support to re-enable the SecureTrack **Policy Analysis** tab.

Security administrators are often faced with challenges such as worms exploiting various vulnerabilities, which should be mitigated both through patches on servers, as well as locking down the affected network ports between certain networks.On the firewall side, the immediate task is to find out which networks are open and vulnerable, and which firewall rules will accept the suspected traffic.

The size and complexity of modern rulebases, however, make it very difficult to pinpoint and understand exactly what types of traffic will be accepted or dropped.Some advanced rulebase options provide a rich set of features, which further complicate rulebase understanding and clarity.

SecureTrack provides an easy method for determining how any rule or rulebase handles a specified connection type.SecureTrack examines the rulebase contained in each policy revision, and calculates the effective rulebase by simulating the rulebase's top-to-bottom first-match logic, and taking complex scenarios into account (disabled rules, network groups, negated objects, groups with exclusion, etc).This feature enables advanced queries based on different parameters, and displays the rules that match the selected traffic pattern.

IPv6 is not supported for this TOS feature.

How Policy Analysis Works

For new installations (from TOS 19-1 and above), **Policy Analysis** will be disabled and removed from the SecureTrack menu of the Tufin Orchestration Suite (TOS R19-1).

From TOS 19-1 and above, many of the **Policy Analysis** features and capabilities will be available via **Policy Browser** and via the **Interactive Map > SEARCH PATHS** queries.

If required, you may contact Tufin Support to re-enable the SecureTrack **Policy Analysis** tab.

In Policy Analysis, a rule is considered to match the query if there is any traffic that is included both in the query and in the rule's definition. The rule is considered to match even if the query also includes some traffic not included in the rule and the rule also includes some traffic not included in the query.

For example, if you need to know whether HTTP is allowed in the selected firewall rulebase, you can query for: Source=Any, Destination=Any, Service Port=80 and Action=Allow, to see whether any rules show up.

Now suppose you need to know whether HTTP traffic can be initiated from subnet 192.168.1.0/255.255.255.0 through a certain firewall rulebase. This time change the query to the following settings: Source=192.168.1.0/255.255.255.0, Destination=Any, Service Port=80 and Action=Any.

With Policy Analysis queries you can audit your network to see which rules are handling traffic between important subnets in the organization. You can also see if essential business services are blocked.

With Policy Analysis queries you can also immediately check access in response to a helpdesk call. If a user says that they cannot reach a certain server, instead of digging through terabytes of log data or running traceroutes from the user's desktop, an administrator can use the Policy Analysis function to confirm if there is a rule blocking the access.

All policies can be queried at the same time. This lets you discover if there is any device in the network that permits specific high-risk traffic, such as a newly found worm that masquerades on a specific port.

Rule Shadowing

Policy Analysis can be used for rulebase optimization, by identifying Shadowed rules.

In Policy Analysis, a rule is considered to match the query if there is any traffic that is included both in the query and in the rule's definition. The rule is considered to match even if the query also includes some traffic not included in the rule and the rule also includes some traffic not included in the query.

In addition to identifying rules that handle the traffic specified in the query, Policy Analysis identifies the following:

- **Partially Shadowed rules**: A rule is considered to be partially shadowed by a previous rule if **some** of the traffic included in both the rule and the query is handled by a previous rule.

- **Fully Shadowed rules**: Rules that match the query, but will never actually handle any of the traffic included in the query. All of the traffic included in both the rule and the query is handled by a rule or rules higher up in the rulebase.

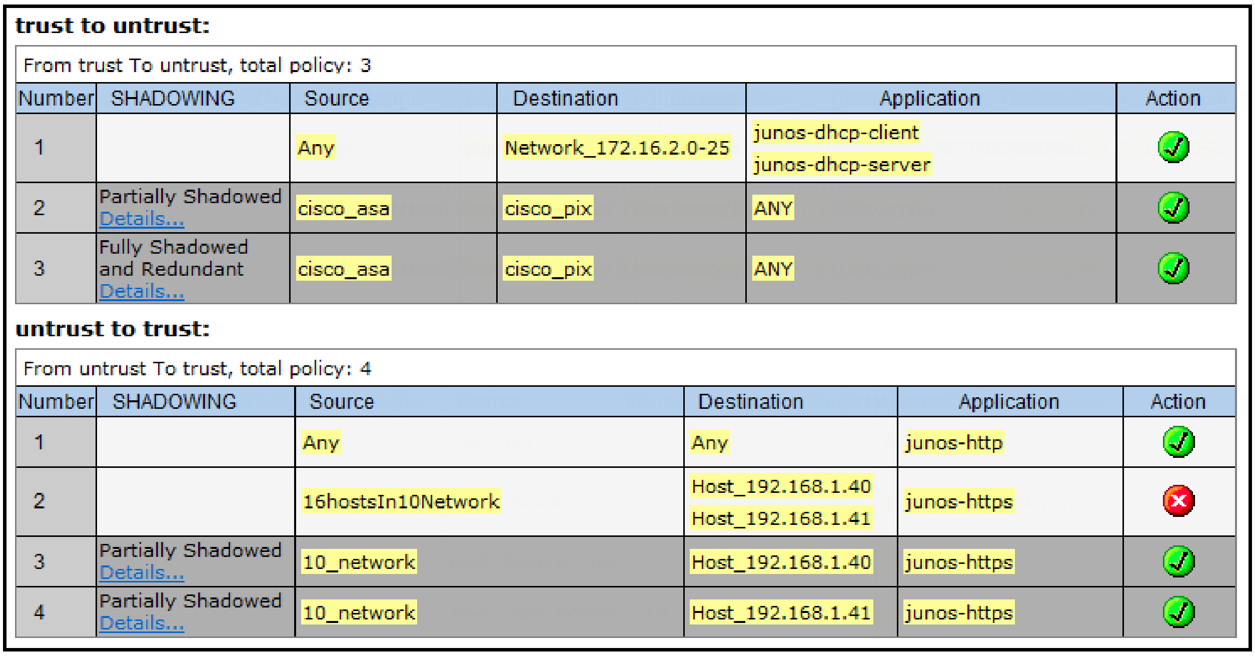
  Shadowed rules may handle traffic not included in the query; they are only shadowed in terms of the traffic specified in the query.

- **Redundant rules**: Rules whose definitions relate only to traffic which is handled by rules higher up in the rules. These rules are superfluous in the current rulebase.

  If the query was defined for all traffic (**Any** sources; **Any** destinations; **Any** services), then any resulting Shadowed rules are marked as Redundant.

In Policy Analysis results, the shadowing status of each rule is displayed in the **Shadowing** column, with a **Details** link to view Shadowing rules in a new window. The shadowing rules that are then displayed each either Partially or Fully Shadow the original rule. Within each shadowing rule, the objects that cause the shadowing are highlighted.

The following example shows partial results of a query for all traffic (**Any** sources; **Any** destinations; **Any** services):



trust to untrust:

From trust To untrust, total policy: 3

Number	SHADOWING	Source	Destination	Application	Action
1		Any	Network_172.16.2.0-25	junos-dhcp-client junos-dhcp-server	✓
2	Partially Shadowed Details...	cisco_asa	cisco_pix	ANY	✓
3	Fully Shadowed and Redundant Details...	cisco_asa	cisco_pix	ANY	✓

untrust to trust:

From untrust To trust, total policy: 4

Number	SHADOWING	Source	Destination	Application	Action
1		Any	Any	junos-http	✓
2		16hostsIn10Network	Host_192.168.1.40 Host_192.168.1.41	junos-https	✗
3	Partially Shadowed Details...	10_network	Host_192.168.1.40	junos-https	✓
4	Partially Shadowed Details...	10_network	Host_192.168.1.41	junos-https	✓

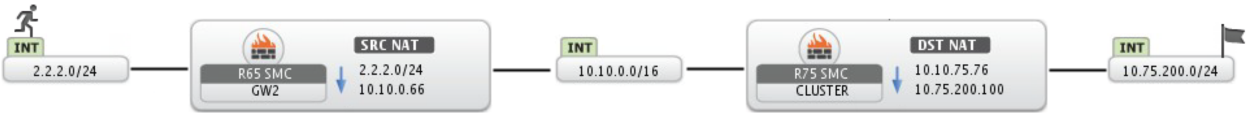
Check Point Authentication rules and Cisco router dynamic rules can be shadowed, but they do not shadow other rules. Cisco firewall dynamic rules are treated as regular (non-dynamic) rules.

For Check Point policies, VPN rules can be shadowed but are not recognized as shadowing other rules.

Creating a Policy Analysis Query

Policy Analysis displays all of the rules that could handle traffic defined in the query. Any rule which matches the traffic, even partially, is shown.

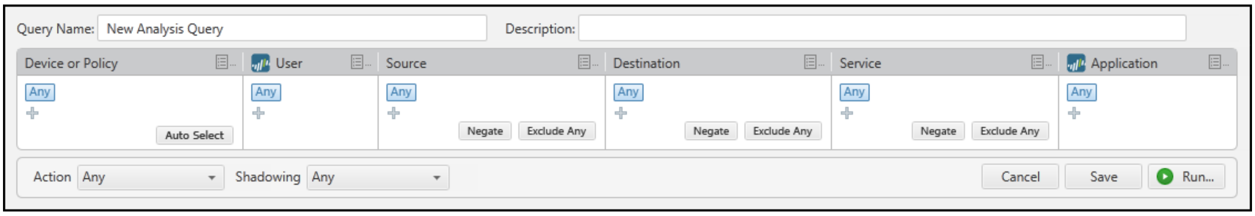
- Within the rule, objects that match the query are highlighted.
- In group object membership details, matching members are highlighted.
- The traffic path shows where the source, destination, or service is changed by Check Point NAT rules and Juniper interfaces in NAT mode using MIP.



To create a Policy Analysis query:

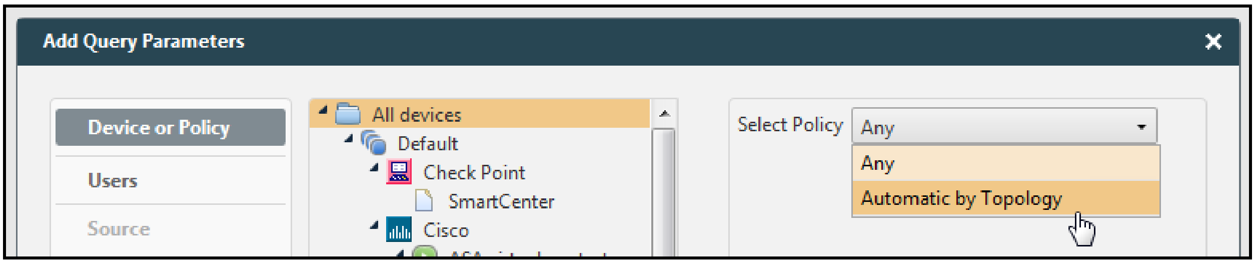
1. Click New Query .
2. Configure the query:

   You can either click the plus + to add query parameters for each field or click ☰… to use advanced options, including selecting objects from devices. The query returns rules that match at least one object in each query field.



- **Device** or **Policy** - Click the plus ✚ to enter the name of the device to analyze or click **Auto Select** to let the devices be determined by topology calculations. The matching targets are shown as you type.

  Or, click ☰… to select the target from the list of devices.

  For each device or domain, you can select a policy by:

  - **Any** - The policy analysis query runs on all policies in the target.
  - **Automatically by Topology** - Analyze only policies that are configured for interfaces in the path of the traffic between the source and destination in the query according to the routing information in Topology. To do this you cannot use Any for the source or destination.
  - **Choose from policy list** - You can choose specific policies from Check Point targets.

  If you select **All devices** in the device tree, you can select **Any** to run the query on all policies for all devices, or **Automatically by Topology** to only run the query on policies that are configured for interfaces on any device in the path of the traffic between the source and destination.

- **Users** (for Palo Alto only) - Click the plus ✚ to enter the names of the users or groups that you want to find in the policy, or click ☰… to paste the names as a comma-delimited list.

- **Source** and **Destination** - Click the plus ✚ to enter an IP address and netmask for the source or destination that you want to use in the query.

  Or, click ☰… to add sources and destinations by:

  - **IP** - Enter the IP address and netmask, either in decimal (x.x.x.x) or CIDR (xx) notation.
  - **Object** - Select an object that is defined in a monitored device. SecureTrack uses the object definition as it appears in the most recent policy revision from that device.
  - **Zone** - Select a zone that is defined in Zones. You can change the subnets in the zone at any time. SecureTrack uses the subnets in the zones at the time you run the query.

  If you select **Negate**, the query returns all rules using any source or destination except for the ones listed in the query. If you select **Exclude Any**, the query does not return rules that include the source or destination in the form of an **Any** object.

- **Service** - Click the plus ✚ to enter the name of a well-known service to use in the query (such as http or ftp).

  Or, click ☰… to add services by:

  - **Protocol** - Select `TCP` or `UDP` and enter a port number, select `ICMP` and enter the ICMP type number, or select `Other` and enter the protocol number. For example: To add HTTP, select `TCP` and enter port `80`. To add OSPF, select `Other` and enter port `89`.

    You can enter the port, type and protocol numbers in these formats:

    - A single number: 80

- A range: 100-200

- An open-ended range of ports with Less Than or Greater Than: >1023

- A combination of the above formats separated by commas: 21, 80-81, >1023

- Negate a single number: !80

You can also type the services into the text editor field. Each line must begin with either TCP, UDP, ICMP or Other and be followed by numbers in the formats above.

- **Object** - Select an object that is defined in a monitored device. SecureTrack uses the object definition as it appears in the most recent policy revision from that device.

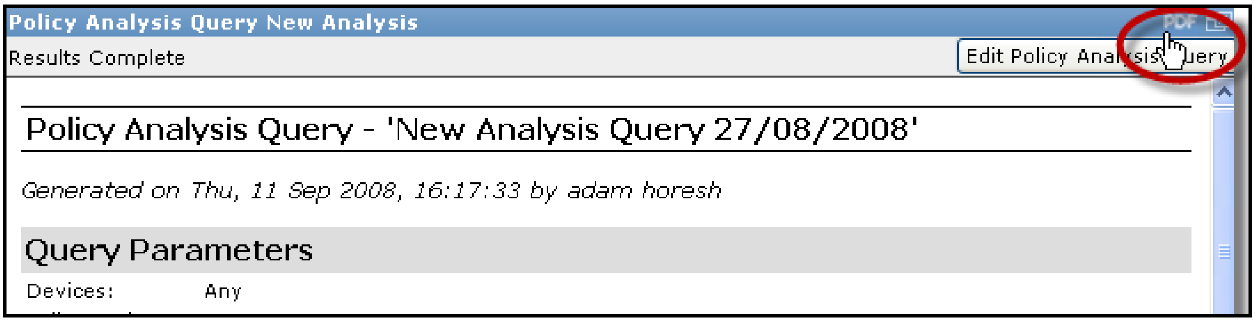
If you select **Negate**, the query returns all rules using any service except for the ones listed in the query. If you select **Exclude Any**, the query does not return rules that include the service in the form of an **Any** object.

- **Application** (for Palo Alto only) - Click the plus + to enter the names of the applications that you want to find in the policy, or click ☰… to paste the names as a comma-delimited list.

3. Select the action of the rules for the query as either **Any** (Allow or Deny), only **Allow**,or only **Deny**.
4. **Shadowing**: Shadowed rules are rules that include some of the parameters defined in the query but will never actually handle any of this traffic because all of the traffic defined in the query is handled by rules higher up in the rulebase. You can choose to filter:
   - **Any** - The results include all rules, and the shadowed and partially shadowed rules are marked in the results
   - **Fully shadowed** - The results only include rules that are fully shadowed so you can clean up your policy
   - **Partially or not shadowed** - The results only include rules that are partially or not shadowed so you can see the rules that actually affect the network traffic
5. Either:
   - Click **Save** to save the query. You can then select the report and **Run**, **Edit**, or **Delete** it.

     You can schedule a saved query to run automatically in a Policy Analysis report.
   - Click **Run** to see the results immediately. When you run the report, you must select to run the report on either:
     - **Last revision** - The last revision received by SecureTrack, even if the revision was not installed on a device
     - **Last installed** - The last revision received by SecureTrack that was installed on a device
     - **Date and time** - Select a date and time and the query will run on the last revision that was received before that time

After you run a query, you can convert the results to a PDF:



Policy Analysis Query New Analysis
PDF
Edit Policy Analysis Query

Results Complete

Policy Analysis Query - 'New Analysis Query 27/08/2008'

Generated on Thu, 11 Sep 2008, 16:17:33 by adam horesh

Query Parameters

Devices: Any

How Do I Get Here?

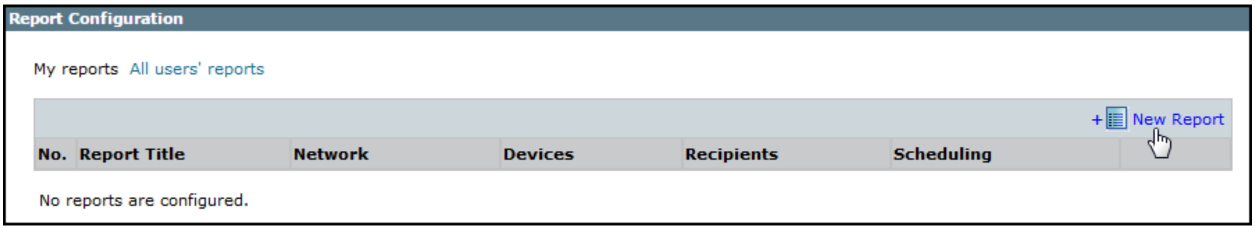
In SecureTrack, go to **Reports** > **Policy Analysis**.

Scheduling a Policy Analysis Report

The Policy Analysis report enables you to run periodically scheduled Policy Analysis queries and automatically send the report to recipients.

To schedule a Policy Analysis report:

1. Go to **Reports** > **General Reports**, and click **New Report.**

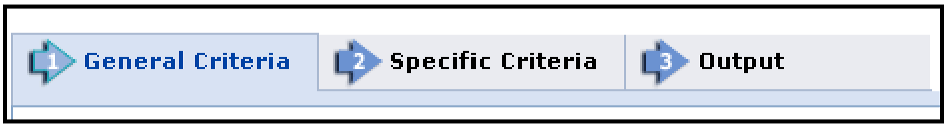
   

   Report Configuration

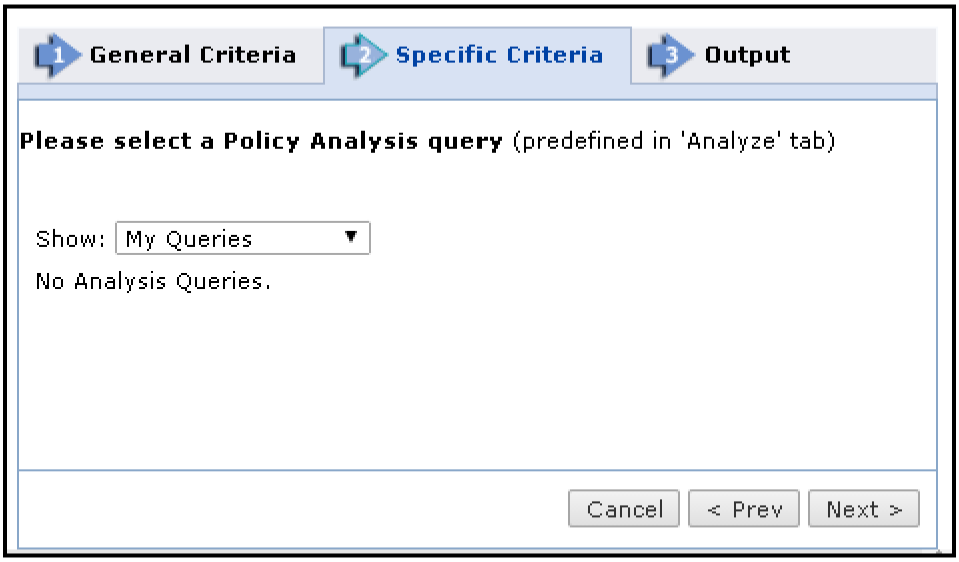
   My reports All users' reports

No.	Report Title	Network	Devices	Recipients	Scheduling
No reports are configured.					

   The report configuration wizard has 3 steps.

2. **STEP 1**: Configure the **General Criteria** and click **Next**. a query from a list of saved queries and click **Next**.
   1. For **Report Type**, select **Policy Analysis**.
   2. Optionally, you can change the **Title**. By default, the report's general name with the current date is the report name.
   3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
   4. Select **Devices** for the report.
   5. If you have selected one domain, you can limit the report to include specific devices in the domain.
      If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.
3. **STEP 2**: Configure the **Specific Criteria** as explained in the table and click **Next**.

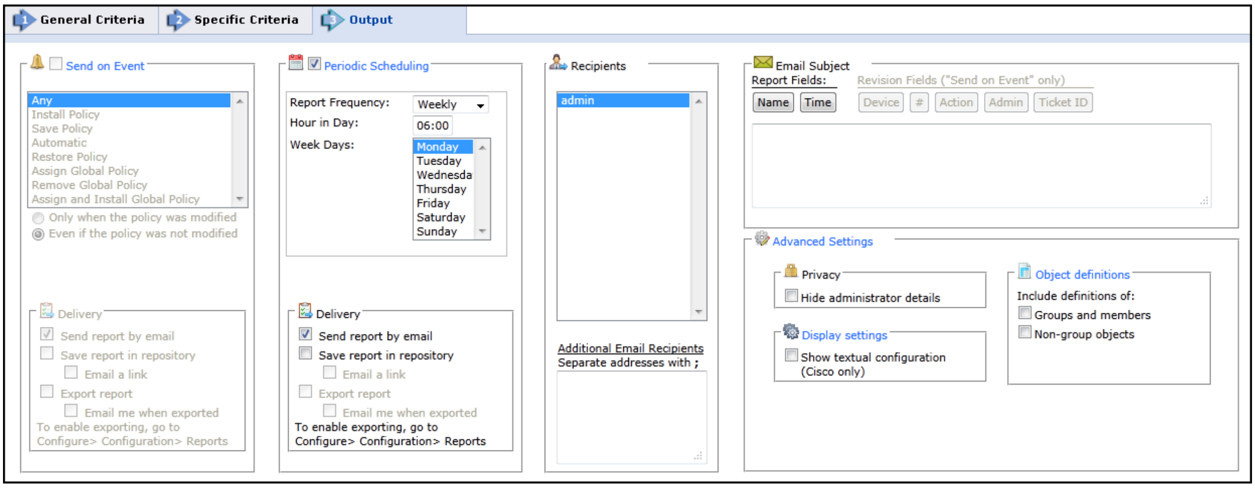
   Please select a Policy Analysis query (predefined in 'Analyze' tab)

   Show: My Queries ▼

   No Analysis Queries.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list. From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✕) it.



□ Send on Event
○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling
Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients: admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name Time

Privacy
□ Hide administrator details

Display settings
□ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
□ Groups and members
□ Non-group objects

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation. The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them. The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page. A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page. To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view). Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification). When a SecureTrack User creates a report, only that User is a recipient. When a SecureTrack Administrator creates a report, multiple recipients can be defined. These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack. Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. Note: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses. Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results. Only the ticket ID is included. This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**:

- **Groups and members** - The report includes the definitions of group objects and their member objects. This is useful for recipients that do not have SecureTrack access. SecureTrack users can click on group objects in the report to see the definitions.
- **Non-group objects** - The report includes definitions of non-group objects.

Object Lookup

Object Lookup shows the rules and groups in which an object is used - across all devices, in a device branch (a selected device with its child devices), or in a single, selected device. In large network environments, it is common to have objects on many network devices that represent the same network resource. It is important to make sure that all of these objects follow your naming convention, that their IP addresses are correct, and that they are used in the correct rules and groups.

Note: IPv6 is supported for this feature, as follows: You can search for IPv6 objects by object name and you can search for IPv6 addresses as text in source and destination.

The search results show all of the objects in the selected devices that match either:

- **Text** in the name, IP address or comment fields - You can also search for exact matches (not case-sensitive) of the search text to narrow the results. By default, the results show all matching objects in all devices, but you can select one or more specific devices to search in.
- **Subnet** defined by IP address and netmask - You can show the objects that contain the subnet that you enter, objects that are contained in the subnet that you enter, or objects that match the subnet exactly.

  For example:

  Subnet that contains - If you enter the subnet 10.10.10.0/24, the results include network objects such as 10.10.0.0/16 and 10.10.10.0/24. If you enter the subnet 10.10.10.1/32, the results include host objects that have the IP address 10.10.10.1.

  Contained in subnet - If you enter the subnet 10.10.0.0/16, the results include network objects such as 10.10.10.0/24 and hosts such as 10.10.10.1/32.

Icons in the **Name** column indicate the following:

Icon	Represents
	Host object / Global host object
	Subnet or range / Global subnet or range
	Group object / Global group object

After you search for objects, you can select an object from the search results and see the rules or groups where the object is used, either explicitly or as part of a group object. You can click **Export** to save the results to a PDF file.

In **Analyze** *>* **Object Lookup***, to search for an object and the rules and groups where the object is used:*

1. From the device tree, select either:
   a. All devices
   b. A parent device with its child devices
   c. A single device
2. Select the **Text** or **Subnet** search and its parameters.
   - To search in all devices, enter the text or a subnet to search for in the search field and press **Enter**.
   - To search in specific devices, select the devices to search in from either the Vendors or Groups tree and enter the text or a subnet to search for in the search field and press **Enter**.

   For text, the parameters are: All, IP, Name, Comment

   For subnet, the parameters are:

   - Subnets that contain - Shows all networks that include the specified subnet, including the subnet itself even if it is a host.
   - Contained in subnet - Shows all objects that have an IP address in the subnet, including the subnet itself.
   - Exact match - Shows only objects that are defined with the specified subnet.
3. Select an object from the list.

The rules where the object is used are shown. By default, the list only includes rules where the object is used explicitly. You can also select **Show rules with object and related groups** to show rules that include groups that contain the selected object.

4. Click **Objects** to see the groups that contain the selected object, and click on a group to see the other objects that are contained in the group.

How Do I Get Here?

In SecureTrack, go to **Analyze** > **Object Lookup**

Automatic Policy Generation

SecureTrack's Automatic Policy Generator™ (APG) automatically creates a secure, effective, and optimized firewall rulebase, limiting allowance of traffic not actually used in your organization.

The APG can be used for:

- Creating a new rulebase, as when deploying a new firewall or adding an interface to a firewall.
- Tightening overly permissive rules.
- Network forensics, such as discovering specific traffic patterns on the network.

This chapter describes the APG included in the SecureTrack web interface. The Legacy APG CLI tool is still available and is described in Automatic Policy Generator (APG) CLI.

IPv6 is not supported for this TOS feature.

How APG Works

The APG analyzes firewall logs (Getting Logs for APG, Collecting Log Files) to determine actual business practices, and creates an optimized rulebase that limits traffic allowance to traffic actually used in the organization.

If you have an existing rulebase, APG identifies the permissiveness level of each 'accept' rule, on a scale from 1 to 100. Permissiveness measures how widely a rule is defined:

- A rule with one source host, one destination host and one service has the smallest value - 1
- A rule with Source "ANY", Destination "ANY" and Protocol "ANY" has the highest value - 100

Rules with high permissiveness can be a security risk because they allow too much access through the firewall. You can use APG to generate tighter, more granular replacement rules, based on actual traffic logs.

If you do not yet have a firewall policy in place, you can begin by configuring a relatively permissive policy, and leave it in place long enough to produce logs. Then, use the APG to translate these logs into a secure, optimized rulebase.

Once logs have been collected and analyzed, APG provides interfaces for selecting the desired balance between rule granularity (less permissive and therefore more secure) and simplicity (fewer rules and therefore more manageable and potentially better performance). For example, if traffic to a specific destination over a specific service comes from several individual sources, you can select to have a rule for each source, thus providing maximum security, or, you can allow traffic from a generalized subnet, thus reducing them to a single rule.

After generating a policy, you should review it to make sure it isn't reflecting illegitimate traffic. For example, a slow port scan or a generic botnet may have been active in the organization and generating logs. In this case, remove this traffic from the log set and generate a new policy.

Because a rulebase generated by APG closely reflects actual traffic in an organization, this rulebase is also useful for visualizing network traffic as a rulebase, even for purposes other than actually replacing the firewall rulebase. For example, if you want to see all the traffic to and from a specific network, you can select to produce a maximum-granularity rulebase that can be read as a list of source-destination-service sets describing traffic.

Getting Logs for APG

You can either:

- Configure the APG job to collect logs directly from the device so that you can analyze future traffic
- Upload existing logs from Check Point or other devices to an APG job so that you can analyze past traffic

You cannot use the logs that SecureTrack stores for the Rule and Object Usage report as the log source for APG.

Getting Log Files for Upload

You can upload log files from your device to an APG job so that you can analyze past traffic, but you must first prepare the log files so that they are in the correct format for analysis. For Check Point devices, you can also do this from the command line.

To prepare log files from firewall devices:

1. Collecting the log files from the firewall for the desired time frame.
2. Remove all logs not related to traffic.
3. Remove drop logs (unless you are analyzing dropped traffic).
4. Filter for other values, if necessary.
5. Identify and extract the relevant fields (source; destination; port; IP-protocol) in the logs.
6. Convert the field values to the standard format: `source destination port IP-protocol`

   For example:

   `10.0.0.1 192.168.1.2 22 6`

   `32.1.33.2 192.168.1.2 53 17`
7. Store the results in a single file.

Getting Check Point Logs for Upload

You can manually fetch Check Point logs with Check Point's `fwm logexport` command, and then standardize them as with non-Check Point logs.

SecureTrack offers a simpler alternative method, using our `st_apg_collect` tool for automatically collecting, standardizing, and filtering Check Point logs. The `st_apg_collect` utility is included in the TOS installation and is typically run in the command line of your SecureTrack machine. When using this tool, SecureTrack takes the logs for the specified time frame from any relevant log files, filters and standardizes them, and generates an output file in the required format for the APG.

You can limit log collection by rule UID or action (drop/accept), and/or by policy package and/or by gateway. This can be useful for forensic purposes as well.

When using the output for an APG job in SecureTrack, if you want to filter the logs by rule you must do that manually in the output before you send it to the APG. When using the output for the APG CLI, you can filter the output by rule and traffic pattern in the APG configuration.

Procedure

To collect and prepare Check Point logs for the APG:

1. Get the SecureTrack device ID for the monitored Check Point management server.

   To see the ID of a device:

   - Either use the command line on the SecureTrack host:

     ```
     # st stat
     ```

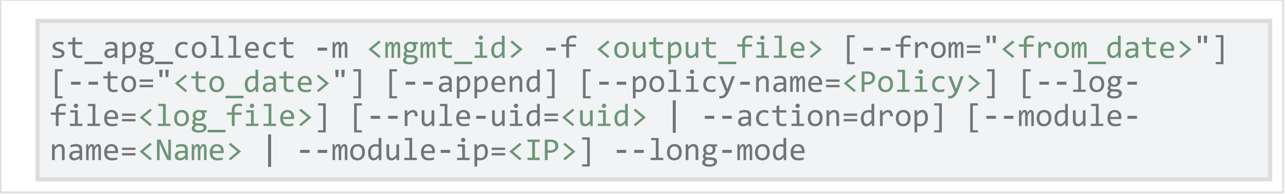
   - Or click the device in the SecureTrack device tree in **Compare** > **Compare Revisions**, and type the letter **t**
2. Before collecting the logs, you can view a list of available log files, by running the `st_apg_collect` utility on your SecureTrack machine:

   ```
   st_apg_collect -m <mgmt_id> --list
   ```

   where `<mgmt_id>` is the SecureTrack device ID for the monitored Check Point management server or for the CLM that is associated with the monitored CMA..

   For each log file, the following is displayed:

   - **File name**: If the default naming has been used, the current file is named fw.log, and all other files are named according to the date and time they were closed.
   - **File time**: The date and time of the first log in the file.
   - **Number of records** in the file.
3. Decide on a time frame for which to collect logs, and run:

   ```
   st_apg_collect -m <mgmt_id> -f <output_file> [--from="<from_date>"]
   [--to="<to_date>"] [--append] [--policy-name=<Policy>] [--log-
   file=<log_file>] [--rule-uid=<uid> | --action=drop] [--module-
   name=<Name> | --module-ip=<IP>] --long-mode
   ```

   where:

- `<mgmt_id>` is the SecureTrack device ID for the monitored Check Point management server or for the CLM that is associated with the monitored CMA..
- `<output_file>` is the path and filename for the generated log file.
- `<from_date>` is the date (and optionally, time) from which to collect logs. This value must be included in quote marks, and its format is:

  `yyyy-mm-dd [hh:mm:ss]`
- `<to_date>` is the date (and optionally, time) until which to collect logs. This value must be included in quote marks, and its format is:

  `yyyy-mm-dd [hh:mm:ss]`
- `--append` indicates that the generated log file should be added to an existing log file, if found, rather than overwrite it.
- `<Policy>` is the name of a policy package. The `--policy-name` flag is used to limit log collection to logs from this package.
- `<log_file>` is the name of a log file. The `--log-file` flag is used to limit log collection to this log file.
- `<uid>` is a rule UID, to limit log collection to logs generated by this rule.
- `--action=drop` limits log collection to drop and reject actions. When this flag is not used, log collection is limited to accept, authenticate, and encrypt actions (unless the `--rule-uid` flag is used, in which case the logs for that rule are collected, regardless of action).

  The `--action` and `--rule-uid` flags cannot both be used.
- `<Name>` is the case-sensitive name of a gateway. The `--module-name` flag is used to limit log collection to logs from traffic handled by this gateway.
- `<IP>` is the primary IP address of a gateway. The `--module-ip` flag is used to limit log collection to logs from traffic handled by this gateway.

  The `--module-name` and `--module-ip` flags cannot both be used.
- `--long-mode` exports verbose data for each log record. This is needed for historical rule usage.

Creating an APG Job

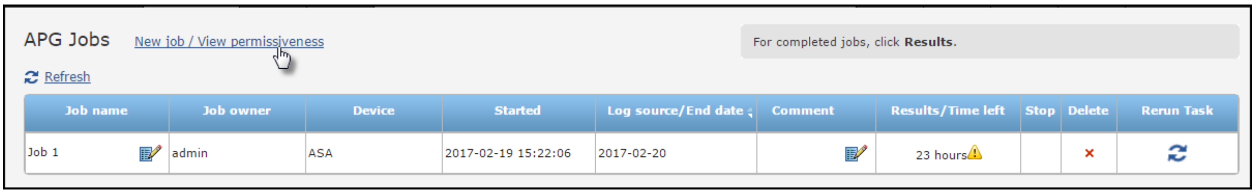
An APG job:

1. Accepts log files or automatically collects logs for a defined time period.
2. Filters the logs by a selected policy rule.
3. Analyzes the logs, and defines the possible rule configurations for varying levels of granularity.

When a job is completed, you can configure the results.

To create an APG job:

1. In **Analyze** view, in the **Automatic Policy Generator** tab, click **Continue** (if no jobs are configured) or **New job** (if there is a job list):



APG Jobs New job / View permissiveness

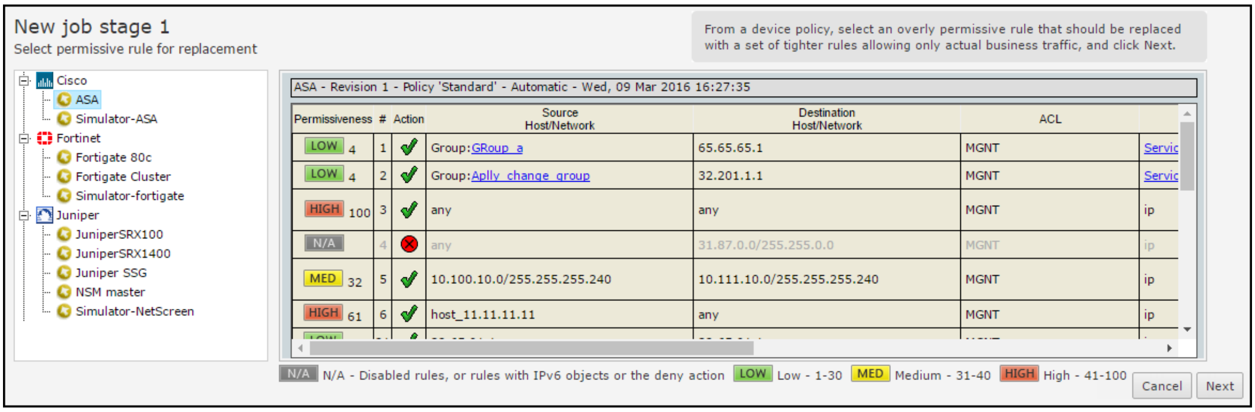
For completed jobs, click **Results**.

Refresh

Job name	Job owner	Device	Started	Log source/End date	Comment	Results/Time left	Stop	Delete	Rerun Task
Job 1	admin	ASA	2017-02-19 15:22:06	2017-02-20		23 hours⚠		×	↻

2. In the device tree on the left, select the relevant device.

   The device's policy is shown. Each 'accept' rule is assigned a permissiveness score. Rules with medium or high permissiveness can be a security risk because they allow too much access through the firewall.



New job stage 1

Select permissive rule for replacement

From a device policy, select an overly permissive rule that should be replaced with a set of tighter rules allowing only actual business traffic, and click Next.

- Cisco
  - ASA
  - Simulator-ASA
- Fortinet
  - Fortigate 80c
  - Fortigate Cluster
  - Simulator-fortigate
- Juniper
  - JuniperSRX100
  - JuniperSRX1400
  - Juniper SSG
  - NSM master
  - Simulator-NetScreen

ASA - Revision 1 - Policy 'Standard' - Automatic - Wed, 09 Mar 2016 16:27:35

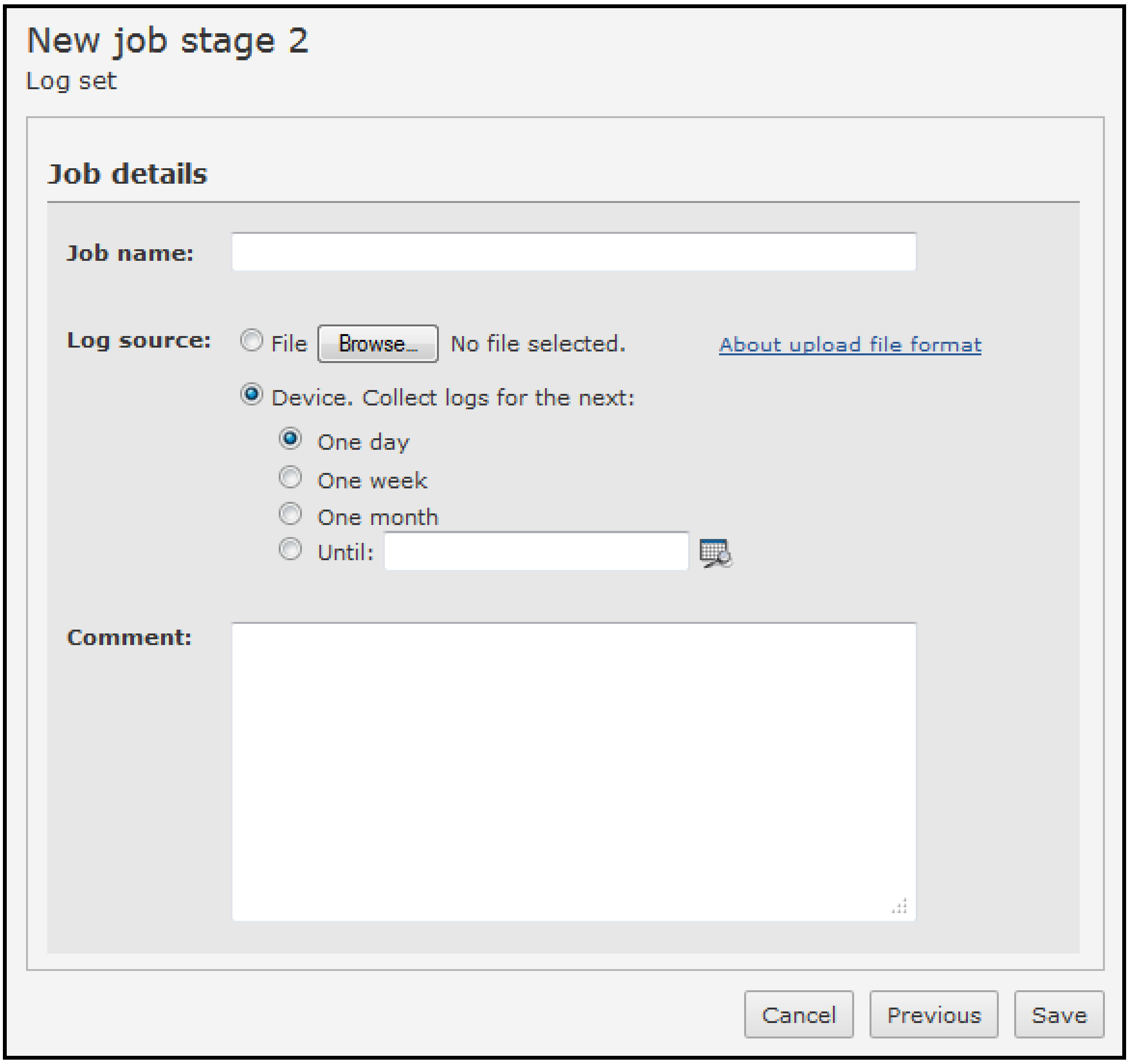
Permissiveness	#	Action	Source Host/Network	Destination Host/Network	ACL	
LOW 4	1	✓	Group:GRoup_a	65.65.65.1	MGNT	Servic
LOW 4	2	✓	Group:Aplly_change_group	32.201.1.1	MGNT	Servic
HIGH 100	3	✓	any	any	MGNT	ip
N/A	4	⊗	any	31.87.0.0/255.255.0.0	MGNT	ip
MED 32	5	✓	10.100.10.0/255.255.255.240	10.111.10.0/255.255.255.240	MGNT	ip
HIGH 61	6	✓	host_11.11.11.11	any	MGNT	ip

N/A N/A - Disabled rules, or rules with IPv6 objects or the deny action LOW Low - 1-30 MED Medium - 31-40 HIGH High - 41-100

3. Select the permissive rule you want to replace, and click **Next**.

   If this job collects future logs, the rule selected here defines log filtering, which means that only logs relevant to the job are collected and analyzed. When you upload log files for APG, the selected rule does not affect the analysis or results. In all cases, the selected rule appears at the top of rule set results as the rule that is intended to be replaced.

4. Type a **Job name**, and select one of the following:



New job stage 2

Log set

Job details

Job name:

Log source: ○ File Browse... No file selected. About upload file format

● Device. Collect logs for the next:

● One day

○ One week

○ One month

○ Until:

Comment:

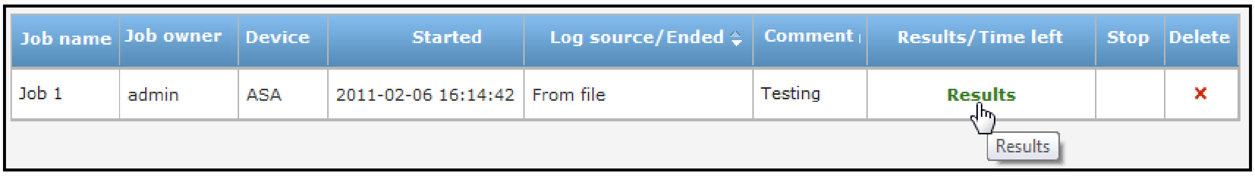
- **File**: Browse to and upload the logs you collected (Getting Logs for APG, Collecting Log Files).
- **Device**: APG will begin collecting logs directly from the monitored device, for the specified period. To define an end date, click:

5. **Save** the job.

Configuring APG Job Results

Once an APG job is completed, APG provides interfaces for selecting the desired balance between rule granularity (less permissive and therefore more secure) and simplicity (fewer rules and therefore more manageable and potentially better performance). For example, if traffic to a specific destination over a specific service comes from several individual sources, you can select to have a rule for each source, thus providing maximum security, or, you can allow traffic from a generalized subnet, thus reducing them to a single rule.

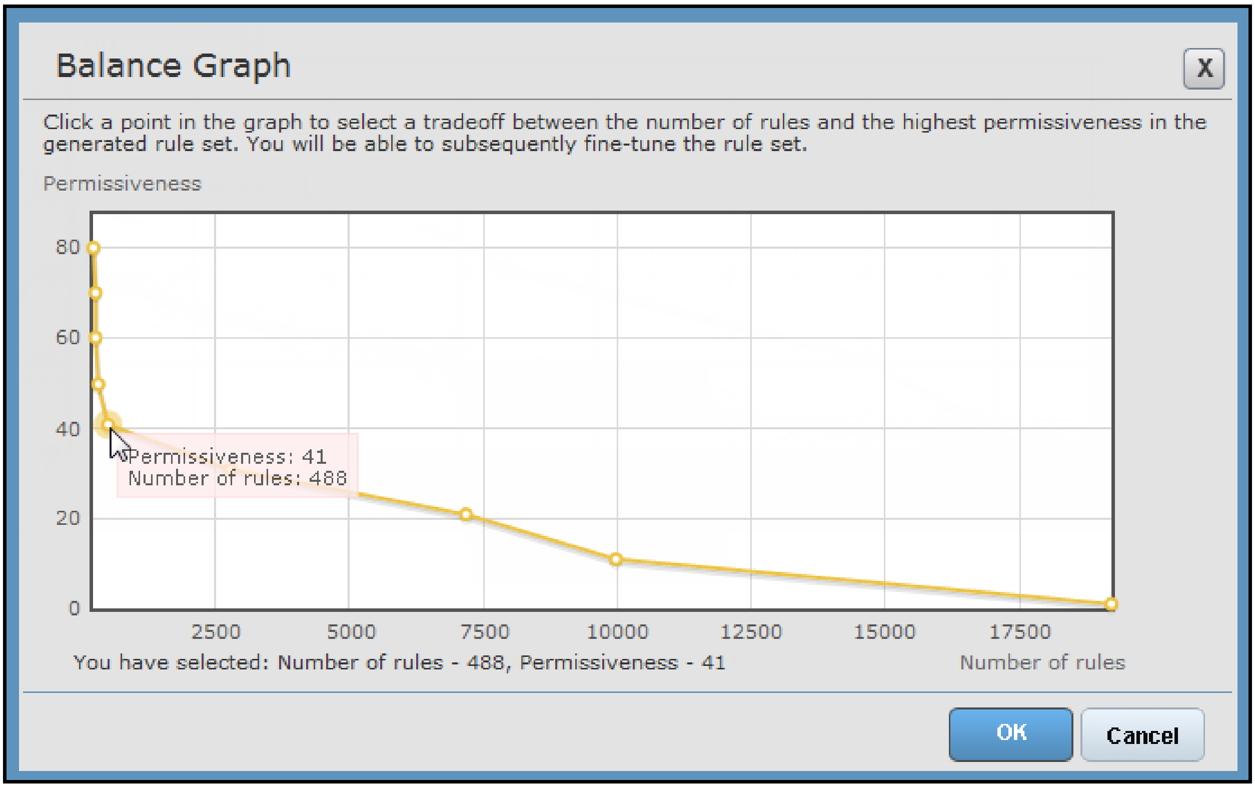
From the Job list, view **Results**:



Job name	Job owner	Device	Started	Log source/Ended	Comment	Results/Time left	Stop	Delete
Job 1	admin	ASA	2011-02-06 16:14:42	From file	Testing	Results		×

APG provides two interfaces for configuring the generated replacement rule set:

- When viewing a job's results for the first time, the **Balance graph** is the first interface presented. The balance graph shows the total number of rules that would result from several options for maximal permissiveness throughout the rule set:



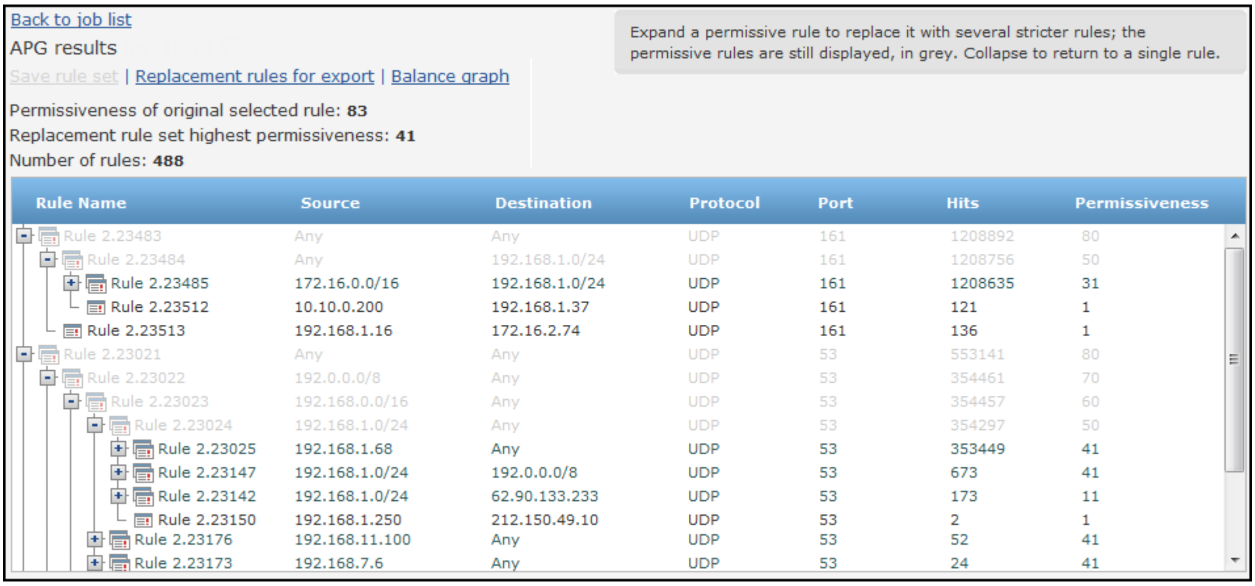
Balance Graph

Click a point in the graph to select a tradeoff between the number of rules and the highest permissiveness in the generated rule set. You will be able to subsequently fine-tune the rule set.

You have selected: Number of rules - 488, Permissiveness - 41

For example, in the above graph, allowing permissiveness of up to about 20 will produce more than 7000 rules; allowing permissiveness of up to 41 will produce very few rules.

- Subsequently, job results are displayed in the **Rule expansion** interface. The Rule expansion interface displays the actual rules, and allows expanding parts of the rule set to multiple, tight rules, or collapsing to single, more permissive rules:



Back to job list

APG results

Save rule set | Replacement rules for export | Balance graph

Permissiveness of original selected rule: **83**
Replacement rule set highest permissiveness: **41**
Number of rules: **488**

Expand a permissive rule to replace it with several stricter rules; the permissive rules are still displayed, in grey. Collapse to return to a single rule.

Rule Name	Source	Destination	Protocol	Port	Hits	Permissiveness
Rule 2.23483	Any	Any	UDP	161	1208892	80
Rule 2.23484	Any	192.168.1.0/24	UDP	161	1208756	50
Rule 2.23485	172.16.0.0/16	192.168.1.0/24	UDP	161	1208635	31
Rule 2.23512	10.10.0.200	192.168.1.37	UDP	161	121	1
Rule 2.23513	192.168.1.16	172.16.2.74	UDP	161	136	1
Rule 2.23021	Any	Any	UDP	53	553141	80
Rule 2.23022	192.0.0.0/8	Any	UDP	53	354461	70
Rule 2.23023	192.168.0.0/16	Any	UDP	53	354457	60
Rule 2.23024	192.168.1.0/24	Any	UDP	53	354297	50
Rule 2.23025	192.168.1.68	Any	UDP	53	353449	41
Rule 2.23147	192.168.1.0/24	192.0.0.0/8	UDP	53	673	41
Rule 2.23142	192.168.1.0/24	62.90.133.233	UDP	53	173	11
Rule 2.23150	192.168.1.250	212.150.49.10	UDP	53	2	1
Rule 2.23176	192.168.11.100	Any	UDP	53	52	41
Rule 2.23173	192.168.7.6	Any	UDP	53	24	41

Clicking ⊞ expands rules into tighter rules; ⊟ collapses into fewer rules. Rules in grey are not part of the actual rule set for the current configuration; rather, they indicate what their child rules can be collapsed into. After making changes, make sure to **Save rule set**.

To change the results with the balance graph:

- Click a marked point on the graph to initially configure the rule set accordingly, and **Save** the configuration.

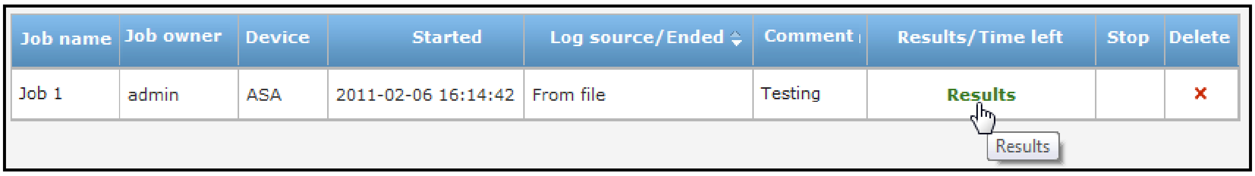
  The rule expansion interface automatically expands according to the balance you defined in the Balance graph.

You can subsequently fine-tune the configuration in the rule expansion interface. You can always click **Balance graph** to return to it.

Viewing and Exporting APG Job Results

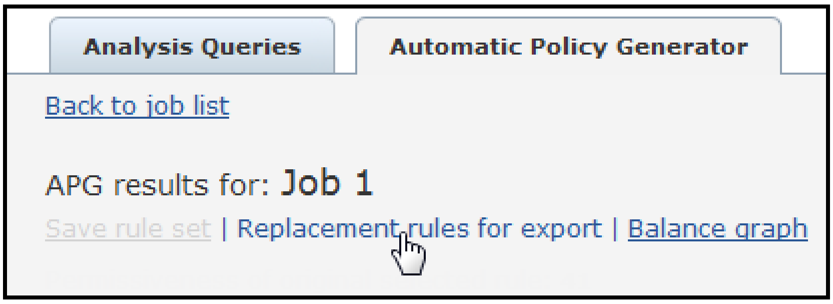
When you are done configuring the results, you can view the results and export then to CSV format.

1. From the Job list, view **Results**:



Job name	Job owner	Device	Started	Log source/Ended	Comment	Results/Time left	Stop	Delete
Job 1	admin	ASA	2011-02-06 16:14:42	From file	Testing	Results		✕

2. From the job results, click **Replacement rules for export**:

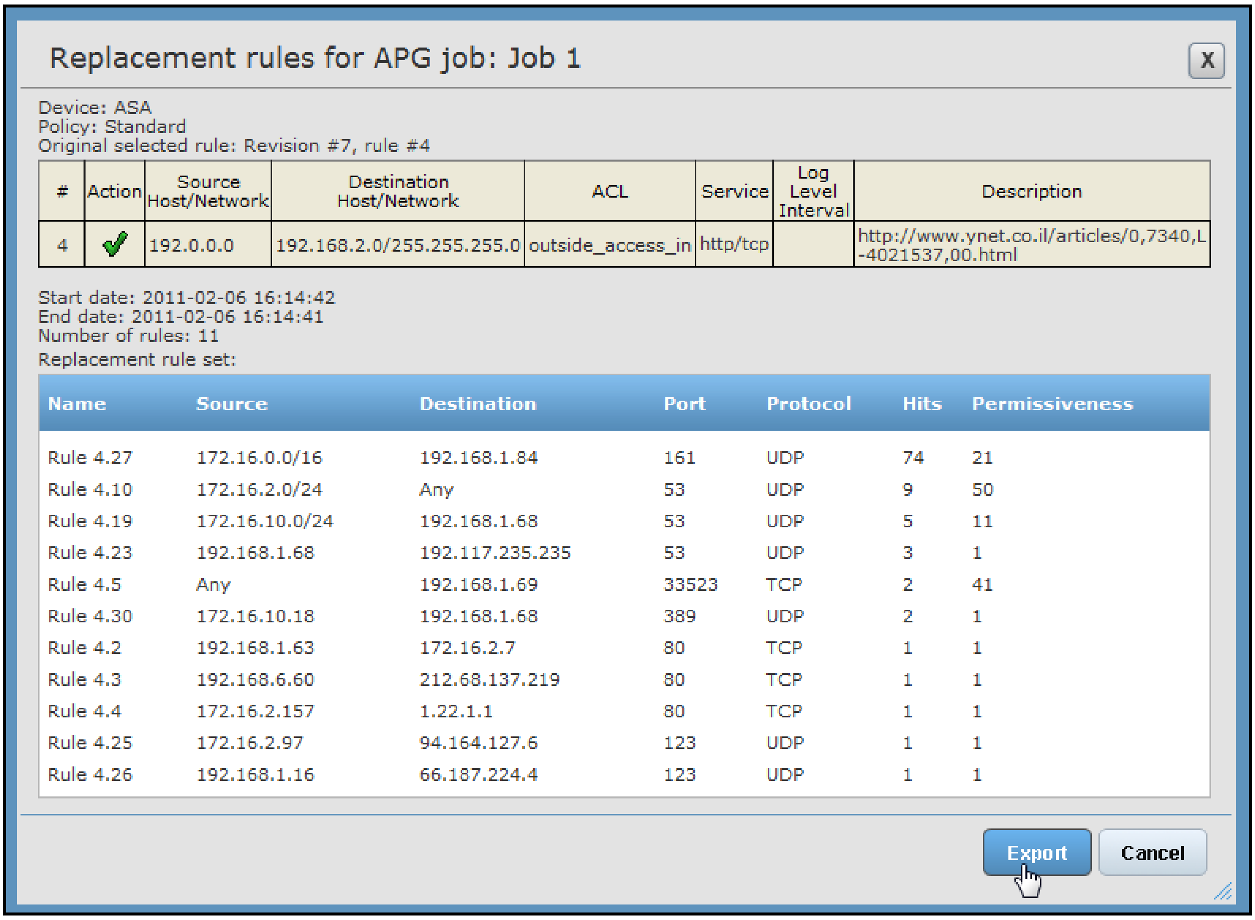


Back to job list

APG results for: Job 1

Save rule set | Replacement rules for export | Balance graph

3. You can then **Export** the rule set to CSV:



Replacement rules for APG job: Job 1

Device: ASA
Policy: Standard
Original selected rule: Revision #7, rule #4

#	Action	Source Host/Network	Destination Host/Network	ACL	Service	Log Level Interval	Description
4	✓	192.0.0.0	192.168.2.0/255.255.255.0	outside_access_in	http/tcp		http://www.ynet.co.il/articles/0,7340,L-4021537,00.html

Start date: 2011-02-06 16:14:42
End date: 2011-02-06 16:14:41
Number of rules: 11
Replacement rule set:

Name	Source	Destination	Port	Protocol	Hits	Permissiveness
Rule 4.27	172.16.0.0/16	192.168.1.84	161	UDP	74	21
Rule 4.10	172.16.2.0/24	Any	53	UDP	9	50
Rule 4.19	172.16.10.0/24	192.168.1.68	53	UDP	5	11
Rule 4.23	192.168.1.68	192.117.235.235	53	UDP	3	1
Rule 4.5	Any	192.168.1.69	33523	TCP	2	41
Rule 4.30	172.16.10.18	192.168.1.68	389	UDP	2	1
Rule 4.2	192.168.1.63	172.16.2.7	80	TCP	1	1
Rule 4.3	192.168.6.60	212.68.137.219	80	TCP	1	1
Rule 4.4	172.16.2.157	1.22.1.1	80	TCP	1	1
Rule 4.25	172.16.2.97	94.164.127.6	123	UDP	1	1
Rule 4.26	192.168.1.16	66.187.224.4	123	UDP	1	1

The results are presented as a replacement for the selected rule; However, if the log source was an uploaded file (not a collection job), and you did not previously filter the log set by the rule, the results are actually for the entire uploaded log set.

APG Customization

To reduce the complexity of APG results, you can use the `apg_ui_conf.xml` XML file in `/usr/local/st/conf` that customizes the results according to your needs. When you modify the parameters in the XML file, you can create more efficient rule sets for to match the traffic in your environment.

The XML file contains all of the tags necessary to customize the APG results. Remove the comment notation (!--) from commented tags that you want to use.

APG customization supports:

- **Service groups** - Service groups are a list of services that are always grouped together in the results. For example, for traffic on services UDP 53-80, TCP53-80, and TCP143, you can define a "UDP53-80,TCP53-80,TCP143" service group with those ports so that hits from a source subnet to a destination subnet on any of these ports are included in one rule with all three services.

  To define service groups, list the service groups in the XML file according to the XML syntax. The Unassigned service group is already defined in the XML file to include all ports that are listed as unassigned by IANA. To enable this service group, remove the comment notation (!--) from the <group> tag of the Unassigned group.

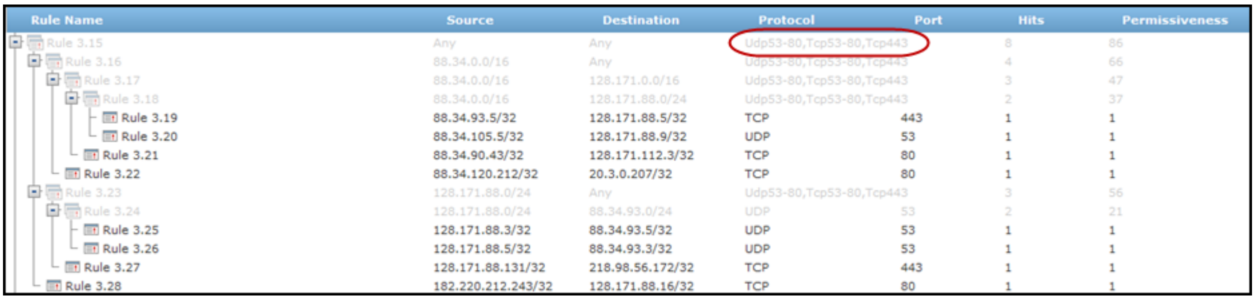
  You can use service groups in the engaged service groups or in predefined rules.

- **Engaged service groups** - Engaged service groups are used to aggregate all hits that include services that match the services in a service group.

  After you define a service group, you can add it to the list of engaged service groups in `<engaged_service_groups>`, for example:

  ```
  <engaged_service_groups>

  <group_name>UDP53-80,TCP53-80,TCP143</group_name>

  </engaged_service_groups>
  ```

In the example below, rules are generated to aggregate hits that use the services in the service group "UDP53-80,TCP53-80,TCP143". In addition, rules are generated for the hits that do not match this service group.

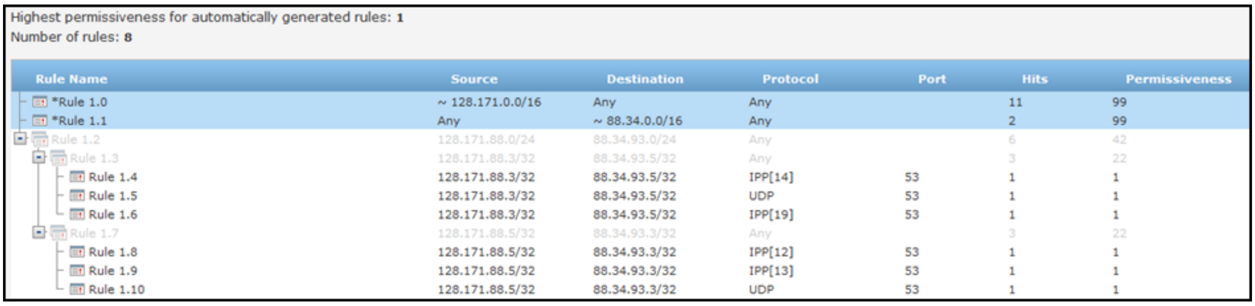


Rule Name	Source	Destination	Protocol	Port	Hits	Permissiveness
Rule 3.15	Any	Any	Udp53-80,Tcp53-80,Tcp443		8	86
Rule 3.16	88.34.0.0/16	Any	Udp53-80,Tcp53-80,Tcp443		4	66
Rule 3.17	88.34.0.0/16	128.171.0.0/16	Udp53-80,Tcp53-80,Tcp443		3	47
Rule 3.18	88.34.0.0/16	128.171.88.0/24	Udp53-80,Tcp53-80,Tcp443		2	37
Rule 3.19	88.34.93.5/32	128.171.88.5/32	TCP	443	1	1
Rule 3.20	88.34.105.5/32	128.171.88.9/32	UDP	53	1	1
Rule 3.21	88.34.90.43/32	128.171.112.3/32	TCP	80	1	1
Rule 3.22	88.34.120.212/32	20.3.0.207/32	TCP	80	1	1
Rule 3.23	128.171.88.0/24	Any	Udp53-80,Tcp53-80,Tcp443		3	56
Rule 3.24	128.171.88.0/24	88.34.93.0/24	UDP	53	2	21
Rule 3.25	128.171.88.3/32	88.34.93.5/32	UDP	53	1	1
Rule 3.26	128.171.88.5/32	88.34.93.3/32	UDP	53	1	1
Rule 3.27	128.171.88.131/32	218.98.56.172/32	TCP	443	1	1
Rule 3.28	182.220.212.243/32	128.171.88.16/32	TCP	80	1	1

- **Predefined rules** - You can define specific rules that you know are required for your device so that analysis runs on all of the traffic that does not match the predefined rules.

  To use predefined rules, list the predefined rules in the XML file according to the XML syntax.

  In the example below, the first two rules are defined in the XML so that rules are only generated for the hits that do not match the predefined rules.

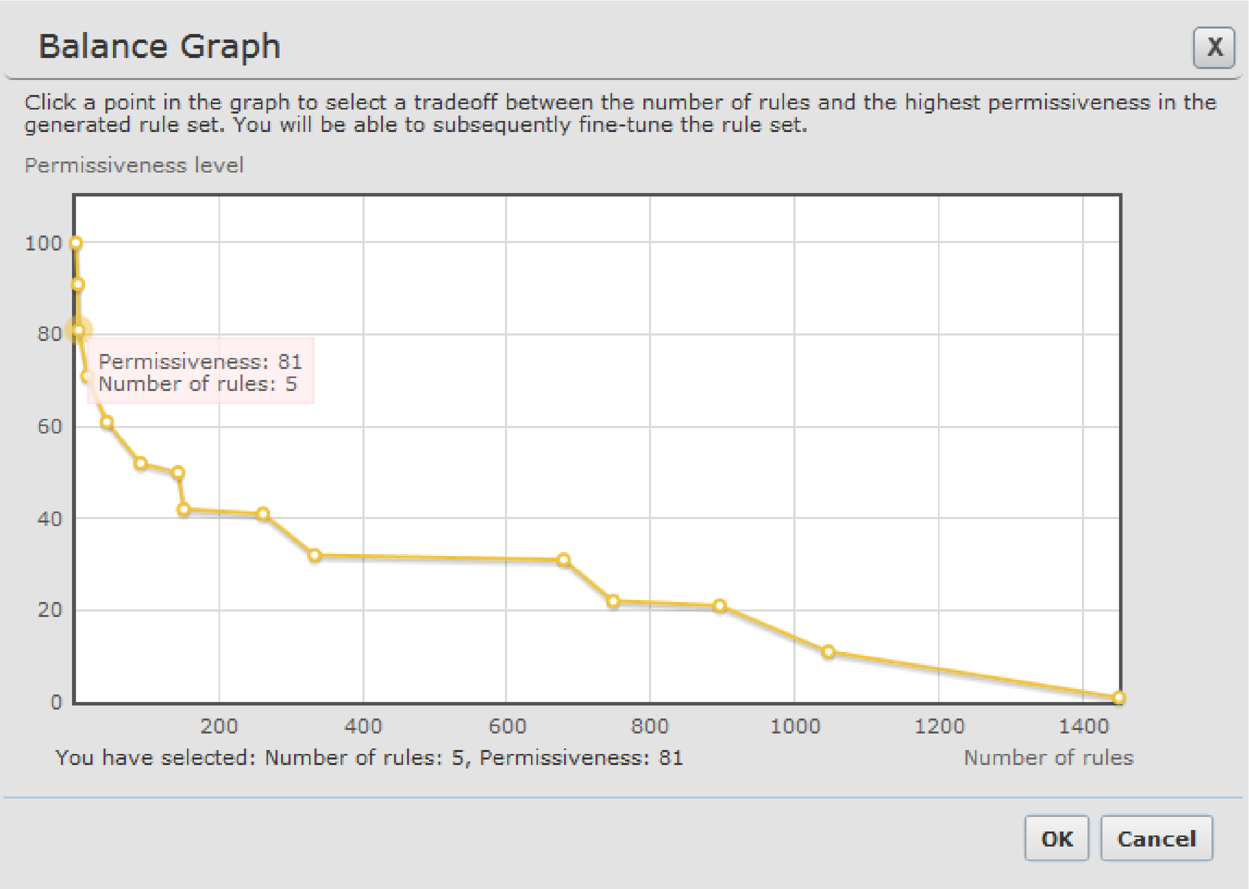


Highest permissiveness for automatically generated rules: **1**
Number of rules: **8**

Rule Name	Source	Destination	Protocol	Port	Hits	Permissiveness
*Rule 1.0	~ 128.171.0.0/16	Any	Any		11	99
*Rule 1.1	Any	~ 88.34.0.0/16	Any		2	99
Rule 1.2	128.171.88.0/24	88.34.93.0/24	Any		6	42
Rule 1.3	128.171.88.3/32	88.34.93.5/32	Any		3	22
Rule 1.4	128.171.88.3/32	88.34.93.5/32	IPP[14]	53	1	1
Rule 1.5	128.171.88.3/32	88.34.93.5/32	UDP	53	1	1
Rule 1.6	128.171.88.3/32	88.34.93.5/32	IPP[19]	53	1	1
Rule 1.7	128.171.88.5/32	88.34.93.3/32	Any		3	22
Rule 1.8	128.171.88.5/32	88.34.93.3/32	IPP[12]	53	1	1
Rule 1.9	128.171.88.5/32	88.34.93.3/32	IPP[13]	53	1	1
Rule 1.10	128.171.88.5/32	88.34.93.3/32	UDP	53	1	1

- **Service aggregation** - You can set APG to automatically group results by service:
  - Intelligent service grouping - This is the most efficient method of creating a restrictive policy according to the network traffic. This is the default method for service aggregation: `<unify_service>1</unify_service>`

    This setting starts with permissiveness 100 (For example, ANY ANY ANY). It finds the segment with the most hits by defining to common source subnet, destination subnet or service and suggests a rule for that. Then it does the same analysis for the remaining rules. The lowest level suggestion will be a rule for each hit.



Balance Graph

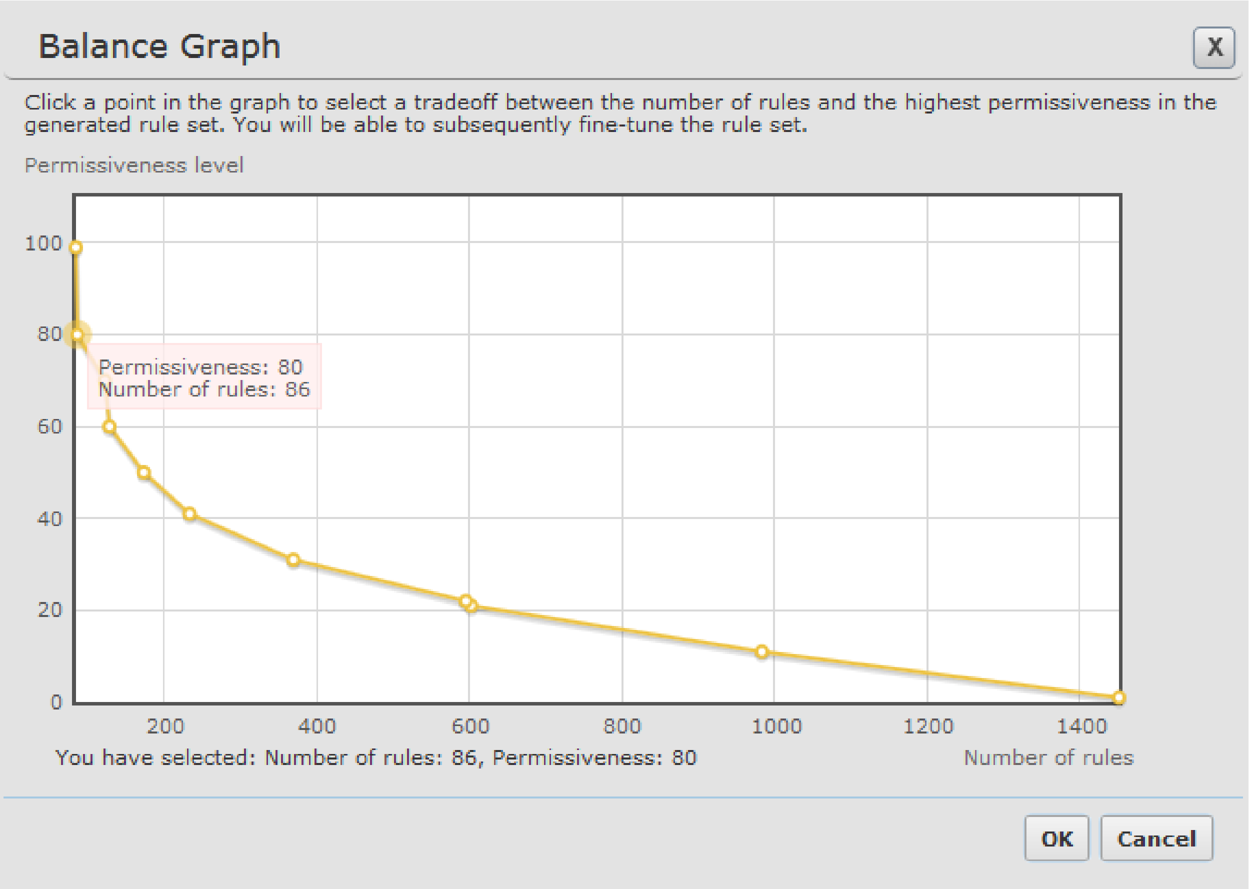
Click a point in the graph to select a tradeoff between the number of rules and the highest permissiveness in the generated rule set. You will be able to subsequently fine-tune the rule set.

You have selected: Number of rules: 5, Permissiveness: 81

- Basic service grouping - . To do this, add the line: `<unify_service>2</unify_service>`

  This setting starts with a rule with permissiveness 80 (For example, ANY ANY <specific service>). It finds the segment with the most hits by defining a common source subnet or destination subnet and suggests a rule for that. The process is repeated for all of the remaining rules. The lowest level suggestion will be a rule for the source, destination and service of each hit.

  Aggregates all services for specific source and destination subnets to ANY. You can expand the results to get rules with specific service values.



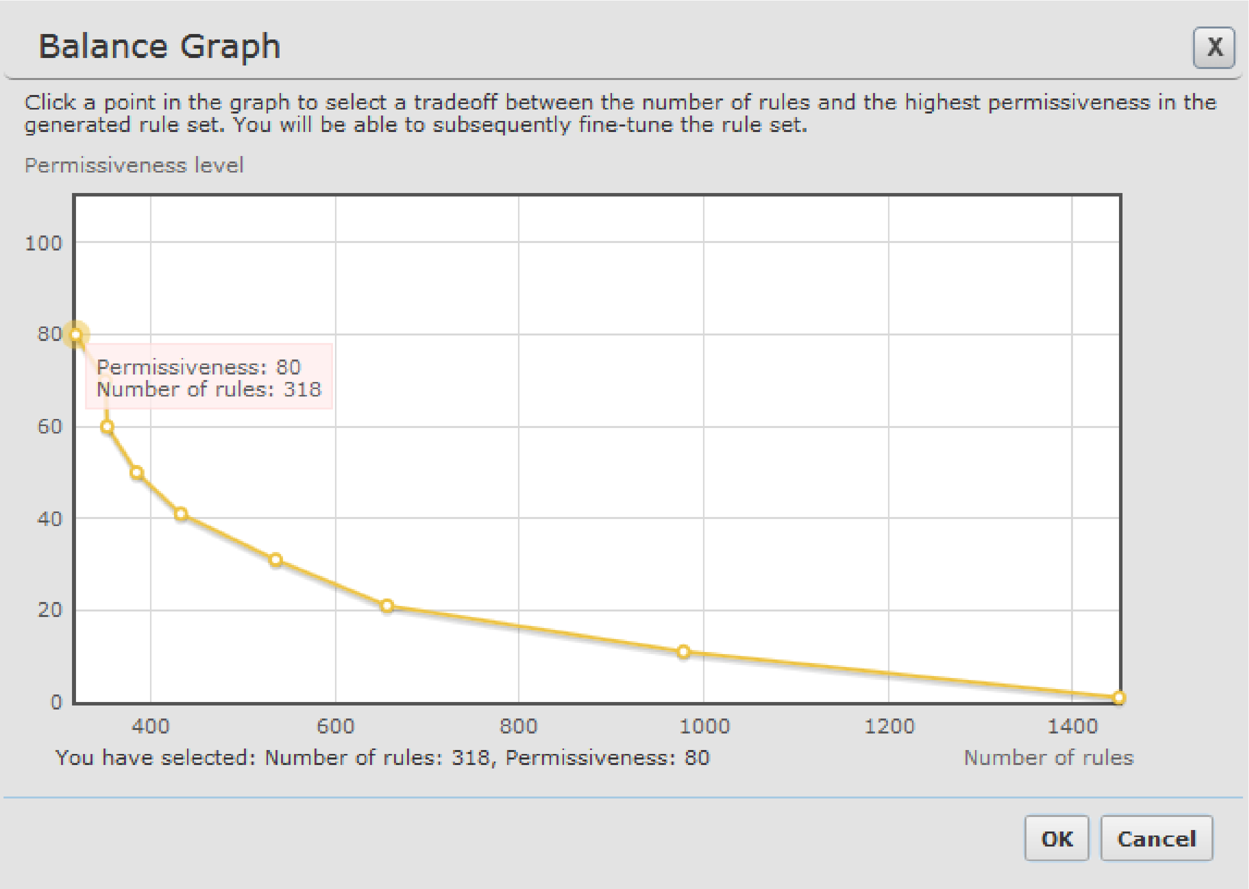
Balance Graph

Click a point in the graph to select a tradeoff between the number of rules and the highest permissiveness in the generated rule set. You will be able to subsequently fine-tune the rule set.

You have selected: Number of rules: 86, Permissiveness: 80

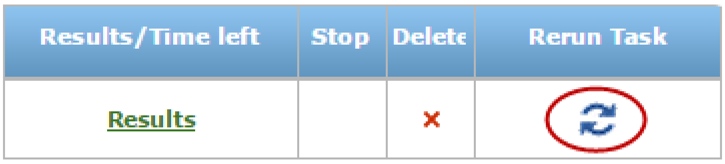
- No service grouping - This is the legacy method of calculating rules. To do this, add the line: `<unify_service>0</unify_service>`

  This setting starts with a rule with permissiveness 80 (For example, ANY ANY <specific service>). It finds the segment with the most hits by defining a common source subnet or destination subnet and suggests a rule for that. The process is repeated for all of the remaining rules. The lowest level suggestion will be a rule for the source, destination and service of each hit.



Balance Graph
X
Click a point in the graph to select a tradeoff between the number of rules and the highest permissiveness in the generated rule set. You will be able to subsequently fine-tune the rule set.
Permissiveness level
100
80
60
40
20
0
Permissiveness: 80
Number of rules: 318
400
600
800
1000
1200
1400
You have selected: Number of rules: 318, Permissiveness: 80
Number of rules
OK
Cancel

- **Rerun job with new XML parameters** - After you save the XML file with your customized settings, you can run the APG job to see the results. If you want to change the XML file to see different APG results, you can edit the XML file and click the Rerun Job button for the job in the APG Jobs list.



Results/Time left	Stop	Delete	Rerun Task
Results		×	

- **Create XML for specific job** - You can also create specific XML files that are used for specific jobs. To do this, run the job and find the `/var/log/st/apg_calc.X` file that ran last. The X is the job ID for the APG job. Then, create an xml file and save it in the format: apg_ui_conf_<job_ID>.xml.

  For example, if you run a job and see that `/var/log/st/apg_calc.10` is the last job to run, duplicate the apg_ui_conf.xml file to `apg_ui_conf_10.xml`. Customize the XML file and click to rerun the job.

APG Customization XML Syntax

Service Group Syntax

In the service group section of the XML file, you can define multiple service groups. Each service group must have a name and a list of members. You can define group members by:

- A single protocol or multiple protocols separated by commas
- A single port or a range of ports

To use service groups, define your service groups in the XML:

Description	Example
	<service_groups>
Give the group a name	<group> <group_name>Web_services</group_name>

	<members>
Define members by protocol and port	<member> <port>443</port> <protocol>6</protocol> </member>
Define members by port range and multiple protocols	<member> <port>80-81</port> <protocol>6,17</protocol> </member>
	</members> </group> </service_groups>

Predefined Rules Syntax

In the predefined rules section of the XML file, you can define multiple predefined rules. Each predefined rule must have a name, source, destination and service.

You can define the source or destination as:

- A single subnet:

  ```
  <subnet>88.34.90.43/32</subnet>
  <negate>0</negate>
  ```

- Multiple subnets

  ```
  <subnet>88.34.90.43/32</subnet>
  <subnet>88.7.90.43/32</subnet>
  <negate>0</negate>
  ```

- Any

  ```
  <subnet>0.0.0.0/0</subnet>
  <negate>0</negate>
  ```

- Any subnet excluding the specified subnet or subnets

  ```
  <subnet>88.34.90.43/32</subnet>
  <negate>1</negate>
  ```

You can define the service as:

- A specific port/protocol:

  ```
  <port>8/1</port>
  ```

- Multiple services that are defined by a service group

  ```
  <group_name>Web_services</group_name>
  ```

- Any

  ```
  <port>Any</port>
  ```

To use predefined rules, list the predefined rules in the XML file according to the syntax below:

Description	XML format
	<predefined_rules> <rule>
Define subnet by IP address with CIDR subnet mask Use negate to define the rule as any subnets not included in the specified subnet	<source> <subnet>128.171.88.3/32</subnet> <negate>0</negate> </source>
Define multiple subnets separated by commas	<destination>

	<subnet>128.171.88.246/24, 88.34.93.3</subnet> <negate>0</negate> </destination>
Use a defined service group as a service	<service> <group_name>Web_services</group_name> </service>
Define the name of the rule	<rule_name>Web accessSource</rule_name>

</rule>

</predefined_rules>

Auditing and Compliance

Best Practice Audits

> This is a Legacy Feature. We recommend you consider using the "Policy Browser" on page 304. This feature allows you to load a much larger number of rules and objects without performance issues.

Most organizations have both formal and informal IT policies.These policies include criteria for security policies, with a variety of requirements, defining what is allowed and what is not allowed in its firewall configuration and rulebases.

SecureTrack's Best Practices feature enables organizations to create best practice baseline policies, and to track violations.The administrator creates the best practice baseline policy by selecting audit checks from a list of industry best practice audit checks for firewalls.

In order to maintain certain minimum security standards in different organizational areas, it is possible to create and maintain a best practices standard for each area.You can choose to run a single Best Practices audit that will apply to all monitored devices, or you may create multiple audits, where each audit will apply to different organizational areas, where each area has differing security needs.

Therefore, you can choose to audit the current active firewall policies as a first step, and subsequently you can audit firewall policies before they are installed.This is a proactive way to ensure compliance to your defined security standards.

You will be presented with the list of best security practices that are stored in the SecureTrack database, and will select which best practices are appropriate for your different organizational areas.Each Best Practices audit check is described in detail in SecureTrack's web interface, along with a pre-defined severity level, and remedial steps needed to resolve configuration errors.

Pre-configured Best Practice audits can be regularly scheduled with a Best Practices Audit report.

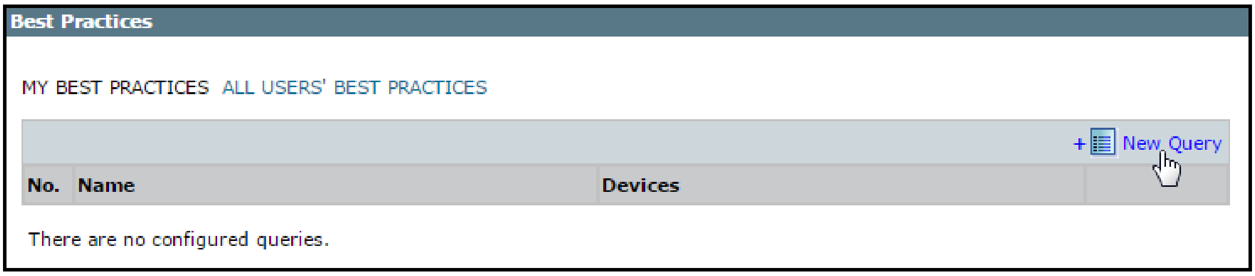
IPv6 is not supported for this TOS feature.

Creating a Best Practices Audit

> This is a Legacy Feature. We recommend you consider using the "Policy Browser" on page 304. This feature allows you to load a much larger number of rules and objects without performance issues.

To create a Best Practice audit:

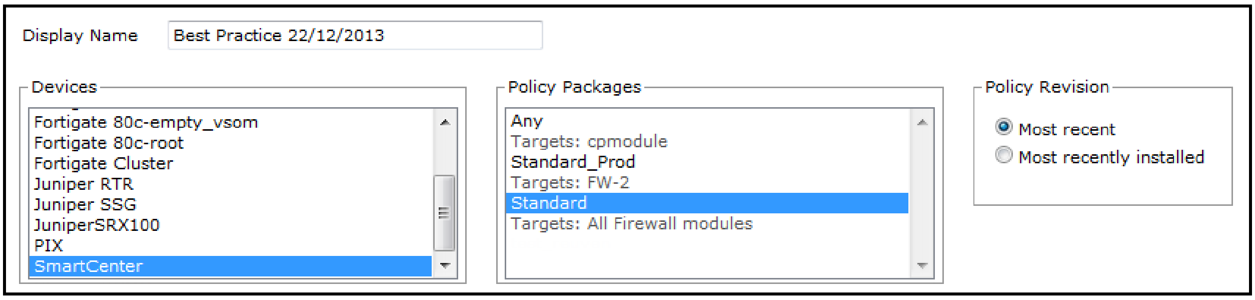
1. Click **New Query**:



No.	Name	Devices

There are no configured queries.

2. The New Best Practices wizard starts:



Display Name: Best Practice 22/12/2013

Devices: SmartCenter

Policy Packages: Standard

Policy Revision: ● Most recent ○ Most recently installed

a. Optionally, you can change the **Title**. By default, the report's general name with the current date is the report name.

b. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.

c. Select **Devices** for the report.

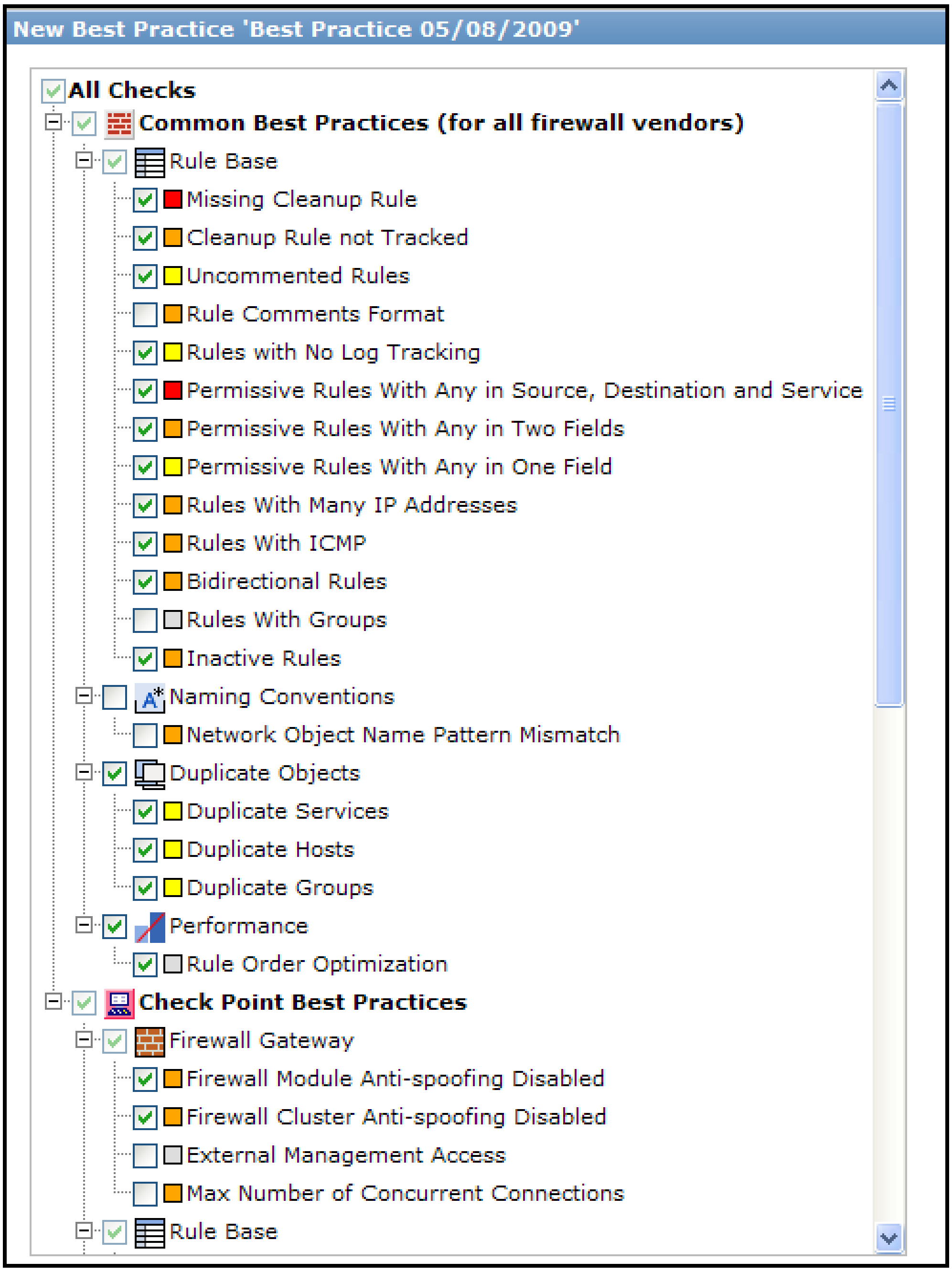
3. If you have selected one domain, you can limit the report to include specific devices in the domain.

   If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.

   For Check Point devices, if you have selected one device, you can limit the report to include specific **Policy Packages**. If you have selected more than one device, then **Any** is selected for **Policy Packages** and all policy packages in the selected devices are included in the report.

4. Select which **Policy Revision** to check: the **Most recent** saved policy (to include Check Point policies that were not installed), or the **Most recent installed** policy.

5. Click **Next**.



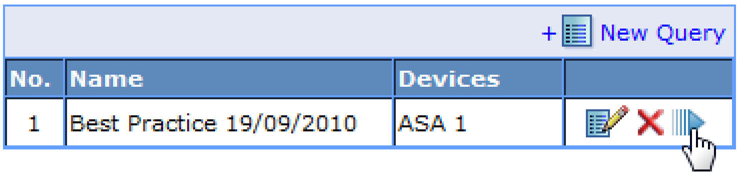
New Best Practice 'Best Practice 05/08/2009'

- ☑ **All Checks**
  - ☑ **Common Best Practices (for all firewall vendors)**
    - ☑ Rule Base
      - ☑ 🟥 Missing Cleanup Rule
      - ☑ 🟧 Cleanup Rule not Tracked
      - ☑ 🟨 Uncommented Rules
      - ☐ 🟧 Rule Comments Format
      - ☑ 🟨 Rules with No Log Tracking
      - ☑ 🟥 Permissive Rules With Any in Source, Destination and Service
      - ☑ 🟧 Permissive Rules With Any in Two Fields
      - ☑ 🟨 Permissive Rules With Any in One Field
      - ☑ 🟧 Rules With Many IP Addresses
      - ☑ 🟧 Rules With ICMP
      - ☑ 🟧 Bidirectional Rules
      - ☐ ⬜ Rules With Groups
      - ☑ 🟧 Inactive Rules
    - ☐ Naming Conventions
      - ☐ 🟧 Network Object Name Pattern Mismatch
    - ☑ Duplicate Objects
      - ☑ 🟨 Duplicate Services
      - ☑ 🟨 Duplicate Hosts
      - ☑ 🟨 Duplicate Groups
    - ☑ Performance
      - ☑ ⬜ Rule Order Optimization
  - ☑ **Check Point Best Practices**
    - ☑ Firewall Gateway
      - ☑ 🟧 Firewall Module Anti-spoofing Disabled
      - ☑ 🟧 Firewall Cluster Anti-spoofing Disabled
      - ☐ ⬜ External Management Access
      - ☐ 🟧 Max Number of Concurrent Connections
    - ☑ Rule Base

The Best Practices list is divided into common best practices, which apply to all vendors, and vendor-specific best practices. Practices are only checked for the relevant devices, so you can safely include both kinds of practices in an audit for devices from multiple vendors.

6. Click **Save**.

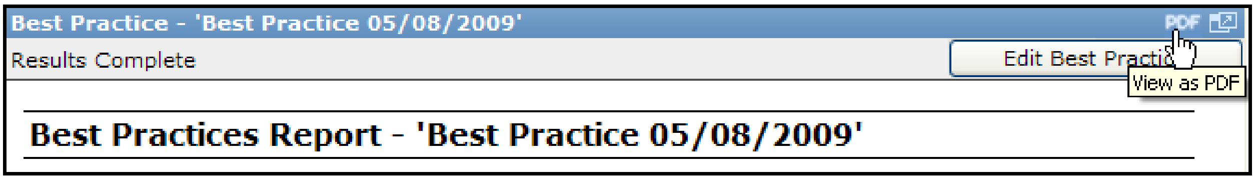
Your configured Best Practices audit is then available to be scheduled as a report, or you can run it manually from the Best Practices list:



+ New Query

No.	Name	Devices	
1	Best Practice 19/09/2010	ASA 1	

Once Best Practices results have been generated, the results can be converted to PDF, by clicking **PDF**:



Best Practice - 'Best Practice 05/08/2009'

Results Complete

Best Practices Report - 'Best Practice 05/08/2009'

How Do I Get Here?

In SecureTrack, go to **Audit** > **Best Practices**.

Scheduling a Best Practices Audit Report

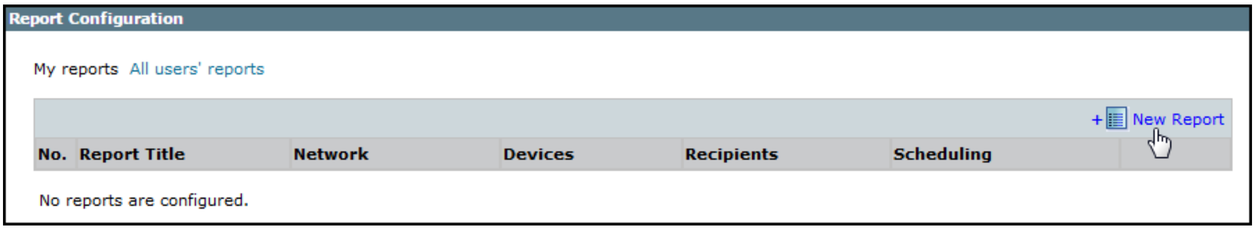
> This is a Legacy Feature. We recommend you consider using the "Policy Browser" on page 304. This feature allows you to load a much larger number of rules and objects without performance issues.

The Best Practices Audit report enables you to run periodically scheduled Best Practices Audits and automatically send the report to recipients.

IPv6 is not supported for this TOS feature.

To schedule a Best Practices Audit report:

1. Click **New Report.+**



Report Configuration

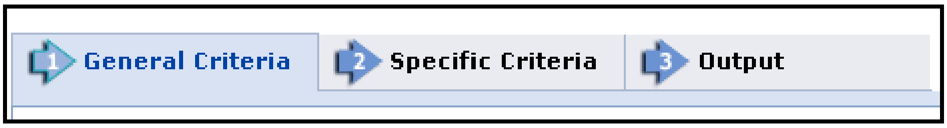
My reports All users' reports

+ New Report

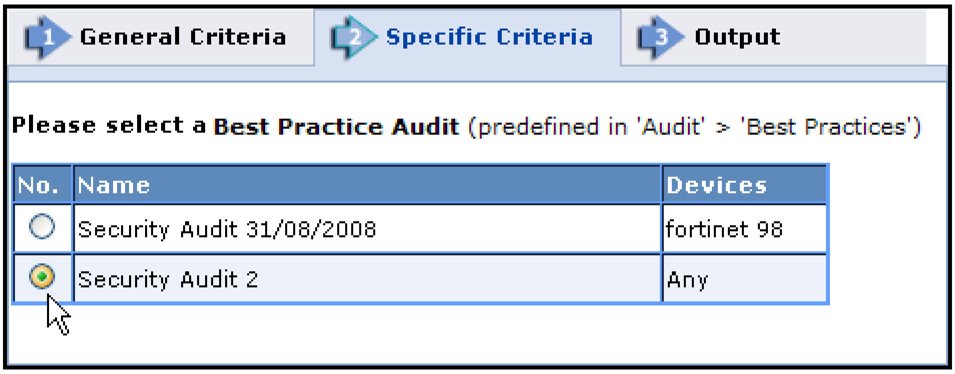
No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.



2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   a. For **ReportType**, select **Best Practices Audit.**
   b. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
3. **STEP 2**: In the **Specific Criteria** tab, select the audit to run from the list of configured audits and click **Next**.



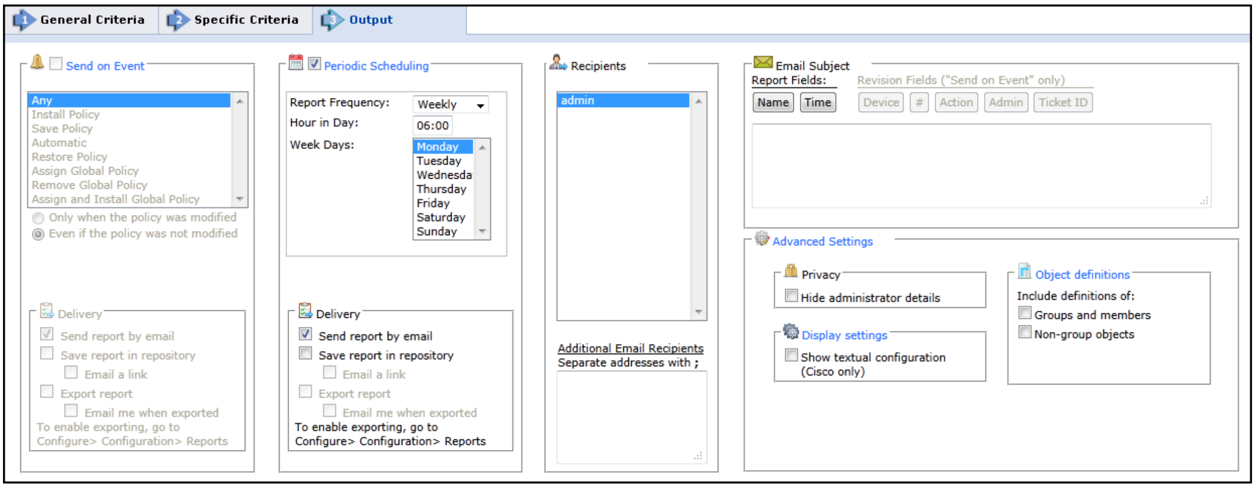
1 General Criteria | 2 Specific Criteria | 3 Output

Please select a **Best Practice Audit** (predefined in 'Audit' > 'Best Practices')

No.	Name	Devices
○	Security Audit 31/08/2008	fortinet 98
●	Security Audit 2	Any

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✕) it.



General Criteria | Specific Criteria | Output

□ Send on Event
Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy
○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling
Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name | Time
Revision Fields ("Send on Event" only): Device | # | Action | Admin | Ticket ID

Advanced Settings
Privacy
□ Hide administrator details
Display settings
□ Show textual configuration (Cisco only)
Object definitions
Include definitions of:
□ Groups and members
□ Non-group objects

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (;) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).

Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**: • **Groups and members** - The report includes the definitions of group objects and their member objects.This is useful for recipients that do not have SecureTrack access.SecureTrack users can click on group objects in the report to see the definitions. **Non-group objects** - The report includes definitions of non-group objects.

How Do I Get Here?

In SecureTrack, go to **Report** > **General Reports**

Regulations Audit Browser

The regulations audit browser lets you view your compliance status at all times in accordance with PCI DSS standard version 3.0 and Sarbanes-Oxley Act of 2002 (SOX).

Instead of periodically validating the status of your organization by running reports to gather the necessary information, the regulations audit browser lets you easily understand your compliance status in real-time.As a result, you can make sure that your organization is continuously compliant with regulations and you can decrease the amount of effort and time required to both prepare and pass an audit.

You can create multiple profiles that represent your organization’s network environment and SecureTrack analyzes every new revision for compliance violations for each profile.

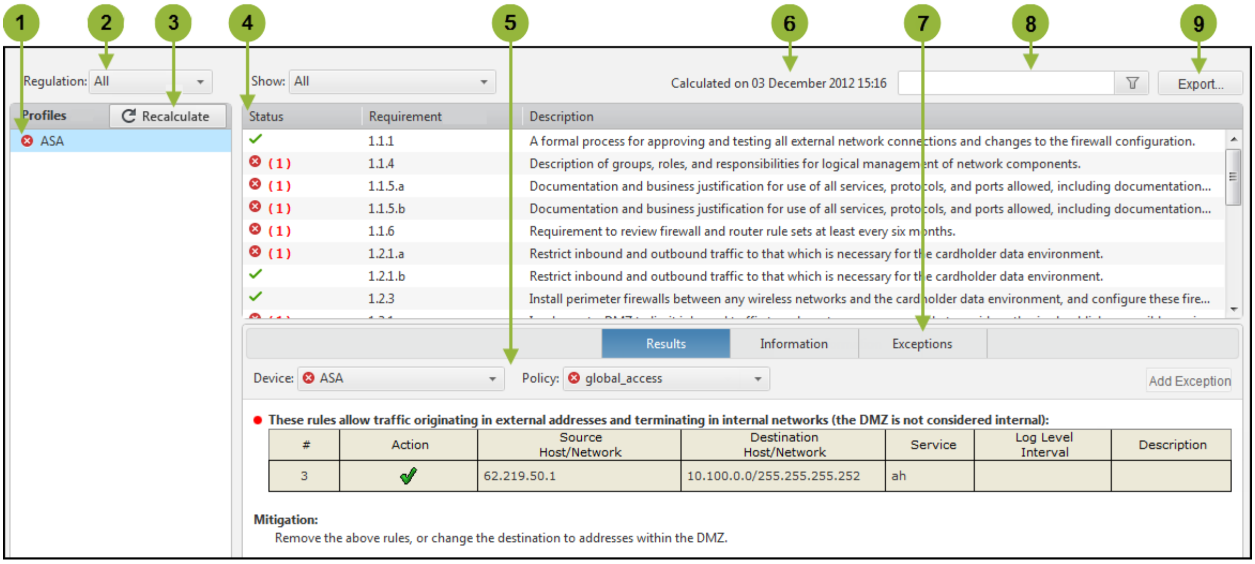
- For more about the PCI DSS standard, see the PCI Security Standards site.
- For more about the Sarbanes-Oxley Act, see the US Securities and Exchange Commission site.

IPv6 is not supported for this TOS feature.

Auditing Compliance with Regulations

After you create a regulations profile, SecureTrack runs all of the tests on the target device selected in the profile every time a new revision is received and when the topology changes. When the tests are completed, you can immediately see which tests passed and which failed, including a detailed analysis of the reason according to the test requirements. You can see the critical violations in the Violations browser.

You can also exclude selected rules from the results as exceptions so that rules that you decide are not relevant to the test do no cause it to fail.



Regulation: All

Show: All

Calculated on 03 December 2012 15:16

Export...

Profiles | Recalculate

✗ ASA

Status	Requirement	Description
✓	1.1.1	A formal process for approving and testing all external network connections and changes to the firewall configuration.
✗ (1)	1.1.4	Description of groups, roles, and responsibilities for logical management of network components.
✗ (1)	1.1.5.a	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation...
✗ (1)	1.1.5.b	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation...
✗ (1)	1.1.6	Requirement to review firewall and router rule sets at least every six months.
✗ (1)	1.2.1.a	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
✓	1.2.1.b	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
✓	1.2.3	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these fire...

Results | Information | Exceptions

Device: ✗ ASA

Policy: ✗ global_access

Add Exception

● **These rules allow traffic originating in external addresses and terminating in internal networks (the DMZ is not considered internal):**

#	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Description
3	✓	62.219.50.1	10.100.0.0/255.255.255.252	ah		

Mitigation:
Remove the above rules, or change the destination to addresses within the DMZ.

The audit results include these features:

1. An indicator for each device which can be:

   ✓**Passed** - All tests passed.

   ✗**Failed** - At least one test failed.

   ↻**Calculating** - The tests are currently being run on a revision. The results are shown for the previous revision.

   ⚠**Invalid profile** - go to **Settings** > **Configuration**> **Regulations** and complete any parts of the profile that are not marked with a green check mark. The results are shown for the last time the profile was complete.

   Error - Contact Tufin Support for assistance. The results are shown for the last revision before the error occurred.

   You can also recalculate the results based on the last revision.

2. Filter the profiles by regulations: **SOX** or **PCI DSS**
3. Manually recalculate the results.

   Results are automatically recalculated when there is a new revision or a change in the topology. To see the results after any other changes that impact the tests, click **Recalculate**.

4. An indicator for each test to show if it passed or failed, including the number of devices that failed.
5. Detailed results for each test.
6. The date that the tests were calculated.
7. A filter box to filter the results by test name.
8. Select rules from the results and click **Add Exception** to exclude them from the regulations test.
9. Export the results as a report that is saved in: **Report** > **Reports Repository**

   You can choose show the list of exceptions in the exported report.

Configuring Regulation Audit Profiles

Before you can audit your network for compliance with PCI DSS or SOX requirements, you must define a regulation profile where you specify the components in your environment that are used in the audit tests. You can configure many profiles to accurately represent your environment. The compliance tests run automatically when:

- A revision is received for the specified targets
- The network topology changes the path calculations
- The profile is changed and saved, for example when you add a new device

For each profile you can configure syslog and email notifications that are sent when a new violation is found. The notification includes a summary of new and existing violations.

The SOX audit profile requires you to select the devices that you want to audit.

The PCI DSS audit profile includes:

- **Targets** - You can define multiple devices to audit for PCI DSS compliance.
    - **Target** - The devices or policies that are tested for compliance
- **Networks** - You can have these automatically defined based on the network topology or you can define them manually with SecureTrack zones, IP addresses and network objects
    - **DMZ Networks** - Networks that are considered as the DMZ networks, such as a web server farm
    - **Internal Networks** - Networks that are considered as the internal networks, such as the internal office network
- **Network components** with PCI DSS-related data - You can define these with SecureTrack zones, IP addresses and network objects
    - **PCI Applications** - Servers that have applications that handle PCI DSS-related data, such as a retail purchasing application
    - **PCI Data** - Servers that store PCI DSS-related data, such as a network storage device
    - **PCI Web** - Servers that host web sites that handle PCI DSS-related data, such as an online store
    - **Wireless Networks** - Networks that use wireless networking
- **Services** - You can select from the list of predefined services, add services from your network devices or add custom services
    - **PCI Service** - Services that are used to transfer PCI DSS-related data between the networks and network components, such as https and PostgreSQL
    - **PCI Risky Service** - Services that are considered risky by the PCI DSS requirements, such as telnet and ftp

When you configure each of these components, a green check mark is shown next to the component name. For the tests to successfully run, all components must be configured.

To configure a SOX profile:

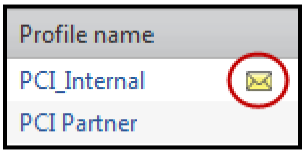
1. Click **New Profile** and enter the profile preferences, including the profile name, the **SOX** profile type, and the alert notification settings.

    To access the profile preferences of an existing profile, select the profile and click ☰.

    Select the alert notification settings for the profile:

    - Select **Syslog** to have syslogs sent to the syslog server configured in Notifications.
    - Select **Mail** to have emails sent to the SecureTrack users that you select in **Users**, and to the addresses that you enter in **Email addresses**.
    - Select the **Alert severity** for the alert notification for the profile.

    Profiles that have notifications configured are marked in the list of profiles.

Profile name
PCI_Internal ✉
PCI Partner

    Click **OK** to save the profile configuration and continue to the profile configuration.

2. Identify the network components for each section of the audit and click **Add** to include them in the SOX profile.
3. Click **Save**.

The results are shown in Regulations.

To configure a PCI DSS profile:

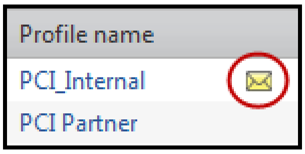
1. Click **New Profile** and enter the profile preferences, including the profile name, the **PCI DSS** profile type, and the alert notification settings.

    To access the profile preferences of an existing profile, select the profile and click ☰.

    Select the alert notification settings for the profile:

    - Select **Syslog** to have syslogs sent to the syslog server configured in Notifications.
    - Select **Mail** to have emails sent to the SecureTrack users that you select in **Users**, and to the addresses that you enter in **Email addresses**.
    - Select the **Alert severity** for the alert notification for the profile.

    Profiles that have notifications configured are marked in the list of profiles.



Profile name
PCI_Internal ✉
PCI Partner

Click **OK** to save the profile configuration and continue to the profile configuration.

To access the profile configuration of an existing profile, select the profile and click ✎.

2. Identify the network components for each section of the audit and click **Add** to include them in the PCI DSS profile.
    - **Target** - Select each device that you want to audit for the profile.

      For Check Point devices, you can select a policy from the list of available policies or select **Any** to audit all policies on the device.
    - **Networks** - For the Internal and DMZ networks you can either select:
        - **By Topology** - SecureTrack uses the networks identified in topology as the networks for the audit.
        - **Manual** - You can manually specify zones, network objects from the devices, or IP address subnets or ranges as the networks for the audit.
    - **Network components** - You can manually specify zones, network objects from the devices, or IP address subnets or ranges as the networks for the audit.

      If you don't have any wireless networks, select **Ignore** so that the PCI DSS results state that there is no wireless networks.
    - **Services** - You can select from the list of predefined services, select objects from the network devices, or manually enter custom protocol and port information.
3. Click **Save**.

The results are shown in in Regulations and you can see the critical violations in the Violations browser.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration** > **Regulations**

Excluding Rules from Regulations Audits

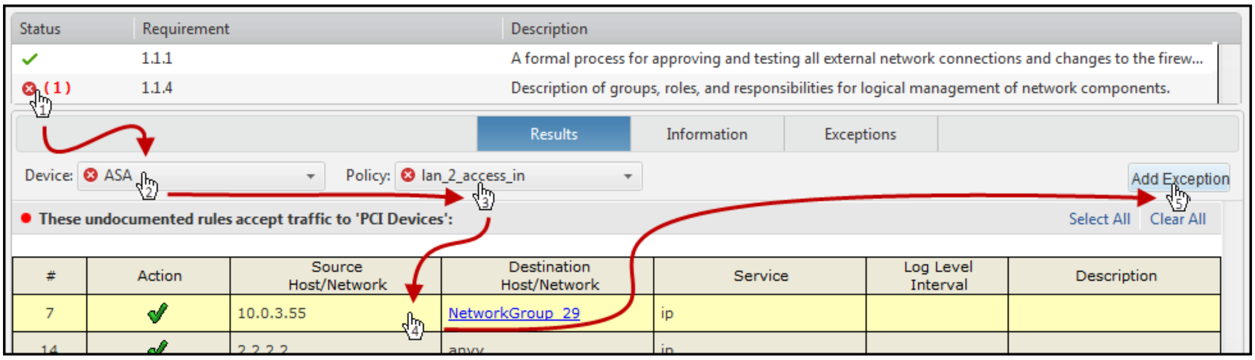
The results of the regulations audits sometimes include rules that the tests do not apply to, but that cannot be easily excluded from the regulations profile. You can select these rules from the audit results and add them as an exception to the audit so that the test does not fail because of these rules.

You can choose how to handle the exception in the event that the rule changes. You can keep the exception with the new rule definition, or remove the exception because the new rule definition does not match the rule that was selected as an exception. A rule is considered changed when:

- Objects are added or removed from the source, destination or service fields
- The IP address or protocol of the objects in the source, destination or service fields change
- Groups membership changes within groups that are in the source, destination or service
- The rule comment is changed in the policy on the device

Notes about remove and keep exception:

- Keep an exception when the rule changes - The rule can be listed as an exception even when it does not impact the test, for example:
    - The rule was removed from the policy
    - The PCI profile changed
    - A comment was added to the rule in SecureTrack Policy Browser
- Remove an exception when the rule changes - The rule can be removed from the list of exceptions even when the changes in the rule do not impact the test.



Status	Requirement	Description
✓	1.1.1	A formal process for approving and testing all external network connections and changes to the firew...
✗ (1)	1.1.4	Description of groups, roles, and responsibilities for logical management of network components.

Results | Information | Exceptions

Device: ASA Policy: lan_2_access_in Add Exception

● These undocumented rules accept traffic to 'PCI Devices': Select All Clear All

#	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Description
7	✓	10.0.3.55	NetworkGroup_29	ip		
14	✓	2.2.2.2	any	ip		

To add rules to the list of exceptions:

1. From the list of tests, select a test that failed.
2. Select a device that failed the test.
3. Select a policy that failed the test.
4. In the list of results, select a rule that failed the test.

   To select a set of rules, select the first rule, press and hold the **Shift** key, and select the last rule.

   To select multiple rules, press and hold the Ctrl key and select the rules.

   To select all rules, click **Select All**.
5. Click **Add Exception**.

   When you add an exception you can add this information to the exception:

   a. **On rule change**: Select what happens to the exception when the source, destination, service or comment of the rule changes in the policy:

      - **Keep exception** (default) - The changed rule is kept as an exception to the audit test and does not cause the test to fail.
      - **Remove exception** - The changed rule is removed from the list of exceptions and causes the test to fail if it does not match the test requirements.

   b. **Justification**: The reason why the rule is added as an exception.

   c. **Expiration**: When the rule is automatically removed from the list of exceptions.

You can see the rules that you selected in the Exceptions tab. To remove them from the exceptions, you can select rules in the list of exceptions just as you did in the list of results and click Remove Exception.

After you add or remove exceptions, the audit pass/fail status is updated to show the new status.

PCI DSS Tests

For each relevant section of the PCI DSS standard, SecureTrack performs a set of tests which validate PCI DSS compliance status. For each section, SecureTrack offers information on the PCI DSS requirement, SecureTrack's testing procedure and offers mitigation steps to be taken in case a violation occurred.

Build and Maintain a Secure Network

Requirement 1: PCI DSS requires that you install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

PCI DSS 1.1.1

PCI DSS Requirement	Examine documented procedures to verify there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.
Testing procedure	Examine documented procedures to verify there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.
Fail condition	SecureTrack has not received any revisions.
Result details	The results show the dates of the first and last revisions, and the total number of revisions retrieved by SecureTrack.
Suggestions for mitigation	Make sure that your devices are correctly configured to be monitored.

PCI DSS 1.1.4

PCI DSS Requirement	Description of groups, roles, and responsibilities for management of network components.Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.
Testing procedure	• Validate how many business ownership reports configured for the policy. • Validate how many rules in the policy are associated with change tickets either in rule documentation or in the policy itself. • Validate what percentage of the rules contain comments either in rule documentation or in the policy itself. • Validate which administrators and users have permission to access the device.
Fail condition	There are no change tickets associated with changes to rules, networks and services, or less than 80% of the rules contains comments.
Result details	The results show: • The name, monitored network, and owner of business ownership report. • The number of change tickets associated with changes to rules, networks or services. • The number of rules that have comments out of total rules contains comments. • The administrators and users with permissions for the device.
Suggestions for mitigation	To improve the results of the test: • Add comments to the uncommented rules. • Integrate SecureTrack with a ticketing system to provide visibility into the approval process for each policy change.

PCI DSS 1.1.5

PCI DSS Requirement	Description of groups, roles, and responsibilities for management of network components Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.
Testing procedure	a. Verify that no insecure services are not either in the rule comments or in SecureTrack rule documentation, and are: • Allowed from 'External' to 'Internal Networks' • Allowed from 'External' to 'DMZ' • Allowed from 'DMZ' to 'Internal Networks' • Allowed from 'External' to 'PCI Devices' • Allowed from ANY to 'PCI Devices' b. Verify that no insecure services are not either in the rule comments or in SecureTrack rule documentation
Fail condition	There are any undocumented rules that allow insecure services
Result details	The results show the services that are allowed in rules that are not documented.
Suggestions for mitigation	Make sure that rules that allow insecure services are documented.

PCI DSS 1.1.6

PCI DSS Requirement	Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2
Testing procedure	• Validate how many compliance policies are configured. • Validate how many scheduled new revision reports are configured. • Validate how many reports are configured to run when a new revision is received.
Fail condition	• No compliance policies are configured. • No scheduled reports are configured, or the period for periodically scheduled reports is more than 6 months. • No reports are configured to run when a new revision is received, or there are no revisions received in the last 6 months.
Result details	The results show:

	• The name and policy type for the configured compliance policies. • The name, type, owner and recipients of configured reports otherwise, it should state that no scheduled reports are configured.
Suggestions for mitigation	• Configure SecureTrack reports to run periodically or when a new revision is received.

PCI DSS 1.2.1

PCI DSS Requirement	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment and specifically deny all other traffic
Testing procedure	**1.2.1.b** Validate that there are rules that include non-**PCI Services** and are not documented, in rule documentation or in the policy itself, for: • Accepting traffic from the **External** to **DMZ** networks. • Accepting traffic from the **DMZ** to **Internal** networks. **1.2.1.c** Validate that the policy has cleanup rules for explicit or implicit deny.
Fail condition	**1.2.1.b** There are undocumented rules accepting traffic from the External to DMZ networks, or from the DMZ to Internal networks. **1.2.1.c** The policy is missing an explicit and an implicit cleanup rule.
Result details	The results show: **1.2.1.b** The rules that accept traffic that includes non-PCI services for traffic from the External to DMZ networks, or from the DMZ to Internal networks. **1.2.1.c** States if the policy contains cleanup rules for explicit or implicit deny
Suggestions for mitigation	**1.2.1.b** Remove or add comments to undocumented rules that accept traffic from the External to DMZ networks, or from the DMZ to Internal networks. **1.2.1.c** Add an explicit cleanup rule to ensure that all undesirable traffic is denied.

PCI DSS 1.2.3

PCI DSS Requirement	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
Testing procedure	(b) Make sure the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic from 'Wireless Networks' to 'PCI Devices' or from 'PCI Devices' to 'Wireless Networks' and that the rules are documented in the rule comment or in SecureTrack rule documentation.
Fail condition	(b) There are rules that either allow traffic from 'Wireless Networks' to 'PCI Devices' or from 'PCI Devices' to 'Wireless Networks' and are not documented in the rule comment or in SecureTrack rule documentation.
Result details	(b) The results show the undocumented rules that either allow traffic from 'Wireless Networks' to 'PCI Devices' or from 'PCI Devices' to 'Wireless Networks'.
Suggestions for mitigation	(b) Remove undocumented rules or add comments to the rules.

PCI DSS 1.3.1

PCI DSS Requirement	Implement a DMZ to limit inbound traffic to only system components that provide authorizedpublicly accessible services, protocols, and ports. Note: Source ports and IPv6 addresses are not used in Policy Analysis calculations.
Testing procedure	• Validate if there are rules that allow traffic from **External** to **DMZ Networks** and are not documented, either in rule documentation or in the policy itself. • Validate if there are rules that allow traffic from **DMZ Networks** to **External** and are not documented, either in rule documentation or in the policy itself.
Fail condition	There are rules that allow traffic from External to DMZ Networks or from DMZ Networks to External and are not documented, either in rule documentation or in the policy itself.
Result details	The results show the rules that allow traffic from External to DMZ Networks or from DMZ Networks to External and are not documented, either in rule documentation or in the policy itself.
Suggestions for mitigation	Remove rules that allow traffic from External to DMZ Networks or from DMZ Networks to External or add comments to the rules.

PCI DSS 1.3.2

PCI DSS Requirement	Limit inbound Internet traffic to IP addresses within the DMZ.

	Note: Source ports and IPv6 addresses are not used in Policy Analysis calculations.
Testing procedure	Validate which rules accept traffic from **External** to **Internal** addresses.
Fail condition	There are rules that accept traffic from External to Internal addresses.
Result details	The results show the rules that accept traffic from External to Internal addresses.
Suggestions for mitigation	Remove the rules or change the destinations to addresses within the DMZ.

PCI DSS 1.3.3

PCI DSS Requirement	Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. Note: Source ports and IPv6 addresses are not used in Policy Analysis calculations.
Testing procedure	• Validate which rules allow inbound traffic from addresses in the **External** network to **PCI APP** or **PCI DATA** addresses. • Validate which rules allow outbound traffic from **PCI APP** or **PCI DATA** addresses to addresses **External** networks.
Fail condition	There are rules that, either: • Allow inbound traffic from addresses in the External network to PCI APP or PCI DATA addresses that are not part of Internal or DMZ networks. • Allow outbound traffic from PCI APP or PCI DATA addresses that are not part of the Internal or DMZ networks to addresses External networks.
Result details	The results show the rules that: • Allow inbound traffic from addresses in the External network to PCI APP or PCI DATA addresses that are not part of Internal or DMZ networks. • Allow outbound traffic from PCI APP or PCI DATA addresses that are not part of the Internal or DMZ networks to addresses External networks.
Suggestions for mitigation	Make sure that both inbound or outbound connections are not allowed for traffic between the Internet and the cardholder data environment.

PCI DSS 1.3.4

PCI DSS Requirement	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.
Testing procedure	Verify that Check Point external interfaces have Anti-Spoofing enabled.
Fail condition	There are Check Point external interfaces that do not have Anti-Spoofing enabled.
Result details	For any Check Point external interface that has Anti-Spoofing disabled, the results show the module name and the interface.For other vendors, this requirement cannot be verified.
Suggestions for mitigation	Enable Anti-Spoofing for Check Point external interfaces.

PCI DSS 1.3.5

PCI DSS Requirement	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. Note: Source ports and IPv6 addresses are not used in Policy Analysis calculations.
Testing procedure	• Validate if there are rules that allow non-**PCI Services** inbound traffic from addresses in the **External** network to **PCI APP** or **PCI DATA** addresses that are not documented, either in rule documentation or in the policy itself. • Validate if there are rules that allow non-**PCI Services** outbound traffic from **PCI APP** or **PCI DATA** addresses to addresses **External** networks that are not documented, either in rule documentation or in the policy itself.
Fail condition	There are undocumented rules that, either: • Allow non-PCI services inbound traffic from addresses in the External network to PCI APP or PCI DATA addresses. • Allow non-PCI services outbound traffic from PCI APP or PCI DATA addresses to addresses External networks.
Result details	The results show the rules that: • Allow non-PCI services inbound traffic from addresses in the External network to PCI APP or PCI DATA addresses that are not part of Internal or DMZ networks. • Allow non-PCI services outbound traffic from PCI APP or PCI DATA addresses that are not part of the

	Internal or DMZ networks to addresses External networks.
Suggestions for mitigation	Make sure that non-PCI Services traffic from PCI APP or PCI DATA terminates only in the DMZ.

PCI DSS 1.3.6

PCI DSS Requirement	Examine firewall and router configurations to verify that the firewall performs stateful inspection (dynamic packet filtering), which makes sure that only established connections should be allowed in, and only if they are associated with a previously established session.
Testing procedure	Verify that out-of-state TCP connections are not allowed.
Fail condition	Out-of-state TCP connections are always allowed, or there are exceptions for hosts to allow out-of-state TCP connections.
Result details	The results show that out-of-state TCP connections are always allowed, or the number of hosts that have exceptions that allow out-of-state TCP connections.
Suggestions for mitigation	Always deny out-of-state TCP connections.

PCI DSS 1.3.7

PCI DSS Requirement	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. Note: Source ports and IPv6 addresses are not used in Policy Analysis calculations.
Testing procedure	Verify that the network addresses for the PCI Data components do not intersect with the DMZ network addresses.
Fail condition	There are network addresses that are used by PCI Data components and are in the DMZ network.
Result details	For any network addresses that are used by PCI Data components and are in the DMZ network, the name, IP address, netmask, and object comments are shown.
Suggestions for mitigation	Assign all PCI Data components in the internal network.

PCI DSS 2.2.1

PCI DSS Requirement	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.(For example, web servers, database servers, and DNS should be implemented on separate servers.)Note: Where virtualization technologies are in use, implement only one primary function per virtual system component. Note: Source ports and IPv6 addresses are not used in Policy Analysis calculations.
Testing procedure	Verify that there is not more than one PCI Service allowed to each PCI Device.
Fail condition	There is at least one PCI Device that has more than one PCI Service allowed.
Result details	The results show the name and IP address of the PCI Device, and the protocol and port of the services allowed.
Suggestions for mitigation	Only allow one PCI Service for each PCI Device.

PCI DSS 2.2.2

PCI DSS Requirement	Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure - for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.
Testing procedure	Verify that only PCI Services are allowed for components listed as PCI Devices.
Fail condition	Firewall rules allow traffic with services that are not listed as PCI Services.
Result details	For each PCI Device, the IP address is shown with the service protocol and port that is allowed.
Suggestions for mitigation	Make sure that the firewall rules block non-PCI Services from reaching PCI Devices.

PCI DSS 2.2.3

PCI DSS Requirement	Examine the system configuration standards to verify that common security parameter settings are included.Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.
Testing	• Validate how many Best Practice Audit queries are configured for this policy.

procedure	• For routers, validate how many Tufin Device Audit reports are configured.
Fail condition	• No Best Practice Audit queries are configured for this policy or • For routers, no Tufin Device Audit reports are configured.
Result details	The results show: • The name for the configured Best Practice Audit queries. • The name for the configured Tufin Device Audit reports.
Suggestions for mitigation	• Configure Best Practice Audits for this policy, • Configure Tufin Device Audit reports for this policy in **Reports**.

Maintain a Vulnerability Management Program

Requirement 6: Develop and maintain secure systems and applications.

PCI DSS 6.1

PCI DSS Requirement	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
Testing procedure	Validate how many Software Version Compliance reports configured for this policy.
Fail condition	No Software Version Compliance reports are configured.
Test details	The results show the name and owner of the Software Version Compliance reports.
Suggestions for mitigation	Configure Software Version Compliance reports in **Reports** > **General Reports**.

Regularly Monitor and Test Networks

Requirement 11: Regularly test security systems and processes

PCI DSS 11.2

PCI DSS Requirement	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in the network topology, firewall rule modifications, product upgrades).
Testing procedure	Run these vulnerability tests: • Any service can enter network • Any TCP can enter network • Any UDP can enter network • Any service from DMZ to internal • Any TCP from DMZ to internal • Any UDP from DMZ to internal • R-Services can enter network • Any service can leave network • Any TCP can leave network • Any UDP can leave network • TFTP can enter network • MS-SQL can enter network • NFS can enter network • LDAP can enter network • IRC can leave network • POP can enter internal network • IMAP can enter internal network • Ports under 20 can enter network • FINGER can enter network • BGP can enter network • SNMP can enter network • TCP on over 1000 ports can leave the network • UDP on over 1000 ports can leave the network • Any service from internal to DMZ • TCP on over 1000 ports can enter the network • UDP on over 1000 ports can enter the network • Risky Microsoft services can enter network • Risky Microsoft services from DMZ to internal • HTTP/HTTPS from DMZ to internal • Known P2P protocols can enter network • Known P2P protocols can leave network • Portmap can enter network • Lockd can enter network • POP can enter DMZ • IMAP can enter DMZ • LPD can enter network • Syslog can enter network • Permissive “Any service” rules exist • Permissive “Any destination” rules exist • TCP on over 1000 ports from DMZ to internal

	• SOCKS can enter network • Any TCP from internal to DMZ • Any UDP from internal to DMZ • X11 can enter network • Telnet can enter network • UDP on over 1000 ports from DMZ to internal • Allow “Any source” rules exist • NNTP can enter network • NNTP can exit network • NTP can enter network
Fail condition	At least one vulnerability test failed.
Result details	The results show each test and whether it passed or failed.
Suggestions for mitigation	Use SecureTrack tools, such as Policy Analysis or Object Lookup to locate the rules that violate the tests.

SOX Tests

The Sarbanes-Oxley Act (SOX) is a United States federal law that requires top management to individually certify the correctness of financial information.

SecureTrack allows you to verify that your IT network meets the SOX requirements, by mapping these requirements to two leading regulation frameworks:

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- The IT Governance Institute’s Control Objective for Information and Related Technology (COBIT)

SecureTrack’s regulations audit covers the COSO components that have implications on firewall policies: Risk Assessment, Control Activities and Monitoring. For each of these components, SecureTrack runs a set of specific tests that are defined by the COBIT framework. This audit structure ensures that the monitored environment complies with SOX.

COSO Risk Assessment Component

COSO risk assessment is mapped to the following COBIT objectives: PO9.0, ME4.5

COBIT PO9 - Assess and Manage IT Risks

Requirement	Require organization to create and maintain a risk management framework, which documents a common and agreed upon level of IT risks, mitigation strategies and residual risks. Any violation of this framework should be assessed and analyzed. The result of the assessment is understandable by the various stakeholders and can be reviewed to align to acceptable level of tolerance.
Testing procedure	Check that SecureTrack in installed.
Fail condition	None
Result details	SecureTrack allows organizations to meet this requirement using an assortment of tools, varying from risk definitions and monitoring, to regulatory compliance and custom compliance policies. All of these can be configured as required to match the organizational framework, including, but not limited to, creating a specific blend of tests, assigning risk level to each of them, monitoring, providing a high level overview of the overall risk level, and generating reports to be reviewed by the various stakeholders.
Suggestions for mitigation	None

COBIT ME4.5 - Risk Management

Requirement	Establish an effective governance framework includes defining organizational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.
Testing procedure	Verifies that SecureTrack has been integrated with a ticketing system
Fail condition	If SecureTrack is not integrated with a ticketing system (SecureChange or another ticketing system), state that this test is not applicable (NA).
Result details	None
Suggestions for mitigation	Integrate SecureTrack with a ticketing system.

COSO Control Activities Component

COSO control activities are mapped to the following COBIT objectives: AI2, AI4, AI6, DS1, DS5, DS8, DS9, DS10

COBIT AI2 - Acquire and Maintain Application Software

Requirement	Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organizations to properly support business operations with the correct automated applications.
Testing procedure	Check if SecureApp is installed.
Fail condition	If SecureApp is not installed, fail.
Result details	• If SecureApp is installed, SecureTrack shows the installation date and adds a statement explaining how SecureApp meets the requirements. • Otherwise, SecureTrack states that since SecureApp is not installed the application status cannot be determined and this test is not applicable (NA).
Suggestions for mitigation	Acquire and maintain the application software.

COBIT AI4 - Enable Operation

Requirement	Organizations have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed-upon technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.
Testing procedure	Check that SecureTrack in installed.
Fail condition	None
Result details	SecureTrack meets the requirements because it allows for the production / representation of documentation for rules that are in the rulebase.
Suggestions for mitigation	None

COBIT AI6 - Manage Changes

Requirement	All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formerly managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.
Testing procedure	• Check if SecureTrack includes active devices. • Check if SecureTrack is integrated with a ticketing system.
Fail condition	Fail in the any of the following conditions: • No devices are configured in SecureTrack • All devices are either broken or disconnected • SecureTrack is not integrated with a ticketing system
Result details	State that SecureTrack monitors the Firewall configuration and includes mechanisms for automated, continuous change tracking. SecureTrack integrates with various change monitoring frameworks to provide a unified change and configuration management interface. If SecureTrack is integrated with ticketing system, state that this integration exists and specify its start time. If not, state that no ticketing system has been integrated and that you are advised to do so.

Suggestions for mitigation	Make sure that your devices are properly configured in SecureTrack and integrate SecureTrack with a ticketing system.

COBIT DS1 - Define and Manage Service Levels

Requirement	Effective communication between IT management and business customers regarding services required is enabled by a documented definition of an agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.
Testing procedure	Test SecureTrack's integration with SecureChange or another ticketing system.
Fail condition	If SecureTrack is not integrated with a ticketing system (SecureChange or another ticketing system), fail.
Result details	If SecureChange is installed, pass. Show the SecureChange installation date and state that SecureChange provides a Service Level Agreement (SLA), monitoring and SLA reports. If another ticketing system is installed, pass. Show the ticketing system's installation date and state that SecureTrack is integrated with a ticketing system, which is assumed to handle service levels. If SecureApp is installed, show its installation date and state that SecureApp allows the organization to define service levels.
Suggestions for mitigation	Make sure that your devices are properly configured and integrate SecureTrack with a ticketing system.

COBIT DS5 - Ensure Systems Security

Requirement	The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimize the business impact of security vulnerabilities and incidents.
Testing procedure	Check if SecureTrack contains any devices.
Fail condition	If no devices are configured in SecureTrack, or if all devices are broken or disconnected, fail.
Result details	If devices are configured in SecureTrack then security policy changes and violations are logged and stored in SecureTrack's revision database. Alerts are sent using email, syslog or SNMP traps. Organizations can use SecureTrack's detailed reports and Compliance Policy alerts to review changes and quickly escalate them. Historical activity reports enable security officers to examine policy change activity using a variety of criteria. SecureTrack can be used to minimize the effects of network downtime caused by configuration errors. During downtime, administrators can use the side-by-side graphical comparison to identify and quickly resolve the configuration errors, and restore normal network operation.
Suggestions for mitigation	Configure devices in SecureTrack.

COBIT DS8 - Manage Service Desk and Incidents

Requirement	Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.
Testing procedure	Check if SecureTrack is integrated with SecureChange or another ticketing system.
Fail condition	If there is no integration with a ticketing system (SecureChange or another ticketing system), fail or state that this test is not applicable (NA).
Result details	If the integration exists, pass. If the ticketing system is SecureChange, specify it. State that since SecureTrack is integrated with a ticketing system, it is assumed that these requirements are met in the organization.

Suggestions for mitigation	Integrate SecureTrack with a ticketing system.

COBIT DS9 - Manage the Configuration

Requirement	Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimizes production issues and resolves issues more quickly.
Testing procedure	Check if SecureTrack contains any devices.
Fail condition	If no devices are configured in SecureTrack, or if all devices are broken or disconnected, fail.
Result details	If devices are configured in SecureTrack then SecureTrack's Firewall Policy Revision Control, policy change reports and graphical comparison view provide effective configuration management for an organization's Firewall Policy.
Suggestions for mitigation	Configure devices in SecureTrack.

COBIT DS10 - Manage Problems

Requirement	Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process maximizes system availability, improves service levels, and reduces costs.
Testing procedure	Check if SecureTrack is integrated with a ticketing system (SecureChange or another ticketing system).
Fail condition	If SecureTrack is not integrated with a ticketing system (SecureChange or another ticketing system), state that this test is not applicable (NA).
Result details	• If there is no integration with a ticketing system, state that this test is not applicable and explain that SecureTrack is not integrated with a ticketing system, so it cannot determine if the organization meets this requirement. • If there is integration with a ticketing system, show the integration start time and explain that SecureTrack can identify the administrator who is responsible for a certain policy change, providing a “root cause” analysis for incidents resulting from Firewall policy changes. In addition, as SecureTrack is integrated with a ticketing system, it is assumed that the organization can identify, track and classify problems and follow up on problem closure.
Suggestions for mitigation	Integrate SecureTrack with a ticketing system.

COSO Monitoring Component

COSO monitoring is mapped to the following COBIT objectives: ME1, ME2, ME3

COBIT ME1 - Monitor and Evaluate IT Performance

Requirement	Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.
Testing procedure	Check that SecureTrack in installed.
Fail condition	None
Result details	SecureTrack gives users with the ability to achieve this requirement through various features such as change monitoring, cleanup monitoring, and scheduled reports. While allowing users to get email or syslog notifications for any violation.
Suggestions for mitigation	None

COBIT ME2 - Monitor and Evaluate Internal Control

Requirement	Establishing an effective internal control program for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.
Testing procedure	Check if there are valid PCI profiles or Compliance Policies.
Fail condition	If there are no valid PCI profiles or Compliance Policies, fail.
Result details	None
Suggestions for mitigation	Configure PCI profiles or compliance reports.

COBIT ME3 - Ensure Compliance With External Requirements

Requirement	Effective oversight of compliance requires the establishment of a review process to ensure compliance with laws, regulations and contractual requirements. This process includes identifying compliance requirements, optimizing and evaluating the response, obtaining assurance that the requirements have been complied with and, finally, integrating IT’s compliance reporting with the rest of the business.
Testing procedure	Check that SecureTrack in installed.
Fail condition	None
Result details	Using SecureTrack's compliance audit, SecureTrack can alert Security Officers on changes in the VPN policy, and violations of specific inter-network communication limitations.
Suggestions for mitigation	None

Security and Compliance Policies

In SecureTrack, you can define your enterprise-wide security and compliance policies that all of your security devices must comply with. Because SecureTrack receives a copy of all of the policies defined on your monitored devices, SecureTrack can also notify you if any of those device policies conflict with your enterprise-wide security and compliance policies.

This gives you the ability to know immediately if your security or compliance posture is compromised by a change made to a security device.

Unified Security Policy

In the Unified Security Policy™ you can define the requirements that you want to use to govern the resources and traffic on your network. The requirements defined in the Unified Security Policy provide continuous compliance and any violations of those requirements are shown in the Violations browser

In the Unified Security Policy you can create security zone matrices. A security zone matrix is a set of requirements of rule definitions, or traffic that must be blocked or allowed between the security zones. At a glance you can review these requirements in an easy-to-read, color-coded matrix and see if changes need to be made. You can define a matrix with requirements from industry standards, such as NERC CIP, or internal corporate network requirements.

- Only administrators and super administrators can access the Unified Security Policy tab.

- Note: IPv6 is not supported for this TOS feature.

- Note: User Networks zones is not supported for USPs.

Handling addresses that are not associated with any zone

SecureTrack includes a predefined **Unassociated Networks**zone that includes all private addresses that are not included in any other defined SecureTrack zones.

You can add this zone to any USP matrix and define the behavior of this zone relative to all other zones or to specific zones in the environment.

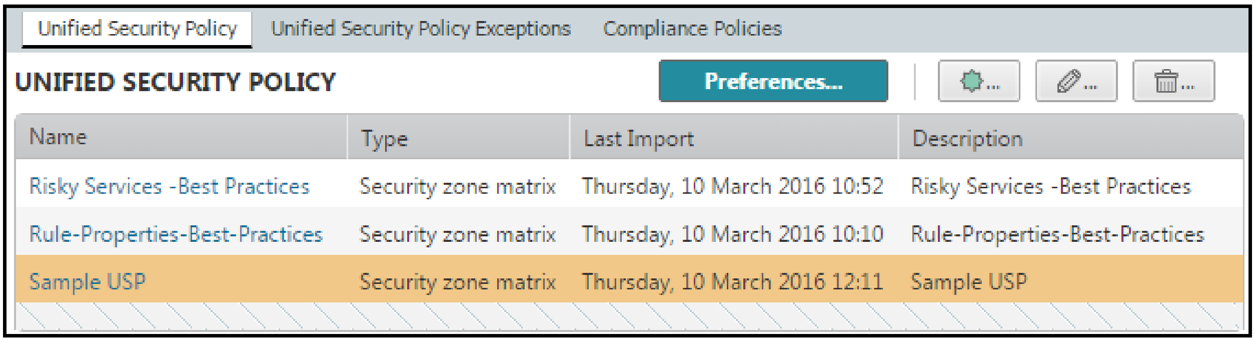
The Unassociated Networks zone is included in the calculations for Violations in SecureTrack, Risk Analysis in SecureChange, and in Compliance checks in SecureApp.

Getting Started

To create a Unified Security Policy component, you need to:

1. Prepare your security zones.
2. Create a new security zone matrix.
3. Prepare a security zone matrix file.
4. Import the security zone matrix file.
5. (**optional**) Configure device and interface preferences for a security zone. This lets you customize the violations results by excluding specific devices from any calculations for a zone, or by indicating that a specific device interface leads to a specific zone.

What can I do on this page?



UNIFIED SECURITY POLICY

Name	Type	Last Import	Description
Risky Services -Best Practices	Security zone matrix	Thursday, 10 March 2016 10:52	Risky Services -Best Practices
Rule-Properties-Best-Practices	Security zone matrix	Thursday, 10 March 2016 10:10	Rule-Properties-Best-Practices
Sample USP	Security zone matrix	Thursday, 10 March 2016 12:11	Sample USP

- View a security zone matrix - Click on the name of a security zone matrix to view it.
- Add a security zone matrix - Click ⚙.
- Configure Device and Interface Preferences - Click **Preferences...** to configure the preferences for a security zone matrix. You can exclude one or more devices from a security zone, or indicate that a specific interface leads to a specific zone.
- Edit a security zone matrix - Select a security zone matrix and click ✎.

  You can edit the name and description fields.
- Delete a security zone matrix - Select a security zone matrix and click 🗑.

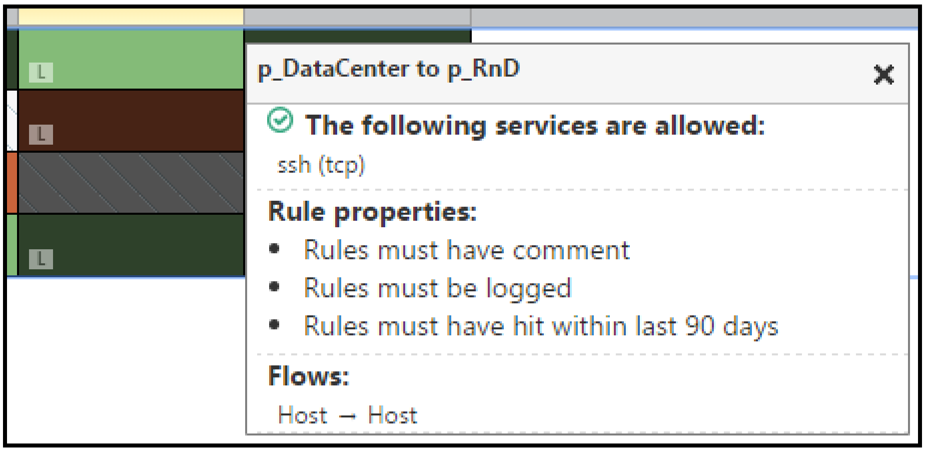
How Do I Get Here?

Audit > **Compliance** > **Unified Security Policy**

Working with Security Zone Matrices

A security zone matrix is a list of the security zones from your environment. The matrix displays what traffic is allowed between each zone. This information is used in the Violations browser, in SecureChange Risk Analysis, and in SecureApp Compliance checks.

- The letter in the bottom left of each cell in the matrix indicates the assigned severity: **L** - low; **M** - medium; **H** - high; **C** - critical
- The color of each cell indicates the access type:
  - **Green** - Allow only. Click on the cell to see the requirements.



p_DataCenter to p_RnD

✓ **The following services are allowed:**

ssh (tcp)

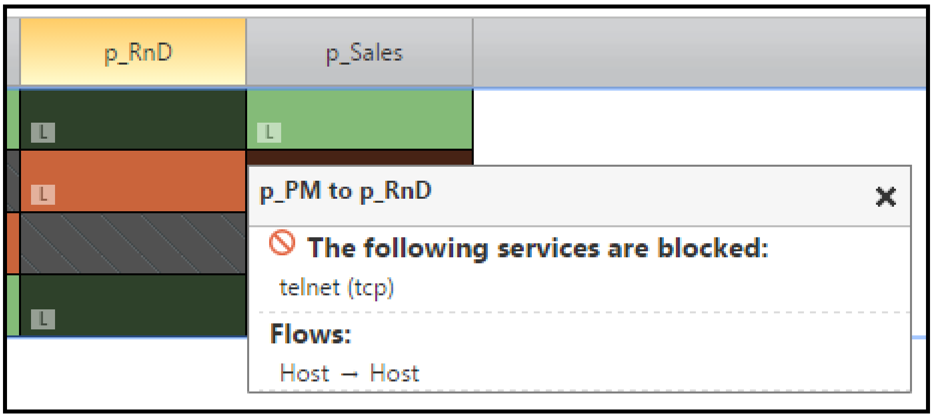
Rule properties:

- Rules must have comment
- Rules must be logged
- Rules must have hit within last 90 days

Flows:

Host → Host

- **Red** - Block only. Click on the cell to see the requirements.



p_RnD	p_Sales
⬛ L	🟩 L
🟥 L	
⬛	
⬛ L	

p_PM to p_RnD ✕

🚫 **The following services are blocked:**

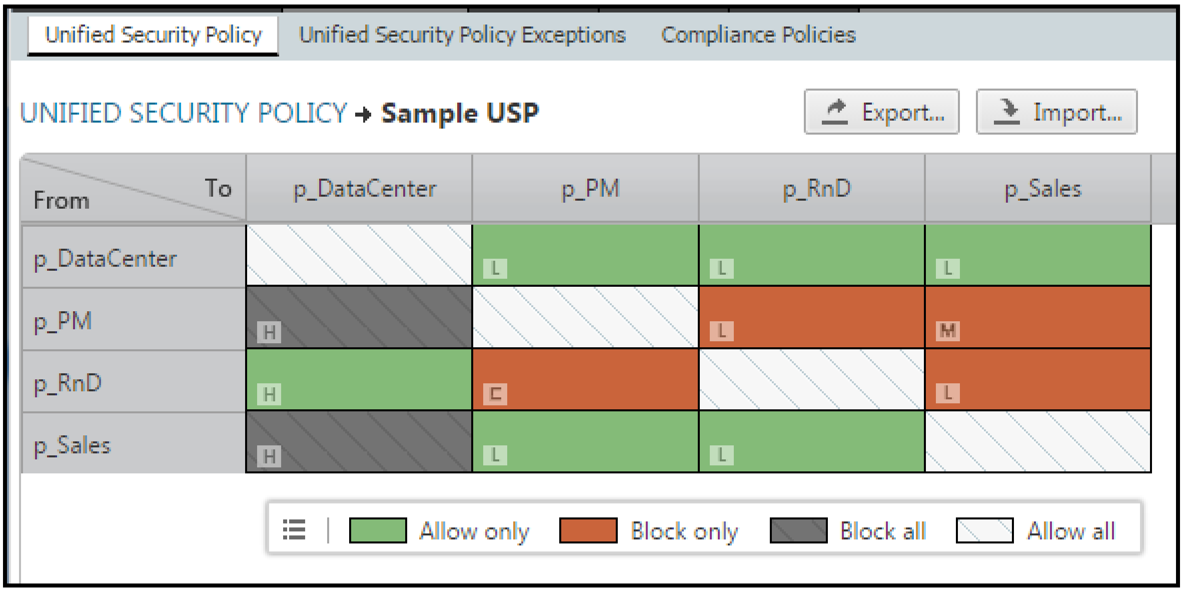
telnet (tcp)

Flows:

Host → Host

- **Grey** - Block all
- **White** - Allow all

What can I do on this page?



UNIFIED SECURITY POLICY → **Sample USP**

From \ To	p_DataCenter	p_PM	p_RnD	p_Sales
p_DataCenter	▨	🟩 L	🟩 L	🟩 L
p_PM	⬛ H	▨	🟥 L	🟥 M
p_RnD	🟩 H	🟥 C	▨	🟥 L
p_Sales	⬛ H	🟩 L	🟩 L	▨

☰ | 🟩 Allow only 🟥 Block only ⬛ Block all ▨ Allow all

- Import a matrix - Click Import to import a security zone matrix file.

  You must first prepare a security zone matrix file.

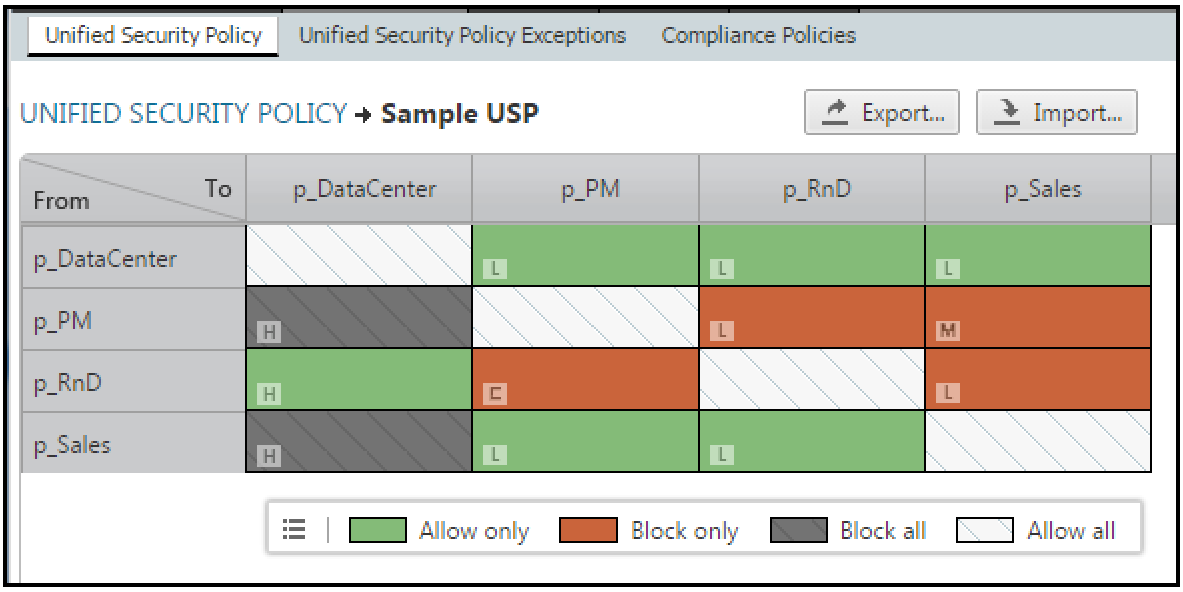
- Export the matrix - Click Export to export the matrix displayed to a CSV file.

- View legend - Click ☰ to toggle the display of the color legend on or off.

How Do I Get Here?

To view a specific USP matrix:

1. Go to the listing of your security zones.
2. Click on the name of a specific security zone matrix. The matrix for the selected security zone appears.



UNIFIED SECURITY POLICY → **Sample USP**

From \ To	p_DataCenter	p_PM	p_RnD	p_Sales
p_DataCenter	▨	🟩 L	🟩 L	🟩 L
p_PM	⬛ H	▨	🟥 L	🟥 M
p_RnD	🟩 H	🟥 C	▨	🟥 L
p_Sales	⬛ H	🟩 L	🟩 L	▨

☰ | 🟩 Allow only 🟥 Block only ⬛ Block all ▨ Allow all

Preparing a Security Zone Matrix File

After you import a CSV file with the specific traffic requirements between zones, you can see a table that represents those requirements. After you define the controls, you can easily find violations of the traffic requirements in: Home > Violations.

Prerequisites

You must define your security zones in Network > Zones before you can import a security zone matrix.

Procedure

To create a security zone matrix file:

When you create a matrix file to import, you must include the following fields:

- From domain (for Multi-Domain deployment only) - The name of the domain that contains the "from zone"

  This column is optional. If Multi-Domain is enabled and this column is not included in the file, the "Default" domain will be assigned to every row as the "from" domain
- From zone - The name of the source network zone in Network > Zones
- To domain (for Multi-Domain only) - The name of the domain that contains the "to zone"

  This column is optional. If Multi-Domain is enabled and this column is not included in the file, the "Default" domain will be assigned to every row as the "to" domain.
- To zone - The name of the destination network zone in Network > Zones
- Severity - The severity assigned to the violation: low, medium, high, critical
- Access Type - Traffic from the source zone and to the destination zone must be:
  - Allow all - All traffic is allowed
  - Block all - All traffic is blocked
  - Allow only - Traffic is allowed only if the traffic service is in the list of services
  - Block only - Traffic is blocked only if the traffic service is in the list of services
- Services (for Allow Only or Block Only access) - The services that are allowed to pass from the source zone and to the destination zone. See List of Tufin Predefined Services.
  1. You can enter multiple values separated by a semicolon, for example: `tcp 80; icmp 8`
  2. You can enter a range of ports, for example: `tcp 67-68`
  3. You can enter `any` so that all services are allowed.
- Rule Properties (for Allow Only or Block Only access) - The rules that match the specified traffic requirements are allowed:
  - `EXPLICIT_SOURCE` - Rules must have an explicit source, not the ANY value
  - `EXPLICIT_DESTINATION` - Rules must have an explicit destination, not the ANY value

- `EXPLICIT_SERVICE` - Rules must have an explicit service, not the ANY value
- `HAS_COMMENT` - Rules must have text in the comment field
- `IS_LOGGED` - Rules must be configured to create log entries
- `LAST_HIT_WITHIN {DAYS: X}` - Rules must have hits within the last X number of days
- `SOURCE_MAX_IP {COUNT:X}` - Source must contain less than X IP addresses
- `DESTINATION_MAX_IP {COUNT:X}` - Destination must contain less than X IP addresses
- `SERVICE_MAX_SERVICES {COUNT:X}` - Service must contain less than X services

Separate multiple values with a semicolon, for example: `IS_LOGGED; Last_Hit_Within {days: 90}`

To enforce Rule Properties on any service, set the Access Type to `Allow Only` and Service to `Any`, then add the desired Rule Properties.

- Flows (for Allow Only or Block Only access) - The rules that match the specified traffic requirements are allowed or blocked. Flows are defined by host and subnet objects. **Host** objects are any object, multiple objects or group of objects where each object represents one IP address. **Subnet** objects are any object, multiple objects or group of objects where each object represents more than one IP address, not including ANY or Internet.

  The syntax for the flow requirement is either:

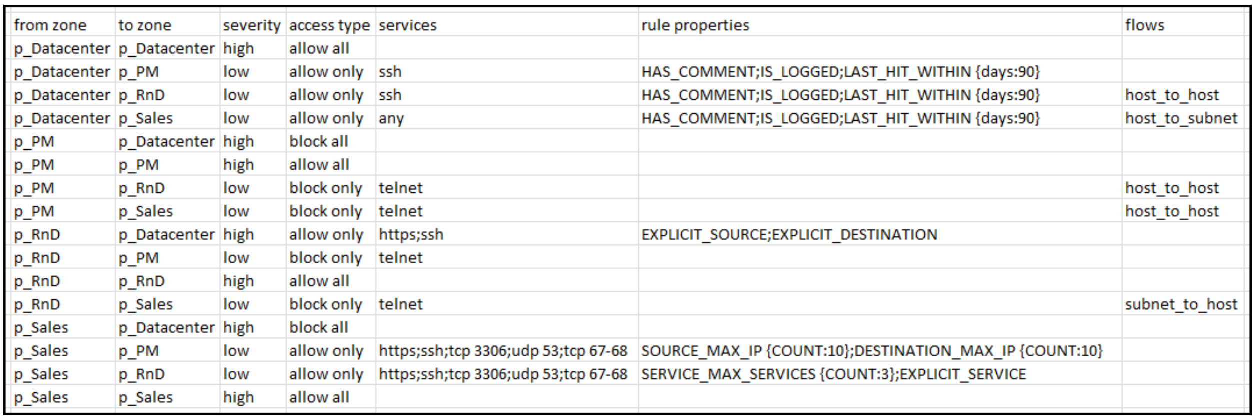
  - `HOST_TO_HOST` - Rules where the source and destination of the traffic flow are defined by hosts objects
  - `SUBNET_TO_HOST` - Rules where the source of the traffic flow is defined by subnet objects and the destination is defined by host
  - `HOST_TO_SUBNET` - Rules where the source of the traffic flow is defined by host objects and the destination is defined by subnet objects

  To enforce flows on any service, set the Access Type to `Allow Only` and Service to `Any`, then add the desired flows.

  The rows of the matrix must be preceded by a line with each of the headings above, followed by the lines of the matrix. You can include up to 70 security zones in a single matrix.

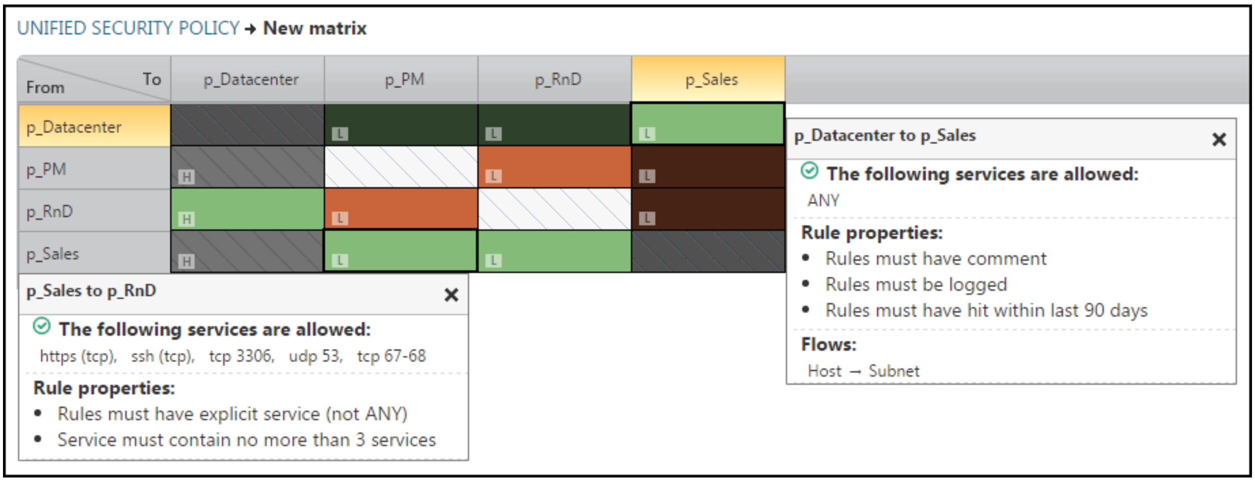
Sample File (You must import the sample zone list before you import the sample security zone matrix)

Sample as shown in Excel



from zone	to zone	severity	access type	services	rule properties	flows
p_Datacenter	p_Datacenter	high	allow all			
p_Datacenter	p_PM	low	allow only	ssh	HAS_COMMENT;IS_LOGGED;LAST_HIT_WITHIN {days:90}	
p_Datacenter	p_RnD	low	allow only	ssh	HAS_COMMENT;IS_LOGGED;LAST_HIT_WITHIN {days:90}	host_to_host
p_Datacenter	p_Sales	low	allow only	any	HAS_COMMENT;IS_LOGGED;LAST_HIT_WITHIN {days:90}	host_to_subnet
p_PM	p_Datacenter	high	block all			
p_PM	p_PM	high	allow all			
p_PM	p_RnD	low	block only	telnet		host_to_host
p_PM	p_Sales	low	block only	telnet		host_to_host
p_RnD	p_Datacenter	high	allow only	https;ssh	EXPLICIT_SOURCE;EXPLICIT_DESTINATION	
p_RnD	p_PM	low	block only	telnet		
p_RnD	p_RnD	high	allow all			
p_RnD	p_Sales	low	block only	telnet		subnet_to_host
p_Sales	p_Datacenter	high	block all			
p_Sales	p_PM	low	allow only	https;ssh;tcp 3306;udp 53;tcp 67-68	SOURCE_MAX_IP {COUNT:10};DESTINATION_MAX_IP {COUNT:10}	
p_Sales	p_RnD	low	allow only	https;ssh;tcp 3306;udp 53;tcp 67-68	SERVICE_MAX_SERVICES {COUNT:3};EXPLICIT_SERVICE	
p_Sales	p_Sales	high	allow all			

Sample after import



UNIFIED SECURITY POLICY → **New matrix**

From \ To	p_Datacenter	p_PM	p_RnD	p_Sales
p_Datacenter		L	L	L
p_PM	H		L	L
p_RnD	H	L		L
p_Sales	H	L	L	

p_Sales to p_RnD ✕

✓ **The following services are allowed:**

https (tcp), ssh (tcp), tcp 3306, udp 53, tcp 67-68

Rule properties:

- Rules must have explicit service (not ANY)
- Service must contain no more than 3 services

p_Datacenter to p_Sales ✕

✓ **The following services are allowed:**

ANY

Rule properties:

- Rules must have comment
- Rules must be logged
- Rules must have hit within last 90 days

Flows:

Host → Subnet

Sample Security Zone Matrix CSV File

Use a text editor, for example Notepad, to save this text as a CSV file and import it into a security zone matrix to see an example of a matrix.

```
# Enter the security zones that you have manually created or imported into
# SecureTrack in Network > Zones and create a unified security policy matrix
# between the zones.
# Only zones that you enter here are impacted by this Security Zone Matrix. You can
# include up to 70 individual security zones.
#
# This example is for a system where multi-domain is disabled.
# If multi-domain is enabled the columns 'from domain' and 'to domain' can be added.
#
from zone,to zone,severity,access type,services,rule properties,flows
p_Datacenter,p_Datacenter,high,allow all,,,
p_Datacenter,p_PM,low,allow only,ssh,HAS_COMMENT;IS_LOGGED;LAST_HIT_WITHIN {days:90},
p_Datacenter,p_RnD,low,allow only,ssh,HAS_COMMENT;IS_LOGGED;LAST_HIT_WITHIN {days:90},host_to_host
p_Datacenter,p_Sales,low,allow only,any,HAS_COMMENT;IS_LOGGED;LAST_HIT_WITHIN {days:90},host_to_subnet
p_PM,p_Datacenter,high,block all,,,
p_PM,p_PM,high,allow all,,,
p_PM,p_RnD,low,block only,telnet,,host_to_host
p_PM,p_Sales,low,block only,telnet,,host_to_host
p_RnD,p_Datacenter,high,allow only,https;ssh,EXPLICIT_SOURCE;EXPLICIT_DESTINATION,
p_RnD,p_PM,low,block only,telnet,,
p_RnD,p_RnD,high,allow all,,,
p_RnD,p_Sales,low,block only,telnet,,subnet_to_host
```

```
p_Sales,p_Datacenter,high,block all,,,

p_Sales,p_PM,low,allow only,https;ssh;tcp 3306;udp 53;tcp 67-68,SOURCE_
MAX_IP {COUNT:10};DESTINATION_MAX_IP {COUNT:10},

p_Sales,p_RnD,low,allow only,https;ssh;tcp 3306;udp 53;tcp 67-68,SERVICE_
MAX_SERVICES {COUNT:3};EXPLICIT_SERVICE,

p_Sales,p_Sales,high,allow all,,,
```

List of Tufin Predefined Services

The names and details of the services that are predefined in TOS are listed by protocol.

- TCP Service
- UDP Services
- ICMP Services
- Other Services

TCP Services

The names of the predefined TCP services in TOS are:

Service Name	Port Range	Comment
AOL	5190	AOL Instant Messenger. Also used by: ICQ &amp; Apple iChat
AP-Defender	2626	Defender Authentication service
AT-Defender	2626	Defender Authentication service
BGP	179	Border Gateway Protocol
Citrix_ICA	1494	Citrix ICA general Service.
CP_Exnet_PK	18262	Check Point Extranet public key resolution
CP_Exnet_resolve	18263	Check Point Extranet remote objects resolution
CP_redundant	18221	Check Point Redundant Management Protocol
CP_reporting	18205	Check Point Reporting Client Protocol
CP_rtm	18202	Check Point Real Time Monitoring
CP_seam	18266	Check Point Eventia Analyzer Server Protocol
CP_SmartPortal	4433	Check Point Smart Portal
CP_SSL_Network_Extender	444	SSL Network Extender port
CPD	18191	Check Point Daemon Protocol
CPD_amon	18192	Check Point Internal Application Monitoring
CPMI	18190	Check Point Management Interface
daytime-tcp	13	Daytime Server Protocol (TCP)
discard-tcp	9	Discard Server Protocol (TCP)

Service Name	Port Range	Comment
domain-tcp	53	Domain Name System Download
echo-tcp	7	Echo Protocol (TCP)
EDGE	981	VPN-1 UTM Edge Portal
Entrust-Admin	710	Entrust CA Administration Service
Entrust-KeyMgmt	709	Entrust CA Key Management Service
epmap-tcp	135	RPC Endpoint Mapper
exec	512	Remote execution (rexec)
FIBMGR	2010	Forwarding Information Base Manager - Dynamic Routing Cluster config
finger	79	UNIX
ftp	21	File Transfer Protocol
FW1	256	Check Point Security Gateway Service
FW1_amon	18193	Check Point OPSEC Application Monitoring
FW1_clntauth_http	900	Check Point Security Gateway Client Authentication (HTTP)
FW1_clntauth_telnet	259	Check Point Security Gateway Client Authentication (Telnet)
FW1_CPRID	18208	Check Point Remote Installation Protocol
FW1_cvp	18181	Check Point OPSEC Content Vectoring Protocol
FW1_ela	18187	Check Point OPSEC Event Logging API
FW1_ica_mgmt_tools	18265	Check Point Internal CA Management Tools
FW1_ica_pull	18210	Check Point Internal CA Pull Certificate Service
FW1_ica_push	18211	Check Point Internal CA Push Certificate Service
FW1_ica_services	18264	Check Point Internal CA Fetch CRL and User Registration Services
FW1_key	265	Check Point VPN-1 Public Key Transfer Protocol
FW1_lea	18184	Check Point OPSEC Log Export API
FW1_log	257	Check Point Security Gateway Logs
FW1_mgmt	258	Check Point Management (Version 4.x)
FW1_netso	19190	Check Point User Authority simple protocol
FW1_omi	18185	Check Point OPSEC Objects Management Interface
FW1_omi-sic	18186	Check Point OPSEC Objects Management Interface with Secure Internal Communication
FW1_pslogon	18207	Check Point Policy Server Logon protocol
FW1_pslogon_NG	18231	Check Point NG Policy Server Logon protocol

Service Name	Port Range	Comment
FW1_sam	18183	Check Point OPSEC Suspicious Activity Monitor API
FW1_sds_logon	18232	Check Point SecuRemote Distribution Server Protocol
FW1_sds_logon_NG	65524	SecuRemote Distribution Server Protocol (VC and higher)
FW1_snauth	261	Check Point Security Gateway Session Authentication
FW1_topo	264	Check Point VPN-1 SecuRemote Topology Requests
FW1_uaa	19191	Check Point OPSEC User Authority API
FW1_ufp	18182	Check Point OPSEC URL Filtering Protocol
gopher	70	The Internet Gopher Protocol
GoToMyPC	8200	Remote Computer Access &amp; Sharing application
H323	1720	videoconference transmissions over IP networks
http	80	Hypertext Transfer Protocol
HTTP_and_HTTPS_proxy	8080	
https	443	HTTP protocol over TLS/SSL
ident	113	Identify RCS keyword strings in files
IKE-tcp	500	IPSEC Internet Key Exchange Protocol over TCP
imap	143	Interactive Mail Access Protocol
IMAP-SSL	993	SSL encrypted IMAP
IPSO_Clustering_Mgmt_Protocol	1111	used for distributing configuration changes among cluster members and cluster wide monitoring
irc2	7000	Internet Relay Chat Protocol
Kerberos_v5_TCP	88	Kerberos authentication protocol (version 5)
ldap	389	Lightweight Directory Access Protocol
ldap-ssl	636	Lightweight Directory Access Protocol over TLS/SSL
login	513	Remote login (rlogin)
lotus	1352	Lotus iNotes Web Access Protocol
lpdw0rm	515	Also used by: Ramen trojan and printer service.
microsoft-ds	445	Microsoft CIFS over TCP
MS-SQL-Monitor	1434	Microsoft SQL Monitor
MS-SQL-Server	1433	Microsoft SQL Server
MSNP	1863	MSN Messenger
MySQL	3306	

Service Name	Port Range	Comment
nbsession	139	NetBios Session Service
NCP	524	Novell NetWare Core Protocol
netshow	1755	Microsoft NetShow (Windows Media Player)
netstat	15	UNIX netstat Protocol
nfsd-tcp	2049	Network File System Daemon over TCP
nntp	119	Network News Transfer Protocol
ntp-tcp	123	Network Time Protocol (TCP)
OAS-NameServer	2649	Oracle Application Server (IIOP) NameServer
OAS-ORB	2651	Oracle Application Server (IIOP) ORB
pcANYWHERE-data	5631	PCs remote access security software
pcTELECOMMUTE-FileSync	2299	Symantec pcTELECOMMUTE File Synchronization
pop-2	109	Post Office Protocol - Version 2
pop-3	110	Post Office Protocol - Version 3
POP3S	995	SSL protocol over POP3S
PostgreSQL	5432	PostgreSQL database server
pptp-tcp	1723	Point-to-Point Tunneling Protocol
RainWall_Command	6374	RainWall high availability daemon
Real-Audio	7070	RealNetworks PNA Protocol
RealSecure	2998	Automatic 'Suspicious Activity Monitoring' activator
Remote_Debug	8787	
Remote_Desktop_Protocol	3389	Microsoft RDP
rtsp	554	Real Time Streaming Protocol
SCCP	2000	Skinny Call Control Protocol
securidprop	5510	Token based Authentication service (TCP)
shell	514	Remote shell (rsh)
sip_tls	5061	Session Initiation Protocol over non-encrypted Transport Layer Security
sip-tcp	5060	Session Initiation Protocol over TCP
smtp	25	Simple Mail Transfer Protocol
SMTPS	465	SSL protocol over SMTPS
sqlnet1-2	1521	Oracle SQL*Net Version 1 and 2
sqlnet2-1525	1525	Oracle SQL*Net Version 2 Services

Service Name	Port Range	Comment
sqlnet2-1526	1526	Oracle SQL*Net Version 2 Services
Squid_NTLM	3128	Squid NTLM authentication
ssh	22	secure shell
StoneBeat-Control	3002	Stonesoft StoneBeat Control
StoneBeat-Daemon	3001	Stonesoft StoneBeat Daemon Heartbeat
T.120	1503	H323
TACACSplus	49	Terminal Access Controller Access Control System over TCP
tcp-high-ports	>1023	TCP Ports 1024-65535
telnet	23	Telnet Protocol
time-tcp	37	Time Server Protocol (TCP)
UserCheck	18300	Check Point Daemon Protocol
uucp	540	Unix-to-Unix Copy Program
wais	210	Wide Area Information Servers
X11	6000-6063	X Window System
Yahoo_Messenger_messages	5050	Yahoo Messenger messages
Yahoo_Messenger_Voice_Chat_TCP	5000-5001	Yahoo Messenger Voice Chat
Yahoo_Messenger_Webcams	5100	Yahoo Messenger Webcams video

UDP Services

The names of the predefined UDP services in TOS are:

Service Name	Port Range	Comment
biff	512	UNIX biff Protocol
bootp	67	Bootstrap Protocol Server
Citrix_ICA_Browsing	1604	UDP Service for general Citrix browsing
daytime-udp	13	Daytime Server Protocol (UDP)
dhcp	68	DHCP
discard-udp	9	Discard Server Protocol (UDP)
domain-udp	53	Domain Name System Queries
E2ECP	18241	Check Point End to End Control Protocol
echo-udp	7	Echo Protocol (UDP)
epmap-udp	135	RPC Endpoint Mapper

Service Name	Port Range	Comment
FW1_load_agent	18212	Check Point ConnectControl Load Agent
FW1_scv_keep_alive	18233	Check Point SecureClient Verification Keepalive Protocol
FW1_snmp	260	Check Point Security Gateway SNMP Agent
H323_ras	1719	RAS and associated connections (H.323 protocols)
Hotline_tracker	5499	Hotline tracker connections
ICQ_locator	4000	Mirabilis ICQ versions
IKE	500	IPSEC Internet Key Exchange Protocol (formerly ISAKMP/Oakley)
IKE_NAT_ TRAVERSAL	4500	Nat Traversal Protocol
Kerberos_v5_UDP	88	Kerberos authentication protocol (version 5)
kerberos-udp	750	secure method for authenticating a request for service
L2TP	1701	Layer 2 Tunneling Protocol
ldap-udp	389	LDAP udp service
MetaIP-UAT	5004	Check Point Meta IP UAM Client-Server Communication
mgcp_CA	2727	Media Gateway Control Protocol - Call-Agent port
mgcp_MG	2427	Media Gateway Control Protocol - Media Gateway port
microsoft-ds-udp	445	Microsoft CIFS over UDP
MS-SQL-Monitor_UDP	1434	Microsoft-SQL-Monitor_UDP
MS-SQL-Server_UDP	1433	Microsoft SQL Server
MSN_Messenger_ 1863_UDP	1863	Microsoft Network Messenger UDP
MSN_Messenger_5190	5190	Microsoft Network Messenger
MSN_Messenger_ Voice	6901	Microsoft Network Messenger Voice communication
name	42	Host Name Server
nbdatagram	138	NetBios Datagram Service
nbname	137	NetBios Name Service
NEW-RADIUS-ACCOUNTING	1812	NEW - Remote Authentication Dial-In User Service
NEW-RADIUS-ACCOUNTING	1813	NEW - Remote Authentication Dial-In User Service accounting
nfsd	2049	Network File System Daemon over UDP (earlier versions of NFS)
ntp-udp	123	Network Time Protocol (UDP)

Service Name	Port Range	Comment
pcANYWHERE-stat	5632	PCs remote access security software
RADIUS	1645	Remote Authentication Dial-In User Service
RADIUS-ACCOUNTING	1646	Remote Authentication Dial-In User Service accounting
RainWall_Daemon	6372	RainWall daemons communication
RainWall_Status	6374	RainWall remote management status
RainWall_Stop	6373	RainWall monitoring
RDP	259	Check Point VPN-1 FWZ Key Negotiations - Reliable Datagram Protocol
rip	520	Routing Information Protocol
RIPng	521	Routing Information Protocol for IPv6
securid-udp	5500	Token based Authentication service (UDP)
sip	5060	Session Initiation Protocol
snmp	161	Simple Network Management Protocol
SWTP_Gateway	9281	VPN-1 Embedded/SofaWare commands
SWTP_SMS	9282	VPN-1 embedded / SofaWare Management Server (SMS)
syslog	514	UNIX syslog Protocol
TACACS	49	Terminal Access Controller Access Control System over UDP
tftp	69	Trivial File Transfer Protocol
time-udp	37	Time Server Protocol (UDP)
tunnel_test	18234	Check Point tunnel testing application
udp-high-ports	>1023	UDP Ports 1024-65535
VPN1_IPSEC_encapsulation	2746	Check Point VPN-1 SecuRemote IPSEC Transport Encapsulation Protocol
wap_wdp	9200	Wireless Datagram Protocol: a simplified protocol suitable for low bandwidth mobile stations enables a connectionless mode.
wap_wdp_enc	9202	Wireless Datagram Protocol with Wireless Transport Layer Security
wap_wtp	9201	Wireless Transaction Protocol: a simplified protocol suitable for low bandwidth mobile stations enables a connection mode.
wap_wtp_enc	9203	Wireless Transaction Protocol with Wireless Transport Layer Security
who	513	UNIX who Protocol

ICMP Services

The names of the predefined ICMP services in TOS are:

Service Name	Type
dest-unreach	3
echo-reply	0
echo-request	8
info-reply	16
info-req	15
mask-reply	18
mask-request	17
param-prblm	12
redirect	5
source-quench	4
time-exceeded	11
timestamp	13
timestamp-reply	14

Other Services

The names of the other predefined services in TOS are:

Service Name	IP Protocol	Comment
AH	51	IPSEC Authentication Header Protocol
egp	8	Exterior Gateway Protocol
ESP	50	IPSEC Encapsulating Security Payload Protocol
FW1_Encapsulation	94	Check Point VPN-1 SecuRemote FWZ Encapsulation Protocol
ggp	3	Gateway-to-Gateway protocol
gre	47	Generic Route Encapsulation Protocol
icmp-proto	1	Internet Control Message Protocol
igmp	2	Internet Group Management Protocol
igrp	9	Cisco Interior Gateway Routing Protocol
IP_Mobility	55	IP Mobility protocol
ospf	89	Open Shortest Path First Interior GW Protocol
PIM	103	Protocol-Independent Multicast
SIT	41	IPv6 encapsulated in IPv4
Sitara	109	Sitara Networks Protocol (SpeedSeeker)
SKIP	57	IPSEC Simple Key Management for Internet Protocols

Service Name	IP Protocol	Comment
SUN_ND	77	Sun ND protocol
SWIPE	53	swIPe protocol
vrrp	112	Virtual Router Redundancy Protocol
other	0-255	for Service Names not listed above

Importing a Security Zone Matrix

A security zone matrix is a list of the security zones in your environment and what traffic is allowed between the zones. You can define the matrix with requirements from industry standards, such as NERC CIP v5, to maintain continuous compliance.

In a Multi-Domain deployment, a Super Admin can create a security zone matrix for the Global context that uses global zones to find violations across domains.

When you import a security zone matrix file to a security zone matrix that already has a security zone matrix, the previous matrix is replaced by the new matrix. All of the violations of the previous matrix are removed from the Violations browser, and the violations are recalculated for the new matrix when the a new revision is received or when the network topology is synchronized.

Prerequisites

Use a text editor such as Notepad to specify the details of the security zone matrix in a CSV file and import the file to SecureTrack. After you import the security zone matrix, the relationships between security zones are shown.

Procedure

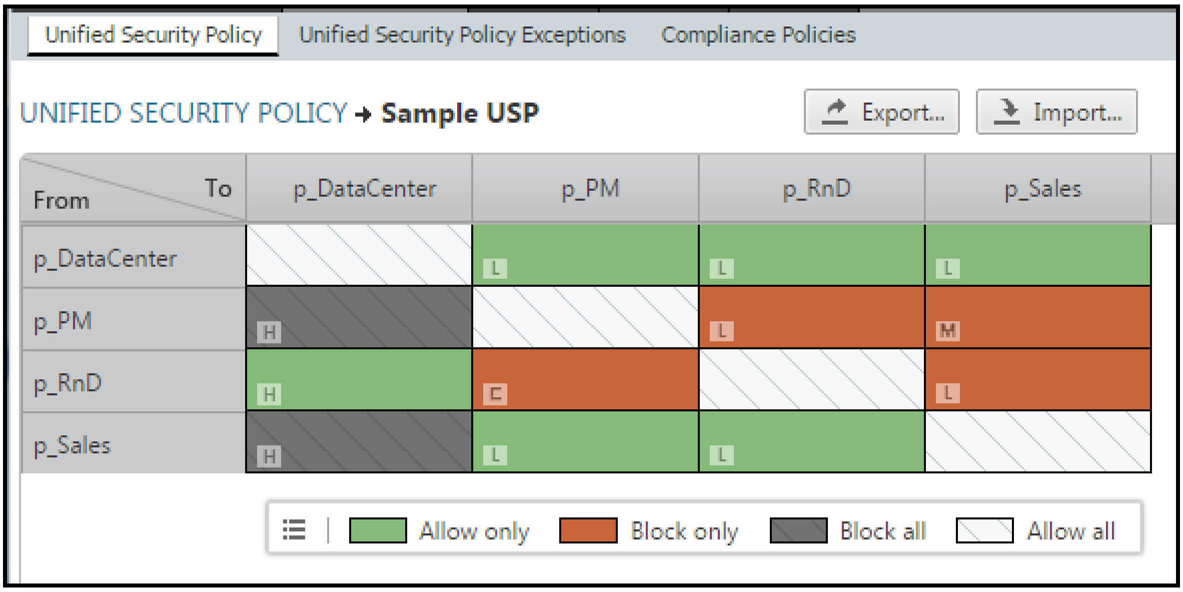
To import a security zone matrix:

1. Use a text editor such as Notepad to specify the details of the security zone matrix in a CSV file.
2. Go to a security zone matrix.
3. Click **Import**.
4. Browse to the prepared CSV file and click **Open**.

How Do I Get Here?

To view a specific USP matrix:

1. Go to the listing of your security zones.
2. Click on the name of a specific security zone matrix. The matrix for the selected security zone appears.



UNIFIED SECURITY POLICY → **Sample USP**

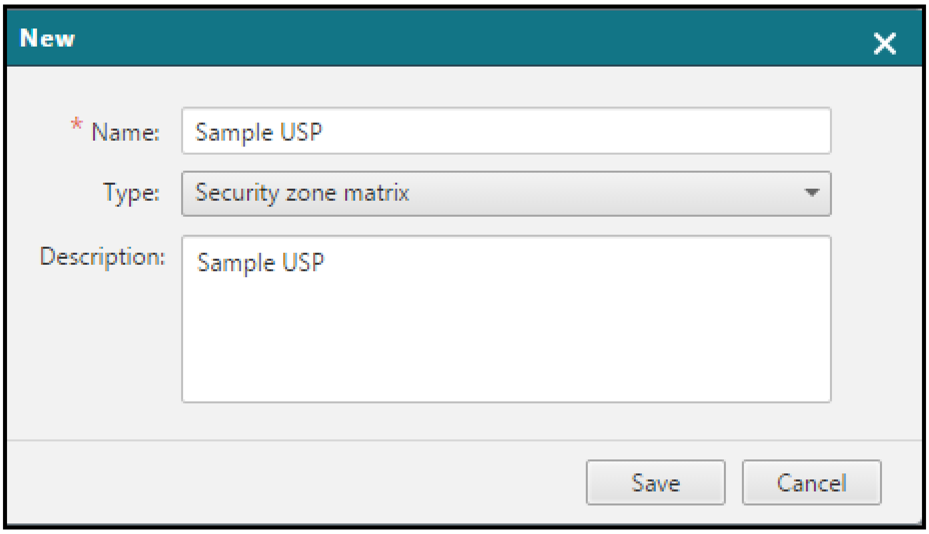
From \ To	p_DataCenter	p_PM	p_RnD	p_Sales
p_DataCenter	⬜	🟩 L	🟩 L	🟩 L
p_PM	⬛ H	⬜	🟧 L	🟧 M
p_RnD	🟩 H	🟧 C	⬜	🟧 L
p_Sales	⬛ H	🟩 L	🟩 L	⬜

🟩 Allow only 🟧 Block only ⬛ Block all ⬜ Allow all

Adding Security Zones

To add a security zone matrix:

1. Go to the listing of your security zone matrices.
2. Click ⚙.
3. Enter the name and description for the security zone matrix.



New

* Name: Sample USP

Type: Security zone matrix

Description: Sample USP

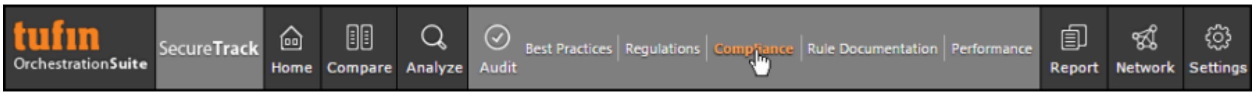
4. Click Save.

You can now create a security zone matrix file and import the matrix.

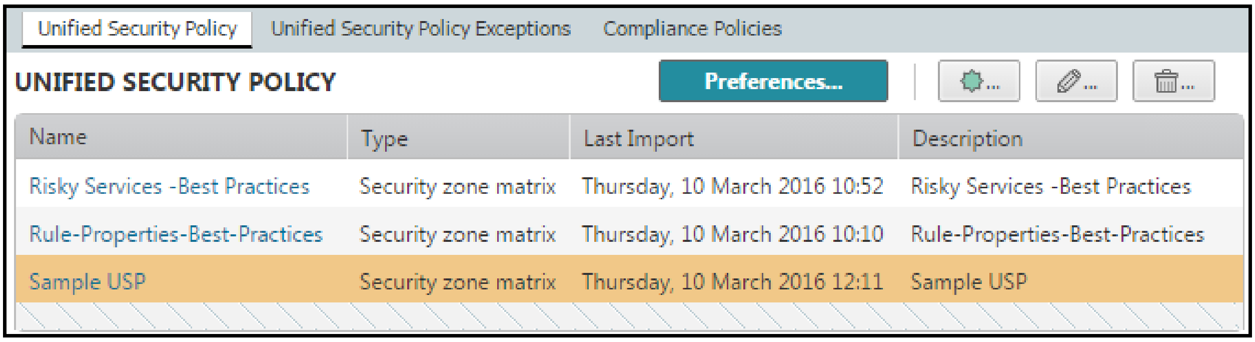
Navigate To USP Listing

To view all your Security Zone matrices:

1. In SecureTrack, go to **Audit** > **Compliance**.



2. Select the **Unified Security Policy** tab.
3. The listing of Unified Security Policy security zones appears



UNIFIED SECURITY POLICY

Name	Type	Last Import	Description
Risky Services -Best Practices	Security zone matrix	Thursday, 10 March 2016 10:52	Risky Services -Best Practices
Rule-Properties-Best-Practices	Security zone matrix	Thursday, 10 March 2016 10:10	Rule-Properties-Best-Practices
Sample USP	Security zone matrix	Thursday, 10 March 2016 12:11	Sample USP

Configure Device and Interface Preferences

To customize the violations results, you can specify how the device relates to the network zones. For each device interface, SecureTrack finds the security zone that contains the IP address of the interface and associates that zone with the interface. In addition to the IP address match, SecureTrack also uses routing tables to associate the zones with interfaces. To customize the associations of interfaces and zones, you can edit the USP preferences and select the zones for each interface. You can also exclude specific devices from all Unified Security Policy (USP) calculations.

The internet zone is not automatically associated with any interfaces. To associate the internet zone with interfaces, edit the USP preferences.

You can specify:

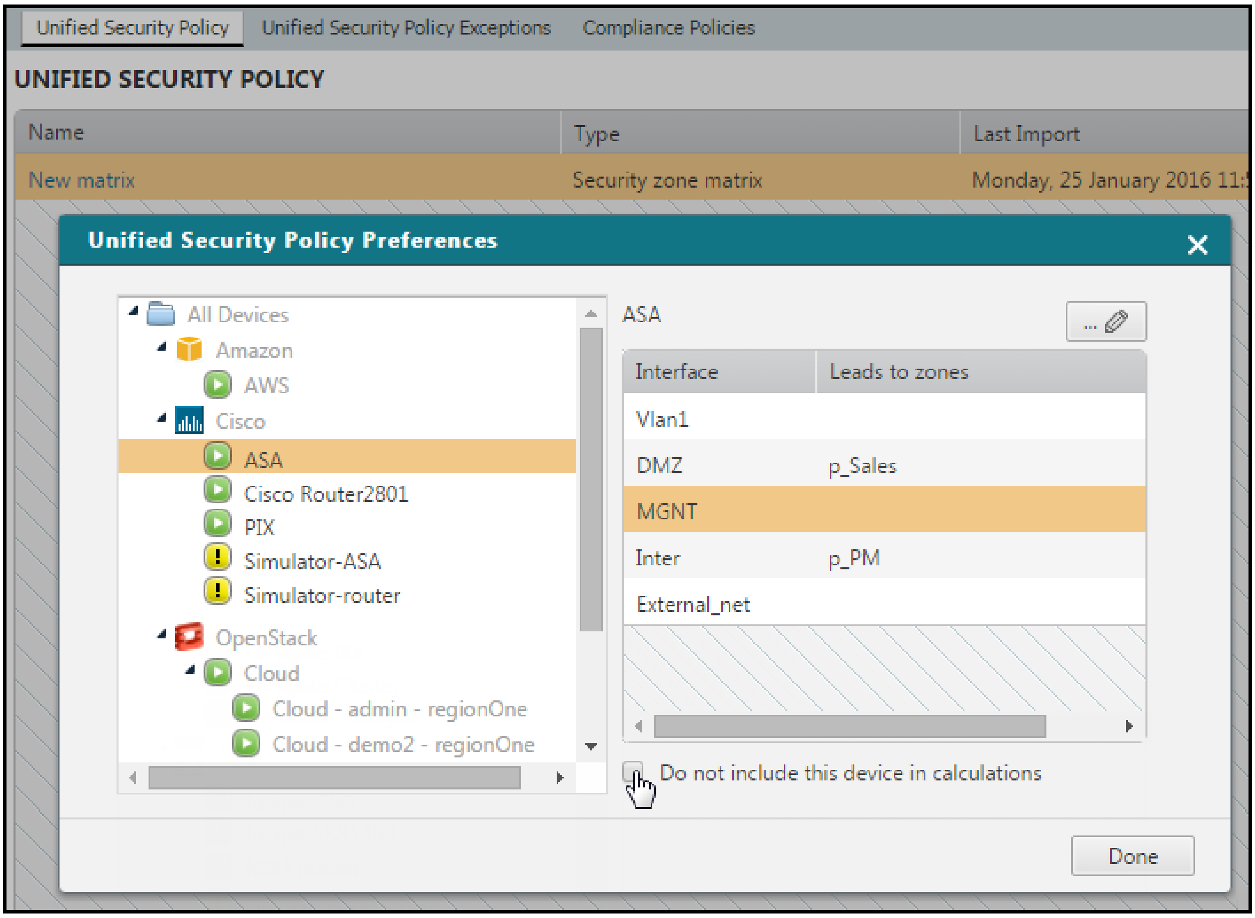
- **AWS devices:** The zones that a subnet can reach
- **All other devices:** The zones to which an interface leads

IPv6 is not supported for this TOS feature.

To exclude devices from a security zone

1. Go to the listing of your security zones.
2. Select a security zone matrix.
3. Click **Preferences**.

   The **Unified Security Policy Preferences** dialog is displayed.



Name	Type	Last Import
New matrix	Security zone matrix	Monday, 25 January 2016 11:

Interface	Leads to zones
Vlan1	
DMZ	p_Sales
MGNT	
Inter	p_PM
External_net	

□ Do not include this device in calculations

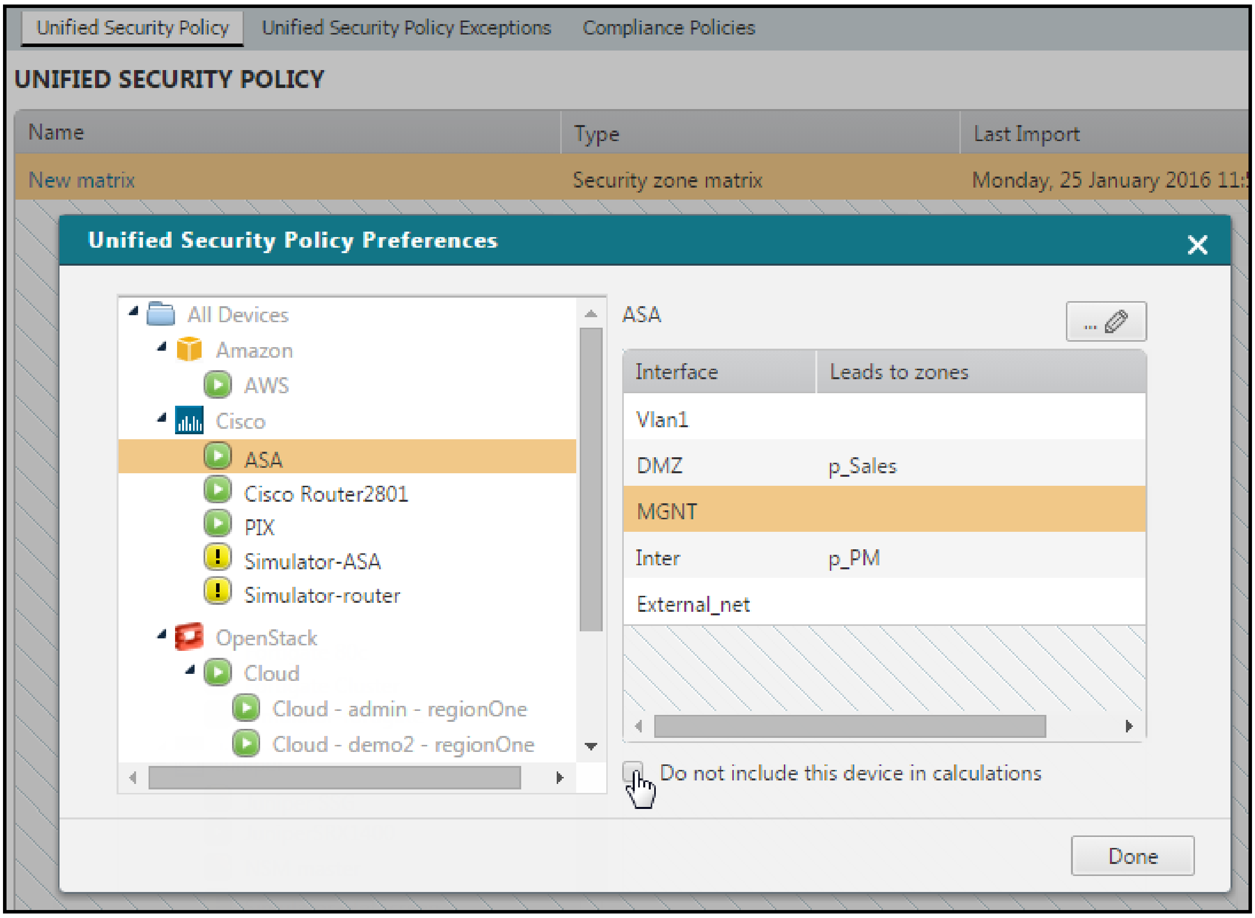
4. Select the device from the device tree.
5. Select **Do not include this device in calculations**.
6. Click **Done**.

Repeat these steps for each device you wish to exclude.

To indicate that a specific device interface leads to a specific zone

1. Go to the listing of your security zones.
2. Select a security zone matrix.
3. Click **Preferences**.

   The **Unified Security Policy Preferences** dialog is displayed.



Unified Security Policy | Unified Security Policy Exceptions | Compliance Policies

UNIFIED SECURITY POLICY

Name	Type	Last Import
New matrix	Security zone matrix	Monday, 25 January 2016 11:!

Unified Security Policy Preferences

- All Devices
  - Amazon
    - AWS
  - Cisco
    - ASA
    - Cisco Router2801
    - PIX
    - Simulator-ASA
    - Simulator-router
  - OpenStack
    - Cloud
      - Cloud - admin - regionOne
      - Cloud - demo2 - regionOne

ASA

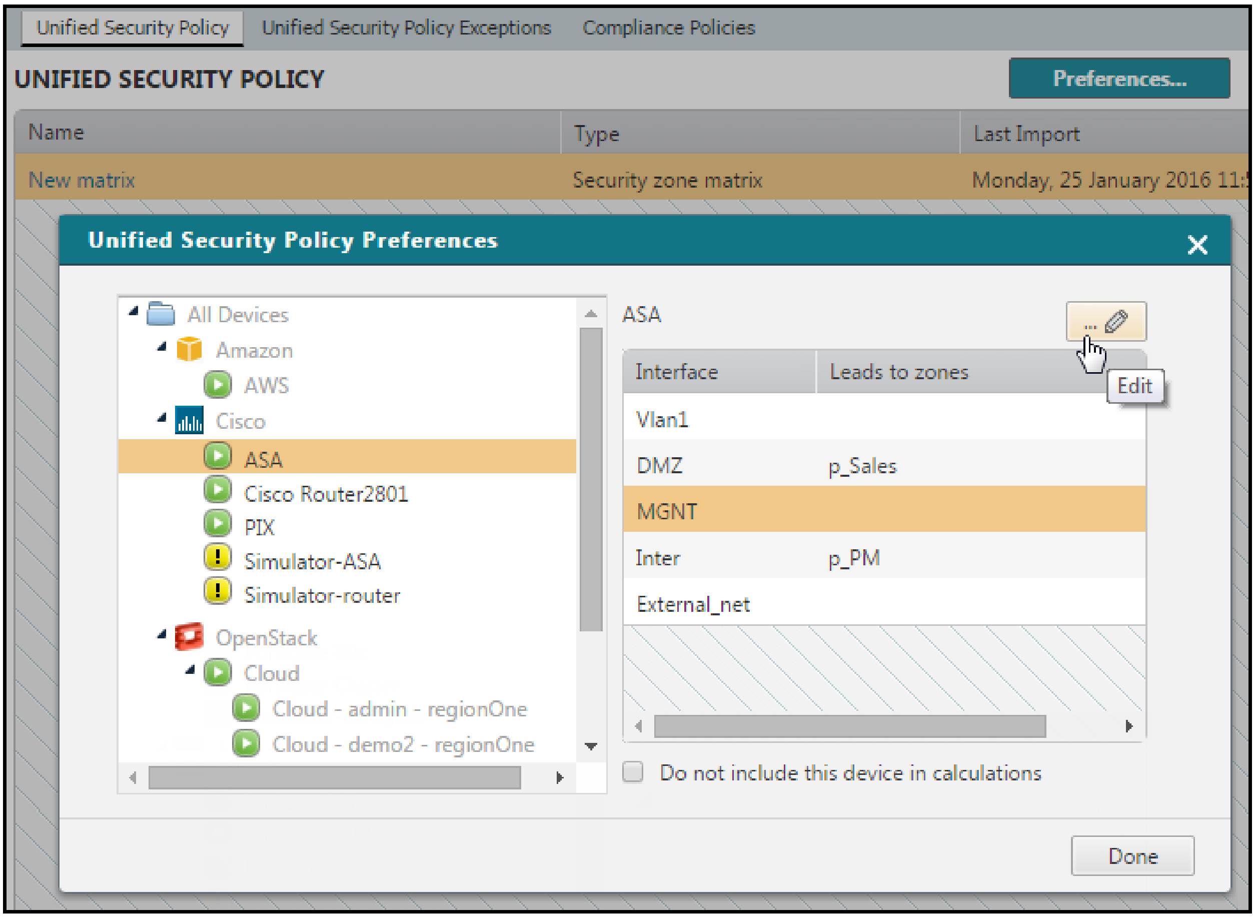
Interface	Leads to zones
Vlan1	
DMZ	p_Sales
MGNT	
Inter	p_PM
External_net	

□ Do not include this device in calculations

Done

4. Select the device from the device tree.

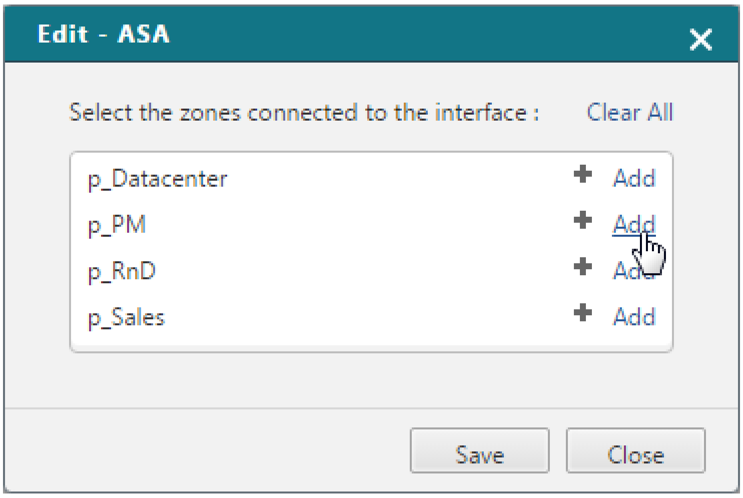
5. Select the interface to customize and click ✎ to edit the interface.



Interface	Leads to zones
Vlan1	
DMZ	p_Sales
MGNT	
Inter	p_PM
External_net	

□ Do not include this device in calculations

6. Add or remove zones from the interface.



Select the zones connected to the interface :

p_Datacenter	✚ Add
p_PM	✚ Add
p_RnD	✚ Add
p_Sales	✚ Add

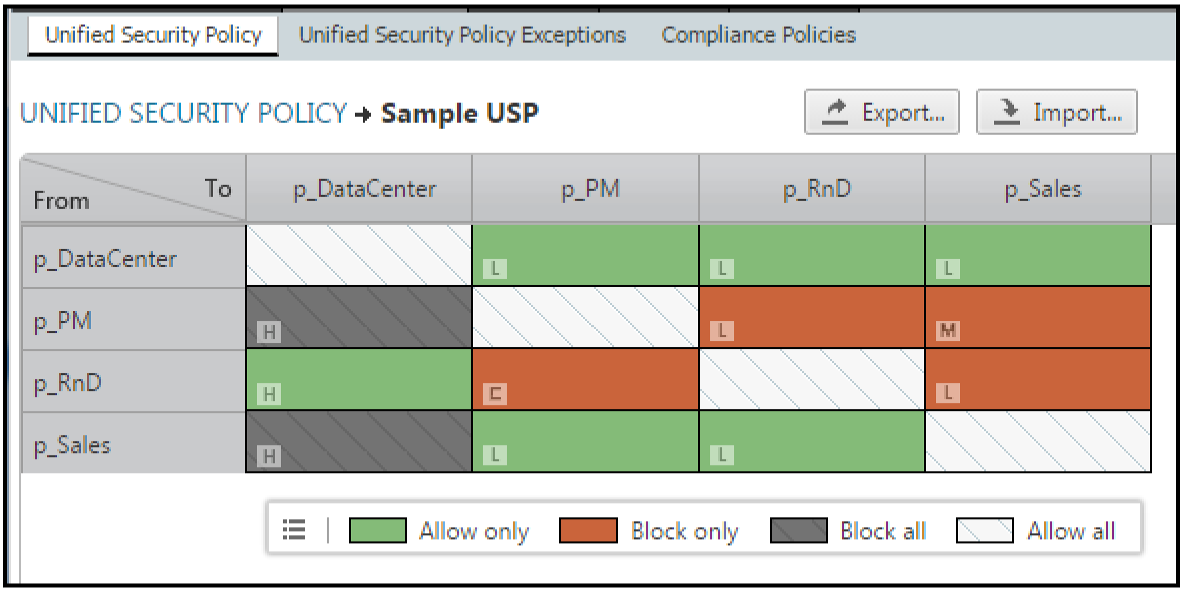
7. Click **Save**.
8. Click **Done**.

Repeat these steps for each device you wish to customize.

Navigate To - USP Matrix

To view a specific USP matrix:

1. Go to the listing of your security zones.
2. Click on the name of a specific security zone matrix. The matrix for the selected security zone appears.



UNIFIED SECURITY POLICY → **Sample USP**

From \ To	p_DataCenter	p_PM	p_RnD	p_Sales
p_DataCenter	▨	🟩 L	🟩 L	🟩 L
p_PM	⬛ H	▨	🟥 L	🟥 M
p_RnD	🟩 H	🟥 C	▨	🟥 L
p_Sales	⬛ H	🟩 L	🟩 L	▨

☰ | 🟩 Allow only 🟥 Block only ⬛ Block all ▨ Allow all

Working with Cloud Tag Policies

A cloud tag policy is the list of the tags you require for each cloud instance. You can use the cloud tag policies to maintain standardized corporate tag policy requirements for each instance and to control the security policy of cloud instances.

After you import a JSON file with the specific Amazon AWS cloud tag requirements, you can see a table that shows those requirements. You can easily find violations of the cloud tag requirements in **Home** > **Violations**. Violations are updated when a new Amazon AWS revision is retrieved.

You can define requirements for:

- **Mandatory tags** - The list of tags that every instance must have. Any instance that does not have all of these tags is shown as a violation of the requirement.
- **Valid values** - The list of values that are possible for a specific tag. Any instance that has a tag value that is not in this list is shown as a violation of the requirement.

What can I do on this page?

- Import a cloud tag policy - Click Import to import a cloud tag policy file.

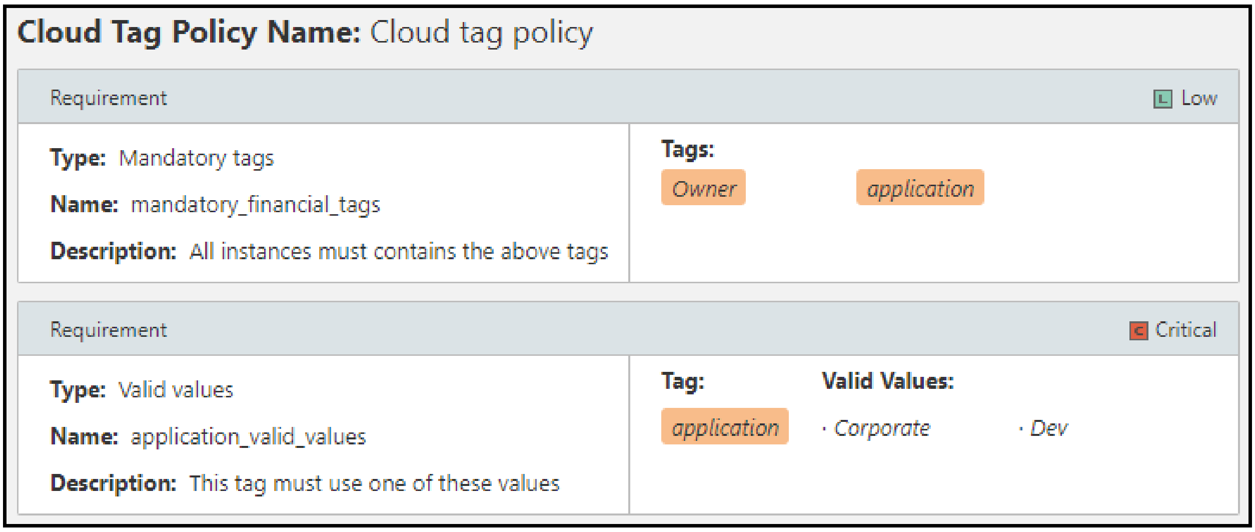
  You must first prepare a cloud tag policy file.

- Export the matrix - Click Export to export the matrix displayed to a JSON file.

How Do I Get Here?

To view a specific USP cloud tag policy:

1. Go to the listing of your security zones.
2. Click on the name of a specific cloud tag policy. The cloud tag policy is shown.



Cloud Tag Policy Name: Cloud tag policy

Requirement — L Low

Type: Mandatory tags

Name: mandatory_financial_tags

Description: All instances must contains the above tags

Tags: Owner application

Requirement — C Critical

Type: Valid values

Name: application_valid_values

Description: This tag must use one of these values

Tag: application

Valid Values: · Corporate · Dev

Preparing a Cloud Tag Policy File

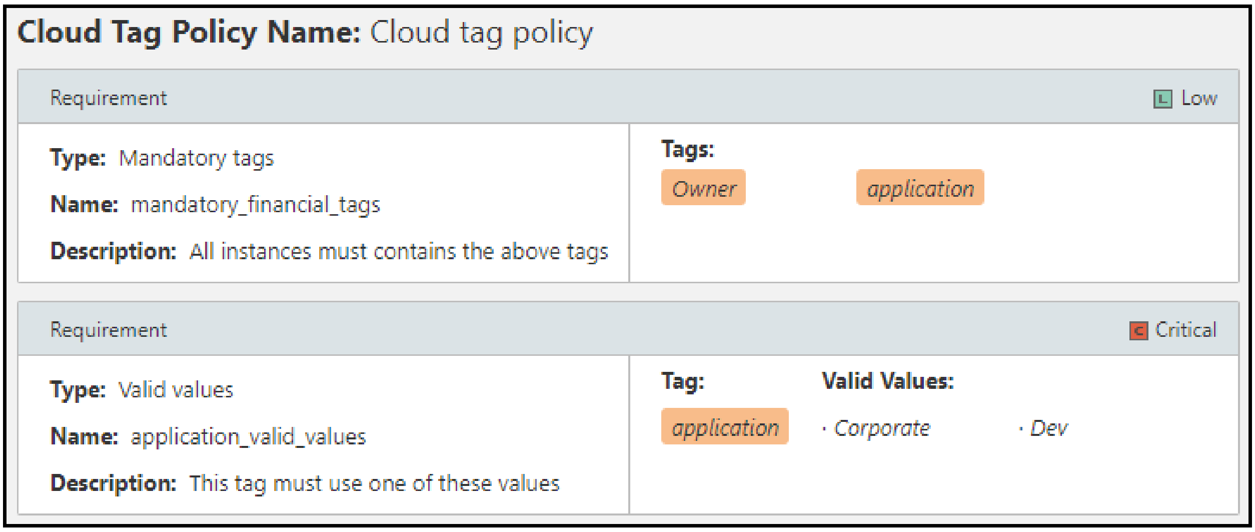
When you create a cloud tag policy file to import, you can include requirements for mandatory tags or valid values or both. You must include these fields:

- For mandatory tag requirements:
  - **policy name** - The name of the cloud tag policy
  - **policy description** - A description that is shown in the list of USP components
  - **requirement type** - `mandatory_tags`
  - **requirement name** - The name of the requirement in the cloud tag policy
  - **requirement description** - A description that is shown in the list of cloud tag policy requirements
  - **requirement severity** - A label that identifies that the requirement is either: `Critical`, `High`, `Medium`, `Low`
  - **tags** - The tags that are required for every instance (case-sensitive)
- For valid values requirements:
  - **policy name** - The name of the cloud tag policy
  - **policy description** - A description that is shown in the list of USP components
  - **requirement type** - Either `mandatory_tags` or `valid_values`
  - **requirement name** - The name of the requirement in the cloud tag policy
  - **requirement description** - A description that is shown in the list of cloud tag policy requirements
  - **requirement severity** - A label that identifies that the requirement is either: `Critical`, `High`, `Medium`, `Low`
  - **tags** - The tag that the values apply to
  - **values** - The list of values that are valid for the tag

Sample file contents

```
{
"policy_name" : "Cloud tag policy",
"policy_description" : "Instances tags in production",
"requirements" : [ {
"requirement_type" : "mandatory_tags",
"requirement_name" : "mandatory_financial_tags",
"requirement_description" : "All instances must contains the above tags",
"requirement_severity" : "Low",
"tags" : [ "Owner", "application" ]
}, {
  "requirement_type" : "valid_values",
  "requirement_name" : "application_valid_values",
  "requirement_description" : "This tag must use one of these values",
  "requirement_severity" : "Critical",
  "tag" : "application",
  "values" : [ "Corporate", "Dev" ]
  } ]
}
```

Sample after import



Cloud Tag Policy Name: Cloud tag policy

Requirement — L Low

Type: Mandatory tags

Name: mandatory_financial_tags

Description: All instances must contains the above tags

Tags: Owner application

Requirement — C Critical

Type: Valid values

Name: application_valid_values

Description: This tag must use one of these values

Tag: application

Valid Values: · Corporate · Dev

Importing a Cloud Tag Policy

A cloud tag policy is a list of requirements that you enforce in your environment for cloud tags.

When you import a cloud tag policy file to a cloud tag policy that already has cloud tag policy requirements, the previous requirements are replaced by the new requirements. All of the violations of the previous requirements are removed from the Violations browser, and the violations are recalculated for the new requirements when the a new revision is received.

Prerequisites

Use a text editor such as Notepad to specify the details of the cloud tag policy in a CSV file and import the file to SecureTrack. After you import the cloud tag policy, you can review the cloud tag policy requirements and the violations that

Procedure

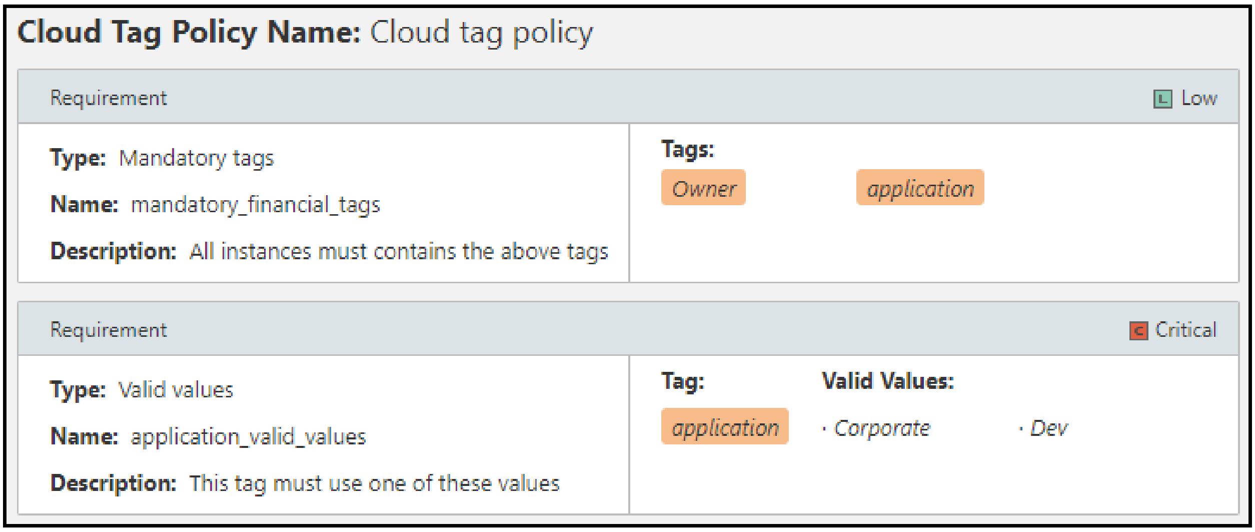
To import a cloud tag policy file:

1. Use a text editor such as Notepad to specify the details of the cloud tag policy in a CSV file.
2. Go to a cloud tag policy.
3. Click **Import**.
4. Browse to the prepared CSV file and click **Open**.

How Do I Get Here?

To view a specific USP cloud tag policy:

1. Go to the USP Listing.
2. Click on the name of a specific cloud tag policy. The cloud tag policy is shown.



Cloud Tag Policy Name: Cloud tag policy

Requirement — L Low

Type: Mandatory tags

Name: mandatory_financial_tags

Description: All instances must contains the above tags

Tags:
Owner application

Requirement — C Critical

Type: Valid values

Name: application_valid_values

Description: This tag must use one of these values

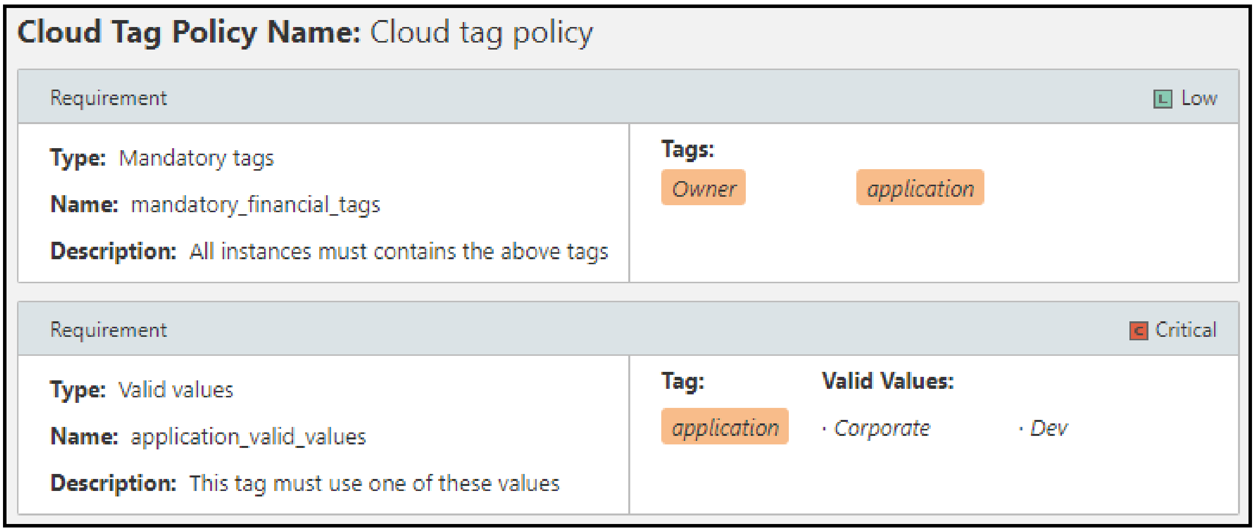
Tag: application

Valid Values:
· Corporate · Dev

Navigate To Cloud Tag Policy

To view a specific USP cloud tag policy:

1. Go to the listing of your security zones.
2. Click on the name of a specific cloud tag policy. The cloud tag policy is shown.



Cloud Tag Policy Name: Cloud tag policy

Requirement — L Low

Type: Mandatory tags

Name: mandatory_financial_tags

Description: All instances must contains the above tags

Tags:
Owner application

Requirement — C Critical

Type: Valid values

Name: application_valid_values

Description: This tag must use one of these values

Tag: application

Valid Values:
· Corporate · Dev

Configuring Exceptions for the Unified Security Policy

In **Audit** > **Compliance** > **Unified Security Policy Exceptions**, you can see exceptions to the Unified Security Policy so that specific traffic that is defined as restricted or blocked by the Unified Security Policy is actually approved to pass through the firewalls in your environment. After you define the exceptions, you can create a report that shows the firewall rules that match the exceptions.

You can use the REST API to create the exceptions. After you create an exception, you can find the rules that match the exception and create a report of all rules that are excluded from USP violations.

To add an exception to the Unified Security Policy:

1. Collect the information that you need to define the exception.
2. Prepare the information in the XML format defined in the REST API documentation.
3. Use this URL to create the exception and send the prepared XML as the payload of the request:

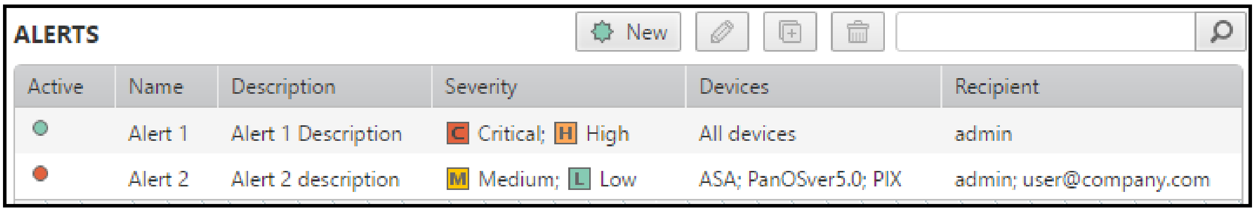
   `POST https://<`**securetrack_ip**`>/securetrack/api/security_policies/exceptions`

After you create an exception, to see all of the rules that match the traffic defined in the exceptions:

- Go to: **Audit** > **Compliance** > **Unified Security Policy Exceptions**
- Click on **Find Matching Rules** to see all of the rules that match the traffic defined in the exceptions.

Unified Security Policy Alerts

USP Alerts give you real time visibility and tracking of USP violations. By responding to the alert and immediately fixing the underlying issue, you can reduce your real-time risk and exposure.



ALERTS New ✎ ⧉ 🗑

Active	Name	Description	Severity	Devices	Recipient
●	Alert 1	Alert 1 Description	C Critical; H High	All devices	admin
●	Alert 2	Alert 2 description	M Medium; L Low	ASA; PanOSver5.0; PIX	admin; user@company.com

The following information is displayed for each alert:

USP Alert Field	Description
Status	Specifies whether the USP Alert is: • Active ● • Inactive ●
Name	USP Alert name
Description	Description of the alert
Severity	Severity level of the USP violation that triggers the alert: • C Critical • H High • M Medium • L Low Multiple severities can be selected
Devices	Devices for which this alert is sent
Send to	List of USP alert recipients There is an option to send the alert by syslog

Alerts are triggered by a new revision, but are not triggered when a new service, source, or destination is added on a cell already marked with a violation, or when a violation is removed. When a device or user is removed from the system, the status of any alert containing that device or user automatically changes to **Inactive**.

The alert email provides a summary of the changes and violations and includes such information as:

- The firewall and policy name
- The relevant revision ID and rule number
- Who performed the change and when the change occurred
- A link to SecureTrack, with detailed information about the specific changes that caused the USP violation

What can I do on this page?

- Create a new alert - Click New and enter the requested information.

  If multi-domain mode is enabled, the **Domain:** field appears, which lets you filter the devices for a specific domain.

- Edit an existing alert - Select an alert, click ✎, and modify the desired information.

  If multi-domain mode is enabled, the **Domain:** field appears, which lets you filter the devices for a specific domain.

- **Duplicate an alert** - Select an alert, click ⧉, and modify the desired information.

- **Delete an alert** - Select one or more alerts and click 🗑.

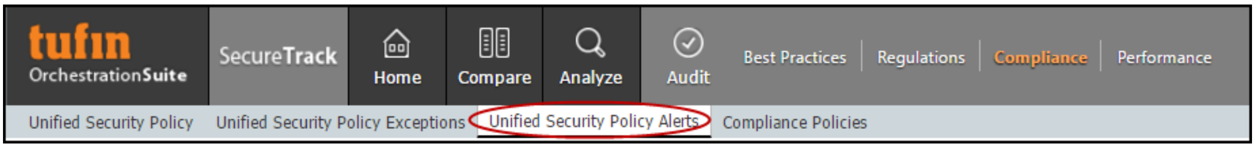
- **Search for alerts** - Enter the search criteria and click 🔍.

  Returns alerts that contain the text in any column.

How Do I Get Here?

To view the Unified Security Policy Alerts:

In SecureTrack, go to **Audit** > **Compliance** > **Unified Security Policy Alerts.**



Creating or Editing a Unified Security Policy Alert

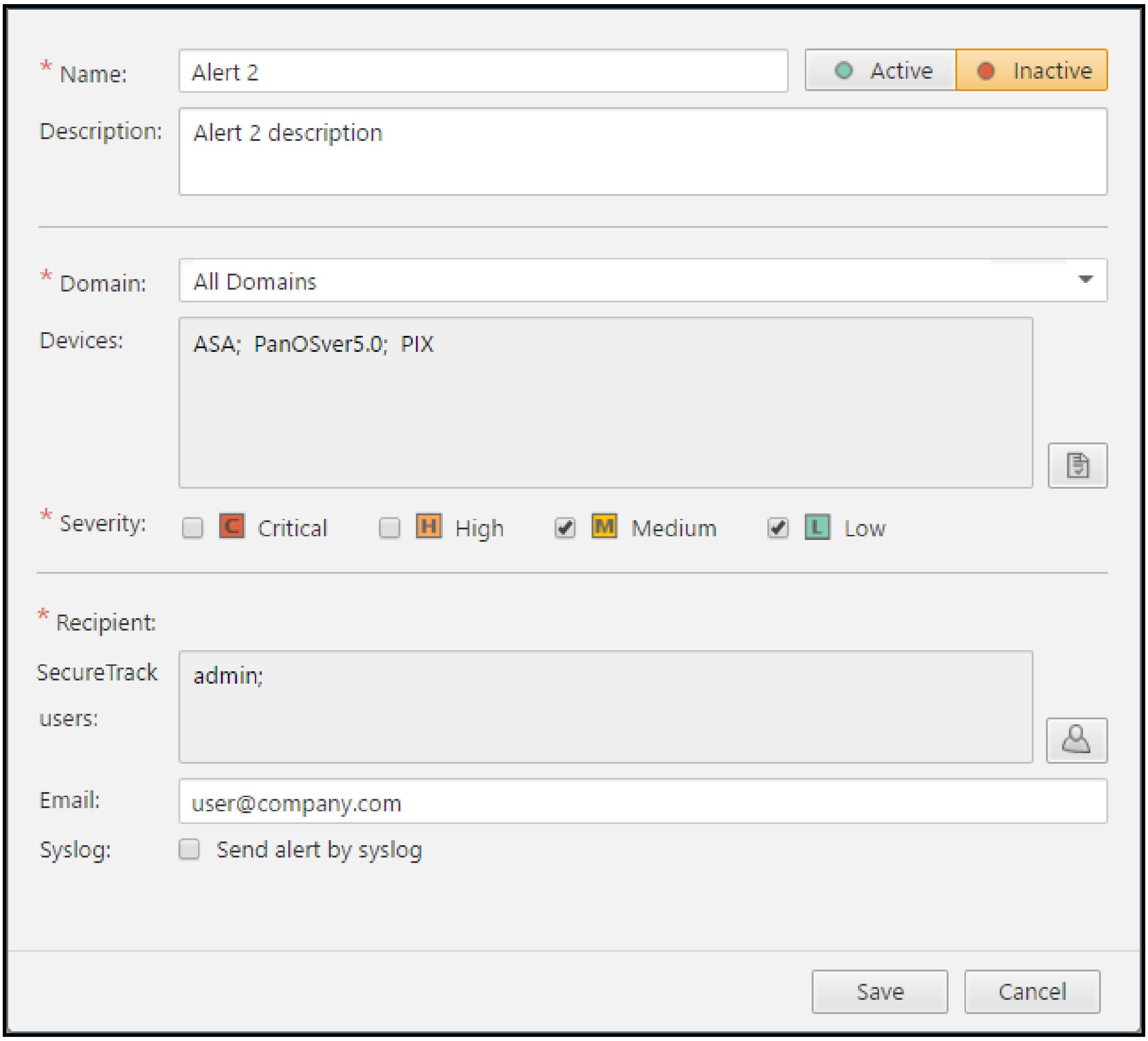
To create or edit an alert:

1. In SecureTrack go to **Audit** > **Compliance** > **Unified Security Policy Alerts**.
2. Do one of the following:
   - Click New to create a new alert.

     The **New Alert** dialog appears.

   - Click ✎ to edit an existing alert.

     The **Edit Alert** dialog appears.



* Name: Alert 2 ● Active ● Inactive

Description: Alert 2 description

* Domain: All Domains

Devices: ASA; PanOSver5.0; PIX

* Severity: □ C Critical □ H High ☑ M Medium ☑ L Low

* Recipient:

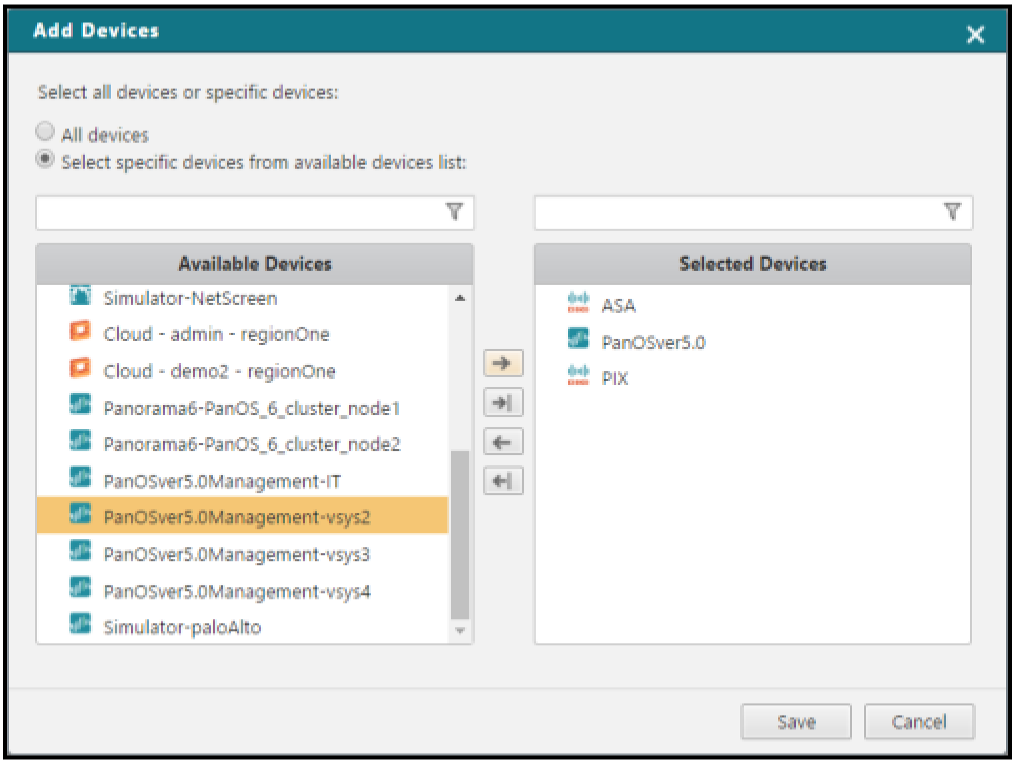
SecureTrack users: admin;

Email: user@company.com

Syslog: □ Send alert by syslog

3. Fill in the desired information:
   - Name
   - Status - Click the **Active** ● or **Inactive** ● button to toggle the alert status.
   - Description
   - Devices - Select the devices for which this alert will be triggered.

     Click 🗎 to open the Add Devices dialog. Add the devices for which this alert is sent.



Add Devices

Select all devices or specific devices:

○ All devices
● Select specific devices from available devices list:

Available Devices	Selected Devices
Simulator-NetScreen	ASA
Cloud - admin - regionOne	PanOSver5.0
Cloud - demo2 - regionOne	PIX
Panorama6-PanOS_6_cluster_node1	
Panorama6-PanOS_6_cluster_node2	
PanOSver5.0Management-IT	
PanOSver5.0Management-vsys2	
PanOSver5.0Management-vsys3	
PanOSver5.0Management-vsys4	
Simulator-paloAlto	

If multi-domain mode is enabled, the **Domain** field appears, which lets you filter the devices for a specific domain.

You can enter text to filter the available and selected devices.

- Severity - Select one or more violation severity levels that will trigger the alert.
- Recipients - List all alert recipients:
  - SecureTrack Users - Click 👤 to add SecureTrack users
  - Email - Enter a list of semi-colon separated email addresses
  - Syslog - Check to send the alert to the Secure Track Syslog Server configured in **Settings** > **Configuration** > **Notifications** > **Configure Servers**

4. Click Save.

Compliance Policies

> This is a Legacy Feature. It will be discontinued as of version R21-3.
>
> We recommend you consider using the following features:
>
> - "Unified Security Policy" on page 366
> - "Unified Security Policy Alerts" on page 389
> - "Configuring Exceptions for the Unified Security Policy" on page 388
>
> These features give you greater flexibility in the number of zones that you can configure and allow you to define the requirements that you need.

You can receive a report when a security policy rule changes access for specified traffic. This is valuable for two purposes:

- **Risk Management**: Report when a rule allows unauthorized connectivity or blocks authorized connectivity.
- **Business Continuity**: Report when a rule blocks business critical traffic.

For a Risk Management policy, you can select to specify blacklisted traffic, or to specify whitelisted traffic. With a whitelist policy, firewall configurations are in violation of the policy if they allow any traffic that is not specified in any of the policy's configured traffic patterns. With a blacklist policy, firewall configurations are in violation of the policy if they allow any blacklisted traffic.

You can define exceptions to a blacklist policy. Traffic defined as an exception is allowed, despite being included in the blacklist. You can restrict exceptions so that they are allowed only when the firewall rule allowing them defines the source or destination host specifically (explicitly or in a group, but not as part of a subnet).

To configure a blacklist policy, you can enter the traffic patterns manually or you can upload a matrix file.

Legacy Compliance Alerts are Compliance Alerts that were defined in SecureTrack 4.1 or lower. If you need to change Legacy Compliance Alerts, contact Tufin Support.

IPv6 is not supported for this TOS feature.

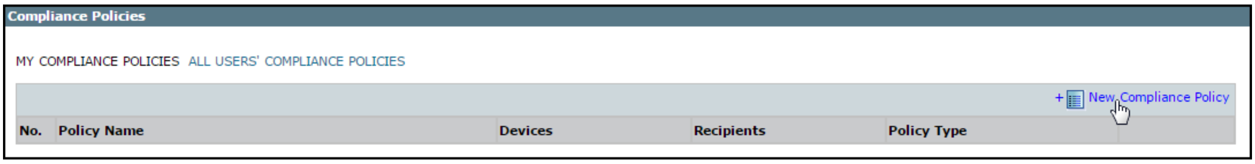
Creating a Compliance Policy

> This is a Legacy Feature. It will be discontinued as of version R21-3.
>
> We recommend you consider using the following features:
>
> - "Unified Security Policy" on page 366
> - "Unified Security Policy Alerts" on page 389
> - "Configuring Exceptions for the Unified Security Policy" on page 388
>
> These features give you greater flexibility in the number of zones that you can configure and allow you to define the requirements that you need.

To configure a Compliance Policy, you define a SecureTrack policy of traffic patterns which should always be allowed, or a SecureTrack policy of traffic patterns which should always be blocked. When a firewall security policy is changed so that it conflicts with this Compliance Policy, an alert, in report form, is sent to the recipients defined for that Compliance Policy. In addition, the Compliance Policy can be run on demand to locate current violations.

To create a new Compliance Policy:

1. Go to **Audit** > **Compliance** and click **New Compliance Policy**:



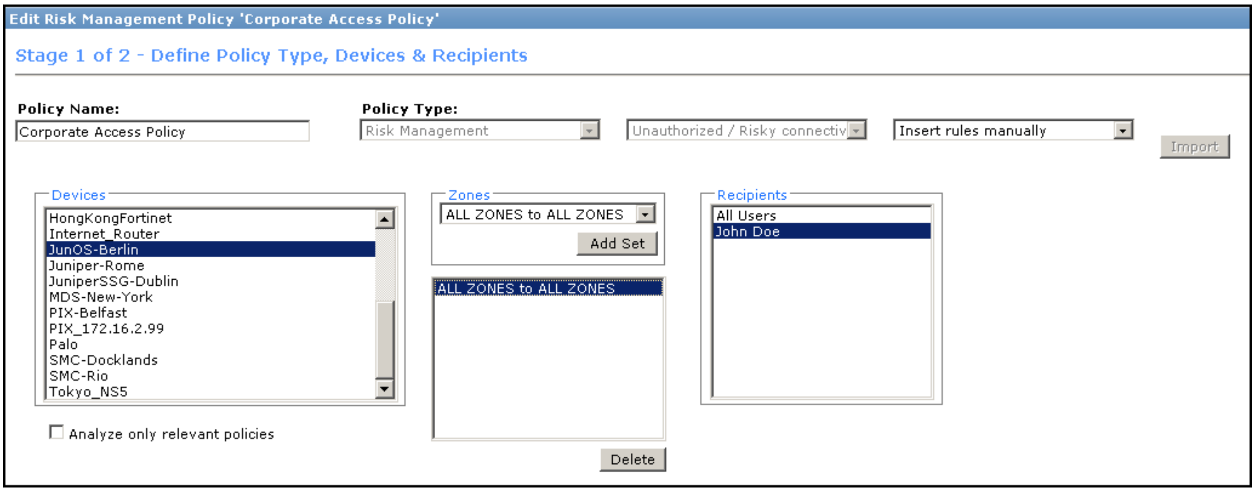
Compliance Policies

MY COMPLIANCE POLICIES ALL USERS' COMPLIANCE POLICIES

+ New Compliance Policy

No.	Policy Name	Devices	Recipients	Policy Type

Stage 1 of the configuration wizard appears:



Edit Risk Management Policy 'Corporate Access Policy'

Stage 1 of 2 - Define Policy Type, Devices & Recipients

Policy Name: Corporate Access Policy

Policy Type: Risk Management | Unauthorized / Risky connectiv | Insert rules manually

Devices: HongKongFortinet, Internet_Router, JunOS-Berlin, Juniper-Rome, JuniperSSG-Dublin, MDS-New-York, PIX-Belfast, PIX_172.16.2.99, Palo, SMC-Docklands, SMC-Rio, Tokyo_NS5

□ Analyze only relevant policies

Zones: ALL ZONES to ALL ZONES

ALL ZONES to ALL ZONES

Recipients: All Users, John Doe

2. Type a **Policy Name**, and select the following:
   - Compliance **Policy Type**:
     - For high-security risk traffic: **Risk Management**. Select whether you will specify the **Unauthorized/Risky connectivity**, or specify exclusively allowed **Authorized connectivity**, to consider all non-specified traffic as high-risk.
     - For business-critical traffic: **Business Continuity**.
   - **Devices** to which the Compliance Policy will apply

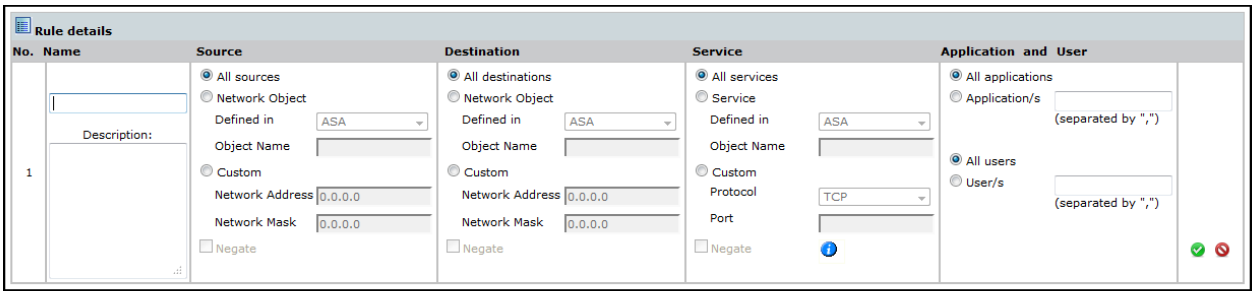
- **Interfaces/Policy Packages/Zones** to add groups of rules that the Compliance Policy will check.
- **Recipients** to receive alerts when installed policy conflicts with this Compliance Policy.

You can also select **Analyze only relevant policies** to let Topology Intelligence find the policies that include rules with the specified zones.

3. Click **Next**.

   Stage 2 of the configuration wizard appears.

4. Configure the traffic patterns to watch:
   1. Click **New Rule**:
   2. Configure a traffic pattern:



Rule details

No.	Name	Source	Destination	Service	Application and User	
1	□ Description: □	● All sources ○ Network Object Defined in ASA Object Name ○ Custom Network Address 0.0.0.0 Network Mask 0.0.0.0 □ Negate	● All destinations ○ Network Object Defined in ASA Object Name ○ Custom Network Address 0.0.0.0 Network Mask 0.0.0.0 □ Negate	● All services ○ Service Defined in ASA Object Name ○ Custom Protocol TCP Port □ Negate	● All applications ○ Application/s (separated by ",") ● All users ○ User/s (separated by ",")	✓ ⊘

Give the traffic pattern a **Name** and **Description**, and configure the traffic's **Source**, **Destination**, and the **Service**. For Palo Alto Networks devices, you can also define the **User** and **Application**. For each of these, you can select:

- **All**
- **Network Object**:

  You can select an object defined in a monitored device, in which case, when the query is run, SecureTrack will use the object definition as it appears in the most recent policy revision from that firewall. Note that object names are case-sensitive. To view exact object names, in **Compare** view, select the most recent policy and click **View Policy**. The object names appear below in the Objects tab.

  Or, for **Source** and **Destination**, you can use an object from **SecureTrack**zones.
- **Custom**:

  For **Source** or **Destination**, explicitly define the **Network Address** and **Network Mask**.

  Under **Service**, either select **TCP**, **UDP**, or **ICMP**, and a **Port** number, or select **Other** to specify an IP **Protocol Number**. You can only create queries for services with IP protocol, such as TCP, ICMP and OSPF. Services that are not IP protocols, such as RPC and DCE/RPC, are not supported.

  For **Port** or for an IP **Protocol Number**, you can do any of the following:

  - Type a range. For example: **100-200** .

  - Specify multiple ports in a list, separated by commas. For example: **80, 81, 443** .

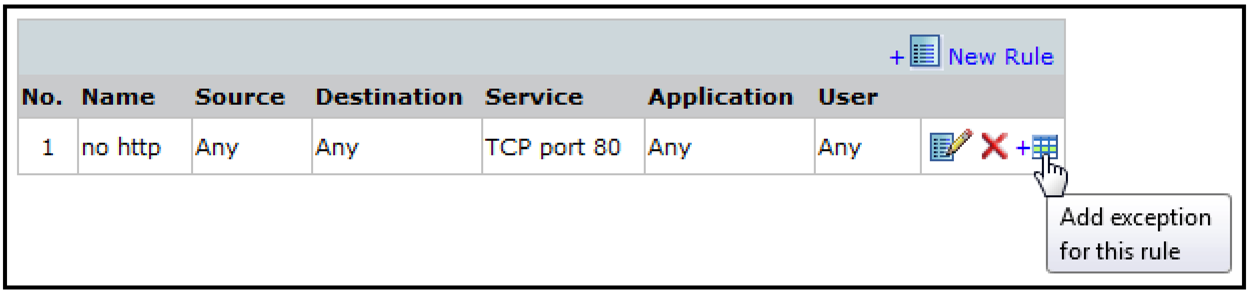
  - Specify an open-ended range with Less Than or Greater Than. for example: **>1023** .

  - Combine elements in a list. For example: **80-81, >1023** .

  To define the Source, Destination, or Service as any host other than the specified, select **Negate**.

   Click ✓.

   3. In a Blacklist Compliance Policy, to define an exception to this traffic pattern (that is, to define a subset of the traffic pattern that can be allowed), click: +▦:



+ New Rule

No.	Name	Source	Destination	Service	Application	User	
1	no http	Any	Any	TCP port 80	Any	Any	✎ ✗ +▦

4. Configure the traffic to be excepted. For Source and/or Destination, you can select **Hosts only** to restrict the exception so that it is allowed only when the firewall rule allowing it defines the source or destination host specifically (explicitly or in a group, but not as part of a subnet). For Service, you can select **Specified ports only** to restrict the exception so that it is allowed only when the firewall rule allowing it defines the service specifically but not as an 'any' object (such as ‘any’ or ‘any-tcp’).

5. Click ✓.

5. Once you have finished configuring traffic patterns for the Compliance policy, **Save** the Compliance Policy.

Your Compliance Policy now appears in the Compliance Policies list. The specified recipients will receive alerts when there is a policy violation. The report is in the format defined in the Reports tab.

From the list, you can select the report and **Run**, **Edit**, or **Delete** it.

Creating a Blacklist from a Matrix

> This is a Legacy Feature. It will be discontinued as of version R21-3.
>
> We recommend you consider using the following features:
>
> - "Unified Security Policy" on page 366
> - "Unified Security Policy Alerts" on page 389
> - "Configuring Exceptions for the Unified Security Policy" on page 388
>
> These features give you greater flexibility in the number of zones that you can configure and allow you to define the requirements that you need.

You can create blacklist policies by configuring a matrix in a CSV file and importing it into SecureTrack. The CSV file refers to source and destination SecureTrack Network Zones, and defines for each source-destination pair whether the traffic should be fully blocked, fully permitted (subnet-to-subnet allowed), or permitted only for firewall rules that define the source and/or destination host specifically (explicitly or in a group, but not as part of a subnet).

To create a matrix file:

1. If they do not already exist, configure SecureTrack network Zones for all subnets that need to be referenced as sources or destinations.
2. Create a text file in CSV format (you can create it in Excel and later save as CSV). The first column of the represented table should contain source Zone names; The first row should contain destination Zone names. Each source-destination intersection cell should contain one of the following:

NA No Access: Access is blacklisted.

S2S Subnet to Subnet: Access is fully permitted.

H2S Host to Subnet: Access permitted only if allowed by a firewall rule that defines the source host specifically.

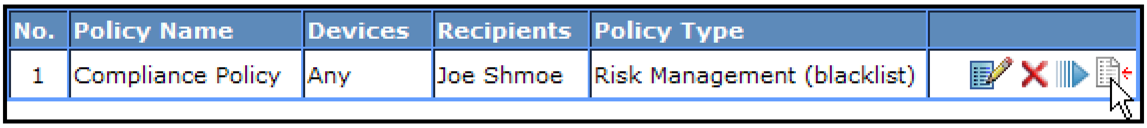
S2H Subnet to Host: Access permitted only if allowed by a firewall rule that defines the destination host specifically.

H2H Host to Host: Access permitted only if allowed by a firewall rule that defines the source and destination hosts specifically.

See the example below.

To then create a Blacklist from the matrix file:

1. Create a Blacklist Compliance Policy for the relevant device(s) and recipient(s). You don't need to define any connectivity items; these will be defined by the imported CSV file, which will overwrite any connectivity items you may define in the web interface.
2. In the Compliance Policies list, for the Blacklist Compliance Policy you just created, click: 📄:



No.	Policy Name	Devices	Recipients	Policy Type	
1	Compliance Policy	Any	Joe Shmoe	Risk Management (blacklist)	

3. Navigate to the CSV file, and click **Open**.

The Blacklist Compliance Policy is populated with the configuration from the file.

The following is an example of a Blacklist configuration file:

```
,Zone1,Zone2,Zone3

Zone1,NA,NA,S2S

Zone2,S2S,NA,S2S
```

```
Zone3,S2H,H2H,H2S
```

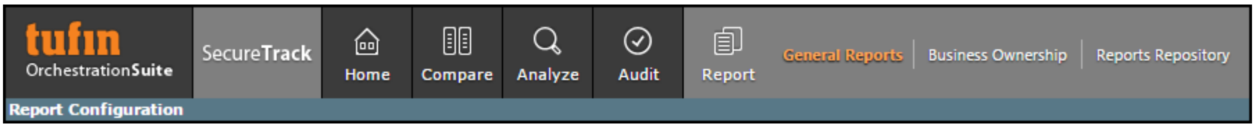
This example represents the following table:

	Zone1	Zone2	Zone3
Zone1	NA	NA	S2S
Zone2	S2S	NA	S2S
Zone3	S2H	H2H	H2S

In this example, hosts from Zone1 can access only IP addresses in Zone3; hosts from Zone2 can access IP addresses in Zones 1 and 3, but not other hosts within their Zone; and hosts from Zone3 cannot access any IP addresses, unless the access is allowed per-individual source host (for Zone3), destination host (for Zone 1), or both (required for Zone2).

Reporting

SecureTrack includes reports that give you real-time information about your security posture. Most reports can be scheduled or manually generated within minutes, and relate to the current policy as monitored in real-time. You can also configure the report for past policies.



Additional device agnostic reports can be found in the SecureTrack Reporting Essentials Tufin Marketplace App.

How Reports Work

Most of SecureTrack's reports can be found in **Report** view. You can configure them for automatic generation on an event or schedule, or you can run them manually and view them as HTML or as a PDF.

Make sure that the time on every TOS server and every client is synchronized.

Automatically generated reports can be configured to run at specified time intervals, or upon a specified event, depending on report type. Automatically generated reports can be configured to be emailed, to be saved in SecureTrack's Report Repository, and/or (Administrators only) to be exported to a repository or portal. When the report is saved to Report Repository, configured recipients can receive a link to the report. When the report is exported, the report owner can be notified.

When the report is created by a SecureTrack Administrator, multiple recipients can be defined, by selecting available SecureTrack users, and other recipients can be defined by using email addresses. In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.

When a report is configured to be emailed or stored in the Report Repository, a separate report is generated for each configured recipient, according to their own configured preferences and permissions.

You can configure the file format for the emailed report and add your corporate logo to the reports.

Reports are subject to Administrative supervision.

Configuring SecureTrack Reports

SecureTrack includes reports that you can configure:

- Immediate updates when changes are made
- Scheduled reports to see what changes were made over a period of time
- A review of the current status of the policies in your environment

After a report has been configured, you can view the report.

Note: IPv6 is supported for this feature, as follows: IPV6 addresses are shown in the New revision and Advanced change reports.

Additional device agnostic reports can be found here.

New Revision Report

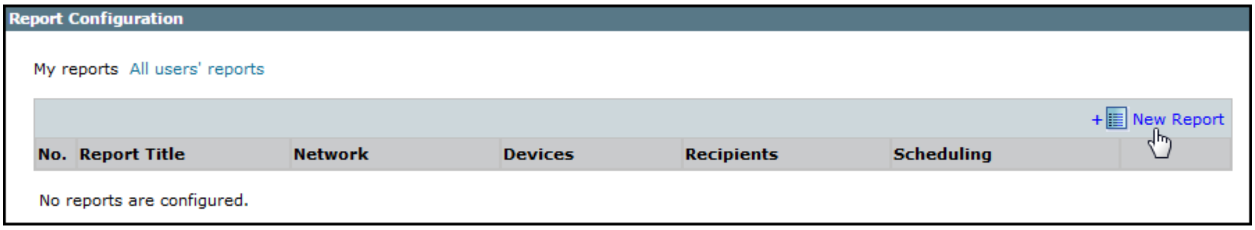
The New Revision report lists all changes on the selected devices since the last revision, such as updates to rules, hosts and global properties. It also includes rules that even though they have not been directly updated, they have been affected by objects and therefore are reported as changed.

It is generated automatically whenever a new revision is retrieved in SecureTrack. The report is sent to recipients that you assign when setting up the report.

You can configure notifications to be sent by syslog or SNMP in the Notifications page.

To configure a New Revision Report:

1. Go to **Report**> **General Reports**, and click **New Report.**



Report Configuration

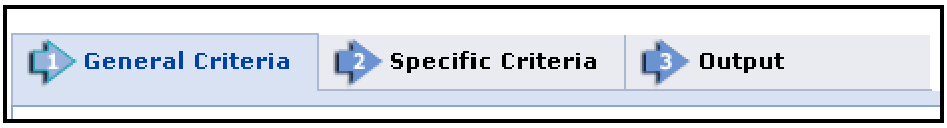
My reports All users' reports

+ New Report

No.	Report Title	Network	Devices	Recipients	Scheduling

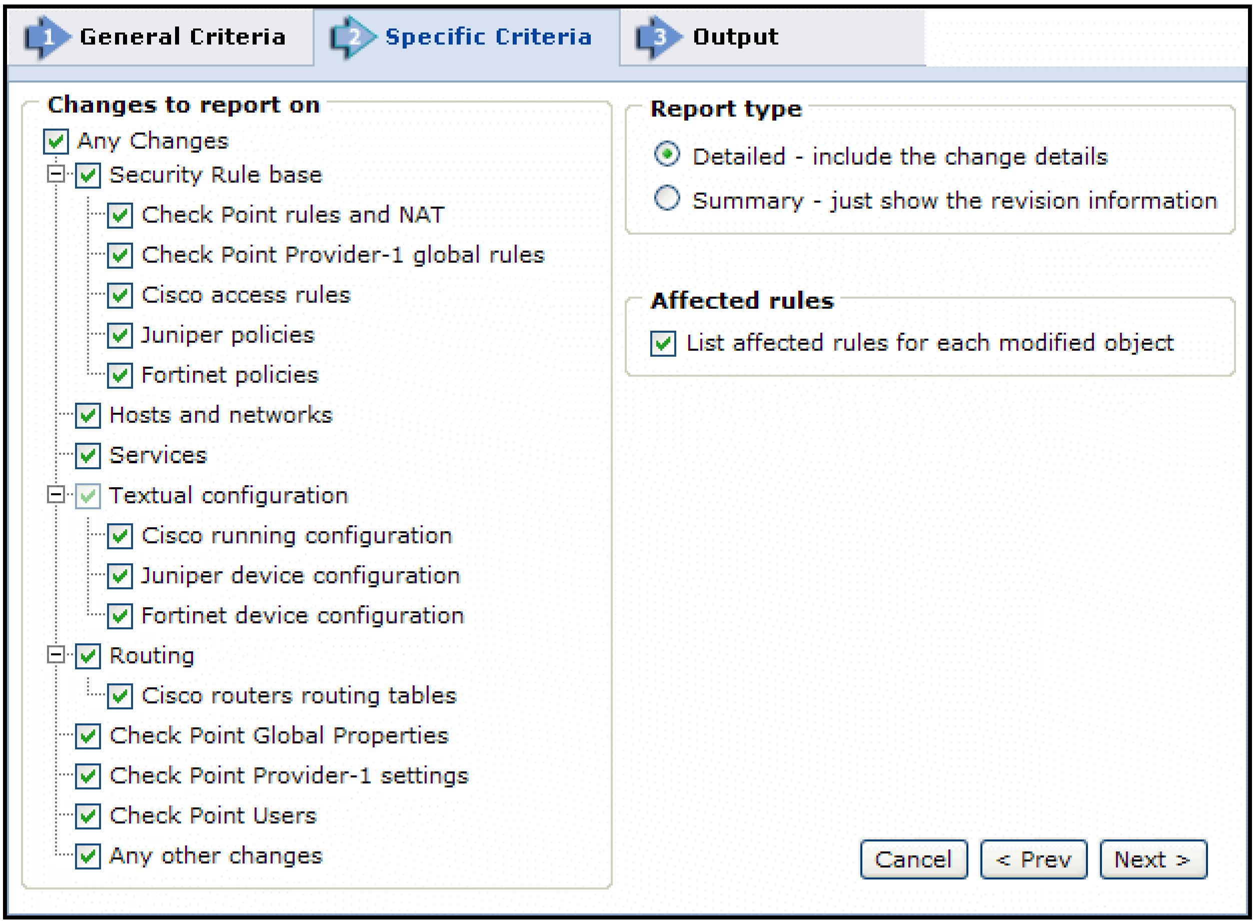
No reports are configured.

The report configuration wizard has 3 steps.



2. **STEP 1**: Configure the **General Criteria** and click **Next**.
    1. For **ReportType**, select **New Revision**.
    2. Optionally, you can change the **Title**. By default, the report's general name with the current date is the report name.
    3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
    4. Select **Devices** for the report.

       If you have selected one domain, you can limit the report to include specific devices in the domain.
       If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.
3. **STEP 2**: Configure the **Specific Criteria** as explained in the table and click **Next**.



Changes to report on

- ☑ Any Changes
  - ☑ Security Rule base
    - ☑ Check Point rules and NAT
    - ☑ Check Point Provider-1 global rules
    - ☑ Cisco access rules
    - ☑ Juniper policies
    - ☑ Fortinet policies
  - ☑ Hosts and networks
  - ☑ Services
  - ☑ Textual configuration
    - ☑ Cisco running configuration
    - ☑ Juniper device configuration
    - ☑ Fortinet device configuration
  - ☑ Routing
    - ☑ Cisco routers routing tables
  - ☑ Check Point Global Properties
  - ☑ Check Point Provider-1 settings
  - ☑ Check Point Users
  - ☑ Any other changes

Report type

● Detailed - include the change details

○ Summary - just show the revision information

Affected rules

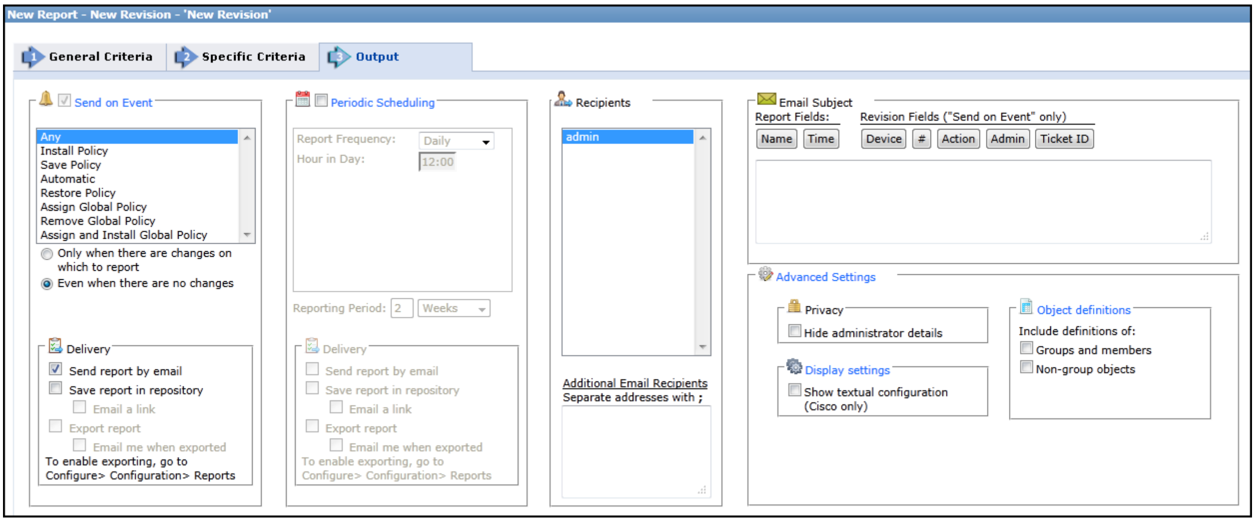
☑ List affected rules for each modified object

Parameter	Description
Changes to report on	To include all changes, select **Any Changes**. To limit the report to include only changes to specific

	parts of the policy, such as rules, host, global properties, select what to include in the report.
Report type	• **Detailed**: A complete report of the changes, including details, is emailed to the recipients. • **Summary**: A summary report of changes is emailed to the recipients.
List affected rules for each modified object:	Select whether the report should list rules that are affected by objects reported as changed.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list. From the list, you can **Run** ( ), **Edit** ( ), or **Delete** ( ) it.



New Report - New Revision - 'New Revision'

1 General Criteria | 2 Specific Criteria | 3 Output

☑ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

○ Only when there are changes on which to report
● Even when there are no changes

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

□ Periodic Scheduling

Report Frequency: Daily
Hour in Day: 12:00
Reporting Period: 2 Weeks

Delivery
□ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name Time
Revision Fields ("Send on Event" only) Device # Action Admin Ticket ID

Advanced Settings

Privacy
□ Hide administrator details

Display settings
□ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
□ Groups and members
□ Non-group objects

Parameter	Description
Send on event	Select the events to trigger this report. You can use the <shift> key to select more than one event. Select one of the following, to decide whether to always run the report after the event, even when there are no changes: • **Only when the policy was modified**: Only if there are changes to be reported on, relative to the previous revision. • **Even if the policy was not modified**: If there are no changes, the report will state that there were no changes. For example, if an administrator first saves a Check Point policy, and then installs the policy on a gateway a few minutes later, the second event has not modified the policy.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them. The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page. A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page. To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view). Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification). When a SecureTrack User creates a report, only that User is a recipient. When a SecureTrack Administrator creates a report, multiple recipients can be defined. These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack. Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. Note: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email	Enter additional email recipient addresses. Separate the addresses with a semicolon (;).

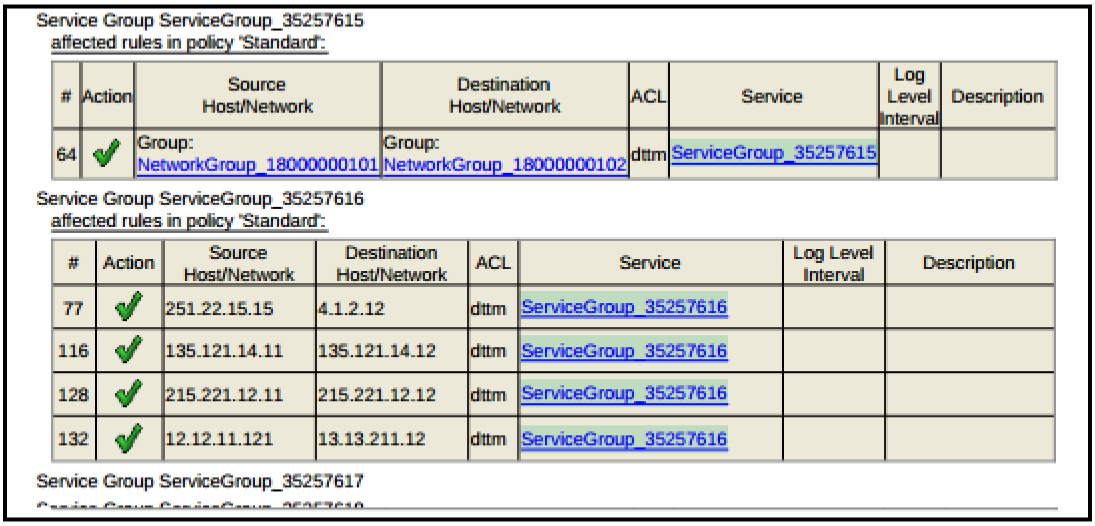
Recipients	
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results. Only the ticket ID is included. This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**: • **Groups and members** - The report includes the definitions of group objects and their member objects. This is useful for recipients that do not have SecureTrack access. SecureTrack users can click on group objects in the report to see the definitions. • **Non-group objects** - The report includes definitions of non-group objects.

Advanced Change Report

The Advanced Change report enables you to examine, in detail, the policy changes of selected devices. You can run this report in two different ways:

- Incremental: Lists the differences between each individual revision with its predecessor.
- Accumulated: Lists the differences between the latest and initial revisions.

For Check Point devices, if multiple policy packages are used for different gateways, you can select packages per Installation Target group. The report will contain a section for each selected package.



Service Group ServiceGroup_35257615
affected rules in policy 'Standard':

#	Action	Source Host/Network	Destination Host/Network	ACL	Service	Log Level Interval	Description
64	✓	Group: NetworkGroup_18000000101	Group: NetworkGroup_18000000102	dttm	ServiceGroup_35257615		

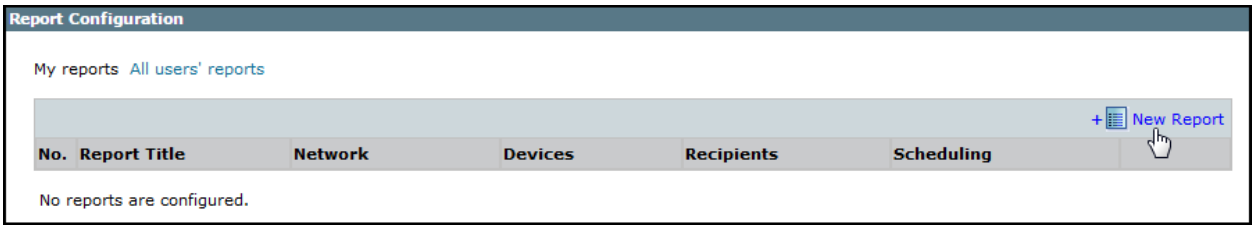
Service Group ServiceGroup_35257616
affected rules in policy 'Standard':

#	Action	Source Host/Network	Destination Host/Network	ACL	Service	Log Level Interval	Description
77	✓	251.22.15.15	4.1.2.12	dttm	ServiceGroup_35257616		
116	✓	135.121.14.11	135.121.14.12	dttm	ServiceGroup_35257616		
128	✓	215.221.12.11	215.221.12.12	dttm	ServiceGroup_35257616		
132	✓	12.12.11.121	13.13.211.12	dttm	ServiceGroup_35257616		

Service Group ServiceGroup_35257617

To configure an Advanced Change Report:

1. Go to **Report** > **General Reports**, and click **New Report.**



Report Configuration

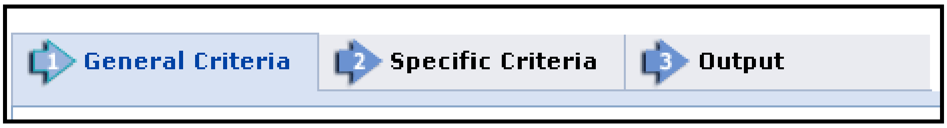
My reports All users' reports

+ New Report

No.	Report Title	Network	Devices	Recipients	Scheduling

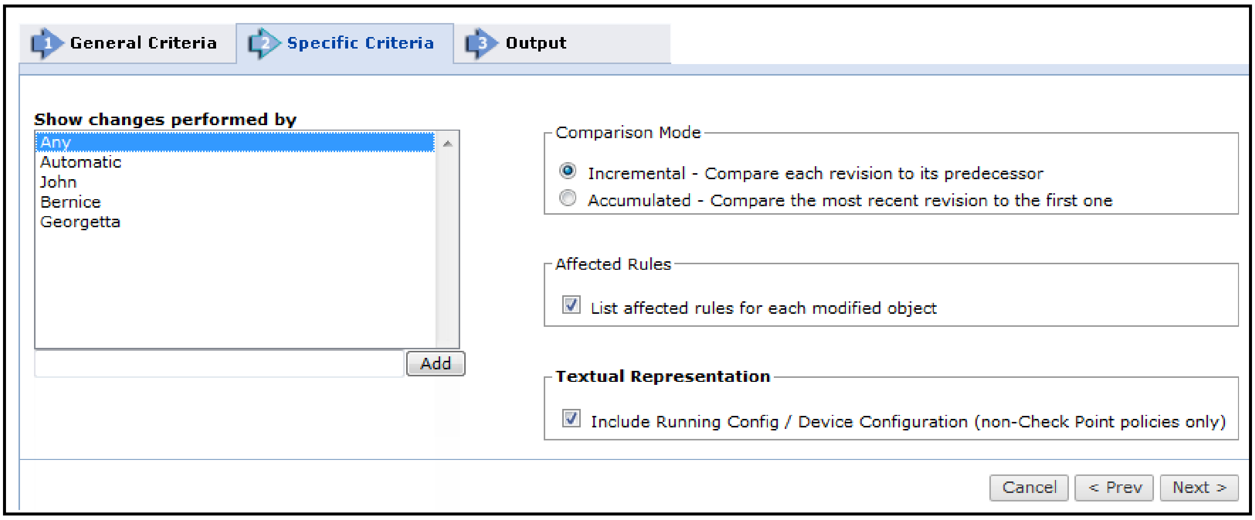
No reports are configured.

The report configuration wizard has 3 steps.



2. STEP 1: Configure the **General Criteria** and click **Next**.
   1. For **ReportType**, select **Advanced Change**:
   2. Optionally, you can change the **Title**. By default, the report's general name with the current date is the report name.
   3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
   4. Select **Devices** for the report.

      If you have selected one domain, you can limit the report to include specific devices in the domain.
      If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.
   5. For Check Point devices, if you have selected one device, you can limit the report to include specific **Policy Packages**. If you have selected more than one device, then **Any** is selected for **Policy Packages** and all policy packages in the selected devices are included in the report.
3. STEP 2: Configure the **Specific Criteria** as explained in the table and click **Next**.



Show changes performed by

Any
Automatic
John
Bernice
Georgetta

Comparison Mode

● Incremental - Compare each revision to its predecessor
○ Accumulated - Compare the most recent revision to the first one

Affected Rules

☑ List affected rules for each modified object

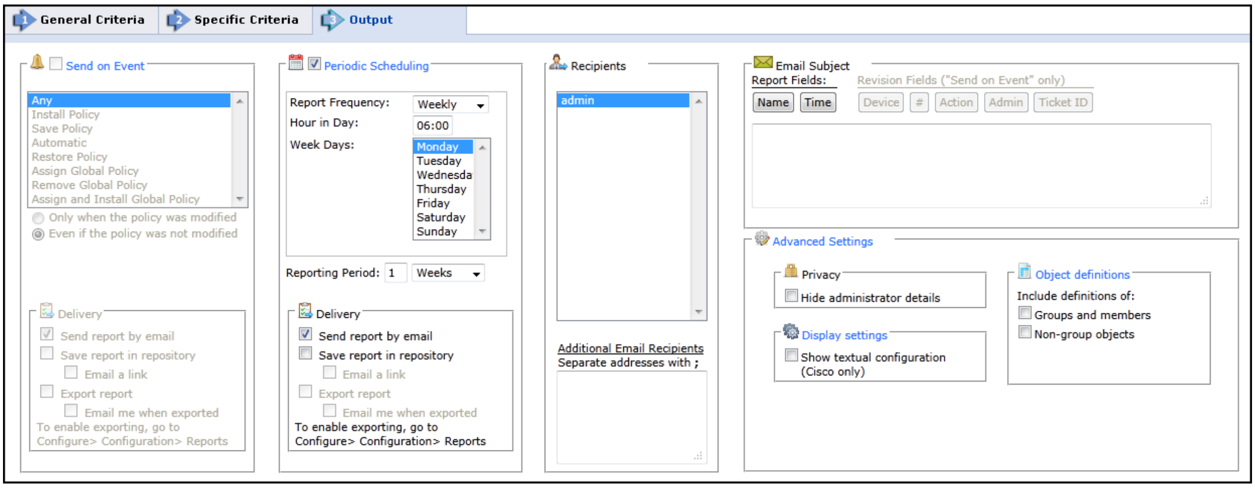
Textual Representation

☑ Include Running Config / Device Configuration (non-Check Point policies only)

Parameter	Description
Show changes performed by	You can limit the report to changes performed by specific people, by selecting their names or select **Any** to list all changes. You can add someone by entering the name in the text box below the list and clicking **Add**.
Comparison Mode	• **Incremental**: Each revision is compared to the previous revision. • **Accumulated**: Only the most recent revision is compared, to the earliest revision in SecureTrack's database.
Affected Rules	Select **List affected rules for each modified object** to have the report list rules that are affected by objects reported as changed.
Textual Representation	Select **Include Running Config / Device Configuration** to include policy textual representation. Not relevant to Check Point policies.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

The saved report appears in the General Reports list. From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✗) it.



General Criteria | Specific Criteria | Output

☐ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Reporting Period: 1 Weeks

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name Time
Revision Fields ("Send on Event" only) Device # Action Admin Ticket ID

Advanced Settings

Privacy
☐ Hide administrator details

Display settings
☐ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
☐ Groups and members
☐ Non-group objects

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation. The report can be generated on a daily, weekly, or monthly basis. **Reporting Period** controls how far back the report will span from the time of generation.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them. The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page. A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page. To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view). Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification). When a SecureTrack User creates a report, only that User is a recipient. When a SecureTrack Administrator creates a report, multiple recipients can be defined. These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack. Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. Note: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses. Separate the addresses with a semicolon (;)..
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results. Only the ticket ID is included. This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**:

- **Groups and members** - The report includes the definitions of group objects and their member objects. This is useful for recipients that do not have SecureTrack access. SecureTrack users can click on group objects in the report to see the definitions.
- **Non-group objects** - The report includes definitions of non-group objects.

Firewall Module Change Report

The Firewall Module Change report provides a detailed analysis of policy changes that were installed on a specific gateway.

It is relevant for IT departments that accumulate changes (via Save) before installing them on gateways, and also in cases where different policies are installed on different gateways.

This report is only available for:

- Check Point devices - lists policy changes installed on the specified Check Point gateways.
- Juniper devices connected to a monitored NSM - lists the policy changes since the last installation for each selected device.

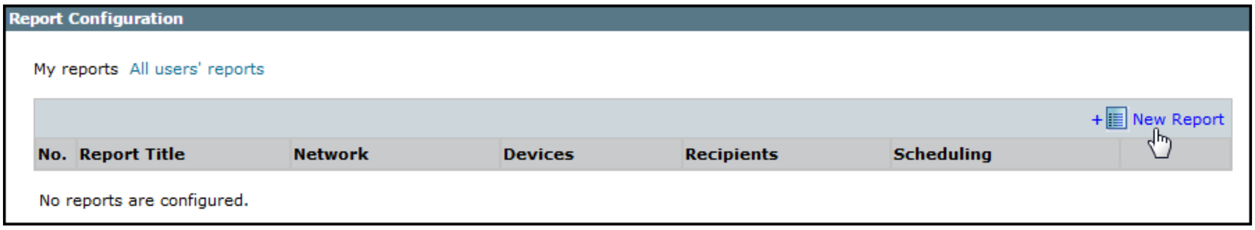
  This report displays each Install Policy event that occurs on specific gateways, displaying all of the changes that were made since the previous policy installation on the gateway.It does not give details on incremental changes that may have occurred, leading up to the current policy installation.The administrator indicated in each step is responsible for the policy installation, but is not necessarily the administrator responsible for all changes to the policy.

The Firewall Module Change report can be scheduled to be automatically generated, and sent to different users.

IPv6 is not supported for this TOS feature.

To configure a Firewall Module Change report:

1. Go to**Report**> **General Reports**, and click **New Report.**

   Report Configuration

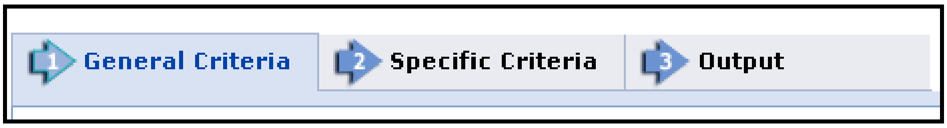
   My reports All users' reports

   + New Report

No.	Report Title	Network	Devices	Recipients	Scheduling

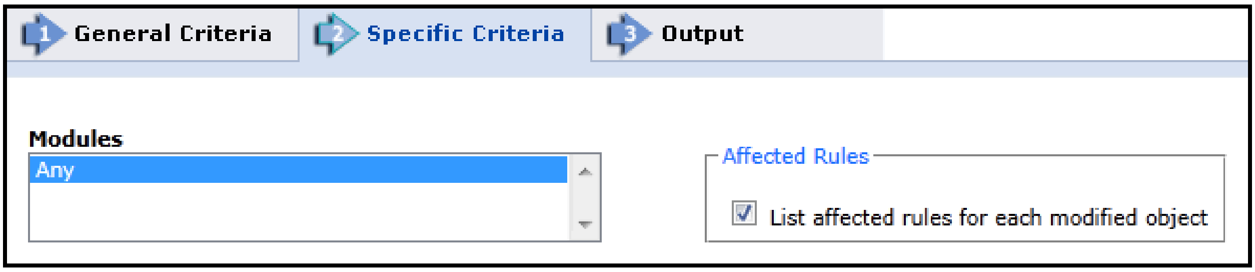
   No reports are configured.

   The report configuration wizard has 3 steps.

2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   1. For **ReportType**, select **Firewall Module Change**:
   2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
   3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
   4. Select **Devices** for the report.

      If you have selected one domain, you can limit the report to include specific devices in the domain.
      If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.
3. **STEP 2**: Configure the following in the **Specific Criteria** tab and click **Next**.
   - **Modules**: Select the modules.
   - **List affected rules for each modified object**: Select this option to have the report include rules that are affected by objects changes.

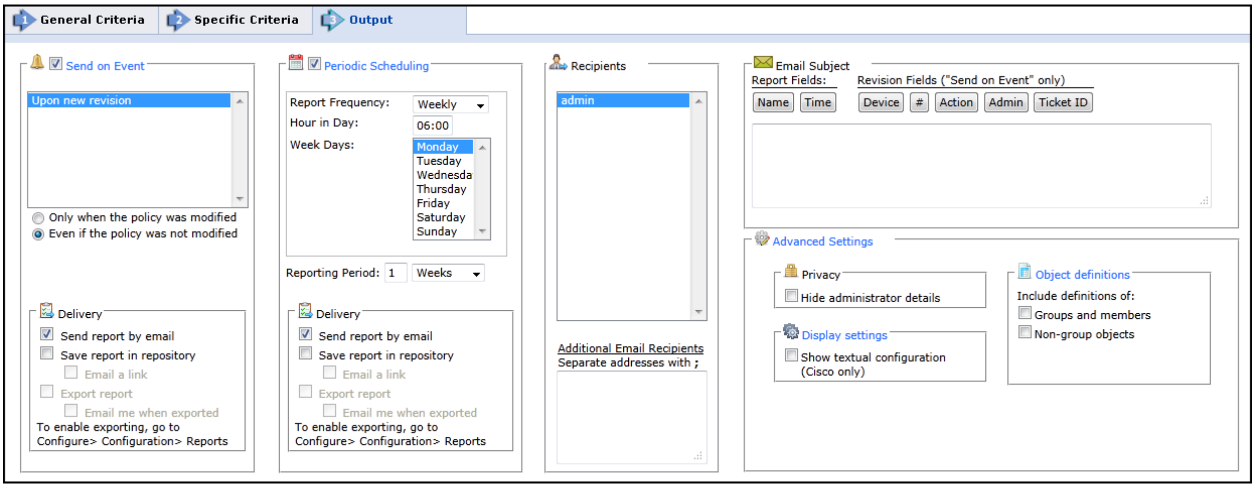


Modules: Any

Affected Rules: ☑ List affected rules for each modified object

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

The saved report appears in the General Reports list. From the list, you can Run (▶), **Edit** (✎), or **Delete** (✕) it.



☑ Send on Event: Upon new revision

○ Only when the policy was modified
● Even if the policy was not modified

Delivery:
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling:
Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday (Monday selected)
Reporting Period: 1 Weeks

Delivery:
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients: admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name | Time
Revision Fields ("Send on Event" only): Device | # | Action | Admin | Ticket ID

Advanced Settings
Privacy: ☐ Hide administrator details
Display settings: ☐ Show textual configuration (Cisco only)
Object definitions: Include definitions of: ☐ Groups and members ☐ Non-group objects

Parameter	Description
Send on Event	Select the events to trigger this report.You can use the <shift> key to select more than one event. Select one of the following, to decide whether to always run the report after the event, even when there are no changes: - **Only when the policy was modified**: Only if there are changes to be reported on, relative to the previous revision. - **Even if the policy was not modified**: If there are no changes, the report will state that there were no changes.For example, if an administrator first saves a Check Point policy, and then installs the policy on a gateway a few minutes later, the second event has not modified the policy.
Deliver	The report can be delivered in any of the following three ways: - **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. - **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. - **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.**Reporting Period** controls how far back the report will span from the time of generation.
Delivery	The report can be delivered in any of the following three ways: - **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. - **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a

	report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**: • **Groups and members** - The report includes the definitions of group objects and their member objects.This is useful for recipients that do not have SecureTrack access.SecureTrack users can click on group objects in the report to see the definitions. • **Non-group objects** - The report includes definitions of non-group objects.

Rule Change Report

The Rule Change report lists the changes made to selected rule/s in a selected firewall over a specified amount of time.

You can use this report to:

- Pinpoint the exact point in time a rule changed and who made the change.
- Notify you immediately when sensitive rules are changed.

This report can also be helpful when you find a firewall rule that appears to be wrong or inconsistent with your corporate policy.You can use this report to see all of the changes made to this rule over time, and track who made what change and when.

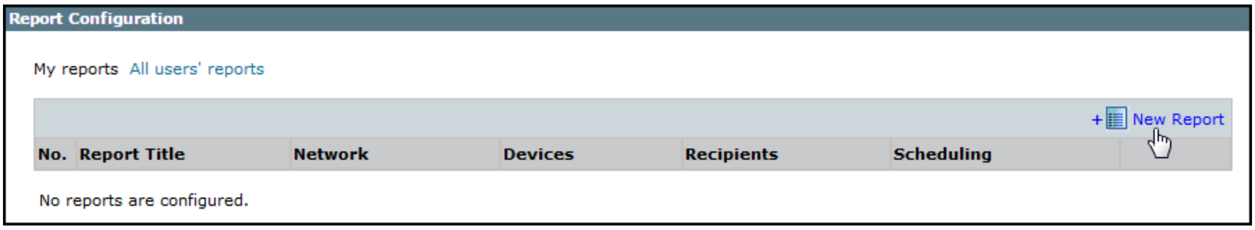
For Check Point devices, if multiple policy packages are used for different gateways, you can select one package per Installation Target group.

You can configure the Rule Change report to generate on a schedule or when a change event happens, and to send the report to multiple users.

IPv6 is not supported for this TOS feature.

To configure a Rule Change report:

1. Go to **Report**> **General Reports**, and click **New Report.**



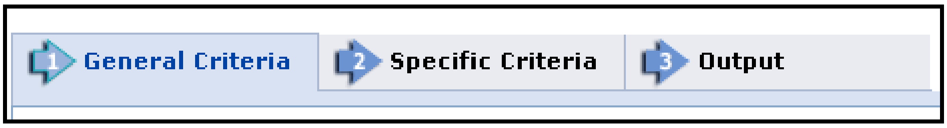
Report Configuration

My reports All users' reports

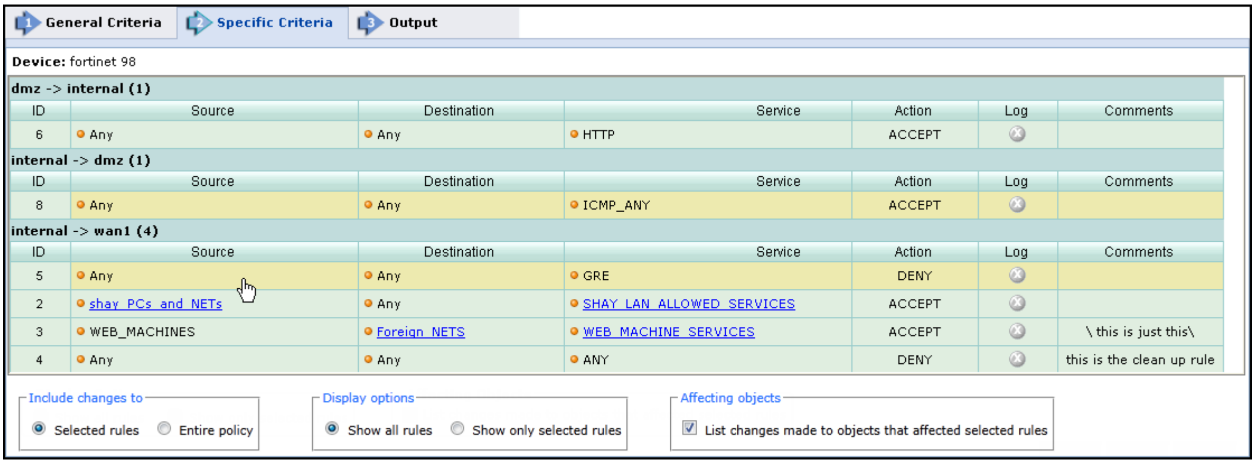
No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.



2. **STEP 1**: Configure the **General Criteria** and click **Next**.
    1. For **ReportType**, select **Rule Change**.
    2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
    3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
    4. Select a device for the report.(For this report, you can only select one device.)
    5. From **Policy Packages**, select **Any** or a specific policy.
3. **STEP 2**: Configure the following in the **Specific Criteria** tab and click **Next**.



Device: fortinet 98

dmz -> internal (1)

ID	Source	Destination	Service	Action	Log	Comments
6	Any	Any	HTTP	ACCEPT	⊗	

internal -> dmz (1)

ID	Source	Destination	Service	Action	Log	Comments
8	Any	Any	ICMP_ANY	ACCEPT	⊗	

internal -> wan1 (4)

ID	Source	Destination	Service	Action	Log	Comments
5	Any	Any	GRE	DENY	⊗	
2	shay_PCs_and_NETs	Any	SHAY_LAN_ALLOWED_SERVICES	ACCEPT	⊗	
3	WEB_MACHINES	Foreign_NETS	WEB_MACHINE_SERVICES	ACCEPT	⊗	\ this is just this\
4	Any	Any	ANY	DENY	⊗	this is the clean up rule

Include changes to: ● Selected rules ○ Entire policy

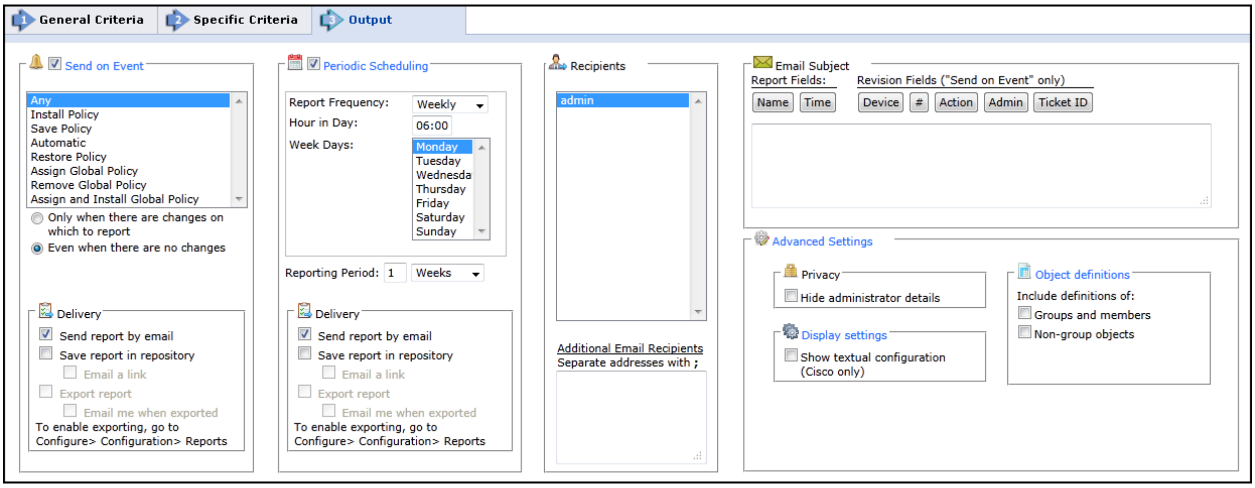
Display options: ● Show all rules ○ Show only selected rules

Affecting objects: ☑ List changes made to objects that affected selected rules

- **Include changes to**: Select either the selected rules or the entire policy.
- **Display Options**: Select to show non-selected rules.
- **Affecting Objects**: Select to include objects changes affecting the specified rules.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✗) it.



☑ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

○ Only when there are changes on which to report
● Even when there are no changes

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Reporting Period: 1 Weeks

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients

admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields:
Revision Fields ("Send on Event" only)

Advanced Settings

Privacy
□ Hide administrator details

Display settings
□ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
□ Groups and members
□ Non-group objects

Parameter	Description
Send on Event	Select the Policy Change events to trigger this report.You can use the <shift> key to select more than one event. Select one of the following, to decide whether to always run the report after the event, even when there are no changes: • **Only when there are changes on which to report**: Only if there are changes to be reported on, relative to the previous revision. • **Even when there are no changes**: If there are no changes to be reported on, the report will state that there were no changes.For example, if an administrator first saves a Check Point policy, and then installs the policy on a gateway a few minutes later, the second event has
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.**Reporting Period** controls how far back the report will span from the time of generation.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (;) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have

	permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**: • **Groups and members** - The report includes the definitions of group objects and their member objects.This is useful for recipients that do not have SecureTrack access.SecureTrack users can click on group objects in the report to see the definitions. • **Non-group objects** - The report includes definitions of non-group objects.

Object Change Report

The Object Change report lists the changes made to specific objects. This report includes network objects, services, and users.

You can use this report to:

- Pinpoint the exact point in time an object was changed and who made the change.
- Notify you immediately when sensitive objects are changed, such as firewall objects or critical network objects.

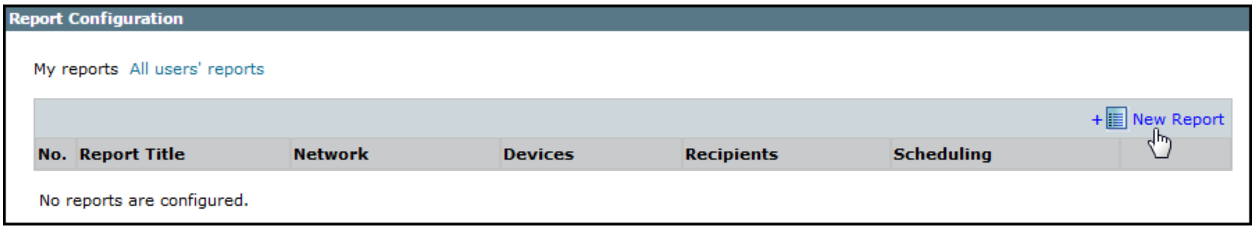
This report can also help when you find an object that appears to be defined incorrectly or inconsistent with corporate policy.Run the report on the object to list the changes made over time, and track who made what change and when.

For Palo Alto policies, Application and LDAP User objects are not supported for this report.Local User objects are supported.

IPv6 is not supported for this TOS feature.

To configure an Object Change report:

1. Go to **Report**> **General Reports**, and click **New Report.**



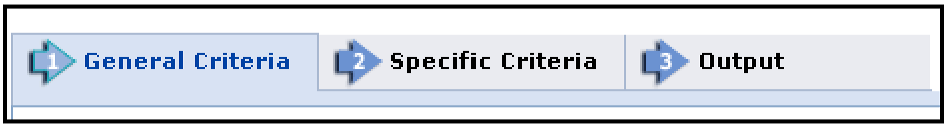
Report Configuration

My reports All users' reports

No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.



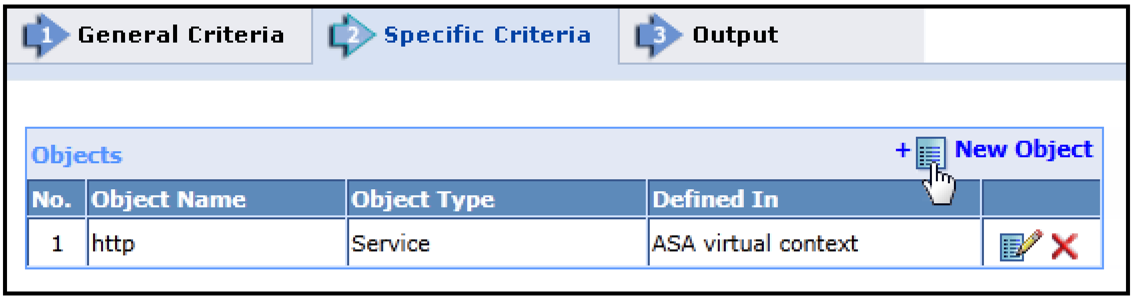
2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   1. For **ReportType**, select **Object Change**:
   2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.

3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
4. Select **Devices** for the report.

   If you have selected one domain, you can limit the report to include specific devices in the domain.
   If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.

3. **STEP 2**: Configure the object(s) to be tracked in the **Specific Criteria** tab and click **Next**.

   The **Objects** list (initially, the list is empty):



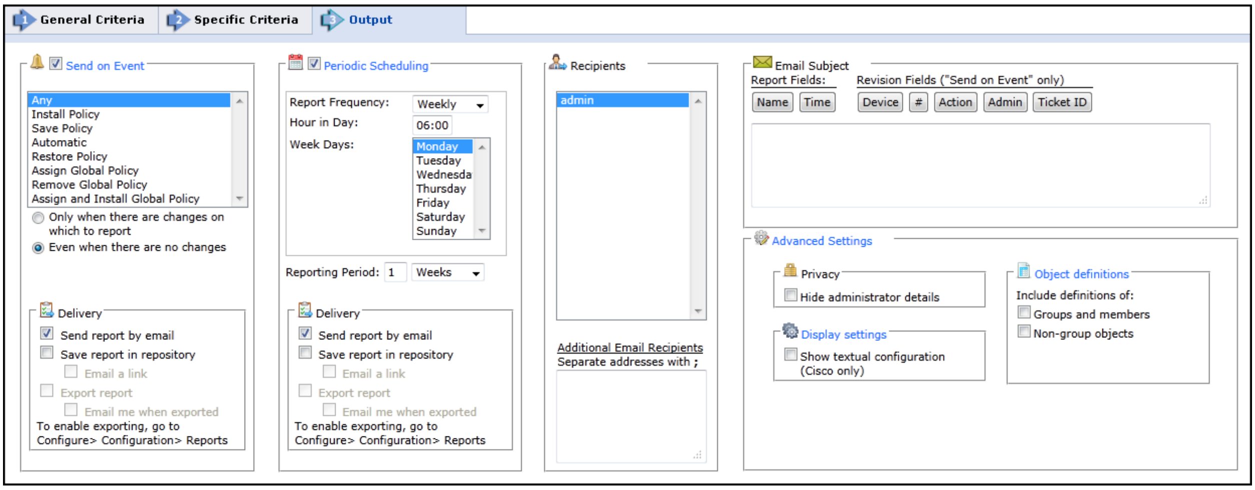
Objects

No.	Object Name	Object Type	Defined In	
1	http	Service	ASA virtual context	✎ ✗

   1. Click **New object**.
   2. Type the **Object Name**, and select the **Object Type** and the policy that it is **Defined In**.
   3. Save the object by clicking: ✓

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✗) it.



☑ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

○ Only when there are changes on which to report
● Even when there are no changes

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday Tuesday Wednesda Thursday Friday Saturday Sunday

Reporting Period: 1 Weeks

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients

admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields:
Revision Fields ("Send on Event" only)

Advanced Settings

Privacy
☐ Hide administrator details

Display settings
☐ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
☐ Groups and members
☐ Non-group objects

Parameter	Description
Send on Event	Select the events to trigger this report.You can use the <shift> key to select more than one event. Select one of the following, to decide whether to always run the report after the event, even when there are no changes: • **Only when the policy was modified**: Only if there are changes to be reported on, relative to the previous revision. • **Even if the policy was not modified**: If there are no changes, the report will state that there were no changes.For example, if an administrator first saves a Check Point policy, and then installs the policy on a gateway a few minutes later, the second event has not modified the policy.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and

	- permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.**Reporting Period** controls how far back the report will span from the time of generation.
Delivery	The report can be delivered in any of the following three ways: - **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. - **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. - **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. - **Report Fields**: You can include the name of the report and the time that the report was generated. - **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** - **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** - **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**: - **Groups and members** - The report includes the definitions of group objects and their member objects.This is useful for recipients that do not have SecureTrack access.SecureTrack users can click on group objects in the report to see the definitions. **Non-group objects** - The report includes definitions of non-group objects.

Expired Rules Report

The Expired Rules Report lists all the rules that have expired.The report displays only those rules that were manually configured to expire using the native expiration date capability of the device (such as the Check Point **Time object**.)

This report is available only for Check Point policies, Cisco routers, Palo Alto Networks devices, and JunOS devices.When multiple policy packages are used (Check Point), this report displays a section per active Policy Package in each family.

For example, some security rule bases enable limiting any rule to specific periods of time.This report allows you to monitor rules like these that become unnecessary after they expire. It can be launched manually, or scheduled to run periodically.

You can select to view:

- **Display rules that expired**
- **Display rules that will expire within the next ___ days** (Enter the number of days)
- **Also display managements without any matching rules** (List devices that do not match the criteria with the message **No expiring rules matching report definition.**)

  For Check Point policies, only the "Days in a month**" Time object** mode is supported: The "Days in week" mode is not supported.

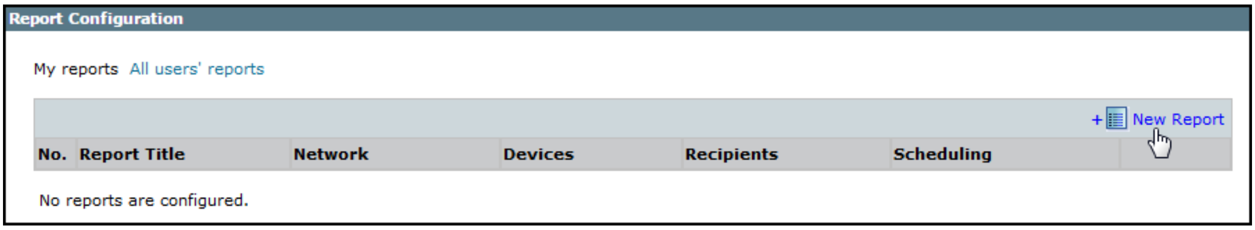
  For Cisco routers, only time objects configured for absolute times are supported: Time objects configured for periodic times are not supported.

Note: For a vendor-agnostic mechanism to set rule expiry within Tufin Orchestration Suite, see Editing Rule Metadata.

IPv6 is not supported for this TOS feature.

To configure an Expired Rules Report:

1. Go to **Report**> **General Reports**, and click **New Report.**



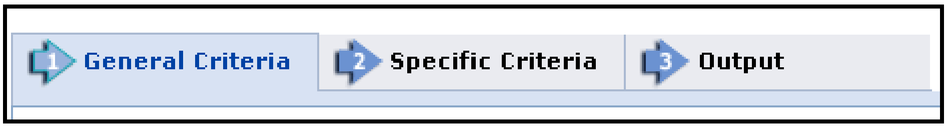
Report Configuration

My reports All users' reports

No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

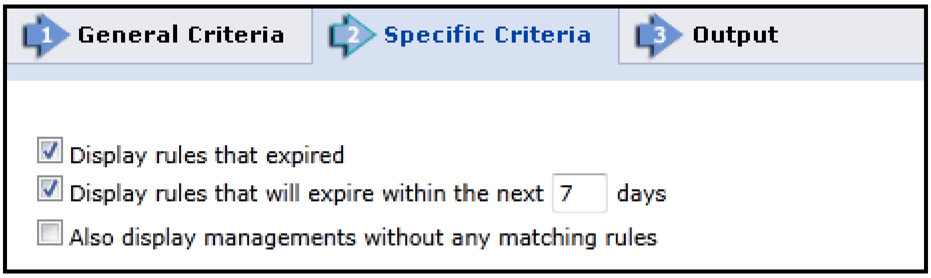
The report configuration wizard has 3 steps.



2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   a. For **ReportType**, select **Expired Rules**.
   b. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
   c. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
   d. Select **Devices** for the report.

      If you have selected one domain, you can limit the report to include specific devices in the domain.
      If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.

3. **STEP 2**: Select one or more of the following options in the **Specific Criteria** tab and click **Next**.

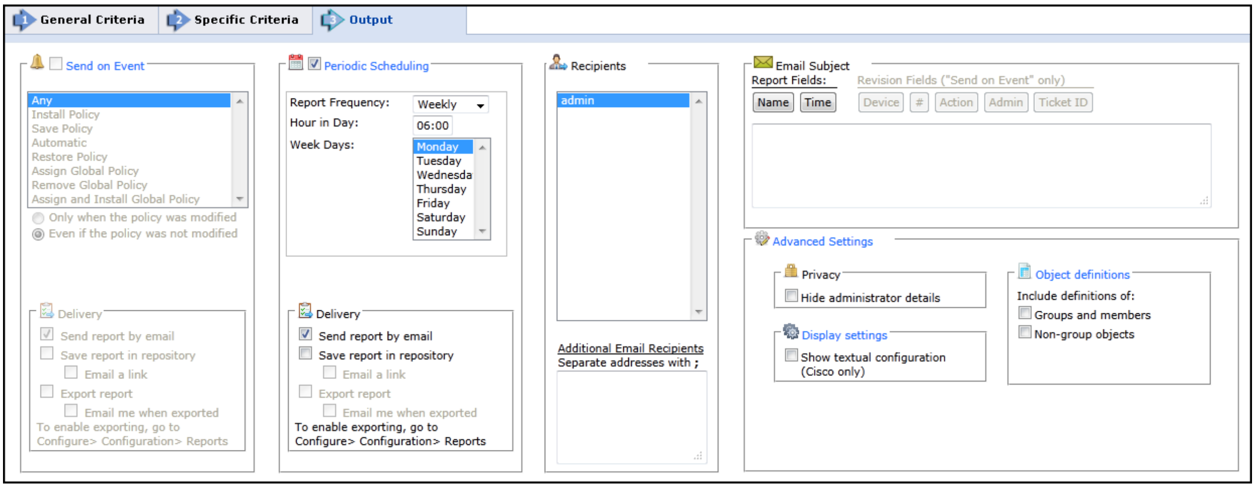


☑ Display rules that expired
☑ Display rules that will expire within the next 7 days
□ Also display managements without any matching rules

   - **Display rules that expired** - List the rules that have expired.
   - **Display rules that will expire within the next _ days** - List the rules that will expire with the amount of days that you enter in the textbox.
   - **Also display managements without any matching rules** - List the policies that do not contain any expired rules.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✗) it.



1 General Criteria | 2 Specific Criteria | 3 Output

☐ Send on Event

- Any
- Install Policy
- Save Policy
- Automatic
- Restore Policy
- Assign Global Policy
- Remove Global Policy
- Assign and Install Global Policy

○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name | Time
Revision Fields ("Send on Event" only) Device | # | Action | Admin | Ticket ID

Advanced Settings

Privacy
☐ Hide administrator details

Display settings
☐ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
☐ Groups and members
☐ Non-group objects

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification). When a SecureTrack User creates a report, only that User is a recipient. When a SecureTrack Administrator creates a report, multiple recipients can be defined. These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack. Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. Note: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advanced Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results. Only the ticket ID is included. This is useful if ticket comments contain confidential information that should not be sent to report recipients,

	such as administrator details.

Rule and Object Usage Report

The Rule and Object Usage Report displays statistics for most-used, least-used and unused rules and objects. It calculates, for each rule or object, the amount of logged network traffic that was passed or blocked.

A Rule and Object Usage Report can be used to:

- Optimize the rulebase by identifying which rules are not being used (should be considered for removal), and which rules are very heavily used (may be moved up in the rulebase).
- Analyze objects usage, including member objects within group objects. Objects which are identified as unused are candidates for removal, even when the rule itself is not.

Rules which have been created or changed during the report period are marked as New (New) or Changed (Changed). For these rules, the presented usage data may not accurately reflect the current situation.

The Rule and Object Usage Report can be scheduled to be automatically generated, and sent to different users.

This report is only available for devices that are enabled for this feature (Configuring Devices to Send Logs). You need to either add a monitored device, or edit an existing monitored device, and select one or more of the Usage Analysis options.

Notes per device vendor:

- Juniper firewalls (Netscreen and JunOS) - The report requires that Juniper Syslogs be configured.
- Fortinet firewalls - The report requires that Fortinet Syslogs be configured
- Cisco routers - Group-member object usage is not provided
- Cisco firewalls - Some recorded object usage may not be relevant to the current configuration, and are marked in the report as 'potential hits'. Examples include:
  - A service port range contains ports that are not included in the current rule configuration during the report period.
  - A Source or Destination subnet contains hosts that are not included in the current rule configuration.
- Palo Alto devices - Object usage for Users and Applications is not supported.
- Check Point policies - Usage statistics are calculated for NAT rules also.
  - For Check Point devices, if multiple policy packages are used for different gateways, you can select packages per Installation Target group. The report will contain a section for each selected package.
  - You can also use the rule usage import CLI command to collect old usage statistics from Check Point devices for analysis in the rule usage report.

The Rule and Object Usage report takes into account only logs that have not been cleaned from the database. You should move rules within the rulebase only after careful consideration, since rules are processed in sequential order.

Rule and object usage statistics are collected per gateway only once a policy revision is received.

Security rules that do not log traffic may negatively impact the accuracy of the NAT rule usage statistics in the report.

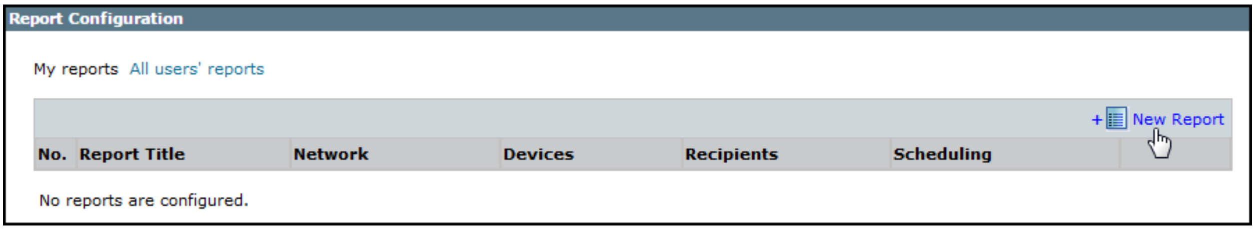
Compressed rule and object usage data is stored in the resolution of 1 day. If you run a Rule and Object Usage report on historical data that includes part of a day, the report time period is changed to include the data available.

Creating a Rule and Object Usage Report

IPv6 is not supported for this TOS feature.

Configure a Rule and Object Usage Report

1. Go to **Report**> **General Reports**, and click **New Report.**



Report Configuration

My reports All users' reports

+ New Report

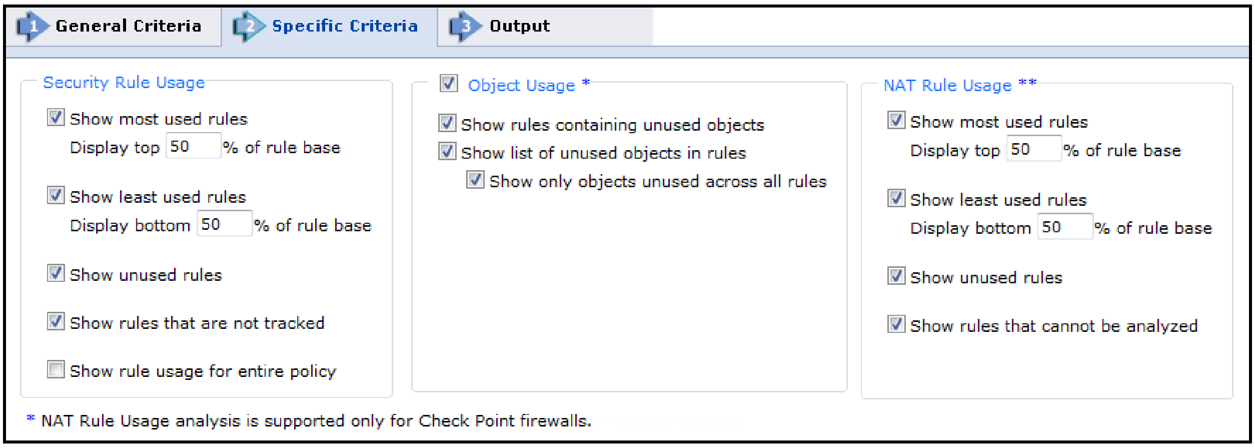
No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.

2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   1. For **ReportType**, select **Rule and Object Usage**.
   2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
   3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
   4. Select **Devices** for the report.

      If you have selected one domain, you can limit the report to include specific devices in the domain.
      If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.
   5. For Check Point devices, if you have selected one device, you can limit the report to include specific **Policy Packages**.If you have selected more than one device, then **Any** is selected for **Policy Packages** and all policy packages in the selected devices are included in the report.
3. Click **Next**.
4. In the **Specific Criteria** tab, select which statistics should be included in the report, as explained in the table below, and click **Next**.



Security Rule Usage

☑ Show most used rules
Display top 50 % of rule base

☑ Show least used rules
Display bottom 50 % of rule base

☑ Show unused rules

☑ Show rules that are not tracked

□ Show rule usage for entire policy

☑ Object Usage *

☑ Show rules containing unused objects
☑ Show list of unused objects in rules
☑ Show only objects unused across all rules

NAT Rule Usage **

☑ Show most used rules
Display top 50 % of rule base

☑ Show least used rules
Display bottom 50 % of rule base

☑ Show unused rules

☑ Show rules that cannot be analyzed

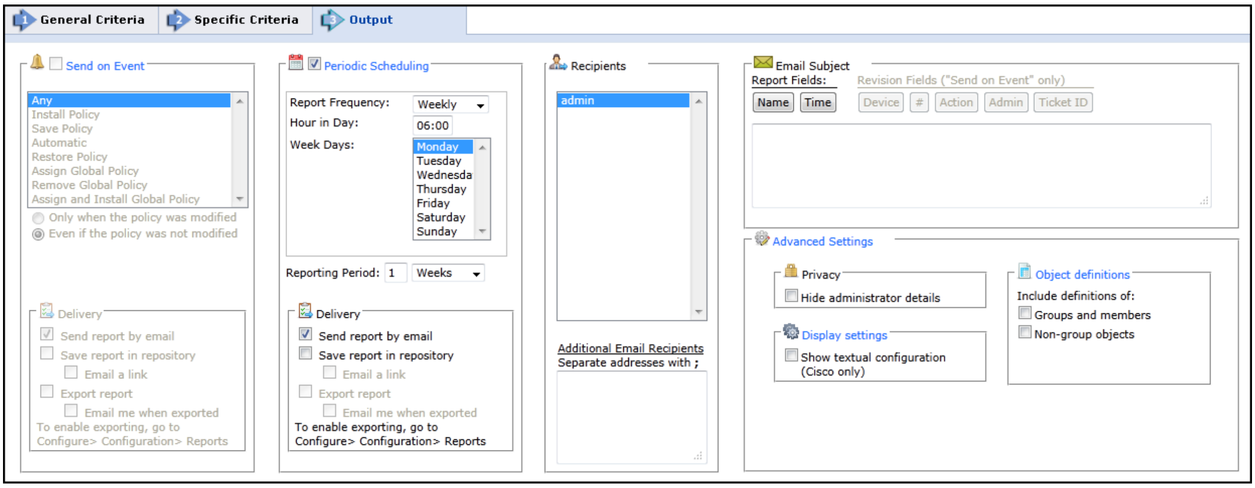
* NAT Rule Usage analysis is supported only for Check Point firewalls.

Parameter	Description
Security Rule Usage	
Show most-used rules	Security rules with the most logged traffic in the rulebase during the specified time.Enter how many of the most used rules (what percentage of the rulebase from the top) you want displayed. From a performance perspective these rules should be as close as possible to the top of the rulebase, to shorten the rulebase lookup time on the gateway.
Show least-used rules	Security rules with the least logged traffic in the rulebase during the specified time.Enter how many of the least used rules (what percentage of the rulebase from the bottom) you want displayed. From a performance perspective these rules should be as close as possible to the bottom of the rulebase, to enable faster rulebase lookup time of other rules on the gateway.
Show unused rules	Logging security rules that have not logged traffic during the specified time. These rules may no longer be required, may pose a security risk, and should be considered as candidates for removal.
Show rules that are not tracked	Security rules for which usage information is unavailable.For example, Check Point or Juniper rules that have **None** specified in the Tracking column.These rules are not accounted for in the firewall's logging mechanisms, with no record being kept for connections on these rules. From a best practice perspective, IT departments should turn off logging only for rules that generate an excessive amount of traffic, and therefore strain the logging servers.Otherwise, all other rules

Parameter	Description
	should be logged. **Note**: In some cases, this kind of rule may have a hit count: For example, if it once was logged and no longer is; or, if a Check Point rule is set not to log, but is logged because of a Global Properties setting. This setting determines only whether these rules appear in an independent section.If such a rule has a hit count, it still may appear in other sections of the report. For Cisco firewalls, usage information is available for all rules, regardless of the logging settings.
Show rule usage for entire policy	Show rule usage for all rules in the policy.
Show rule usage for entire policy	Show usage statistics for all rules, not just the above categories.
Object Usage (When logging security rules, usage information is displayed for each element in source, destination, and service fields.)	
Show rules containing unused objects	When logging security rules that have more than one element in the source, destination or service field, the unused elements are highlighted.These objects are candidates for removal, to remove possible security holes and to reduce processing effort required by the firewall.
Show list of unused objects in rules	An additional section is added to the report, listing network and service objects that are unused in the context of one or more logging rules.For each such object, the report lists the rule in which the object is unused, and the group in which it appears in the rule.To limit this section to objects that are unused in all rules, select **Show only objects unused across all rules**.
NAT Rule Usage	
Show most-used rules	NAT rules with the most logged traffic in the rulebase during the specified time.Enter how many of the most used rules (what percentage of the rulebase from the top) you want displayed. From a performance perspective, these rules should be closer to the top of the rule baserulebase, to shorten the rulebase lookup time on the firewall.
Show least-used rules	NAT rules with the least logged traffic in the rulebase.during the specified time.Enter how many of the least used rules (what percentage of the rulebase from the bottom) you want displayed. From a performance perspective, these rules should be closer to the bottom of the rulebase, to enable faster rulebase lookup time of other rules on the firewall.
Show unused rules	NAT rules that had no logged traffic in during the specified time. These rules may no longer be required, may pose a security risk, and should be considered as candidates for removal.
Show rules that cannot be analyzed	Nat rules that are translated to "original" in source, destination, and service will be marked as “cannot be analyzed” and will not be analyzed in the report, because no NAT translation occurred.

5. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✕) it.



□ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Reporting Period: 1 Weeks

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields:
Revision Fields ("Send on Event" only)

Advanced Settings

Privacy
□ Hide administrator details

Display settings
□ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
□ Groups and members
□ Non-group objects

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.**Reporting Period** controls how far back the report will span from the time of generation.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.You can download this report from the repository in HTML, PDF or CSV format.(Only PDF and HTML formats include NAT rule statistics for the supported vendors)
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.

Parameter	Description
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**: • **Groups and members** - The report includes the definitions of group objects and their member objects.This is useful for recipients that do not have SecureTrack access.SecureTrack users can click on group objects in the report to see the definitions. • **Non-group objects** - The report includes definitions of non-group objects.

Importing Rule Usage from Check Point Devices

You can run reports or APG for a Check Point device that you do not have rule usage logs for in SecureTrack, by retrieving the logs from the management device and importing them into SecureTrack from the command line. After you retrieve the rule usage logs from the device, you can also edit the logs to focus on the logs that are important to your analysis.

To import rule usage logs from a Check Point device:

1. Export the log file from the Check Point management device; run: `fwm log export`
2. Use **grep** or awk commands to remove any log files that are not necessary and to change the logs to this format:

   Source-IP Destination-IP Port IP-Protocol Number Action Date Time;
3. Import the edited log file into SecureTrack; run:

   ```
   # st_rule_usage_importer <DeviceID> <PolicyName> <ModuleName> < <InputFileName>
   ```

   Where:

   `DeviceID` - The SecureTrack ID of the Check Point management device; to find the device ID, open a command line connection to the SecureTrack server and run: **st stat**

   `PolicyName` - The name of the Check Point policy on the device

   `ModuleName` - The name of the module that is managed by the device with the specified DeviceID.

   `InputFileName` - The name of the edited rule usage log file

Sample Code

The following example demonstrates how to use `sed` and `awk` to create a file with the required format:

```
# cat sample.log

1 31-Oct-21 23:58:59 accept 10.245.43.13 10.230.10.215 udp 902

2 31-Oct-21 23:58:59 accept 192.168.11.30 192.168.205.172 tcp 80

3 31-Oct-21 23:58:59 accept 10.245.31.2 10.245.34.3 udp 53

# cat sample.log | sed 's/udp/17/g' | sed 's/tcp/6/g' | awk '{print $5 " " $6 " " $8 " " $7 " " $1 " " $4 "
" $2 " " $3}' > transformed.log

# cat transformed.log

10.245.43.13 10.230.10.215 902 17 1 accept 31-Oct-21 23:58:59

192.168.11.30 192.168.205.172 80 6 2 accept 31-Oct-21 23:58:59

10.245.31.2 10.245.34.3 53 17 3 accept 31-Oct-21 23:58:59

#
```

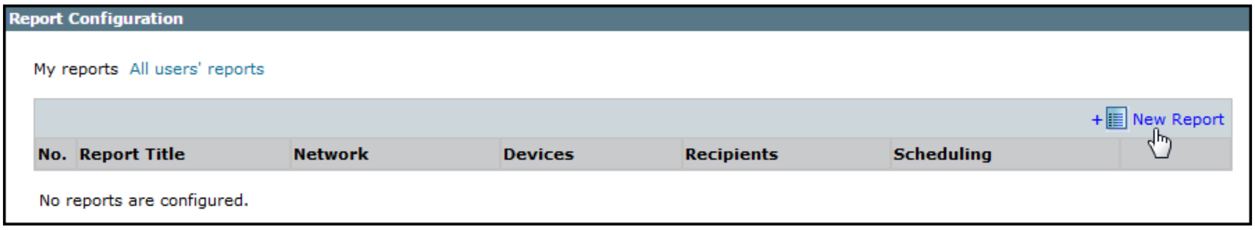
Policy Analysis Report

The Policy Analysis report enables you to run periodically scheduled Policy Analysis queries and automatically send the report to recipients.

IPv6 is not supported for this TOS feature.

To schedule a Policy Analysis report:

1. Go to **Report**> **General Reports**, and click **New Report.**



Report Configuration

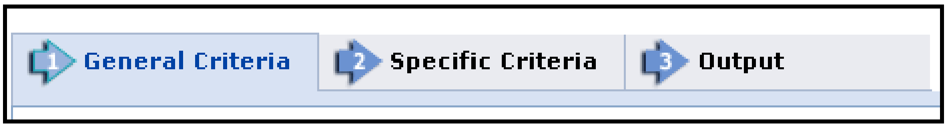
My reports All users' reports

+ New Report

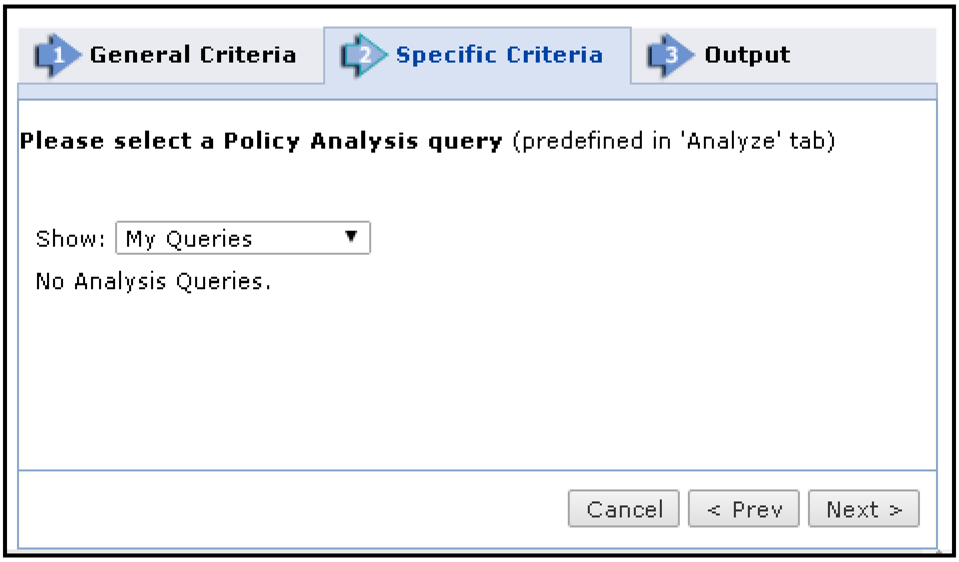
No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.



2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   a. For **ReportType**, select **Policy Anaysis**.
   b. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
3. **STEP 2**: Configure the **Specific Criteria**and click **Next**.
   - Select one of the saved queries to run.(From the **Show** dropbox, you can filter the list saved queries.)



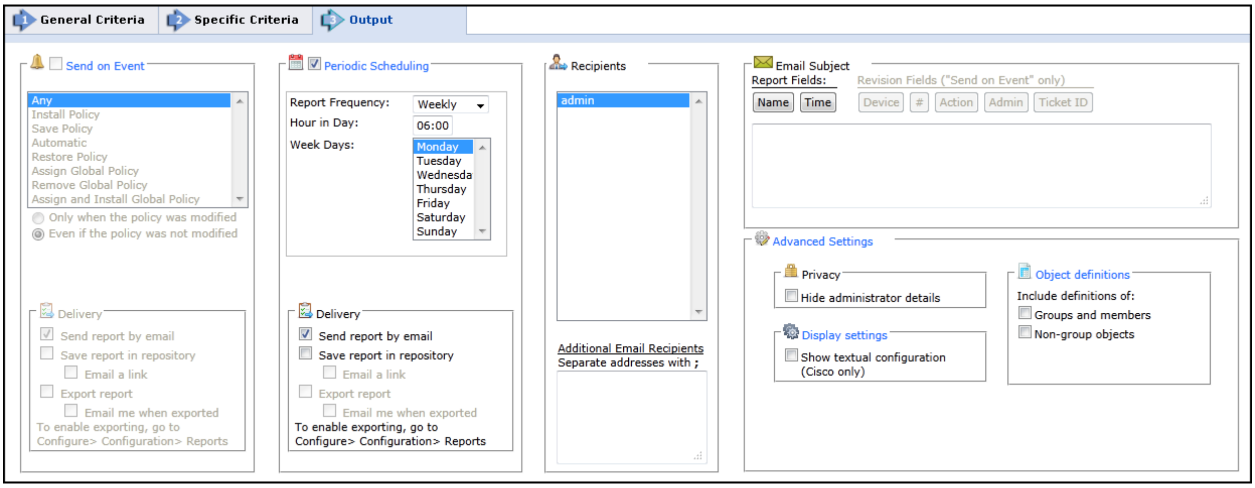
Please select a Policy Analysis query (predefined in 'Analyze' tab)

Show: My Queries ▼

No Analysis Queries.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✗) it.



□ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields:
Revision Fields ("Send on Event" only)

Advanced Settings

Privacy
□ Hide administrator details

Display settings
□ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
□ Groups and members
□ Non-group objects

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**:

- **Groups and members** - The report includes the definitions of group objects and their member objects.This is useful for recipients that do not have SecureTrack access.SecureTrack users can click on group objects in the report to see the definitions.
- **Non-group objects** - The report includes definitions of non-group objects.

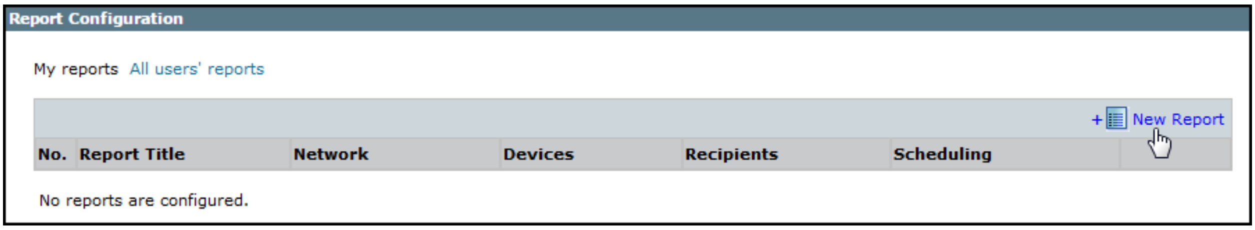
Best Practices Audit Report

The Best Practices Audit report enables you to run periodically scheduled Best Practices Audits and automatically send the report to recipients.

IPv6 is not supported for this TOS feature.

To schedule a Best Practices Audit report:

1. Go to **Report**> **General Reports**, and click **New Report.**



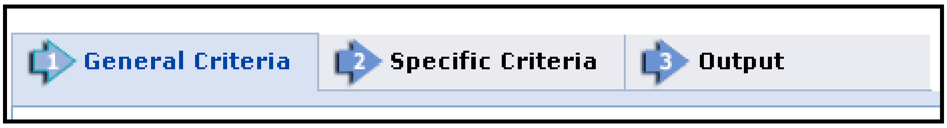
Report Configuration

My reports All users' reports

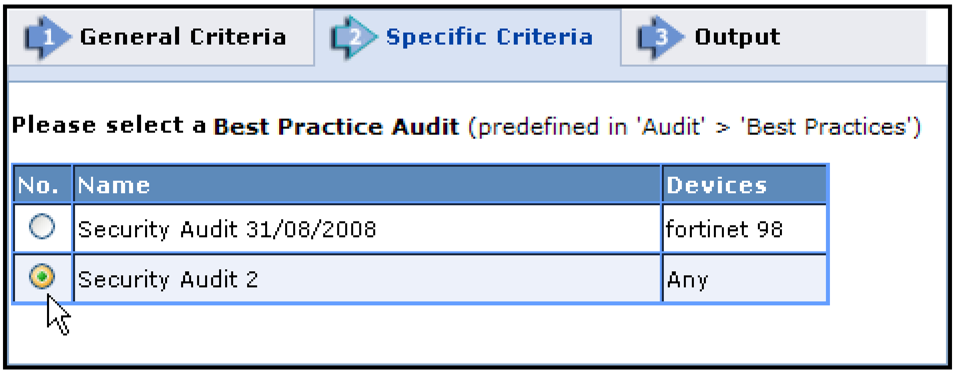
No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.



2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   1. For **ReportType**, select **Best Practices Audit.**
   2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
3. **STEP 2**: In the **Specific Criteria** tab, select the audit to run from the list of configured audits and click **Next**.

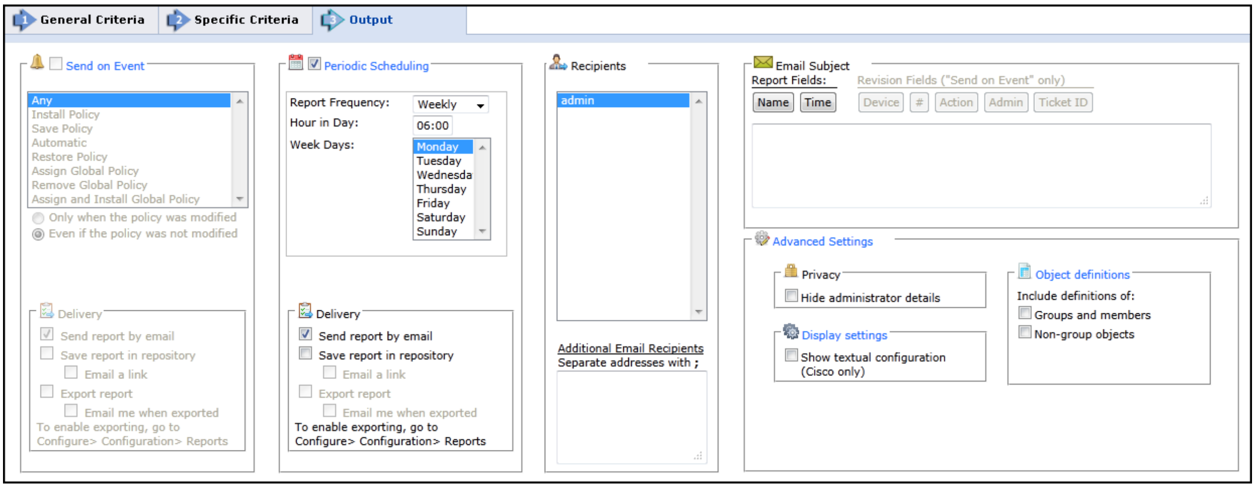


Please select a **Best Practice Audit** (predefined in 'Audit' > 'Best Practices')

No.	Name	Devices
○	Security Audit 31/08/2008	fortinet 98
●	Security Audit 2	Any

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✕) it.



□ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients

admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name Time
Revision Fields ("Send on Event" only) Device # Action Admin Ticket ID

Advanced Settings

Privacy
□ Hide administrator details

Display settings
□ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
□ Groups and members
□ Non-group objects

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**:

- **Groups and members** - The report includes the definitions of group objects and their member objects.This is useful for recipients that do not have SecureTrack access.SecureTrack users can click on group objects in the report to see the definitions.

Non-group objects - The report includes definitions of non-group objects.

Baseline Settings Compliance Report

Baseline Settings Compliance Reports compare Check Point management servers' (SmartCenter or CMA) settings with the settings on another Check Point management server. This is useful to align server configurations and meet organization standards.

The server and the baseline server need to be the same version (for example: NGX R65) To ensure uniform versions, you can use the Software Version Compliance Report.

Baseline Settings Compliance reports compare SmartDefense/Web Intelligence and Global Properties settings. If there are specific settings that do not need to comply with the baseline, you can configure the report to exclude these settings from the comparison. To compare OS-level settings, use the Firewall OS Comparison report.

The reports can be automatically generated according to a schedule, and/or upon change events.

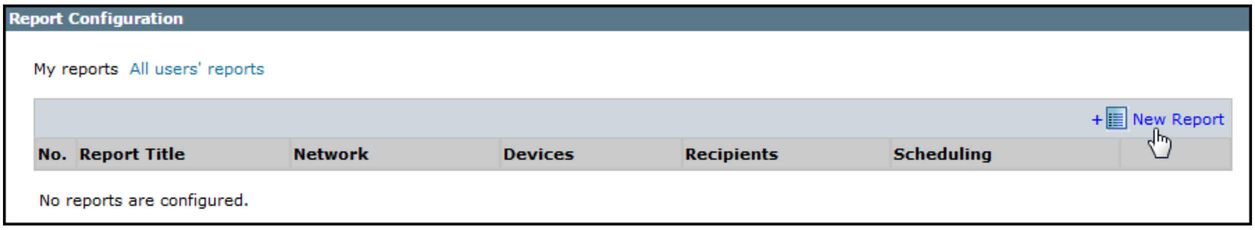
When multiple policy packages are used, this report displays a section per active Policy Package in each family.

Creating a Baseline Settings Compliance Report

IPv6 is not supported for this TOS feature.

To configure a Baseline Settings Compliance Report:

1. Go to **Report**> **General Reports**, and click **New Report.**



Report Configuration

My reports All users' reports

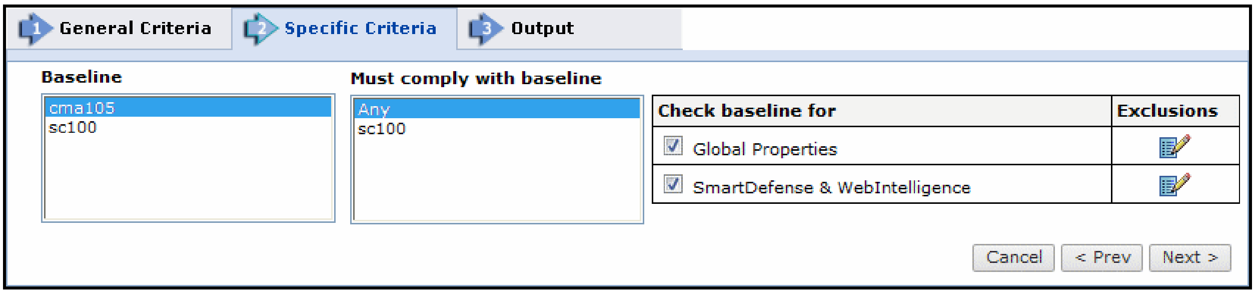
+ New Report

No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.

2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   1. For **ReportType**, select **Baseline Settings Compliance.**
   2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
   3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
3. **STEP 2**: Configure the following in the **Specific Criteria** tab and click **Next**.



Baseline: cma105, sc100

Must comply with baseline: Any, sc100

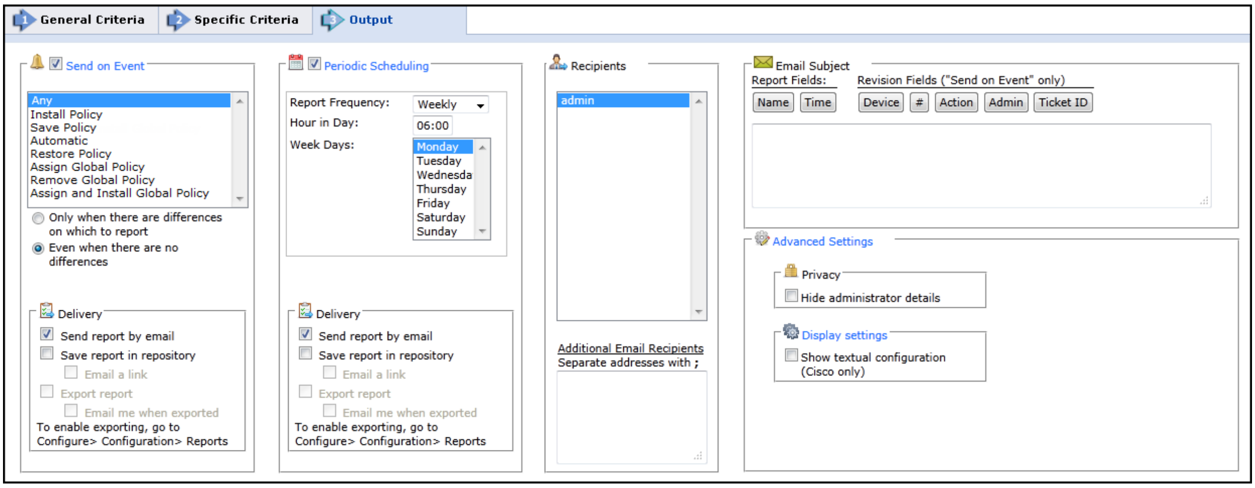
Check baseline for	Exclusions
☑ Global Properties	📝
☑ SmartDefense & WebIntelligence	📝

Parameter	Description
Baseline	Select a management server to be a baseline for comparison
Must comply with baseline	Select one or more management servers to compare to the baseline.
Check baseline for	You can select either or both: of the following items to compare:

	- Global Properties - SmartDefense and Web Intelligence
Exclusions	Click on the Exclusions icon to view what is being excluded from the comparison. To add and remove **Exclusions**, see Excluding Specified Settings from Compliance.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✗) it.



☑ Send on Event

- Any
- Install Policy
- Save Policy
- Automatic
- Restore Policy
- Assign Global Policy
- Remove Global Policy
- Assign and Install Global Policy

○ Only when there are differences on which to report
● Even when there are no differences

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling
Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name Time
Revision Fields ("Send on Event" only): Device # Action Admin Ticket ID

Advanced Settings
Privacy
☐ Hide administrator details
Display settings
☐ Show textual configuration (Cisco only)

Parameter	Description
Send on Event	Select the events to trigger this report.You can use the <shift> key to select more than one event. Select one of the following, to decide whether to always run the report after the event, even when there are no changes: - **Only when the policy was modified**: Only if there are changes to be reported on, relative to the previous revision. - **Even if the policy was not modified**: If there are no changes, the report will state that there were no changes.For example, if an administrator first saves a Check Point policy, and then installs the policy on a gateway a few minutes later, the second event has not modified the policy.
Delivery	The report can be delivered in any of the following three ways: - **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. - **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. - **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: - **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. - **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. - **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.

Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details.

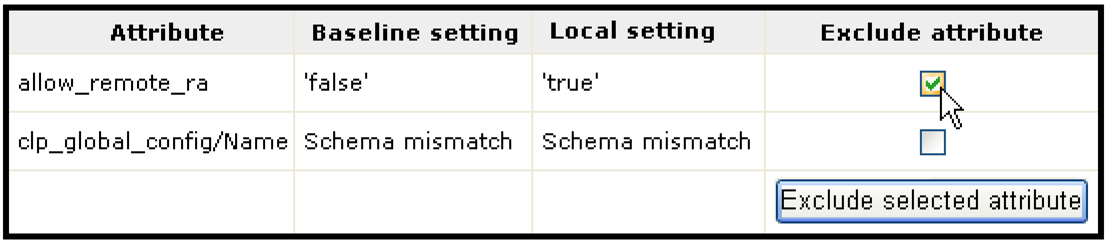
Excluding Specified Settings from Compliance

If there are specific settings that do not need to comply with the baseline, you can configure the report to exclude them from the comparison.

To exclude a setting:

1. If the report has not yet been created, create the report.
2. From this configured report, generate report results.

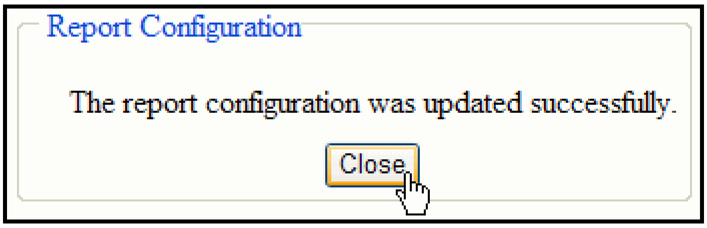
   The report appears in the browser, with details of non-compliant settings.
3. In the section of the report for one of the compared devices, under **Details**, for each setting to be excluded, select the check box in the **Exclude attribute** column:



Attribute	Baseline setting	Local setting	Exclude attribute
allow_remote_ra	'false'	'true'	☑
clp_global_config/Name	Schema mismatch	Schema mismatch	□
			Exclude selected attribute

4. Click **Exclude selected attributes**.

   A confirmation message appears:



Report Configuration

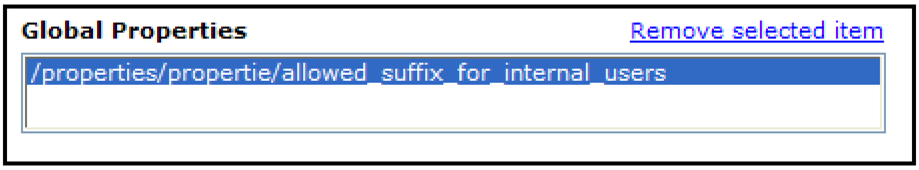
The report configuration was updated successfully.

Run the report again. The excluded settings will be excluded from comparison of all devices in this report.

To cancel an exclusion:

1. In **Report** view, select the **General Reports** tab.
2. In the line for the relevant report, click to edit it.
3. In the **Specific Criteria** tab, in the relevant **Exclusions** row, click .

   A list of configured exclusions appears:



Global Properties Remove selected item

/properties/propertie/allowed_suffix_for_internal_users

4. Select the excluded setting to be removed, and click **Remove selected item**.
5. Click **Next**, and then **Save**.

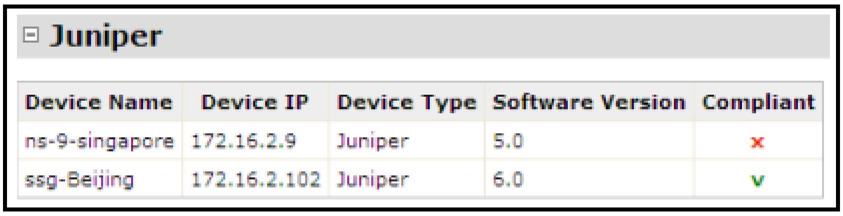
Software Version Compliance Report

The Software Version Compliance report enables you to obtain information on the software versions of the devices in your deployment, and to ensure that all your devices conform to organizational policies regarding software versions.

When you configure the report, you define allowed software versions for the various device types in your deployment. For each device in your deployment, the Software Version Compliance report provides the following information:

- Its software version (major and minor number only)
- Whether its software complies with one or more of the versions allowed for its device type

This is an example of part of a report output for two Juniper firewalls, checking that they are of versions 6.x:



⊟ **Juniper**

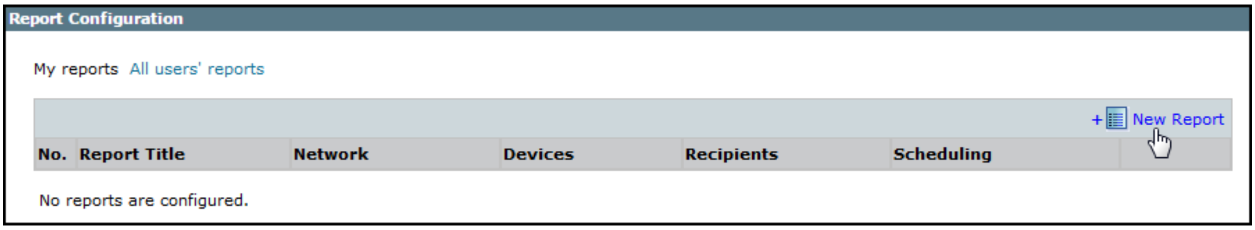
Device Name	Device IP	Device Type	Software Version	Compliant
ns-9-singapore	172.16.2.9	Juniper	5.0	✗
ssg-Beijing	172.16.2.102	Juniper	6.0	✓

Creating a Software Version Compliance Report

IPv6 is not supported for this TOS feature.

To configure a Software Version Compliance Report:

1. Go to **Report**> **General Reports**, and click **New Report.**



Report Configuration

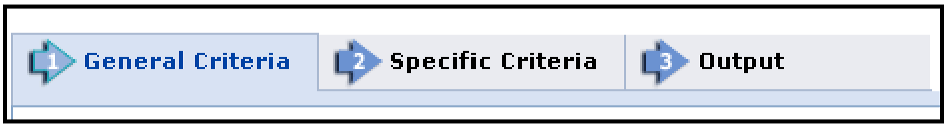
My reports All users' reports

+ New Report

No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

   The report configuration wizard has 3 steps.



2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   1. For **ReportType**, select **Software Version Compliance**.
   2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
   3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.

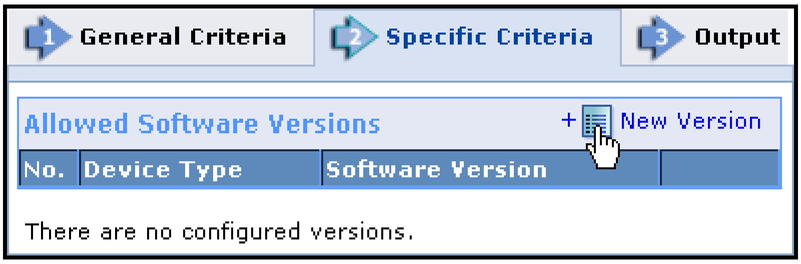
4. Select **Devices** for the report.

   If you have selected one domain, you can limit the report to include specific devices in the domain.
   If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.

   Check Point Software Version Source

   If you select a Check Point device, by default the software version information is received from the Firewall device.If you manage Check Point software with SmartUpdate, select SmartUpdate to see a complete list of installation packages.

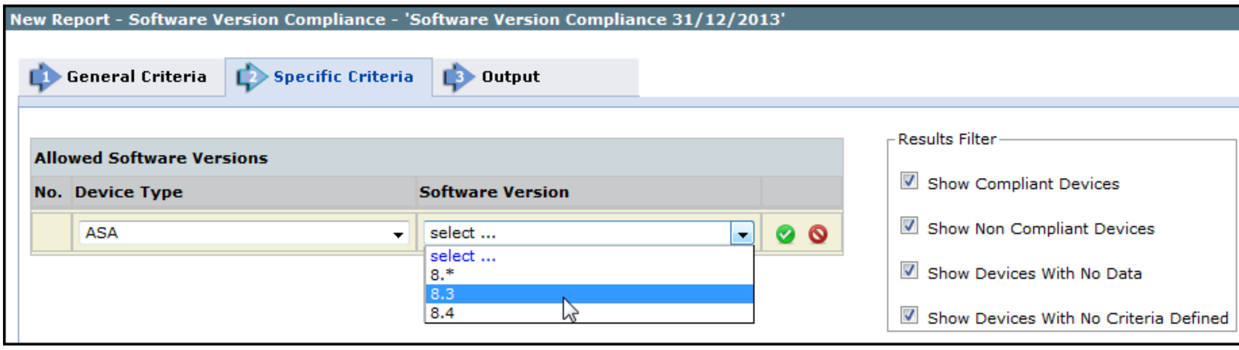
3. **STEP 2**: Configure the **Specific Criteria** as explained below and click **Next**.
   1. The **Specific Criteria** page shows the **Allowed Software Versions** list (initially, the list is empty).To add a new version:
      1. Click **New Version**.



No.	Device Type	Software Version	

There are no configured versions.

      2. Select the **Device Type**, and a **Software Version** to be allowed for that device type.Only software versions that actually exist in your deployment are available to be selected.
      3. Save the device/version combination by clicking: ✓.


New Report - Software Version Compliance - 'Software Version Compliance 31/12/2013'

No.	Device Type	Software Version	
	ASA	select ...	✓ ⊘

Results Filter

☑ Show Compliant Devices

☑ Show Non Compliant Devices

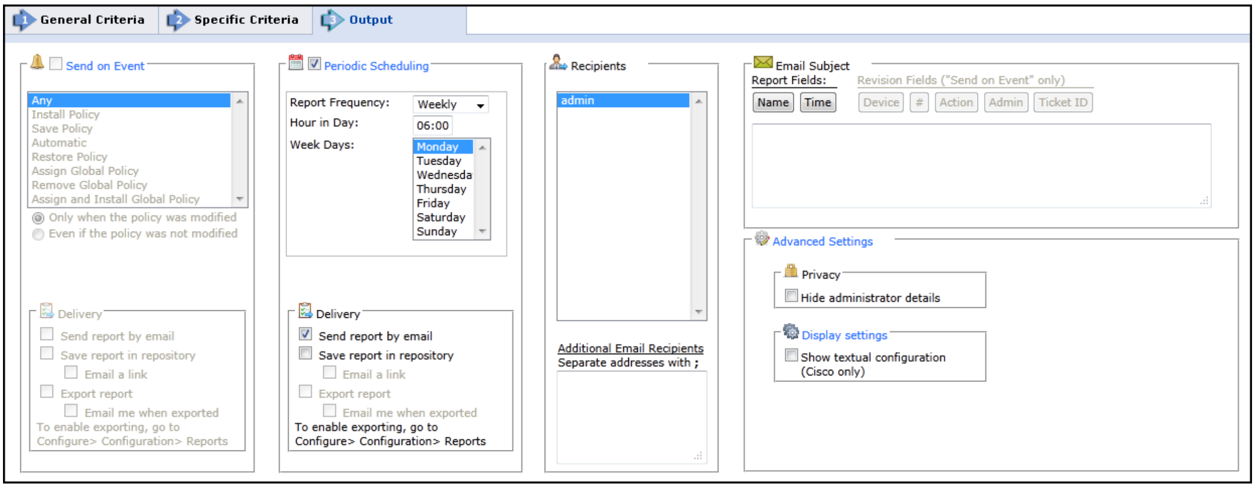
☑ Show Devices With No Data

☑ Show Devices With No Criteria Defined

   2. In the **Results Filter** section, select which devices to include in the report.
      - **Show Compliant Devices**: Include devices that match the software version criteria selected.
      - **Show Non Compliant Devices**: Include devices that do not match the software version criteria selected.
      - **Show Devices with No Data**: :Include devices that do not have data available.
      - S**how Devices with No Criteria Defined**: Include devices that do not have a software version defined.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✗) it.



General Criteria | Specific Criteria | Output

□ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

● Only when the policy was modified
○ Even if the policy was not modified

Delivery
□ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients

admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name | Time
Revision Fields ("Send on Event" only): Device | # | Action | Admin | Ticket ID

Advanced Settings

Privacy
□ Hide administrator details

Display settings
□ Show textual configuration (Cisco only)

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details.

Firewall OS Comparison Report

The Firewall OS Comparison report compares firewalls to each other, checking for OS configuration and software installation differences.

Two types of comparison are available:

- Comparing clustered firewalls to each other, to ensure consistency within the cluster
- Comparing multiple firewalls to a specified baseline firewall

The report checks for differences in the following:

- Interfaces
- Routing
- Installed packages
- Devices
- Storage
- Firewall version

If there are specific attributes that do not need to be consistent, you can configure the report to exclude these specified attributes from all device comparisons.

The report can be manually run, set to be generated upon receiving a new revision, or scheduled to be automatically generated.

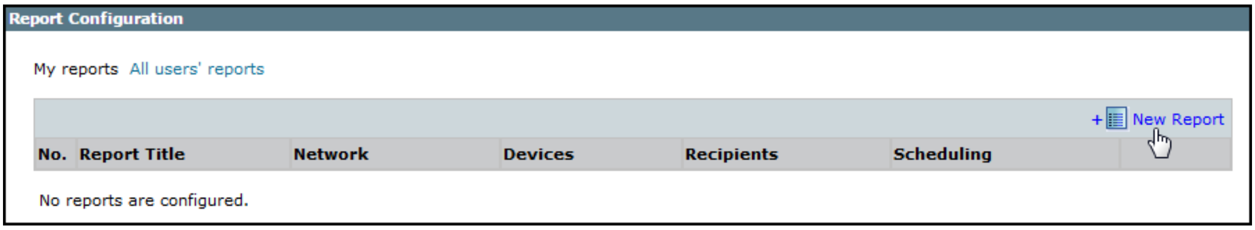
The Firewall Comparison Report is supported only for Check Point gateways that have been added in SecureTrack for Firewall OS Monitoring.

Creating a Firewall OS Comparison Report

IPv6 is not supported for this TOS feature.

To configure a Firewall OS Comparison Report:

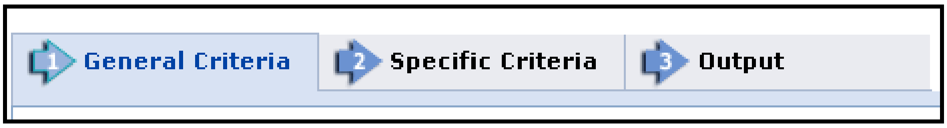
1. Go to **Report**> **General Reports**, and click **New Report.**

No.	Report Title	Network	Devices	Recipients	Scheduling

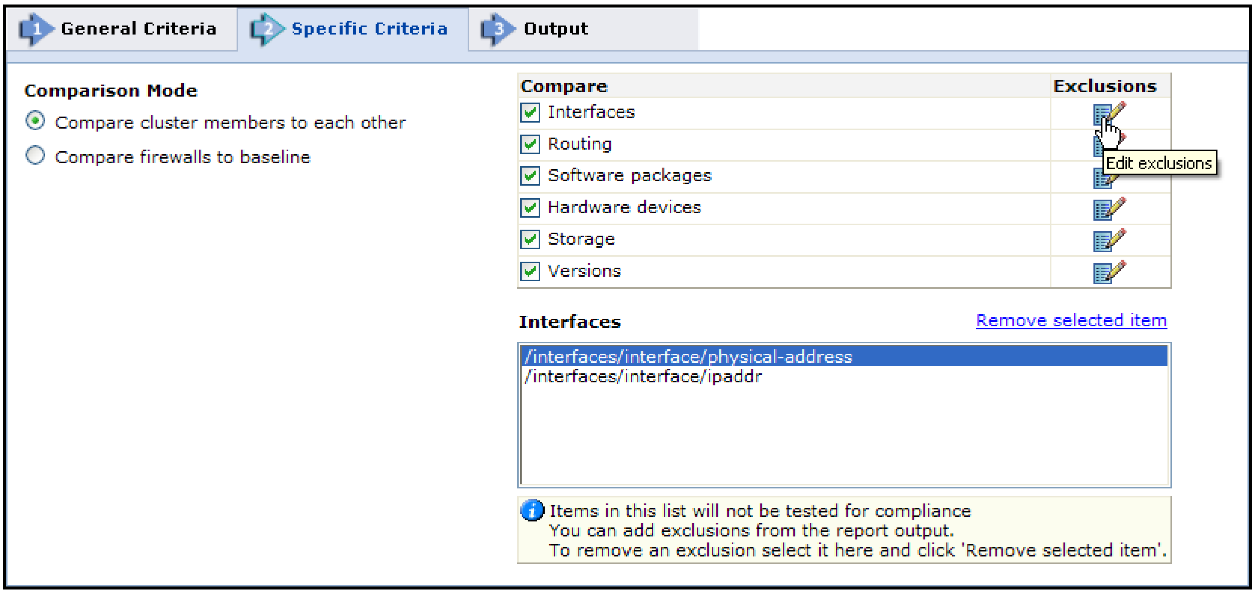
   No reports are configured.

   The report configuration wizard has 3 steps.

2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   1. For **Report Type**, select **Firewall OS Comparison**.
   2. Optionally, you can change the Title.By default, the report's general name with the current date is the report name.
   3. In a Multi-Domain environment, select the Domains that contain the devices you want to run the report on.

3. **STEP 2**: Configure the **Specific Criteria** as explained below and click **Next**.



Comparison Mode

● Compare cluster members to each other

○ Compare firewalls to baseline

Compare	Exclusions
☑ Interfaces	✎
☑ Routing	✎
☑ Software packages	✎
☑ Hardware devices	✎
☑ Storage	✎
☑ Versions	✎

Interfaces Remove selected item

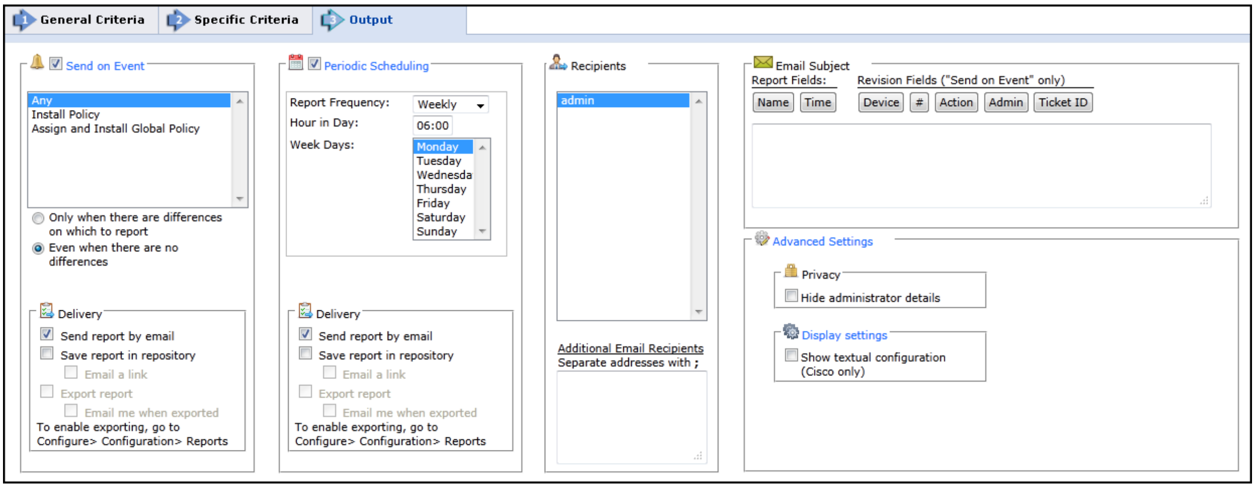
/interfaces/interface/physical-address
/interfaces/interface/ipaddr

Items in this list will not be tested for compliance
You can add exclusions from the report output.
To remove an exclusion select it here and click 'Remove selected item'.

1. Select one of the **Comparison Mode** options:
   - **Compare cluster members to each other**: Clusters are checked for inconsistencies among cluster members.
   - **Compare firewalls to baseline**: After selecting this option, two firewall trees are displayed.Select a baseline firewall, and the firewalls that must comply with it.
2. Select the items to compare.
3. For each item to compare, you can click ✎ to view what is being excluded from the comparison.To add and remove **Exclusions**, see Excluding Specified Settings from Comparison.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

5. The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✕) it.



☑ Send on Event

Any
Install Policy
Assign and Install Global Policy

○ Only when there are differences on which to report

● Even when there are no differences

Delivery

☑ Send report by email

☐ Save report in repository

☐ Email a link

☐ Export report

☐ Email me when exported

To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly

Hour in Day: 06:00

Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery

☑ Send report by email

☐ Save report in repository

☐ Email a link

☐ Export report

☐ Email me when exported

To enable exporting, go to Configure> Configuration> Reports

Recipients

admin

Additional Email Recipients
Separate addresses with ;

Email Subject

Report Fields: Name Time

Revision Fields ("Send on Event" only) Device # Action Admin Ticket ID

Advanced Settings

Privacy

☐ Hide administrator details

Display settings

☐ Show textual configuration (Cisco only)

Parameter	Description
Send on Event	Select the events to trigger this report.You can use the <shift> key to select more than one event. Select one of the following, to decide whether to always run the report after the event, even when there are no changes: • **Only when the policy was modified**: Only if there are changes to be reported on, relative to the previous revision. • **Even if the policy was not modified**: If there are no changes, the report will state that there were no changes.For example, if an administrator first saves a Check Point policy, and then installs the policy on a gateway a few minutes later, the second event has not modified the policy.

Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details.

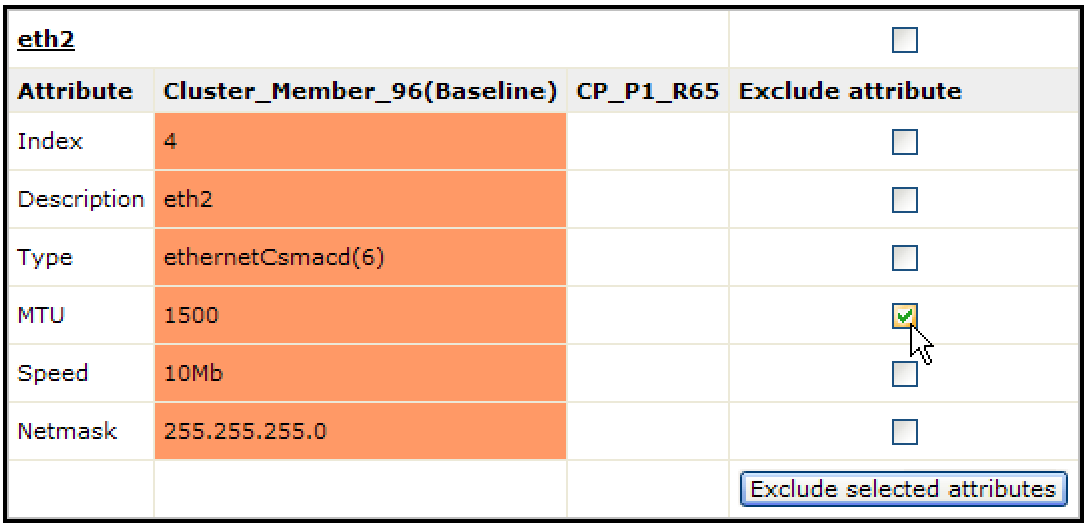
Excluding Specified Settings from Comparison

If there are specific settings that do not need to be consistent, you can configure the report to exclude them from the comparison of all devices.

To exclude a setting:

1. If the report has not yet been created, create the report.
2. From this configured report, generate report results.

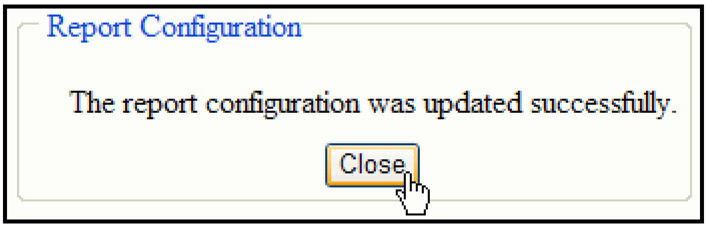
   The report appears in the browser, with details of non-compliant attributes.
3. In the section of the report for the relevant device, under the relevant category (**Devices**, **Interfaces**, etc.), for each setting to be excluded, select the checkbox in the **Exclude attribute** column:



eth2			☐
Attribute	**Cluster_Member_96(Baseline)**	**CP_P1_R65**	**Exclude attribute**
Index	4		☐
Description	eth2		☐
Type	ethernetCsmacd(6)		☐
MTU	1500		☑
Speed	10Mb		☐
Netmask	255.255.255.0		☐
			Exclude selected attributes

4. Click **Exclude selected attributes**.

   A confirmation message appears:



Report Configuration

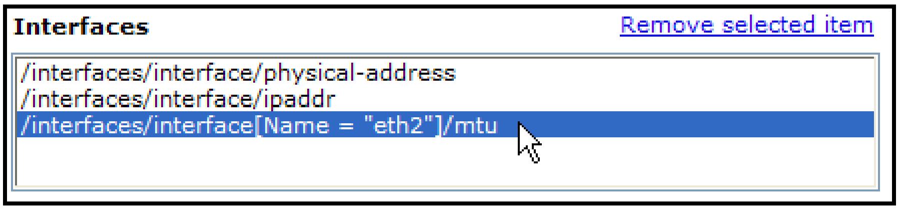
The report configuration was updated successfully.

The excluded settings will be excluded from comparison of all devices in this report.

To subsequently cancel an exclusion:

1. In **Report** view, select the **General Reports** tab.
2. In the line for the relevant report, open it for editing by clicking: 📝 .
3. Go to the **Specific Criteria** page.
4. In the relevant row, click **Exclusions**📝 .

   A list of configured exclusions appears:



Interfaces

```
/interfaces/interface/physical-address
/interfaces/interface/ipaddr
/interfaces/interface[Name = "eth2"]/mtu
```

5. Select the excluded setting to be removed, and click **Remove selected item**.
6. Click **Next**, and then **Save**.

Security Risk Report

The Security Risk report provides the security policies with violations. It bases the list on predefined tests for risky rules and compliance with organizational security guidelines. The report also calculates a Security Score, and tracks its trend over examining every registered SecureTrack firewall.

You can configure the report to test for violations of any of the predefined tests for risky rules, and of any of the risk management Compliance Policies configured in SecureTrack. You can set the Security Risk report to automatically include risk management Compliance Policies configured in the future, as well. You can define policy rules to be excluded from specific tests.

For Check Point devices, if multiple policy packages are used for different gateways, you can select packages per Installation Target group. The report will contain a section for each selected package.

You can run the Security Risk report:

- Manually
- Automatically on change events so that the report includes new and resolved risks
- Schedule a report to run periodically

The report includes:

- Test results (pass fail) and detailed violation for each configured test
- Security Scores provides the FW security level (percentage)
- Graphs that track the trend of Security Scores from previously generated report results and from Security Scores calculated automatically on an event

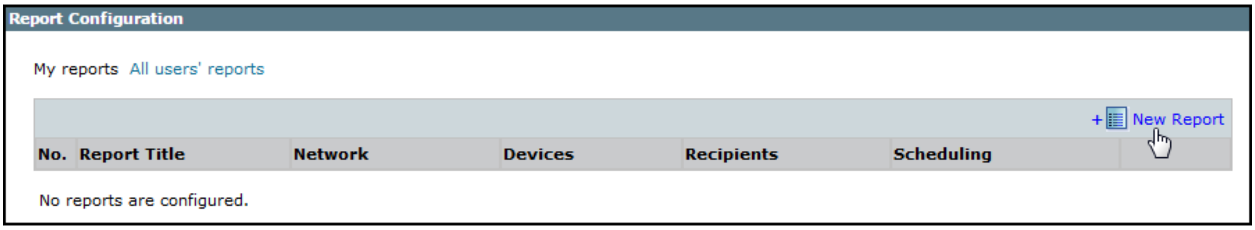
  The Security Score represents passed tests relative to total configured tests. If you change the configuration of the report, the score may change even if the tested policies do not change.

Creating a Security Risk Report

> This is a Legacy Feature. It will be discontinued as of version R21-3.
>
> We recommend you consider using the following features:
>
> - "Unified Security Policy" on page 366
> - "Unified Security Policy Alerts" on page 389
> - "Configuring Exceptions for the Unified Security Policy" on page 388
>
> These features give you greater flexibility in the number of zones that you can configure and allow you to define the requirements that you need.

To configure a Security Risk report:

1. Go to **Report**> **General Reports**, and click **New Report.**



Report Configuration

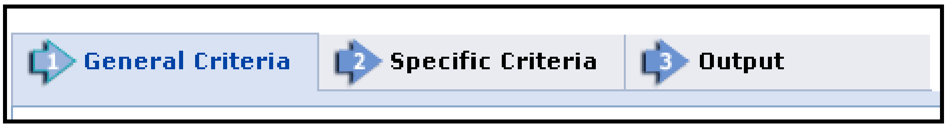
My reports All users' reports

+ New Report

No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.



2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   a. For **ReportType**, select **Security Risk**:
   b. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
   c. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
   d. Select **Devices** for the report.

      If you have selected one domain, you can limit the report to include specific devices in the domain.
      If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.

e. For Check Point devices, if you have selected one device, you can limit the report to include specific **Policy Packages**.If you have selected more than one device, then **Any** is selected for **Policy Packages** and all policy packages in the selected devices are included in the report.

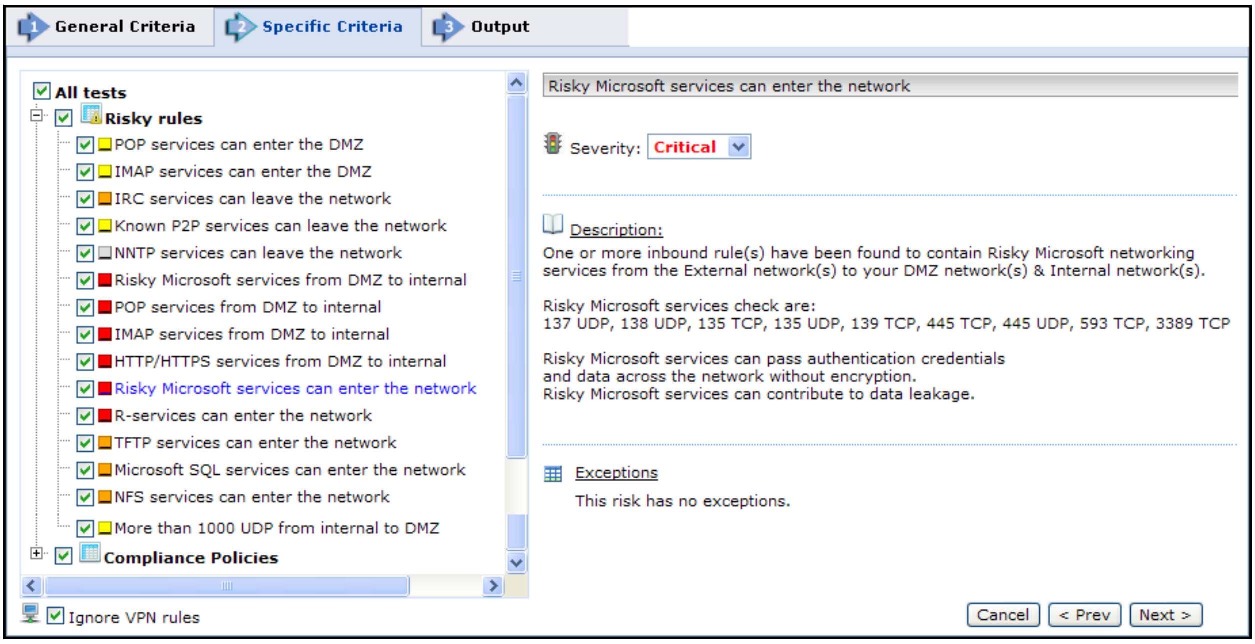
f. Select the zones to use for vulnerability tests. You can select, either:

- Use Topology - Calculate vulnerability based on the networks and clouds that are defined as Internal, External, and DMZ using Topology Intelligence.
- Manual - Calculate vulnerability based on the zones defined in **Zones**

  You can also select **Analyze only relevant policies** to let Topology Intelligence find the policies that include rules with the specified zones.

3. **STEP 2**: Configure the **Specific Criteria** as explained in the table and click **Next**.

   In the **Specific Criteria** page, select tests to be included in the report.You can also change the **Severity** setting of selected tests.



☑ **All tests**
- ☑ **Risky rules**
  - ☑ 🟨 POP services can enter the DMZ
  - ☑ 🟨 IMAP services can enter the DMZ
  - ☑ 🟧 IRC services can leave the network
  - ☑ 🟨 Known P2P services can leave the network
  - ☑ ⬜ NNTP services can leave the network
  - ☑ 🟥 Risky Microsoft services from DMZ to internal
  - ☑ 🟥 POP services from DMZ to internal
  - ☑ 🟥 IMAP services from DMZ to internal
  - ☑ 🟥 HTTP/HTTPS services from DMZ to internal
  - ☑ 🟥 Risky Microsoft services can enter the network
  - ☑ 🟥 R-services can enter the network
  - ☑ 🟧 TFTP services can enter the network
  - ☑ 🟧 Microsoft SQL services can enter the network
  - ☑ 🟧 NFS services can enter the network
  - ☑ 🟨 More than 1000 UDP from internal to DMZ
- ☑ **Compliance Policies**

☑ Ignore VPN rules

Risky Microsoft services can enter the network

Severity: Critical

Description:
One or more inbound rule(s) have been found to contain Risky Microsoft networking services from the External network(s) to your DMZ network(s) & Internal network(s).

Risky Microsoft services check are:
137 UDP, 138 UDP, 135 TCP, 135 UDP, 139 TCP, 445 TCP, 445 UDP, 593 TCP, 3389 TCP

Risky Microsoft services can pass authentication credentials
and data across the network without encryption.
Risky Microsoft services can contribute to data leakage.

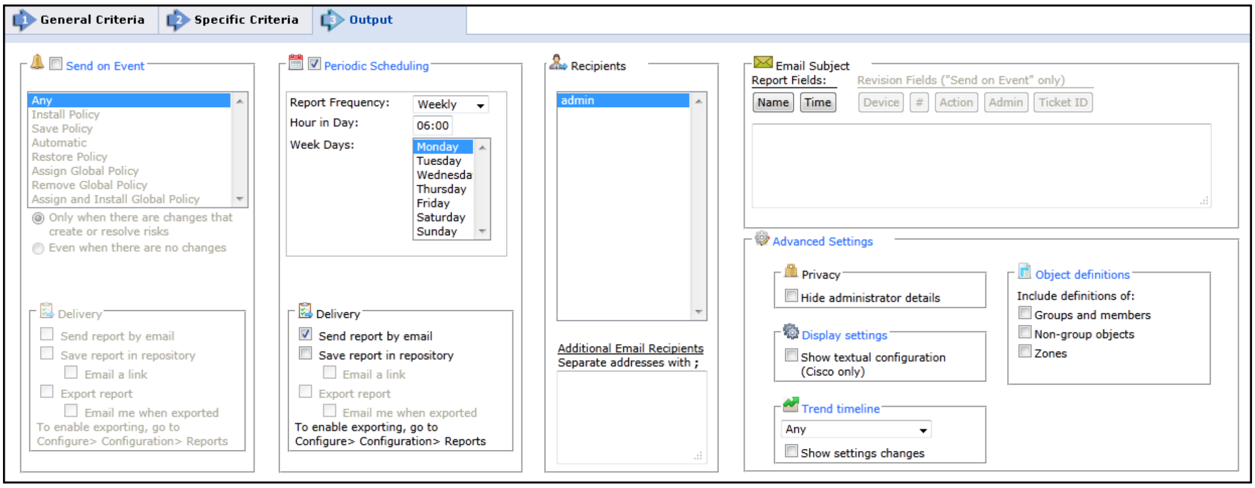
Exceptions
This risk has no exceptions.

Ignore VPN rules prevents VPN rules from being considered as risks.This setting affects Risky rules; Compliance Policies ignore VPN rules in any case.

Click **Next**.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

   The saved report appears in the General Reports list.From the list, you can **Run** ( ), **Edit** ( ), or **Delete** ( ) it.



☐ Send on Event
Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy
● Only when there are changes that create or resolve risks
○ Even when there are no changes

Delivery
☐ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling
Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name Time
Revision Fields ("Send on Event" only) Device # Action Admin Ticket ID

Advanced Settings

Privacy
☐ Hide administrator details

Display settings
☐ Show textual configuration (Cisco only)

Trend timeline
Any
☐ Show settings changes

Object definitions
Include definitions of:
☐ Groups and members
☐ Non-group objects
☐ Zones

Parameter	Description
Send on Event	Select the events to trigger this report.You can use the <shift> key to select more than one event. Select one of the following, to decide whether to always run the report after the event, even when there are no changes: • **Only when the policy was modified**: Only if there are changes to be reported on, relative to the previous revision. • **Even if the policy was not modified**: If there are no changes, the report will state that there were no changes.For example, if an administrator first saves a Check Point policy, and then installs the policy on a gateway a few minutes later, the second event has not modified the policy.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context.SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**: • **Groups and members** - The report includes the definitions of group objects and their member objects.This is useful for recipients that do not have SecureTrack access.SecureTrack users can click on group objects in the report to see the definitions. • **Non-group objects** - The report includes definitions of non-group objects. **Trend Timeline** • Select the date range for the security trend graph.

Excluding Specified Rules from the Risk Report

This is a Legacy Feature. It will be discontinued as of version R21-3.

We recommend you consider using the following features:

- "Unified Security Policy" on page 366
- "Unified Security Policy Alerts" on page 389
- "Configuring Exceptions for the Unified Security Policy" on page 388

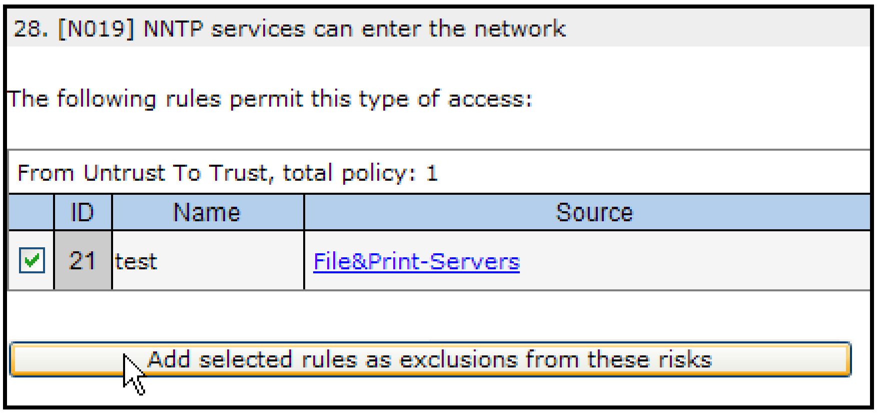
These features give you greater flexibility in the number of zones that you can configure and allow you to define the requirements that you need.

If there are specific rules that should be ignored by specific tests in the report, you can configure exclusions.

To exclude a setting:

1. If the report has not yet been created, create the report.
2. From this configured report, generate report results.

   The report appears in the browser, with details of failed tests.
3. In the section of the report for the relevant device/policy package, under the relevant found risk, select each rule to be excluded, and click **Exclude selected rules from these tests**:



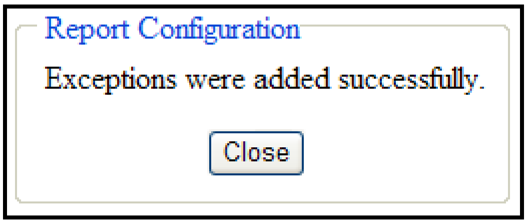
28. [N019] NNTP services can enter the network

The following rules permit this type of access:

From Untrust To Trust, total policy: 1

	ID	Name	Source
☑	21	test	File&Print-Servers

A confirmation message appears:



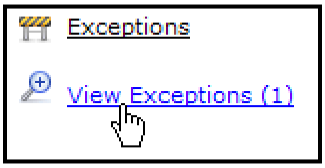
Report Configuration

Exceptions were added successfully.

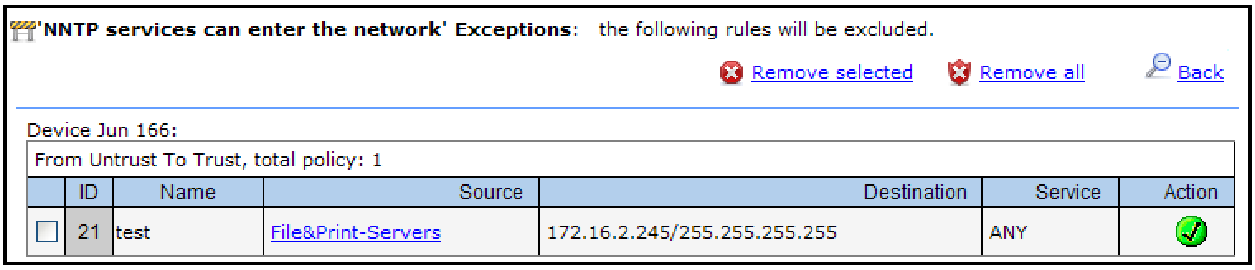
The selected rules will be excluded from the specified tests in this report.

To subsequently cancel an exclusion:

1. Go to **Report**> **General Reports**.
2. In the line for the relevant report, open it for editing by clicking: 📝 .
3. Go to the **Specific Criteria** page.
4. Select the relevant test, and click **View Exceptions**:



A list of configured exclusions appears:



'NNTP services can enter the network' Exceptions: the following rules will be excluded.

Device Jun 166:

From Untrust To Trust, total policy: 1

	ID	Name	Source	Destination	Service	Action
□	21	test	File&Print-Servers	172.16.2.245/255.255.255.255	ANY	✓

5. Select the excluded rules to be removed, and click **Remove selected**.
6. Click **Next**, and then **Save**.

Rule Documentation Report

The Rule Documentation Report presents all of the Policy Browser details, or metadata, that are saved in SecureTrack for each rule of a device's most recent policy revision.

The rule metadata includes a few types of information:

- **Rule Statistics**
  - Permissiveness level (high/medium/low) - An indication of how widely a rule is defined, for example:
    - A rule with one source host, one destination host and one service is low permissiveness
    - A rule with Source "ANY", Destination "ANY" and Protocol "ANY" is high permissiveness

    Rules with high permissiveness can be a security risk because they allow too much access through the firewall. N/A indicates that the platform is not supported for permissiveness calculations.
  - Violations - The number of PCI DSS and Unified Security Policy violations caused by the rule
  - Last Hit - The last time traffic that passed through the device matched either the rule, user, or application identities details
  - Last Modified - The last time a revision showed that the source, destination or service changed in the rule, including changes group members

    After you upgrade to R16-4 or higher, SecureTrack analyzes the revisions to identify the last time any part of the rule was changed, for example source, destination, service, log, or comment. Rules are labeled with the last modified date of yesterday, 3 months ago, 6 months ago, 12 months ago, or longer, whichever is the most recent change. This process can take up to a few days to complete.
  - Shadowing Status - For rules that are marked as fully shadowed, you can click on **Details** to see the rules that shadow it.
- **Metadata per rule**
  - Technical owner - One of the SecureTrack admin users: Typically, the firewall administrator who is responsible for the technical accuracy of the rule.
  - Rule description - A useful description stored in SecureTrack
  - Advanced options:
    - Legacy rule - When a rule is marked as legacy, SecureChange Designer will treat a rule marked as legacy as a shadowed rule when making recommendations, and SecureChange Verifier will ignore a rule marked as legacy when verifying access.

      Marking rules as legacy can be used to let you methodically replace overly permissive rules over a period of time. Only rules that have an Allow action can be marked as Legacy.

      When the traffic in an access request is fully or partially implemented by traffic that is handled by legacy rules, Designer locates the recommended rules above the related legacy rule with the highest position in the policy.
    - Stealth rule - When a rule as is marked as stealth, SecureChange Designer recommendations will place any new rules recommended for an access request below the stealth section of the policy. Only rules that have a Deny action can be marked as stealth.

      The stealth section is comprised of all rules above and including the last rule marked as stealth in the device policy and is therefore always the top section in the device policy. Stealth rules can be used to protect a firewall device from attack by denying unwanted access to specific firewalls.

- **Record sets for each workflow ticket associated with the rule**
  - Ticket ID - Entered manually or matched automatically with SecureChange authorized tickets that allow new traffic.

    For tickets marked as **SecureChange Ticket ID**, the **Ticket ID** column is populated when a change triggers a revision on a rule. Rules are mapped to a ticket when active rules intersect with another ticket’s traffic, whether or not a policy change has occurred within an Access Request.

    In Policy Browser, click on the ticket ID to go to the SecureChange ticket in Tasks (Requires permission to view the ticket). In the rule documentation report, you can see the expiration date of the ticket, if one is configured.
  - Business owner name and email - The user who opens the ticket

    Assigned automatically
  - Expiration date - Entered manually or matched automatically with SecureChange ticket expiration
- Application details for SecureApp application connections that match firewall rules:
  - Application name
  - Application owner

Automatically updated when new revisions are retrieved, when a connection change is saved in SecureApp or when there is a change in the Topology. Also, rules marked with application information are selected based on the potential traffic for each device in the path as defined in the rule, and not based on the effective traffic that passes through the device which may be blocked by another device or changed by NAT rules before reaching the device.

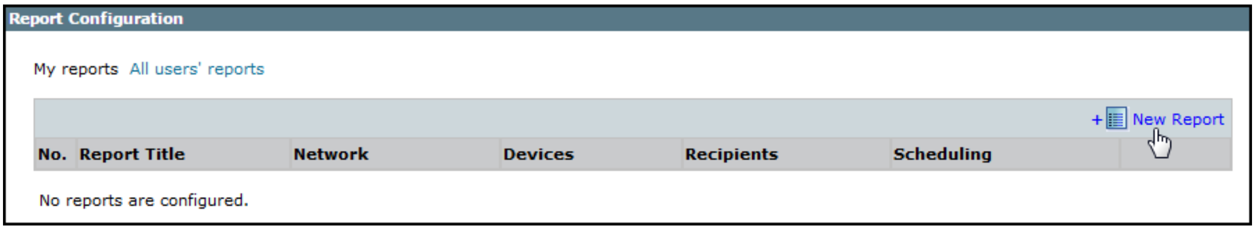
After you add Policy Browser to policy rules, you can create reports for SecureTrack to send on a schedule or to run manually.

Creating a Rule Documentation Report

IPv6 is not supported for this TOS feature.

To configure a Rule Documentation report:

1. Go to **Report**> **General Reports** and click **New Report.**

   Report Configuration

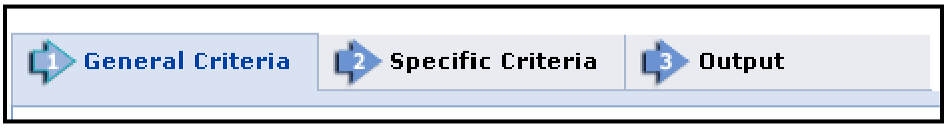
   My reports All users' reports

   + New Report

No.	Report Title	Network	Devices	Recipients	Scheduling

   No reports are configured.

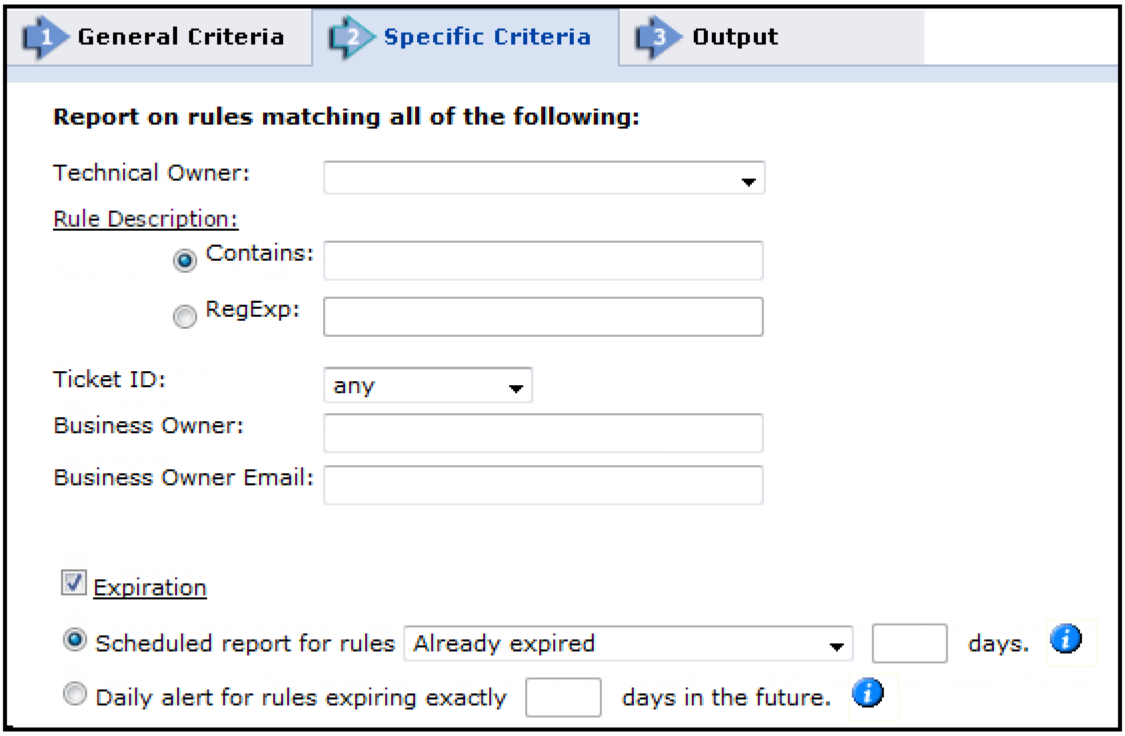
   The report configuration wizard has 3 steps.

2. **STEP 1**: Configure the **General Criteria** and click **Next**.
   1. For **ReportType**, select **Rule Documentation**:
   2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
   3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
   4. Select **Devices** for the report.

      If you have selected one domain, you can limit the report to include specific devices in the domain.
      If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.
   5. For Check Point devices, if you have selected one device, you can limit the report to include specific **Policy Packages**.If you have selected more than one device, then **Any** is selected for **Policy Packages** and all policy packages in the selected devices are included in the report.

3. **STEP 2**: Configure the **Specific Criteria** as explained below and click **Next**.



Report on rules matching all of the following:

Technical Owner:

Rule Description:

● Contains:

○ RegExp:

Ticket ID: any

Business Owner:

Business Owner Email:

☑ Expiration

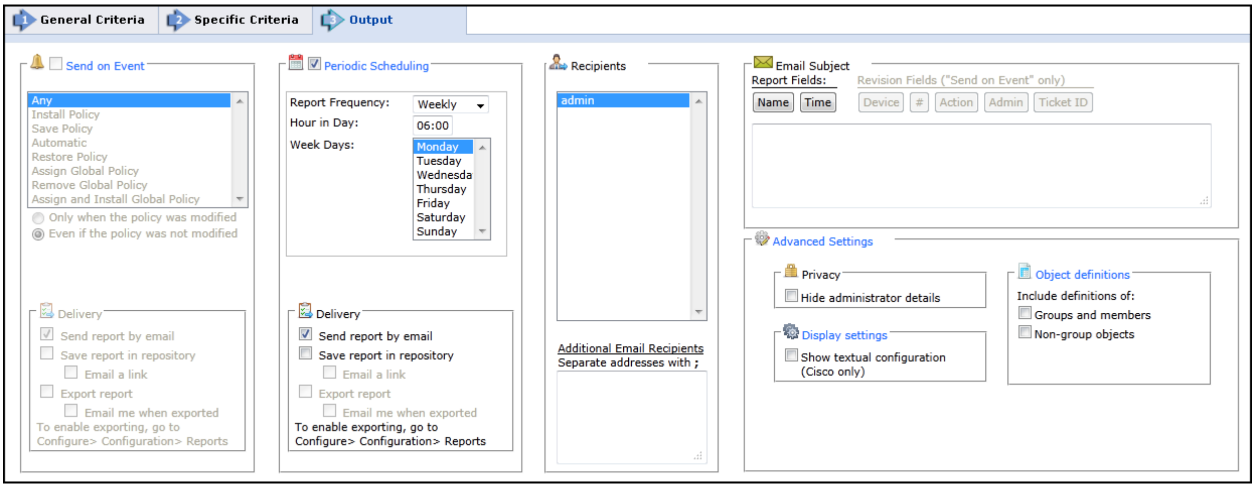
● Scheduled report for rules Already expired days.

○ Daily alert for rules expiring exactly days in the future.

Parameter	Description
Technical Owner	Select any of the SecureTrack users who already appear as technical owners.
Rule Description	Select one of the Rule Description options: • **Contains** - The comment includes the text that you enter. • **RegExp** - The comment matches the Regular Expression that you enter.
Ticket ID	Select Any / Empty or Contains.For Contains enter the text that you want to match.
Business Owner / Business Owner Email -	A rule is considered a match when either the rule's Business Owner Name or Business Owner Email address exactly matches the text you type here.
Expiration	• **Scheduled Report** - Schedule a report to be sent at specific times that will include, either: **Already expired** - Rules with expiration dates in the past **Expiring within** - Rules that will expire during the next specified number of days.Enter the number of days. **Already expired, or expiring within:** - Both sets of rules If no rules match the expiration, SecureTrack sends a blank report. • **Daily Alert** - Sends a report of rules that expire on the day specified.For example, if you set the alert to 2 days, then on Monday you receive a report for all rules that expire on Wednesday. This report runs daily at the time specified in Output.If no rules expire on the specified day, SecureTrack sends a blank report.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

5. The saved report appears in the General Reports list.From the list, you can **Run** (▶), **Edit** (✎), or **Delete** (✗) it.



1 General Criteria | 2 Specific Criteria | 3 Output

□ Send on Event

- Any
- Install Policy
- Save Policy
- Automatic
- Restore Policy
- Assign Global Policy
- Remove Global Policy
- Assign and Install Global Policy

○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name | Time
Revision Fields ("Send on Event" only): Device | # | Action | Admin | Ticket ID

Advanced Settings

Privacy
□ Hide administrator details

Display settings
□ Show textual configuration (Cisco only)

Object definitions
Include definitions of:
□ Groups and members
□ Non-group objects

Parameter	Description
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. Note: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results.Only the ticket ID is included.This is useful if ticket comments contain confidential information that should not be sent to report recipients,

	such as administrator details.

Tufin Device Audit Report

The Tufin Device Audit report verifies that your network devices meet your organization's standards for device configurations. (For Cisco IOS routers only)

You can select tests that look at the device's configuration for requirements such as:

- Require SSH Access Control - Management access to the device must be restricted on all VTY lines.
- Require Enable Secret - An **enable secret** password is defined using strong encryption to protect access to privileged EXEC mode (enable mode).
- Require Primary NTP Server - Make sure that a specified NTP server address is in the configuration. This enables time to be synchronized across all of your organization's devices.

The report searches through the device configuration and tells you if the test passed or failed.

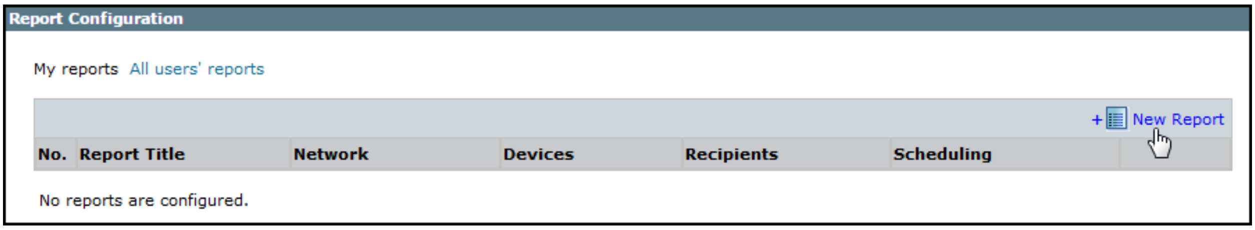
The pre-configured tests are for Cisco Routers. The tests use the NSA’s Router Security Configuration Guide as a guideline. To request additional device configuration tests, contact Tufin Support.

Creating a Tufin Device Audit Report

IPv6 is not supported for this TOS feature.

To create a Tufin Device Audit report:

1. Go to **Report**> **General Reports** and click **New Report.**



Report Configuration

My reports All users' reports

+ New Report

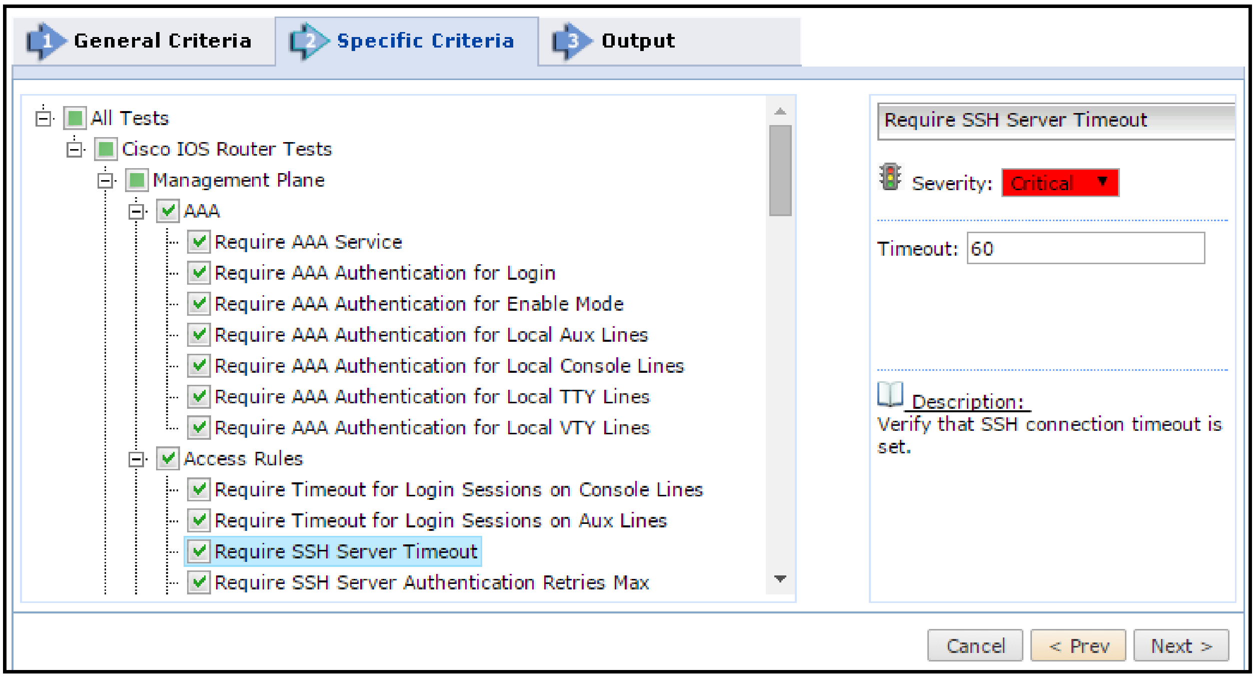
No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

The report configuration wizard has 3 steps.

2. **STEP 1**: Configure the **General Criteria** and click **Next**.
    1. For **ReportType**, select **Tufin Device Audit**:
    2. Optionally, you can change the **Title**.By default, the report's general name with the current date is the report name.
    3. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
    4. Select **Devices** for the report.

       If you have selected one domain, you can limit the report to include specific devices in the domain.
       If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.
3. **STEP 2**: Configure the **Specific Criteria** as explained below and click **Next**.
    1. Select the tests to run.You can click on the each test to view the test's description and severity level.
    2. For each test, you can change the test severity level as needed.
    3. Where applicable, you can change the threshold value that sets the severity.



- All Tests
  - Cisco IOS Router Tests
    - Management Plane
      - ☑ AAA
        - ☑ Require AAA Service
        - ☑ Require AAA Authentication for Login
        - ☑ Require AAA Authentication for Enable Mode
        - ☑ Require AAA Authentication for Local Aux Lines
        - ☑ Require AAA Authentication for Local Console Lines
        - ☑ Require AAA Authentication for Local TTY Lines
        - ☑ Require AAA Authentication for Local VTY Lines
      - ☑ Access Rules
        - ☑ Require Timeout for Login Sessions on Console Lines
        - ☑ Require Timeout for Login Sessions on Aux Lines
        - ☑ Require SSH Server Timeout
        - ☑ Require SSH Server Authentication Retries Max

Require SSH Server Timeout

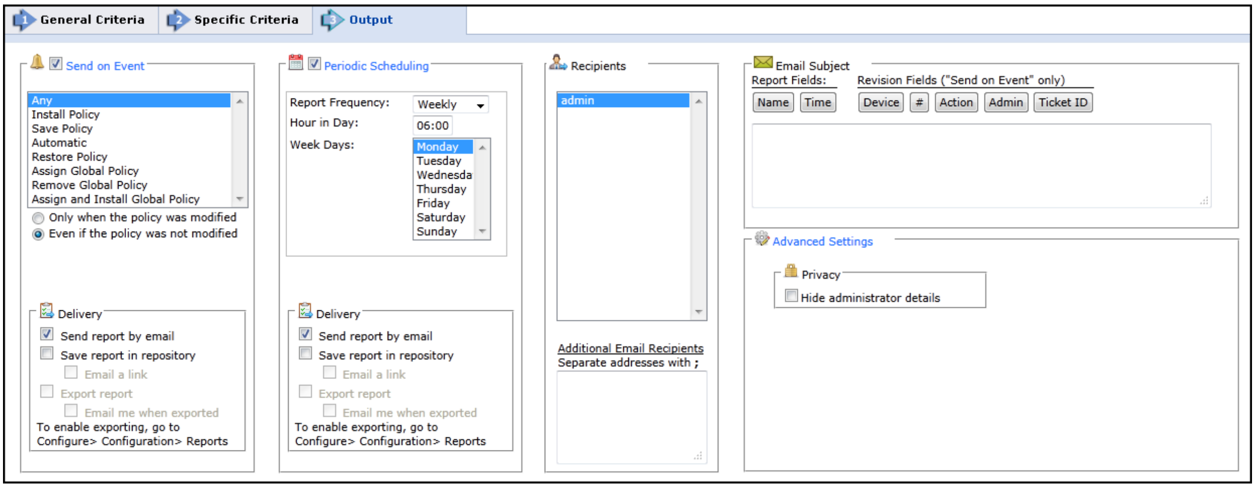
Severity: Critical

Timeout: 60

Description:
Verify that SSH connection timeout is set.

4. **STEP 3:** Configure the report **Output** as explained in the table below and click **Save**.

The saved report appears in the General Reports list.From the list, you can **Run** ( ), **Edit** ( ), or **Delete** ( ) it.



☑ Send on Event

Any
Install Policy
Save Policy
Automatic
Restore Policy
Assign Global Policy
Remove Global Policy
Assign and Install Global Policy

○ Only when the policy was modified
● Even if the policy was not modified

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery
☑ Send report by email
☐ Save report in repository
☐ Email a link
☐ Export report
☐ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients
admin

Additional Email Recipients
Separate addresses with ;

Email Subject
Report Fields: Name Time
Revision Fields ("Send on Event" only): Device # Action Admin Ticket ID

Advanced Settings
Privacy
☐ Hide administrator details

Parameter	Description
Send on Event	Select the events to trigger this report.You can use the <shift> key to select more than one event. Select one of the following, to decide whether to always run the report after the event, even when there are no changes: • **Only when the policy was modified**: Only if there are changes to be reported on, relative to the previous revision. • **Even if the policy was not modified**: If there are no changes, the report will state that there were no changes.For example, if an administrator first saves a Check Point policy, and then installs the policy on a gateway a few minutes later, the second event has not modified the policy.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and

	permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Periodic Scheduling	Defines a recurring schedule for report generation.The report can be generated on a daily, weekly, or monthly basis.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page.A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page.To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view).Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification).When a SecureTrack User creates a report, only that User is a recipient.When a SecureTrack Administrator creates a report, multiple recipients can be defined.These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack.Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses.Separate the addresses with a semicolon (;).
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advance Settings	**Privacy** • **Hide administrator details** - Select to have the report not include the names of users that made changes to policies or the name of the report creator.

Business Ownership Change Report

Business Ownership change reports are scheduled reports that contain information on changes made to access control for a specified network segment, within a specified span of time.This can be valuable for administrators who are responsible for, or 'own', those network segments.

The reported changes include enabling or blocking traffic.The report can be configured to include incoming traffic, outgoing traffic, or both types of traffic.

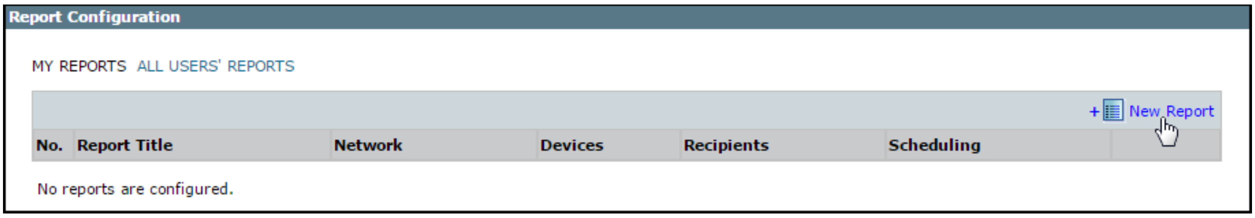
For Check Point devices, the Business Ownership change report includes only access control changes installed (not merely saved) during the specified time frame.

IPv6 is not supported for this TOS feature.

Creating a Business Ownership Change Report

To configure a Business Ownership Change Report:

1. Go to **Report** > **Business Ownership**,and click **New Report**:



Report Configuration

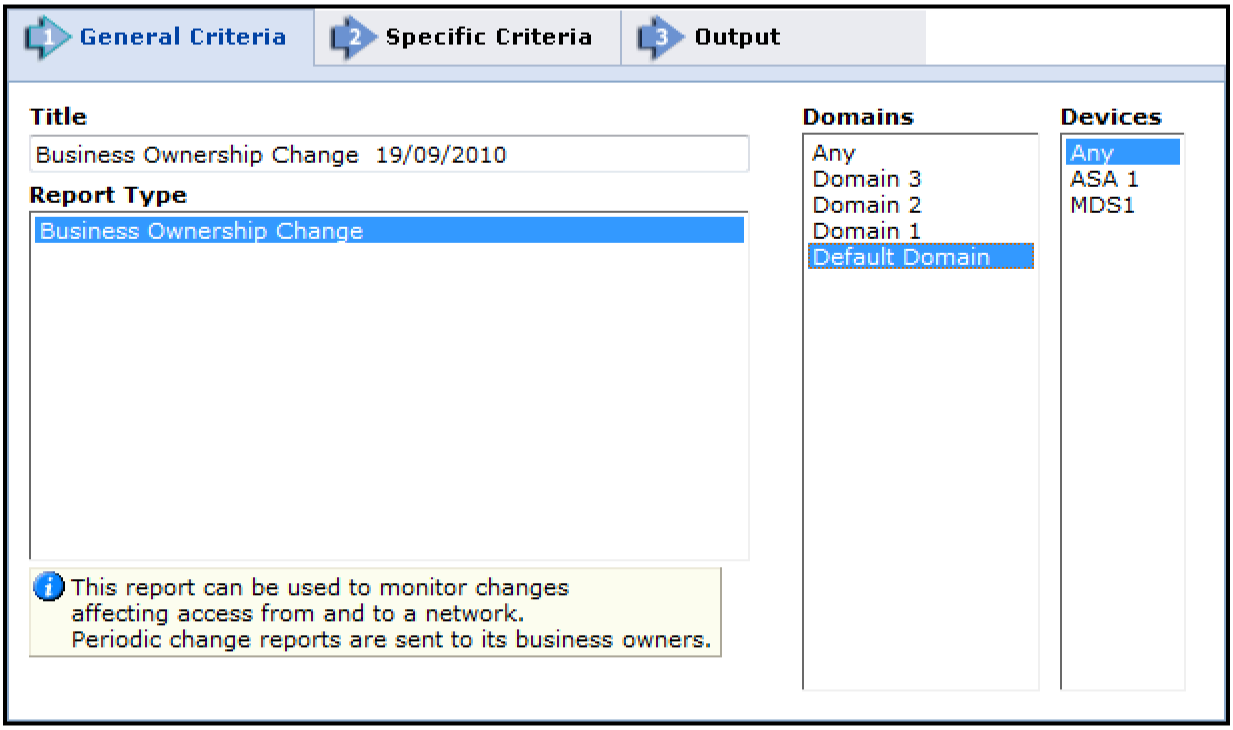
MY REPORTS ALL USERS' REPORTS

+ New Report

No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

2. In the **General Criteria** page, type a report **Title**:



Title: Business Ownership Change 19/09/2010

Report Type: Business Ownership Change

This report can be used to monitor changes affecting access from and to a network.
Periodic change reports are sent to its business owners.

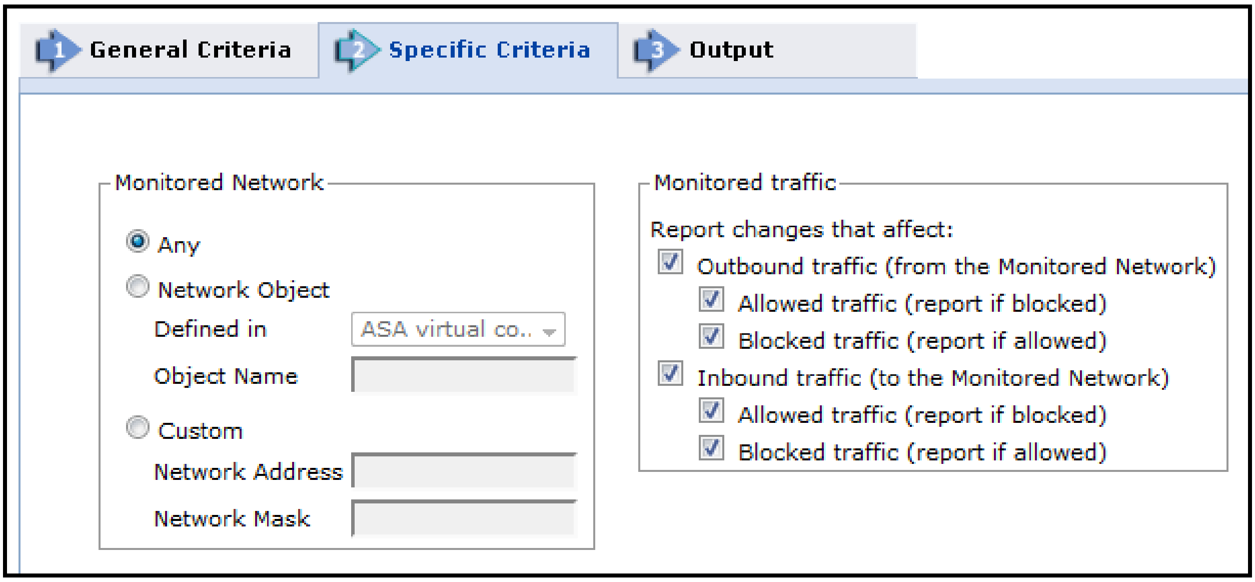
Domains: Any, Domain 3, Domain 2, Domain 1, Default Domain (selected)

Devices: Any (selected), ASA 1, MDS1

   1. Optionally, you can change the **Title**. By default, the report's general name with the current date is the report name.
   2. In a Multi-Domain environment, select the **Domains** that contain the devices you want to run the report on.
   3. Select **Devices** for the report.

3. If you have selected one domain, you can limit the report to include specific devices in the domain.
   If you have selected more than one domain, then **Any** is selected for **Devices**, and all devices in the selected domains are included in the report.
4. Click **Next**.

   Configure the **Specific Criteria** page:



1 General Criteria | 2 Specific Criteria | 3 Output

Monitored Network

● Any

○ Network Object

Defined in: ASA virtual co..

Object Name:

○ Custom

Network Address:

Network Mask:

Monitored traffic

Report changes that affect:

☑ Outbound traffic (from the Monitored Network)

☑ Allowed traffic (report if blocked)

☑ Blocked traffic (report if allowed)

☑ Inbound traffic (to the Monitored Network)

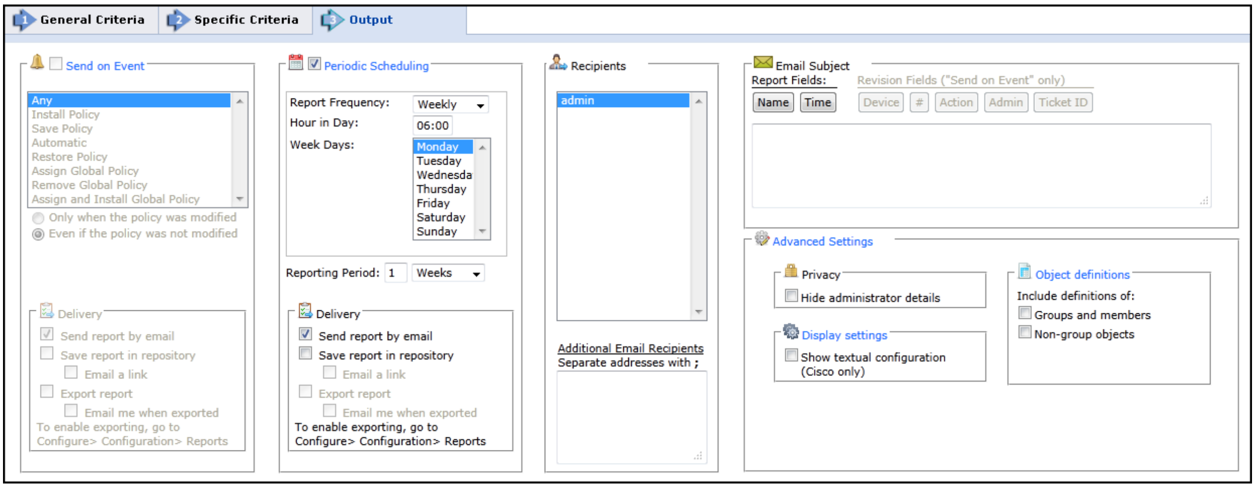
☑ Allowed traffic (report if blocked)

☑ Blocked traffic (report if allowed)

- **Report changes that affect**: One or both of the following:
  - **Outbound traffic from the network**
  - **Inbound traffic into the network**
- The **Monitored Network** to be reported on. You can use the precise case-sensitive name of a **Network Object** defined on a monitored device or in **SecureTrack**Network Zones, or explicitly define a network address.

Click **Next**.

5. Configure the report output:



1 General Criteria | 2 Specific Criteria | 3 Output

□ Send on Event

Any

Install Policy

Save Policy

Automatic

Restore Policy

Assign Global Policy

Remove Global Policy

Assign and Install Global Policy

○ Only when the policy was modified

● Even if the policy was not modified

Delivery

☑ Send report by email

□ Save report in repository

□ Email a link

□ Export report

□ Email me when exported

To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly

Hour in Day: 06:00

Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Reporting Period: 1 Weeks

Delivery

☑ Send report by email

□ Save report in repository

□ Email a link

□ Export report

□ Email me when exported

To enable exporting, go to Configure> Configuration> Reports

Recipients

admin

Additional Email Recipients

Separate addresses with ;

Email Subject

Report Fields: Name | Time

Revision Fields ("Send on Event" only): Device | # | Action | Admin | Ticket ID

Advanced Settings

Privacy

□ Hide administrator details

Display settings

□ Show textual configuration (Cisco only)

Object definitions

Include definitions of:

□ Groups and members

□ Non-group objects

- **Periodic Scheduling**: Defines a recurring schedule for report generation. The report can be generated on a daily, weekly, or monthly basis. **Reporting Period** controls how far back the report will span from the time of generation.

  Delivery: The report can be delivered in any of the following three ways:

  - **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them.

    The recipients' email addresses must have been configured in the user profile. The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users.

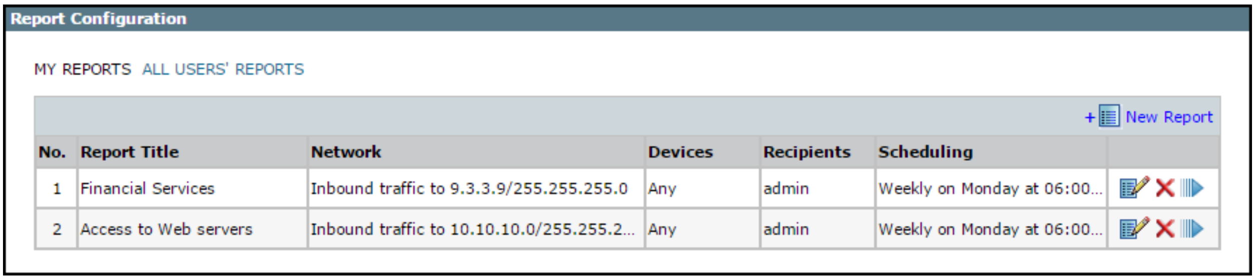
  - **Save report in Repository**: The report is saved and users can later view it in the **Reports Repository**. Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
  - **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page. A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page. To be notified when a report is generated, select **Email me when exported**.
- **Recipients**: the SecureTrack users who receive the report (or a link or notification). When a SecureTrack User creates a report, only that User is a recipient. When a SecureTrack Administrator creates a report, multiple recipients can be defined. Recipients

can be SecureTrack Administrators and Users (their email addresses must have been configured), or email addresses can be defined here explicitly, separated by semicolons (;).

- In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
- **Privacy**:
  - **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator.
  - **Show only ticket ID in name and comments** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results. Only the ticket ID is included. This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details.
- **Include definitions of**:
  - **Groups and members** - The report includes the definitions of group objects and their member objects. This is useful for recipients that do not have SecureTrack access. SecureTrack users can click on group objects in the report to see the definitions.
- **Non-group objects**- The report includes definitions of non-group objects.

6. Click **Save**.

The saved report appears in the Business Ownership Reports list. From the list, you can select the report and **Run**, **Edit**, or **Delete** it.



Report Configuration

MY REPORTS ALL USERS' REPORTS

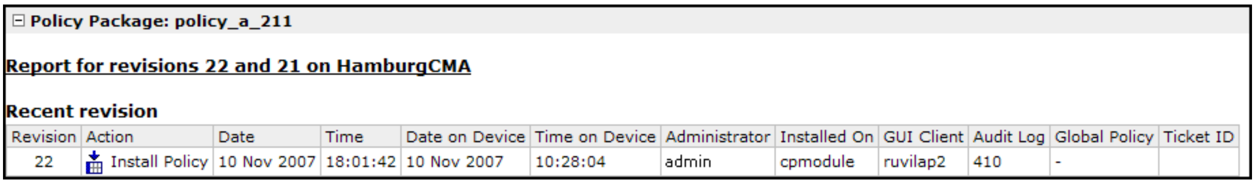
+ New Report

No.	Report Title	Network	Devices	Recipients	Scheduling	
1	Financial Services	Inbound traffic to 9.3.3.9/255.255.255.0	Any	admin	Weekly on Monday at 06:00...	✎ ✕ ▶
2	Access to Web servers	Inbound traffic to 10.10.10.0/255.255.2...	Any	admin	Weekly on Monday at 06:00...	✎ ✕ ▶

Understanding the Business Ownership Change Report

For each relevant Policy Package, the Business Ownership change report lists the following:

- The numbers of the compared revisions (the first installed revision within the specified time frame, and the latest installed revision within the specified time frame, respectively), and details of the recent revision:



⊟ Policy Package: policy_a_211

Report for revisions 22 and 21 on HamburgCMA

Recent revision

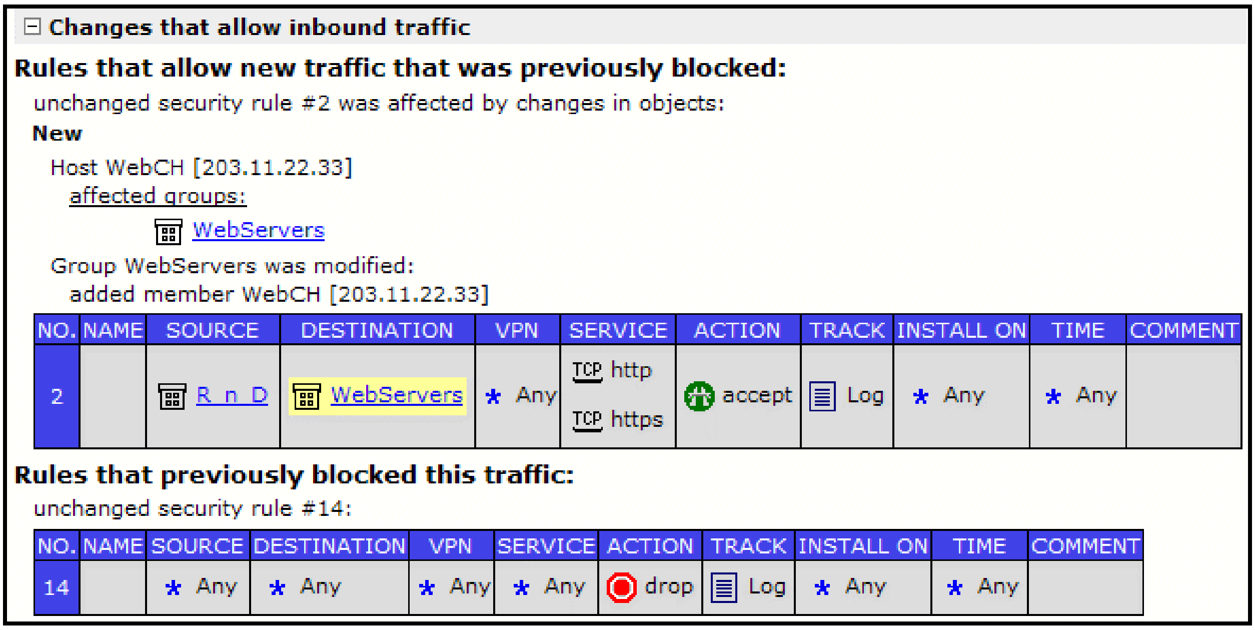
Revision	Action	Date	Time	Date on Device	Time on Device	Administrator	Installed On	GUI Client	Audit Log	Global Policy	Ticket ID
22	Install Policy	10 Nov 2007	18:01:42	10 Nov 2007	10:28:04	admin	cpmodule	ruvilap2	410	-	

For Check Point deployments, the Business Ownership change report includes access control changes installed (not saved) during the specified time frame.

- For outgoing traffic, for incoming traffic, or for each, depending on the report, the following appears:
  - Newly allowed traffic
  - Newly blocked traffic

For each of these categories, for each relevant change, the report displays the rule that previously affected the traffic, the rule that now affects the traffic, and, if the change is to a rule (rather than to something else, such as an object's definitions), the previous form of the changed rule. The change fields are highlighted and summarized.

In the following example, a member was added to a group, causing new inbound traffic to be allowed:



⊟ Changes that allow inbound traffic

Rules that allow new traffic that was previously blocked:

unchanged security rule #2 was affected by changes in objects:

New

Host WebCH [203.11.22.33]

affected groups:

WebServers

Group WebServers was modified:

added member WebCH [203.11.22.33]

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
2		R_n_D	WebServers	Any	TCP http TCP https	accept	Log	Any	Any	

Rules that previously blocked this traffic:

unchanged security rule #14:

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
14		Any	Any	Any	Any	drop	Log	Any	Any	

If there is a revision of the policy package that was installed in the specified time frame, but was not yet analyzed by SecureTrack at the time the report was generated, the following message appears in the report:

There is an installed version within the given time frame in which this policy package is not available for analysis. Report may not include all changes performed within given time frame.

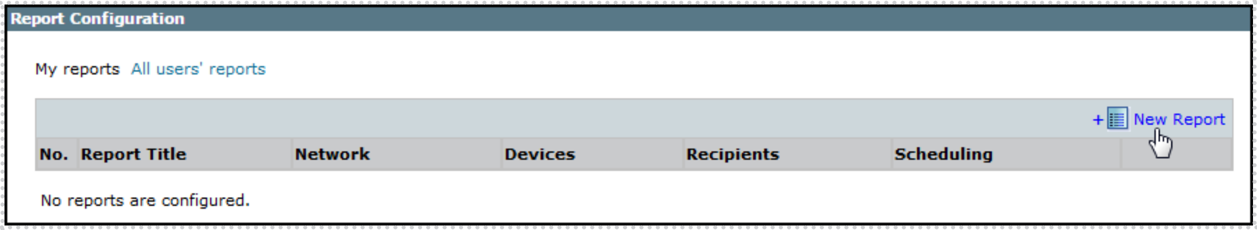
Adding Reports and Generating Results

After you create and configure your reports, you can view the reports that are generated based on a schedule in the reports repository. You can also generate configured report results (except for the New Revision report), and view them in the browser or have them saved in SecureTrack's Report Repository.

Adding a Report

Every general report that you create uses a 3-step report configuration wizard. The specific configurable details displayed for each step varies, depending on the report type selected. To create a report and add it to the repository:

1. Go to **Report** > **General Reports**, and click **New Report**.



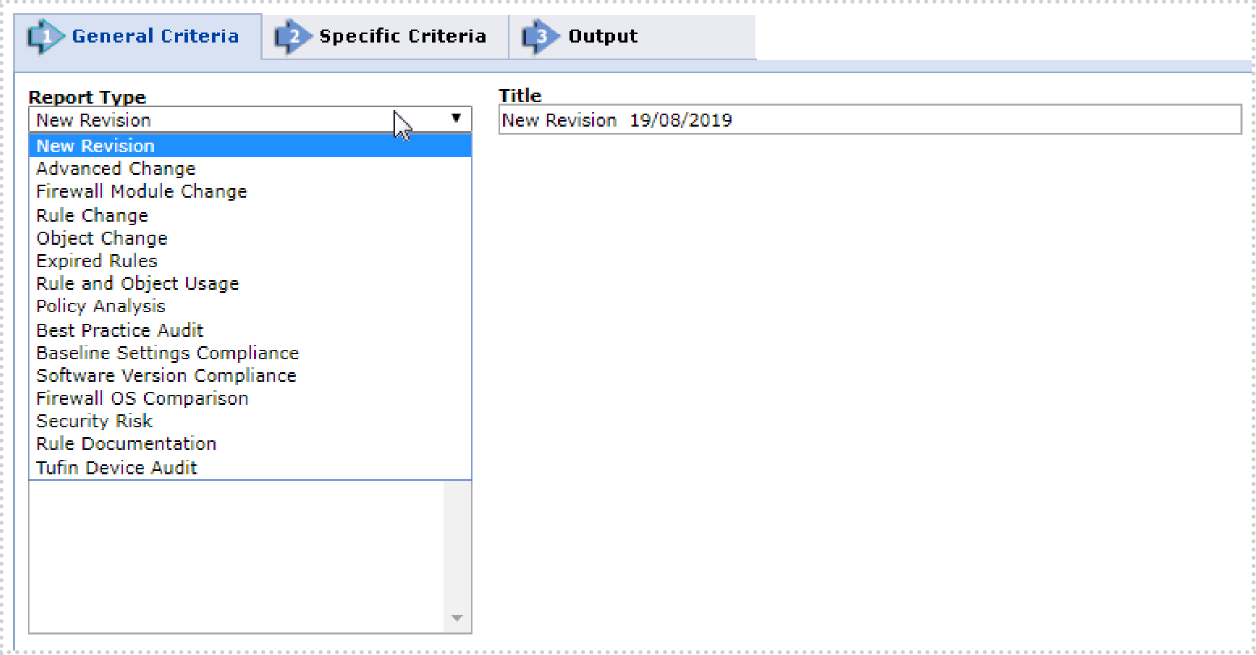
Report Configuration

My reports All users' reports

No.	Report Title	Network	Devices	Recipients	Scheduling

No reports are configured.

2. **Step 1- General Criteria**: Select the **Report Type** and **Title** for the report. Configure all the report specific additional information, as prompted for by the wizard.

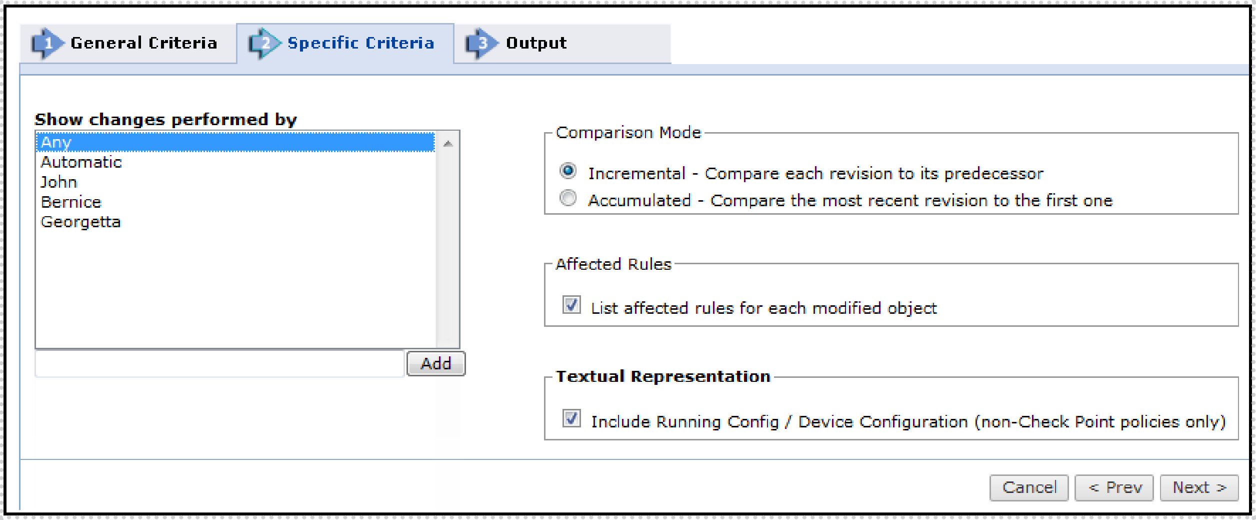


Report Type: New Revision ▼

- New Revision
- Advanced Change
- Firewall Module Change
- Rule Change
- Object Change
- Expired Rules
- Rule and Object Usage
- Policy Analysis
- Best Practice Audit
- Baseline Settings Compliance
- Software Version Compliance
- Firewall OS Comparison
- Security Risk
- Rule Documentation
- Tufin Device Audit

Title: New Revision 19/08/2019

3. **Step 2 - Specific Criteria**: Select the specific criteria required for the report type selected, for example rules for the Rule Change report or the users and the comparison mode for the Advanced Change report.



Show changes performed by

- Any
- Automatic
- John
- Bernice
- Georgetta

Comparison Mode

● Incremental - Compare each revision to its predecessor
○ Accumulated - Compare the most recent revision to the first one

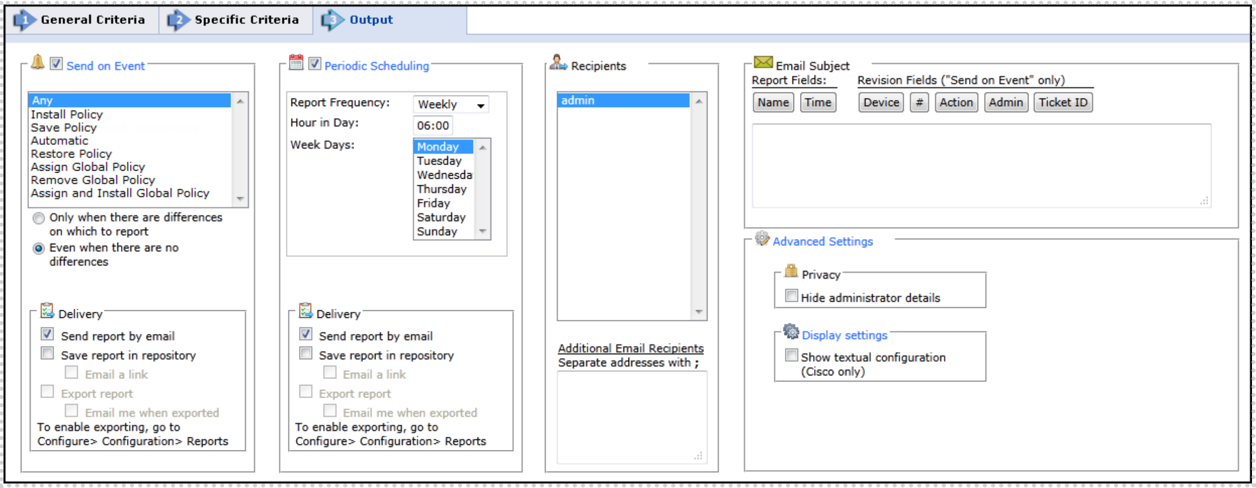
Affected Rules

☑ List affected rules for each modified object

Textual Representation

☑ Include Running Config / Device Configuration (non-Check Point policies only)

4. **Step 3 - Output**: Configure the report output elements. The specific elements enabeld will vary, depending on the report type selected.



☑ Send on Event

- Any
- Install Policy
- Save Policy
- Automatic
- Restore Policy
- Assign Global Policy
- Remove Global Policy
- Assign and Install Global Policy

○ Only when there are differences on which to report
● Even when there are no differences

Delivery

☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

☑ Periodic Scheduling

Report Frequency: Weekly
Hour in Day: 06:00
Week Days: Monday, Tuesday, Wednesda, Thursday, Friday, Saturday, Sunday

Delivery

☑ Send report by email
□ Save report in repository
□ Email a link
□ Export report
□ Email me when exported
To enable exporting, go to Configure> Configuration> Reports

Recipients

- admin

Additional Email Recipients
Separate addresses with ;

Email Subject

Report Fields: Revision Fields ("Send on Event" only)

Advanced Settings

Privacy

□ Hide administrator details

Display settings

□ Show textual configuration (Cisco only)

Parameter	Description
Send on event	Select the events to trigger this report. You can use the <shift> key to select more than one event. The event details available are specific to a report type and the specific devices selected.
Periodic Scheduling	Defines a recurring schedule for report generation. The report can be generated on a daily, weekly, or monthly basis. **Reporting Period** controls how far back the report will span from the time of generation.
Delivery	The report can be delivered in any of the following three ways: • **Send report by email**: The report is generated for each of the selected **Recipients** and emailed to them. The emailed report's formatting (embedded HTML, MHT attachment or PDF attachment) is globally configurable for all users. • **Export report**: This option is available only to SecureTrack Administrators, and only when enabled in the Reports page. A report is generated according to the owner's configured preferences and permissions, and exported according to the configuration in the Reports page. To be notified when a report is generated, select **Email me when exported**. • **Save report in Repository**: The report is saved and users can later view it by selecting the **Reports Repository** tab (in **Report** view). Select **Email a link** to have a link to the report sent to recipients when a report is generated, provided the recipient's email is configured.
Recipients	**Recipients**: The SecureTrack users who receive the report (or a link or notification). When a SecureTrack User creates a report, only that User is a recipient. When a SecureTrack Administrator creates a report, multiple recipients can be defined. These **Recipients** are SecureTrack Administrators or Users whose email addresses have been configured in SecureTrack. Other email addresses can be defined, separated by semicolons (**;**) in the **Additional Email Recipients** text box. **Note**: In a Multi-Domain environment, administrators (Super and Multi-Domain) can only add users who have permissions for the current Global or Domain context. SecureTrack does not send the report if a specified recipient does not have permission for a device or Domain included in the report configuration when the report is generated.
Additional Email Recipients	Enter additional email recipient addresses. Separate the addresses with a semicolon (;)
Email Subject	You can click on the field buttons to add the fields to the subject line of the email notifications. • **Report Fields**: You can include the name of the report and the time that the report was generated. • **Revision Fields**: When the report is configured to **Send on Event**, you can include the name of the device, the revision number, the action that triggered the notification, the name of the administrator who did the action, and the ticket ID associated with the change in the new revision.
Advanced Settings	**Privacy** • **Hide administrator details** - The report does not include the names of users that made changes to policies or the name of the report creator. **Display Settings** • **Show textual configuration (Cisco only)** (when ticket ID recognition is configured) - If selected, the rule Name and Comment fields are removed from the report results. Only the ticket ID is included. This is useful if ticket comments contain confidential information that should not be sent to report recipients, such as administrator details. **Object definitions - Include definitions of**: • **Groups and members** - The report includes the definitions of group objects and their member objects. This is useful for recipients that do not have SecureTrack access. SecureTrack users can click on group objects in the report to see the definitions. • **Non-group objects** - The report includes definitions of non-group objects.

5. Click **Save**.

Saved reports appear in the General Reports list, from which you can **Run** (▶), **Edit** (✎), or **Delete** (✗) any report.

See [Configuring SecureTrack Reports] for a step-by-step guide to adding and configuring a specific report type.

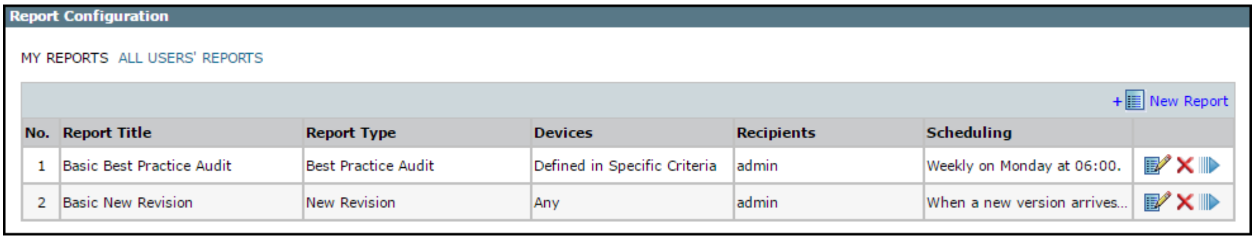
Generating Report Results

This section is not applicable to PCI DSS Reports.

To generate report results from a configured report:

1. Select **General Reports** or **Business Ownership** as required.

   A list of configured reports (except Business Ownership reports) available for the connected user appears. Each line in the table displays basic information for one report: the report's title, type, relevant devices, recipients and scheduling.



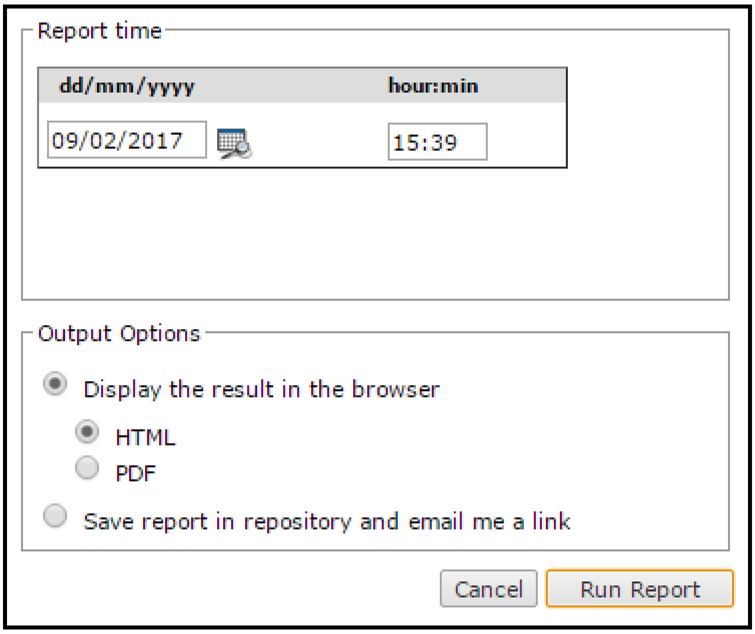
Report Configuration

MY REPORTS   ALL USERS' REPORTS

+ New Report

No.	Report Title	Report Type	Devices	Recipients	Scheduling	
1	Basic Best Practice Audit	Best Practice Audit	Defined in Specific Criteria	admin	Weekly on Monday at 06:00.	✎ ✗ ▶
2	Basic New Revision	New Revision	Any	admin	When a new version arrives...	✎ ✗ ▶

2. For the desired report, click: ▶
3. Configure the following.



Report time

dd/mm/yyyy	hour:min
09/02/2017	15:39

Output Options

● Display the result in the browser

● HTML

○ PDF

○ Save report in repository and email me a link

- **Report Period**: The time period to be reported upon. For some reports, this setting is a **Report Time**.
- **Output options**: How the report should be displayed or saved:
  - **Display the result in the browser**: View the result now, as either HTML or a PDF.
  - **Save report in repository and email me a link**: Report results saved in the repository can be viewed at any time as either HTML or a PDF.

4. Click **Run Report**.

The report is generated.

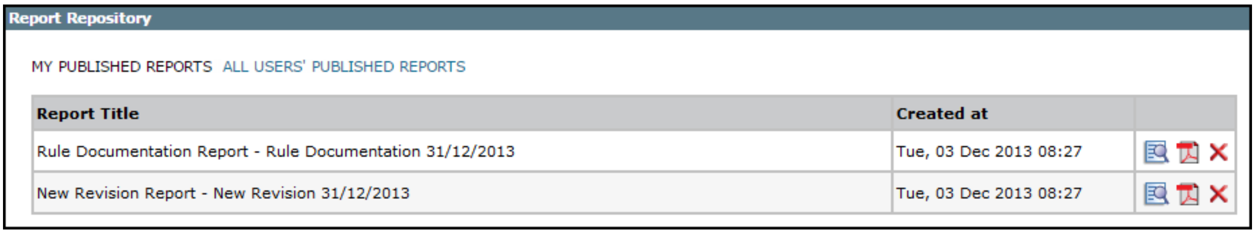
How Do I Get Here?

In SecureTrack, go to **Report> General Reports**

Viewing a Generated Report Saved in the Reports Repository

To view a report that was previously generated and saved to the Reports Repository:

1. In **Report** View, select**Reports Repository**:



Report Repository

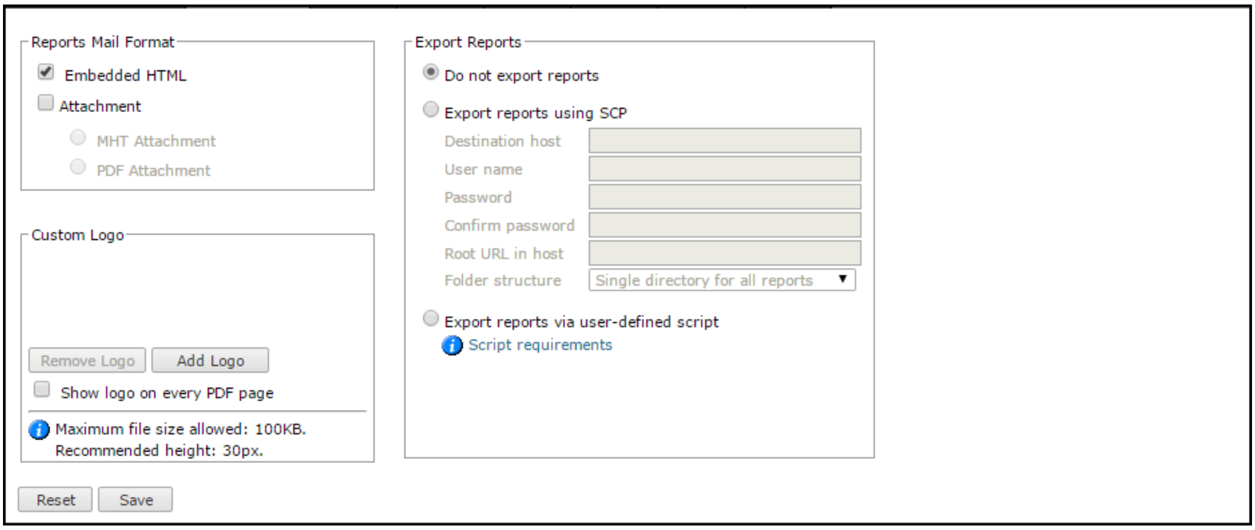
MY PUBLISHED REPORTS ALL USERS' PUBLISHED REPORTS

Report Title	Created at	
Rule Documentation Report - Rule Documentation 31/12/2013	Tue, 03 Dec 2013 08:27	🔍 📄 ✕
New Revision Report - New Revision 31/12/2013	Tue, 03 Dec 2013 08:27	🔍 📄 ✕

2. In the row for the desired report, click 🔍 to view HTML or 📄 to view a PDF.

Reports Configuration Settings

Only a SecureTrack Administrator - in a Multi-Domain environment, only a Super Administrator - can configure the Reports page.



Reports Mail Format
☑ Embedded HTML
☐ Attachment
○ MHT Attachment
○ PDF Attachment

Custom Logo
Remove Logo | Add Logo
☐ Show logo on every PDF page
Maximum file size allowed: 100KB.
Recommended height: 30px.

Export Reports
● Do not export reports
○ Export reports using SCP
Destination host
User name
Password
Confirm password
Root URL in host
Folder structure: Single directory for all reports
○ Export reports via user-defined script
Script requirements

Reset | Save

How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration** > **Reports**.

Setting Format and Logo for Reports

You can set the file format for emailed reports, and upload your corporate logo to appear in reports. This page is also used to configure report export.

Reports Mail Format settings affect emailed reports. A **Custom Logo**, if added, will appear in all reports, query results, and audits. For PDF format, you can **Show logo on every PDF page** or just at the beginning of the report.

Custom Logo lets you remove the Tufin logo from the reports or add your own logo. Your logo can be in GIF or JPG format. For best results, we recommend that your logo be in GIF format and 30 pixels high.

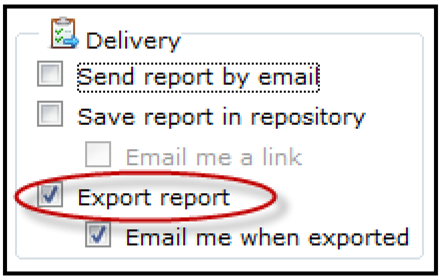
For settings to take effect, you must click **Save**.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration** > **Reports**.

Configuring Report Export

In report output configuration, there is an option for the on-event or scheduled report to be automatically exported to an external repository or portal:



Delivery

□ Send report by email

□ Save report in repository

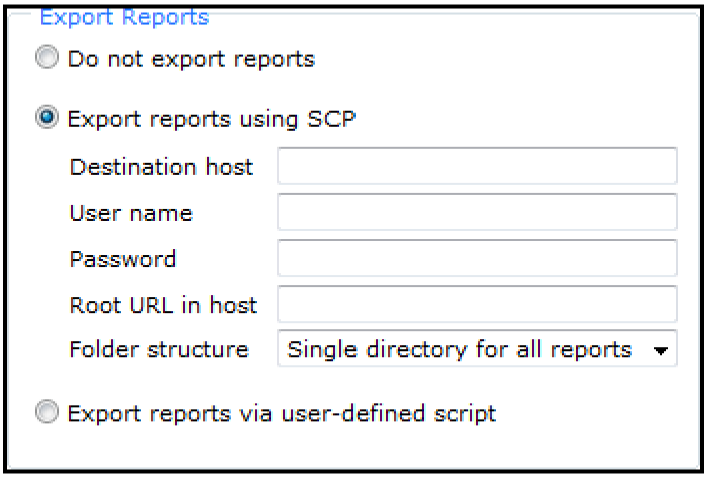
□ Email me a link

☑ Export report

☑ Email me when exported

Export settings for the entire SecureTrack system are defined in the Reports page at **Settings > Configuration > Reports**. Only a SecureTrack Administrator - in a Multi-Domain environment, only a Super Administrator - can configure the Reports page. This page is also used for setting report format and logo.

The export settings in the Reports page are:



Export Reports

○ Do not export reports

● Export reports using SCP

Destination host:

User name:

Password:

Root URL in host:

Folder structure: Single directory for all reports

○ Export reports via user-defined script

- **Do not export reports:** In report output configurations, the export option is disabled.
- **Export reports using SCP:** SecureTrack connects via SCP to the specified Destination host, using the specified User name and Password, and copies the report to the host's file system, to the specified Root URL in host (path on host to target location).

  Folder structure defines how reports should be arranged in folders under the target location:

  - Single directory for all reports: All reports are placed directly in the target location.
  - Directory per report type: A folder is created for each report type (New revision report, Advanced change report, etc.).
  - Directory per context: In a Multi-Domain environment, the reports configured in each domain context are placed in a separate folder.
- **Export reports via user-defined script:**
  - SecureTrack executes the script located at: /usr/local/st/export_report_script.sh
  - This must be a Unix-formatted file written as a Bash shell script.
  - The file must have execute permissions for user: st

    chmod 777 /usr/local/st/export_report_script.sh
  - The script should copy the report to a target that authorizes users: st and root
  - SecureTrack will pass the following arguments to the script:

Argument	Description
1	Source PDF file path and name
2	Report owner
3	Report name
4	Report type
5	In a Multi-Domain environment: Report context In a regular environment: This string is empty
6	The string “-mgmt_id”
7	The value of the management id
8	The string “-version”

9	The value of the policy version
10	"-report_id"
11	The value of the report output id.
12	Revision ID

When the triggering event parameter configured in **Report > Report Configuration > ...Output > Send on Event** occurs, SecureTrack will pass arguments 6-11 to the script. The following sample script renames the file and copies it to another location on the SecureTrack host:

```
#!/bin/bash
SOURCEFILE=1
REPORTOWNER=$2
REPORTNAME=$3
REPORTTYPE=$4
CONTEXT=$5
#Make sure to use quote marks in case of spaces or special characters
TARGETFILENAME="$REPORTOWNER$REPORTNAME$REPORTTYPE$CONTEXT.pdf"
TARGETDIR="/var/tmp"
cp "$SOURCEFILE" "$TARGETDIR/$TARGETFILENAME"
```

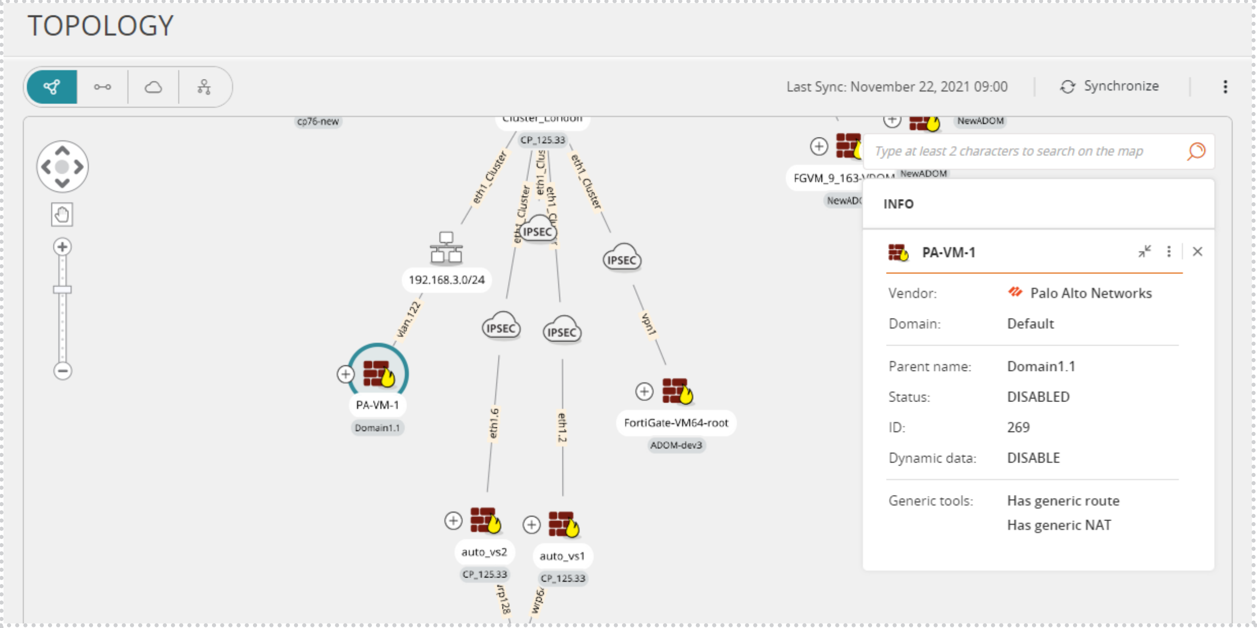
Network Mapping

SecureTrack helps you map out your network with:

- Topology, including:
  - Topology intelligence, which calculates how traffic flows through your network according to the routing information from your devices
  - Interactive map, which graphically displays the topology of your network and lets you edit the topology to better match your real-world network
- Network Zones, which let you group subnets together into zones that are used in risk and security calculations

Interactive Map

The interactive map, also known as the topology map or the network map, is a dynamic map of your monitored devices and the subnets to which they are connected. The map is created using Topology Intelligence.



PA-VM-1

Vendor: Palo Alto Networks

Domain: Default

Parent name: Domain1.1

Status: DISABLED

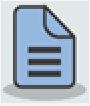
ID: 269

Dynamic data: DISABLE

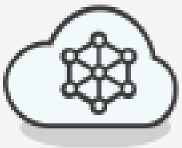
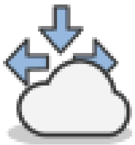
Generic tools: Has generic route
Has generic NAT

You can enter the details of a network traffic flow to see the path of the traffic on the map.

The interactive map includes:

Object	Description	Actions
Cloud	A group of subnets for which a device routes traffic through an interface to an unknown gateway. The default name of the cloud includes the gateway listed for the routes.	Right click a cloud to see the known subnets that are in the cloud. For a cloud, you can: • Change its name • Change its zone type • Join or detach other clouds
Generic Device 	A network device that is not monitored by SecureTrack but is included in topology calculations.	Click on a generic device to see its interfaces, IP addresses and routing table. For a generic device you can: • Change its name • Upload a new interface and routing file

Object	Description	Actions
Monitored Device	A network device that is monitored by SecureTrack. The names of the interfaces are shown on the connections from the device.	Click on a device to see its interfaces, IP addresses and routing table.
Subnet	A network subnet that is connected to at least one device interface.	Click on a subnet to see the device interfaces that are connected to it and the IP addresses of the interfaces. For a subnet, you can: • Change its subnet type (Internal, External or DMZ) • Join or detach interfaces to the subnet
Subnet and Cloud Groups ⊕	A group of subnets or clouds that are all only connected to one monitored device.	Click on ⊕ to open the group and see the subnets and clouds in the group.
Connectivity between virtual systems	Connectivity between two virtual systems (such as virtual firewalls for Panorama)	None
	F5 devices	
IPSEC	A connection that is established over IPSEC.	None
PBR	Policy-based routing (PBR) for Cisco IOS routers	None
VXLAN EVPN	VxLAN EVPN for Cisco Nexus switches	None
	A vNet peering connection; two virtual networks (VNets) connected through the Azure backbone network	None

Object	Description	Actions
	A VPC peering connection; a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses	None
	Transit Gateway; a service that enables you to connect thousands of Amazon Virtual Private Clouds (Amazon VPCs) and their on-premises networks using a single gateway	None
	Cisco ACI	Right click a Cisco ACI device to display its associated routes and subnets. Click ⊕ to see the subnets.

Prerequisites

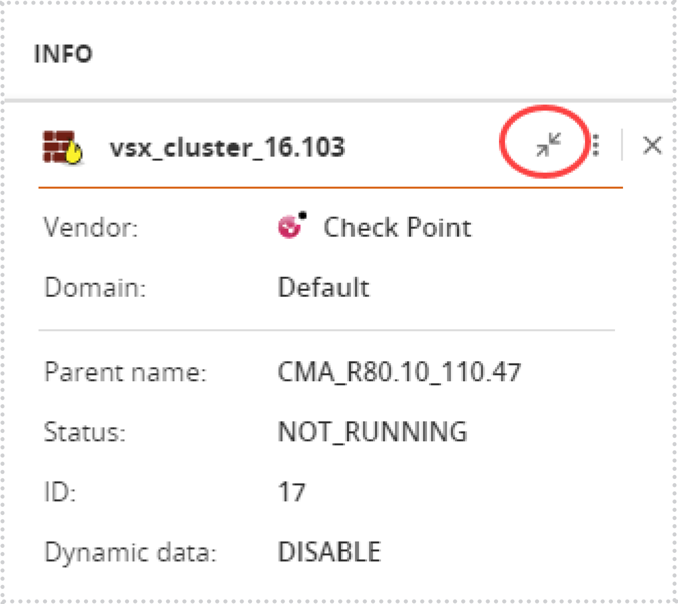
- Make sure that all of the devices that impact your topology are monitored by SecureTrack.

  For devices that are not monitored, you can add a generic device to represent the device with its interfaces and routes.
- Permissions

  Access to the map is given only to users with sufficient permissions. The menu option **Map** will appear only for these users:
  - Administrators
  - Super Administrators
  - Multi-domain administrators, when a domain context is selected and not when All Domains is selected.

What can I do on this page?

- View the Interactive Map - Click to view and navigate the interactive map.
- View device details - Click ↗ to expand and ↙ to collapse device details.

  INFO

  vsx_cluster_16.103

  Vendor: Check Point

  Domain: Default

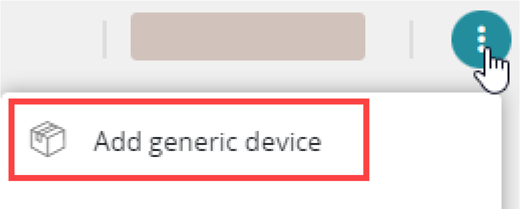
  Parent name: CMA_R80.10_110.47

  Status: NOT_RUNNING

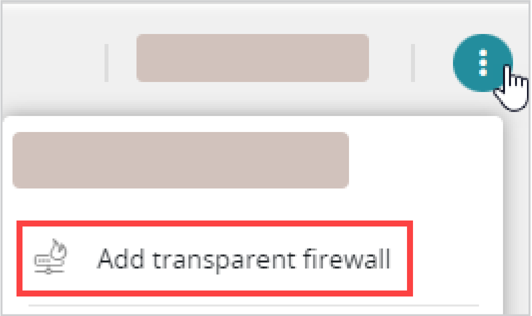
  ID: 17

  Dynamic data: DISABLE
- View cloud suggestions: Click the Cloud Suggestions link in **JOIN CLOUDS**

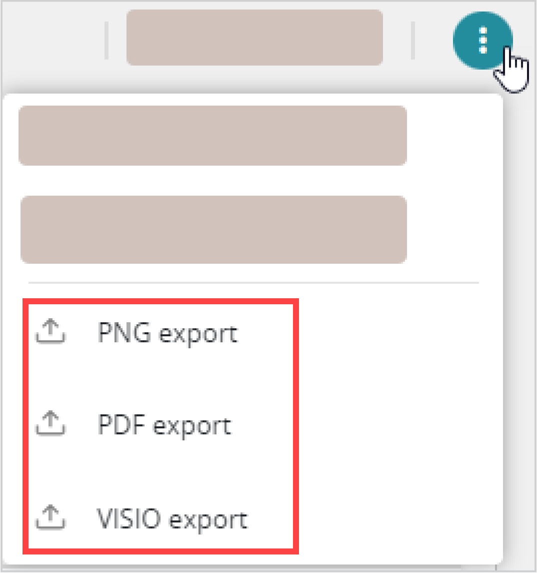
- Investigate traffic paths: Click to investigate a specific traffic path or to Diagnose Broken Traffic Paths.
- Join or split subnets: Click to join or split subnets
- Join or split clouds: Click to join or split clouds
- Refresh the map: Click to synchronize the topology for the interactive map
- Add generic device: Click **Add generic device** to enter the details for a generic device



- Add Transparent Devices: Click **Add transparent firewall** to enter details for transparent devices



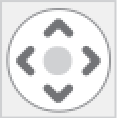
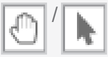
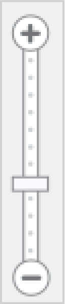
- Export interactive map: Click one of the export options: PNG, PDF, Visio



- Multi-domain only - Click Global (bottom-left of the window) All Domains to switch domain contexts and view the devices for a specific domain. Users with "Super admin" permission can also view the Global domain context (see "Multi-Domain Management" on page 606).

Page Controls

Use these controls to navigate in the map page.

Control	Description
	Use the arrows to pan around the map, sliding the view up, down, right or left.
	Use the hand to slide the map. Click the hand to toggle to the arrow, which you use to highlight a group of objects in the map.
	Use the slider or +/- buttons to control the zoom level of the map.

How Do I Get Here?

In SecureTrack, click **Network** > **Interactive Map**.

Topology Intelligence

Topology Intelligence lets you use the routing information in your devices to make better decisions about your network's security. For all devices that have topology enabled in the device settings, SecureTrack collects the interface information and routing tables with the policy revisions. SecureTrack updates the network topology once a day.

Topology calculations also include NAT information from supported devices or with the generic NAT model.

SecureTrack uses this information for:

- Interactive Map - SecureTrack builds a dynamic and editable map of your network devices and networks.
- Risk - You can define your risks based on the zone types from the topology map.
- Security Risk Report - You can run the Security Risk report based on the zone types from the topology map.
- Compliance Policies - You can have SecureTrack identify the relevant policies for the compliance criteria automatically.

Also, **SecureChange** uses topology intelligence to:

- Suggest target devices for access requests
- In Designer, SecureChange calculates the necessary change and shows a picture of the path between the source and destination
- Automatically verify if an Access Request was successfully added

Enabling or Disabling Topology for Devices

Topology intelligence calculations combine the routes for all virtual systems in a device together, and do not treat the virtual devices as separate entities. All supported devices are enabled for topology intelligence data collection by default.

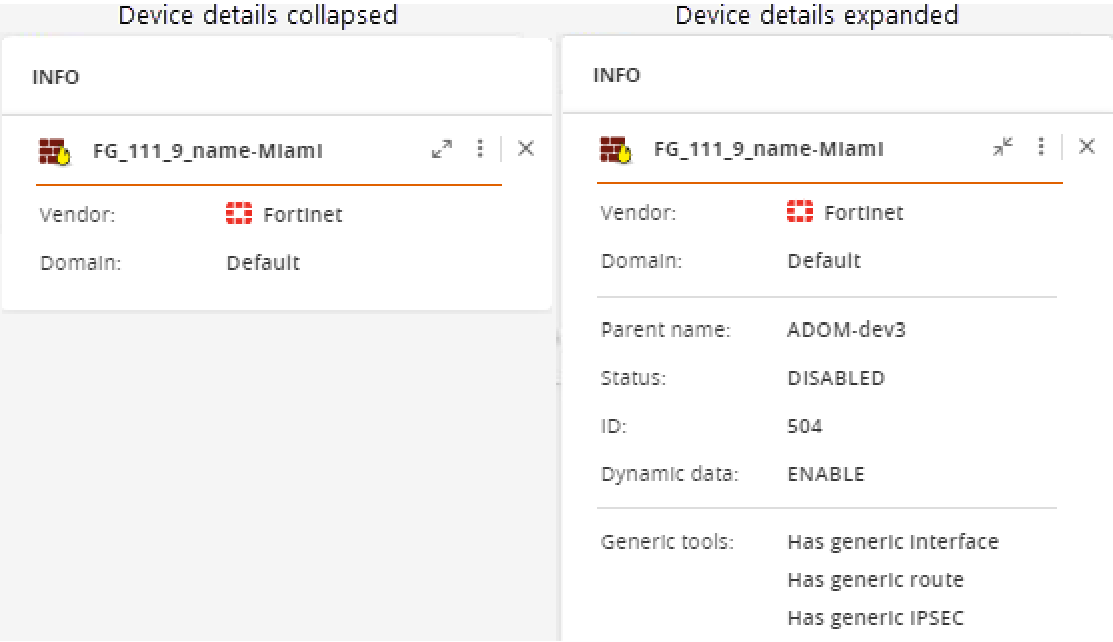
To improve router performance and resolve issues associated with retrieving the networks for devices with many dynamic routes, contact Tufin Support to add or delete specific networks and routes, rather than retrieving the entire network for these devices.

To enable or disable topology data collection for a device:

1. Go to Monitoring Devices.
2. Select the device and click **Edit Configuration**.
3. Select or clear **Enable Topology**.
4. Complete the Edit Device wizard and click **Save**.

Viewing Device Details

Click ⤢ to expand and ⤡ to collapse the device details in the **INFO** panel.



Device details collapsed

INFO

FG_111_9_name-Miami

Vendor: Fortinet

Domain: Default

Device details expanded

INFO

FG_111_9_name-Miami

Vendor: Fortinet

Domain: Default

Parent name: ADOM-dev3

Status: DISABLED

ID: 504

Dynamic data: ENABLE

Generic tools: Has generic interface
Has generic route
Has generic IPSEC

Click ⋮ to show the available device options:

- **Show routes**
- **Show interfaces**
- **Show route base VPNs**
- **Show peering information**

Click ✖ to close the **INFO** panel.

Investigating Traffic Paths

Click ⊶ to display the **Path Analysis** panel. Enter the traffic details of devices and cloud platforms for the paths you want to investigate, including the source, destination, and the predefined services or predefined application identities (optional). This panel displays the selected path in the order of the minimum distance (least number of hops) from any source to any destination. Devices with an equal distance between the source and destination are listed in alphabetical order.

In the interactive map you can enter the name of a firewall object (host, subnet, IP range, LDAP users, or group), or an IP address. To search for a user group, enter **user.name** in front of the group. For example: `user.name/QA-devices`. For IP addresses, IPv4 is supported for all devices and IPv6 is supported for specific devices. See SecureTrack Features by Vendor.

Click **Export** next to the search result to generate a PDF report with details of the search results, including matching rules, interfaces, and NAT information. If there are multiple paths, you can select which paths to include in the report. The report includes a map of the paths and details of each device in a path.

Click **Manage queries** to create and manage path queries.

The icons on the map are:

Icon	Meaning	Description
◎	Start point	First element that SecureTrack can identify in each path. If the start point is not in an identified network, SecureTrack shows the start point in a cloud.
✓	Routes traffic	Device that allows traffic.
⊖	Drops traffic	Device includes a rule that blocks traffic.

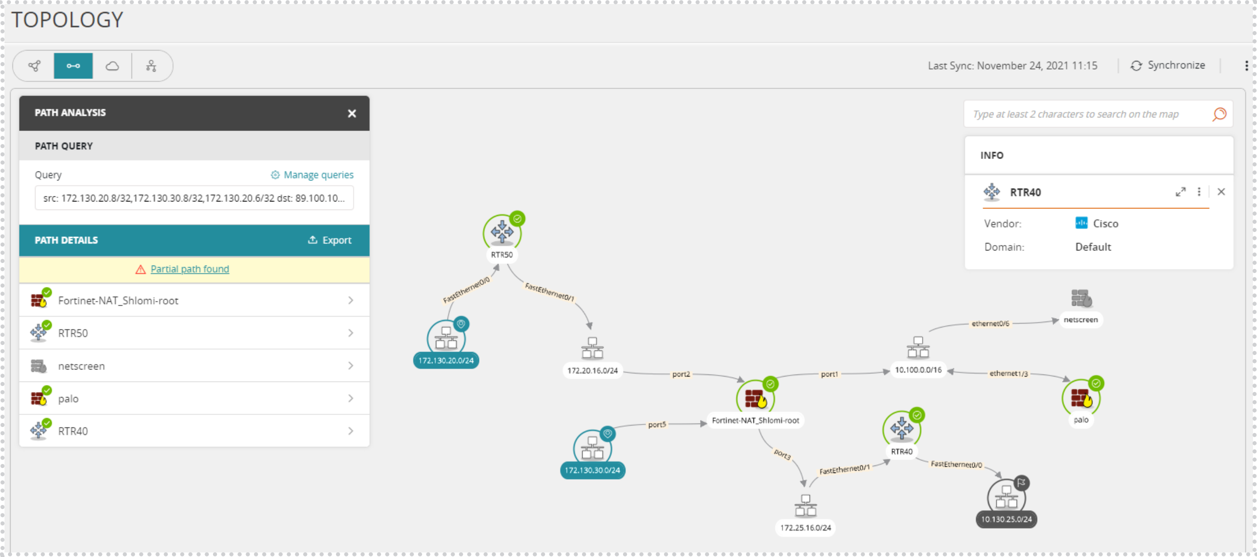
Icon	Meaning	Description
▦	Incomplete path	Source traffic goes to this point, but does not reach the destination.
⚑	End point	Last element that SecureTrack can identify in each path. If the next device in the path is an unmonitored device, SecureTrack shows the end point in a cloud.
→	Directional arrow	Direction of the modeled traffic (Traffic can also be bidirectional)

What can I do on this page?

- Select an object: Click the object.
- Add objects to the list of selected objects: Ctrl-click multiple objects or type text, contained in the object name, in the search box.
- Reveal actions for objects: Right-click the object or open the information menu for the selected objects.
- For each object, you can:
  - Drag and drop the object in the **Interactive Map**
  - For monitored devices - Show routes and interfaces

    For default route use the value 0.0.0.0/0
  - For networks: Set as source or destination for path analysis

    When a path is highlighted, in the Path panel you can select a device or cloud platform that passes the traffic. This lets you view the incoming interfaces (for cloud, coming from) and the next devices (for cloud, going to).



TOPOLOGY

PATH ANALYSIS

PATH QUERY

Query: src: 172.130.20.8/32,172.130.30.8/32,172.130.20.6/32 dst: 89.100.10...

PATH DETAILS

Partial path found

- Fortinet-NAT_Shlomi-root
- RTR50
- netscreen
- palo
- RTR40

Last Sync: November 24, 2021 11:15

INFO

RTR40

Vendor: Cisco

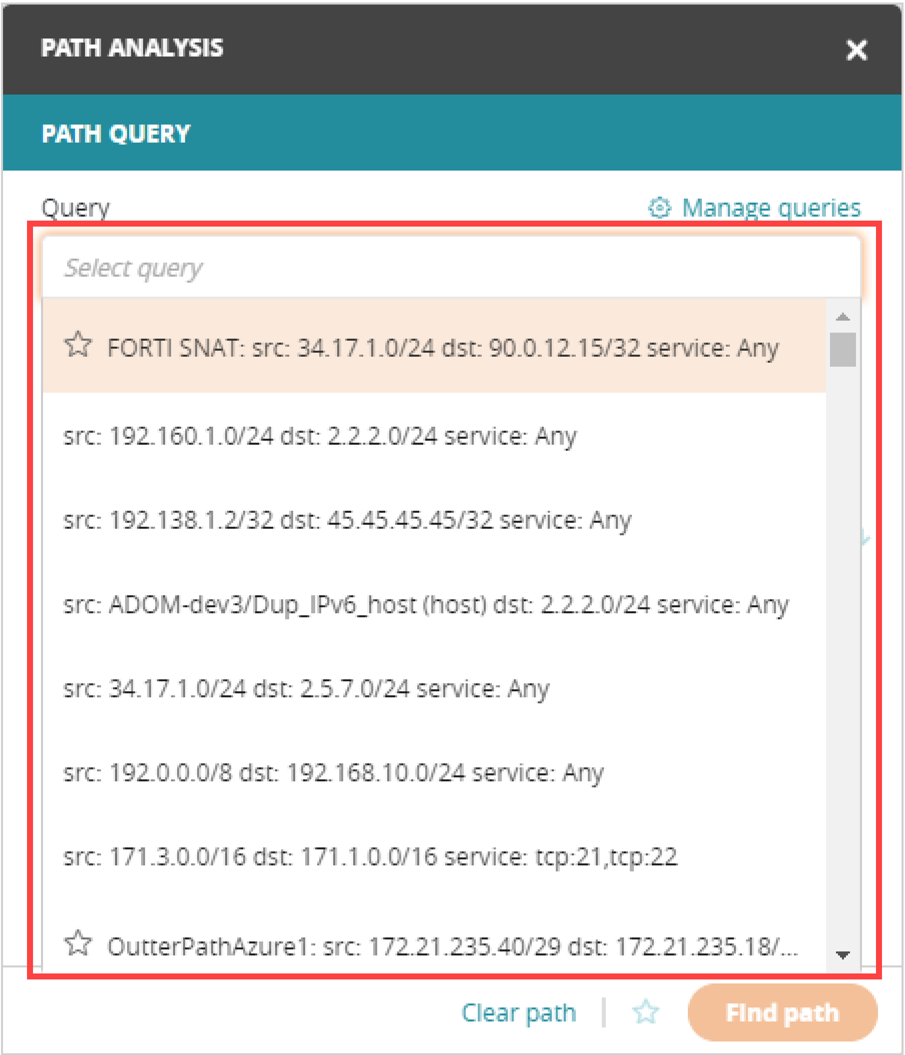
Domain: Default

How Do I Get Here?

1. Navigate to the Interactive Map: In SecureTrack, click **Network** > **Interactive Map**.
2. Click ⚯.

Saving and Managing Interactive Map Search Path Queries

You can use the **Path Query** panel to view recent queries, save a query, and manage your saved queries. Click in the **Select query** search box to display the 50 most recent queries:



☆ FORTI SNAT: src: 34.17.1.0/24 dst: 90.0.12.15/32 service: Any

src: 192.160.1.0/24 dst: 2.2.2.0/24 service: Any

src: 192.138.1.2/32 dst: 45.45.45.45/32 service: Any

src: ADOM-dev3/Dup_IPv6_host (host) dst: 2.2.2.0/24 service: Any

src: 34.17.1.0/24 dst: 2.5.7.0/24 service: Any

src: 192.0.0.0/8 dst: 192.168.10.0/24 service: Any

src: 171.3.0.0/16 dst: 171.1.0.0/16 service: tcp:21,tcp:22

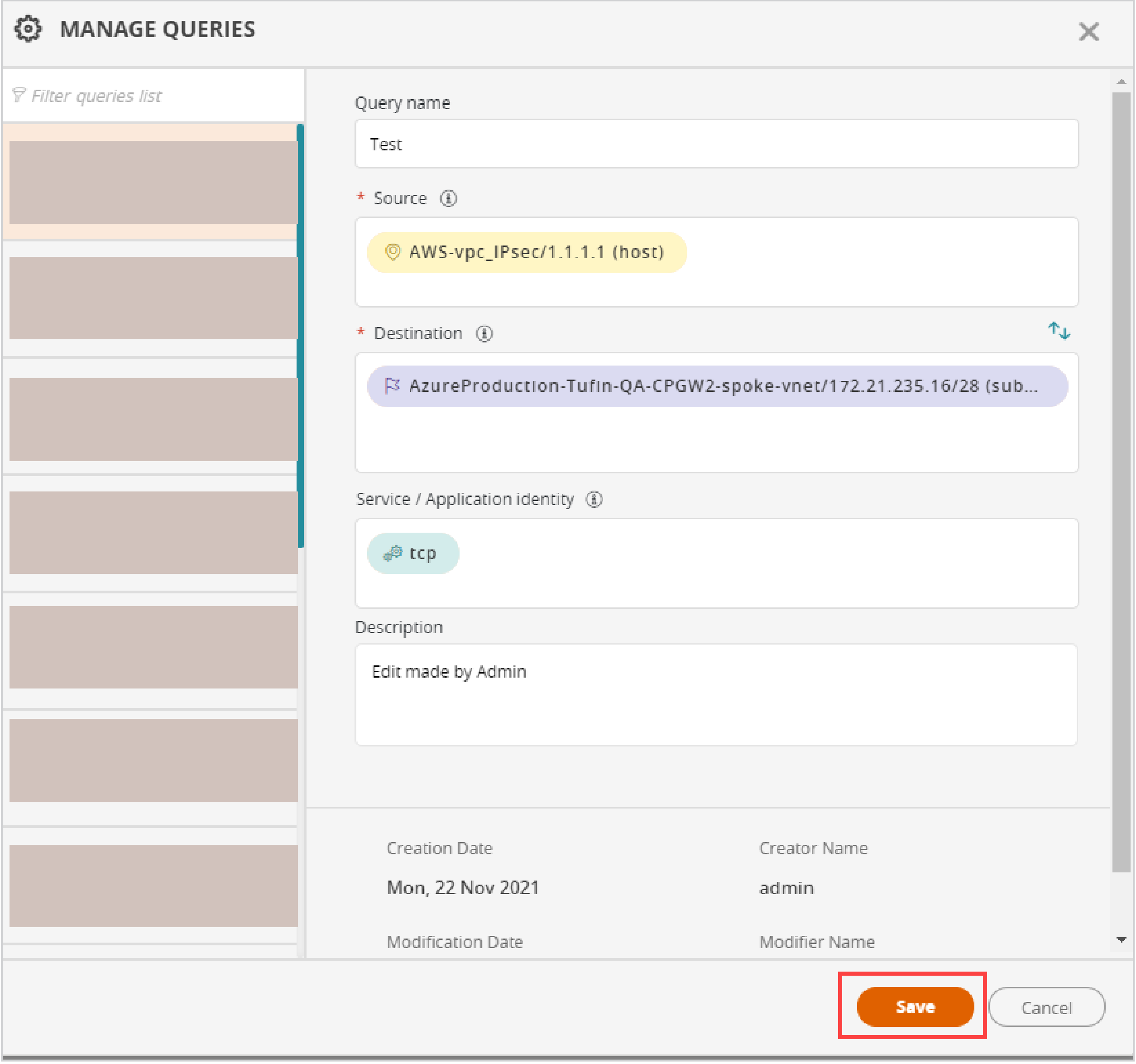
☆ OutterPathAzure1: src: 172.21.235.40/29 dst: 172.21.235.18/...

Save a Query

1. Click **Path Analysis > Manage queries**.
2. Enter a **Query Name** (required), **Description** (optional), and the traffic details of devices and cloud platforms for the paths you want to investigate, including the **Source**, **Destination**, and the predefined services or predefined application identities.

   The query fields are validated:

   - **Query name:** Unsupported characters and duplicate query names
   - **Source and Destination:** Firewall object (host, subnet, IP range, LDAP user, or group) or IP addresses
   - **Service/Application Identity:** List of predefined services and application identities



Query name: Test

* Source: AWS-vpc_IPsec/1.1.1.1 (host)

* Destination: AzureProduction-Tufin-QA-CPGW2-spoke-vnet/172.21.235.16/28 (sub...

Service / Application identity: tcp

Description: Edit made by Admin

Creation Date: Mon, 22 Nov 2021

Creator Name: admin

Modification Date

Modifier Name

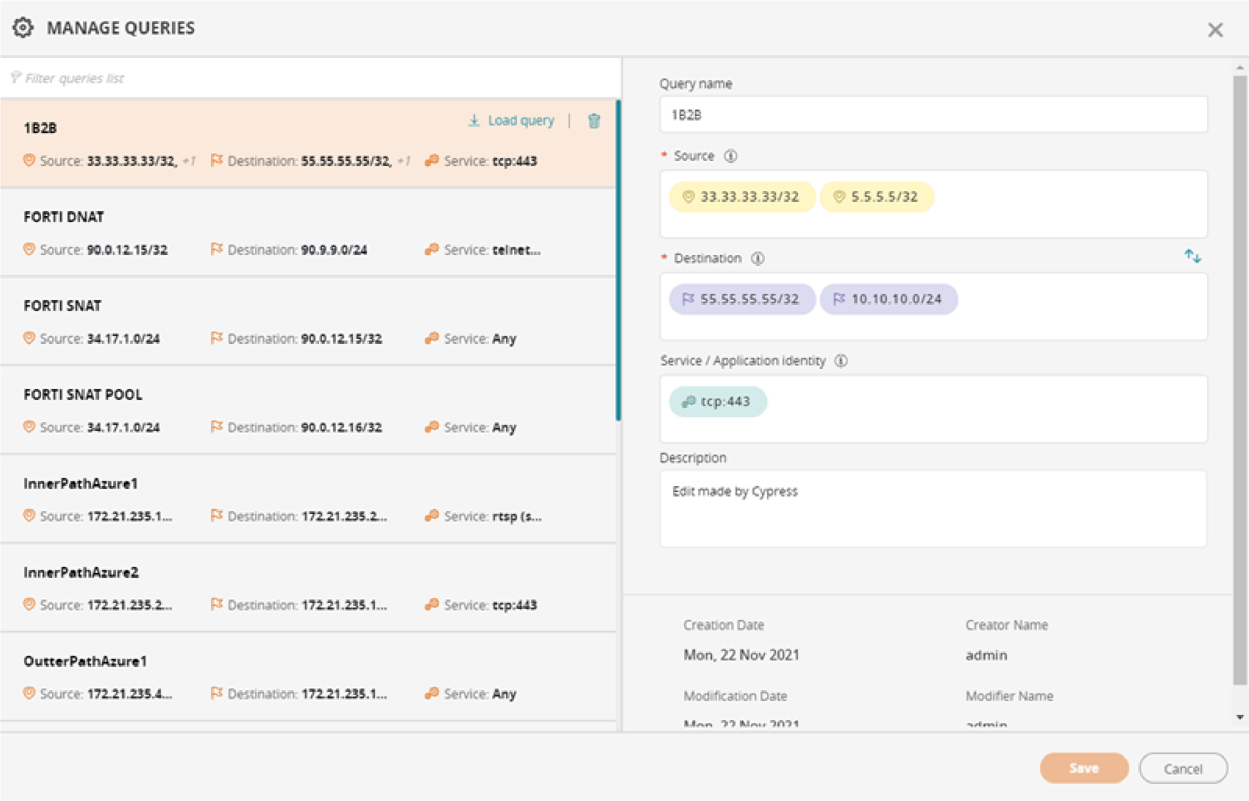
[redacted]

3. Click **Save**.

   The saved query appears in the **Query** list.

Manage Queries

Click **Path Analysis > Manage queries** to view the traffic details of a specific query, and to edit and delete saved queries:



MANAGE QUERIES

Filter queries list

1B2B
Load query
Source: 33.33.33.33/32, +1 Destination: 55.55.55.55/32, +1 Service: tcp:443

FORTI DNAT
Source: 90.0.12.15/32 Destination: 90.9.9.0/24 Service: telnet...

FORTI SNAT
Source: 34.17.1.0/24 Destination: 90.0.12.15/32 Service: Any

FORTI SNAT POOL
Source: 34.17.1.0/24 Destination: 90.0.12.16/32 Service: Any

InnerPathAzure1
Source: 172.21.235.1... Destination: 172.21.235.2... Service: rtsp (s...

InnerPathAzure2
Source: 172.21.235.2... Destination: 172.21.235.1... Service: tcp:443

OutterPathAzure1
Source: 172.21.235.4... Destination: 172.21.235.1... Service: Any

Query name: 1B2B

* Source: 33.33.33.33/32 5.5.5.5/32

* Destination: 55.55.55.55/32 10.10.10.0/24

Service / Application identity: tcp:443

Description: Edit made by Cypress

Creation Date: Mon, 22 Nov 2021
Creator Name: admin
Modification Date: Mon, 22 Nov 2021
Modifier Name: admin

View or Edit a Saved Query

1. Enter text in **Filter queries list** or select the query from the list.

   The traffic details appear.

2. Edit the query fields.
3. Click **Save**.

Delete a Saved Query

1. Enter text in **Filter queries list** or select the query from the list.
2. Click 🗑 and confirm the **Delete Query** action.

View Results of a Query

1. Type in the **Select query** search field and select the query you want to run.
2. Click **Find Path** to display the query results.

How Do I Get Here?

1. Navigate to the Interactive Map: In SecureTrack, click **Network** > **Interactive Map**.
2. Click ⊶.

Diagnosing Broken Traffic Paths

When you click the ⊶ button you can see the **Path Analysis** panel in which you enter traffic details and see the path of the specified traffic.

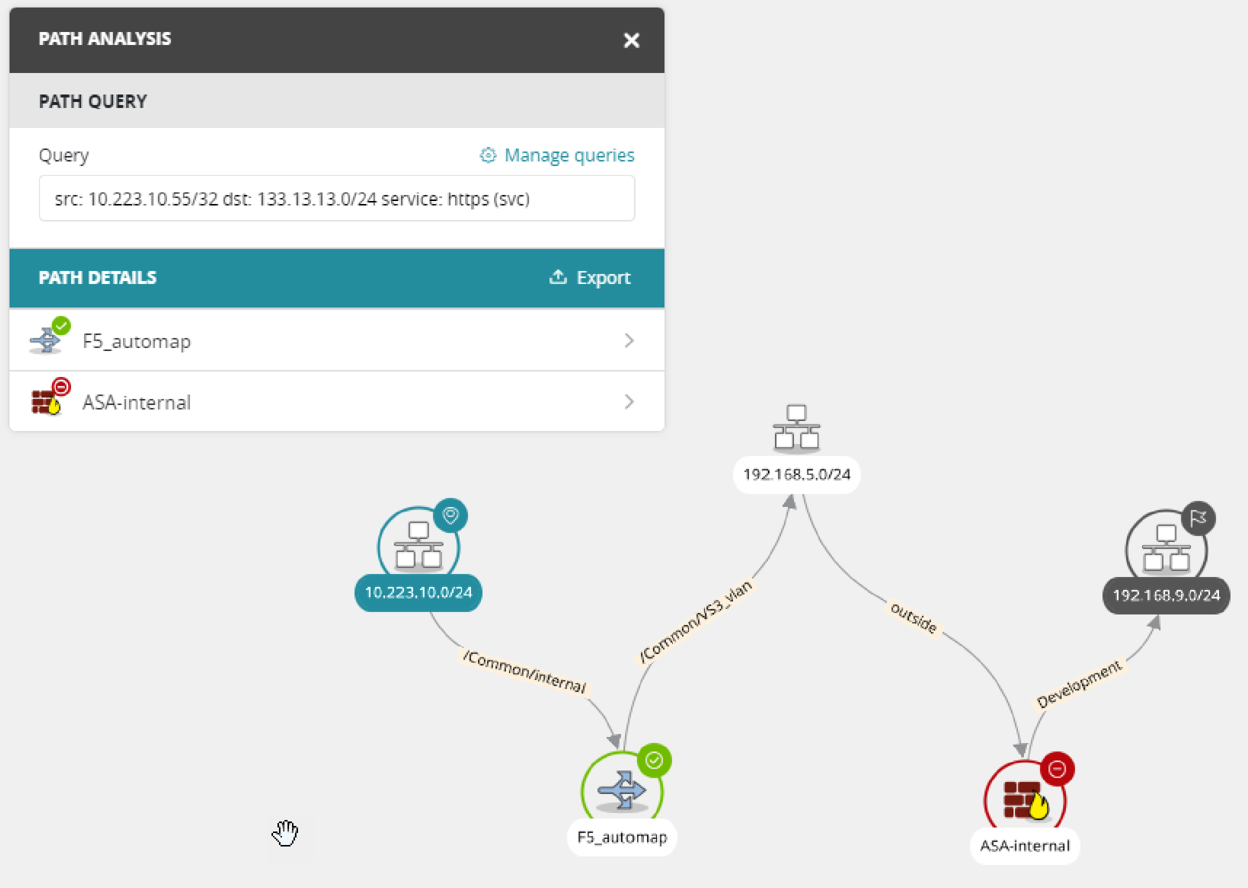
Path results typically include the following:

Icon	Meaning	Description
◎	Start point	First element that SecureTrack can identify in each path. If the start point is not in an identified network, SecureTrack shows the start point in a cloud.

Icon	Meaning	Description
✓	Routes traffic	Device that allows traffic.
⊖	Drops traffic	Device includes a rule that blocks traffic.
▦	Incomplete path	Source traffic goes to this point, but does not reach the destination.
⚑	End point	Last element that SecureTrack can identify in each path. If the next device in the path is an unmonitored device, SecureTrack shows the end point in a cloud.

You can right-click on any device to see routing and interface information, or select the device in the **Path Details** to see other technical information.

Traffic path with monitored device that routes traffic



PATH ANALYSIS

PATH QUERY

Query

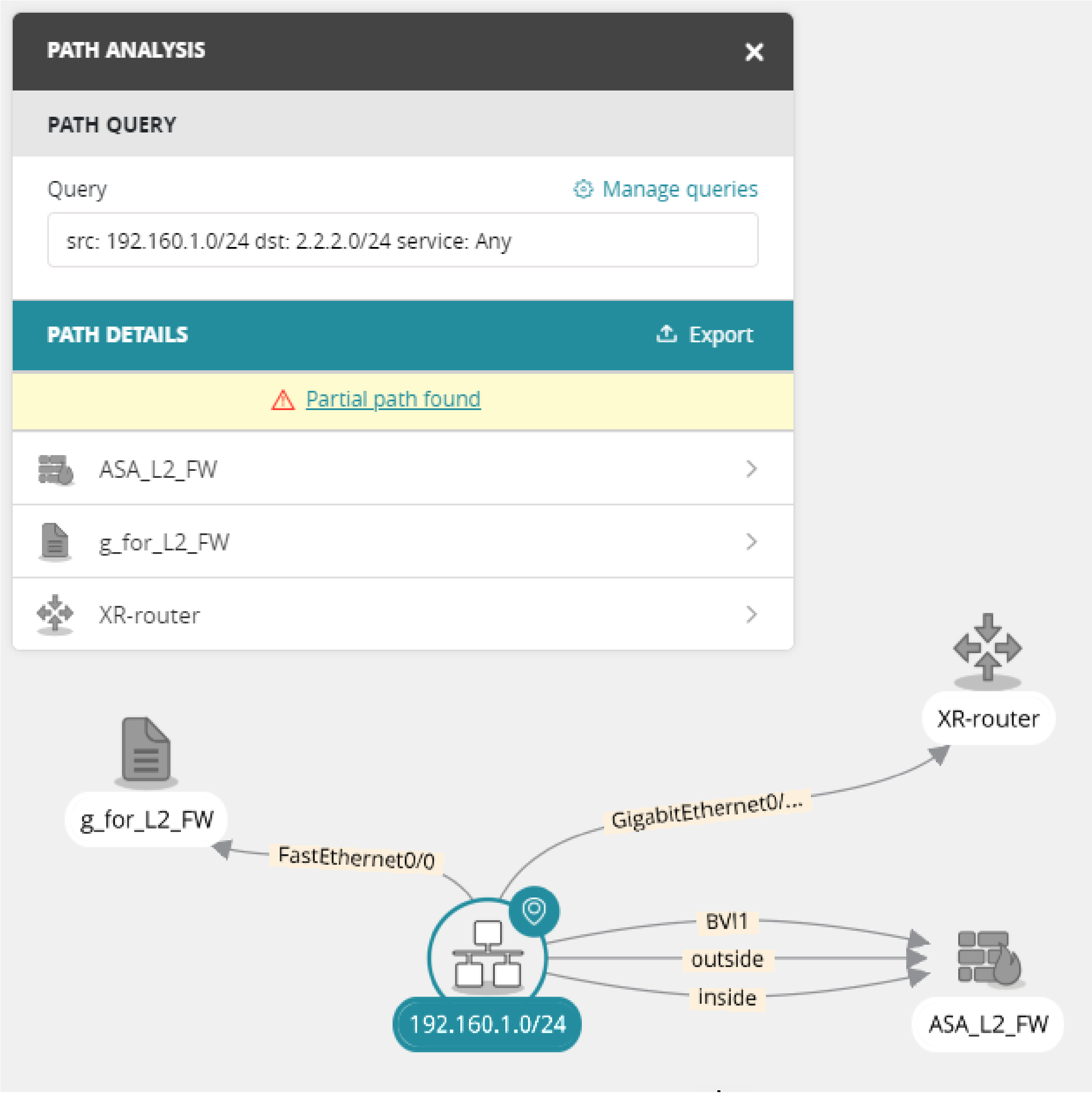
src: 10.223.10.55/32 dst: 133.13.13.0/24 service: https (svc)

PATH DETAILS

F5_automap

ASA-internal

Traffic path with monitored device that does not route traffic



PATH ANALYSIS

PATH QUERY

Query

Manage queries

src: 192.160.1.0/24 dst: 2.2.2.0/24 service: Any

PATH DETAILS

Export

Partial path found

- ASA_L2_FW
- g_for_L2_FW
- XR-router

Joining or Splitting Subnets

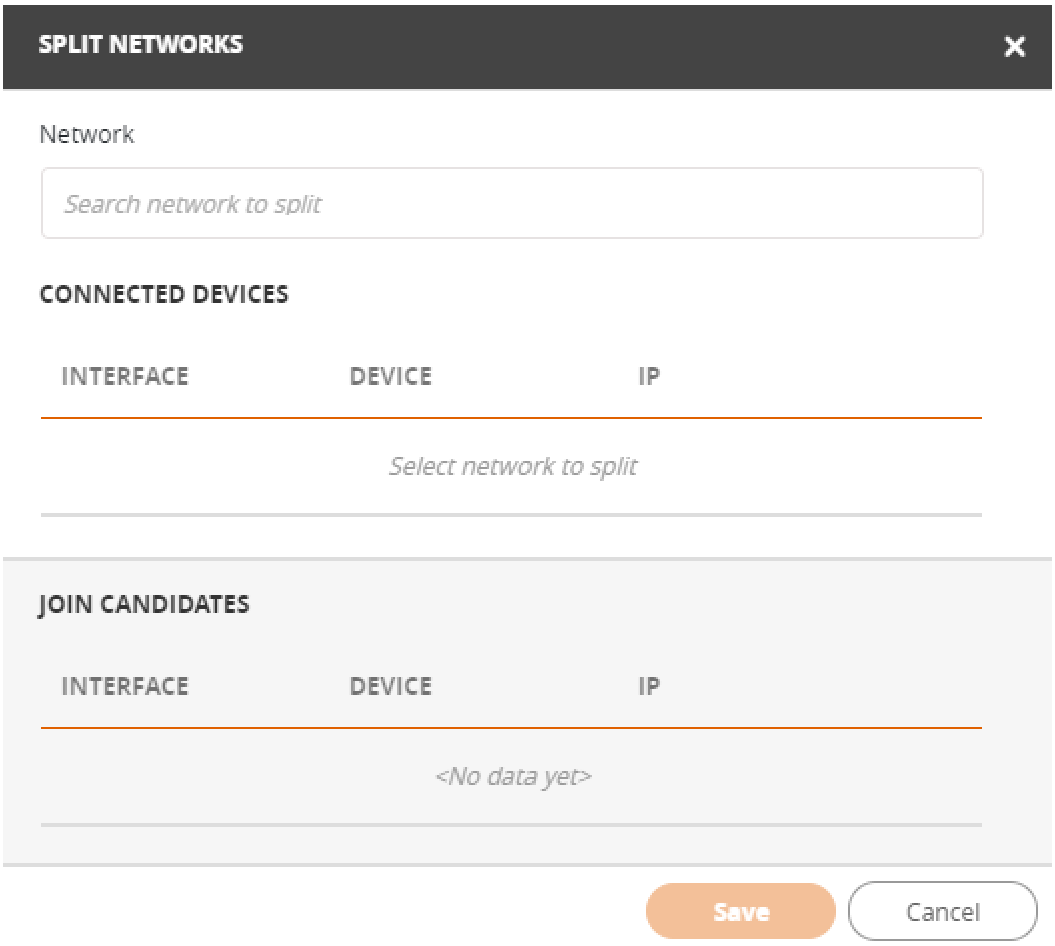
When you click on a subnet in the map, you see the details of the subnet. The details include the name and IP address of the network. You can also join or split networks from the Interactive map.

If a network has been joined, the menus will display Split Networks. If the network has not been joined, the menu will say Join Networks. Both options direct you to the same dialog.

Join or Split Networks

1. Click ⚇.

   The **Split Networks** window appears.



SPLIT NETWORKS

Network

Search network to split

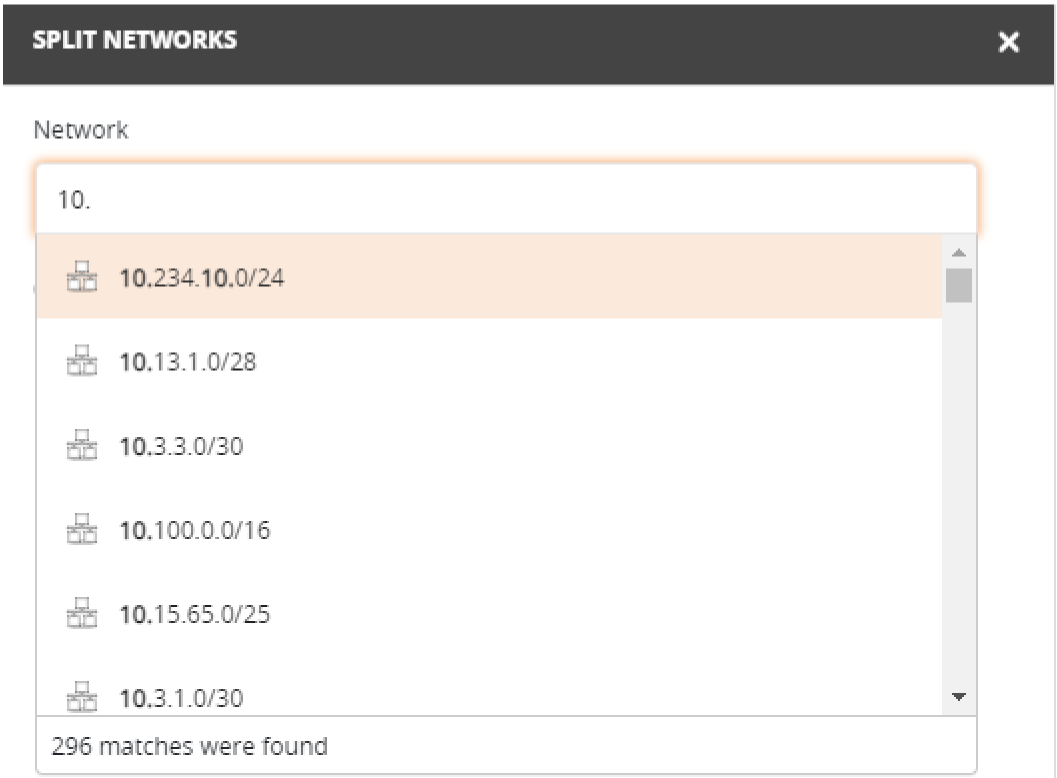
CONNECTED DEVICES

INTERFACE	DEVICE	IP
Select network to split		

JOIN CANDIDATES

INTERFACE	DEVICE	IP
<No data yet>		

2. Enter the desired network name. Matching networks appear as you type. You may enter multiple names.



SPLIT NETWORKS

Network

10.

- 10.234.10.0/24
- 10.13.1.0/28
- 10.3.3.0/30
- 10.100.0.0/16
- 10.15.65.0/25
- 10.3.1.0/30

296 matches were found

3. Click ⊕ to add a network from the join candidates list.

   Click ⊖ to remove a network from the connected devices list.
4. Click **Save**.

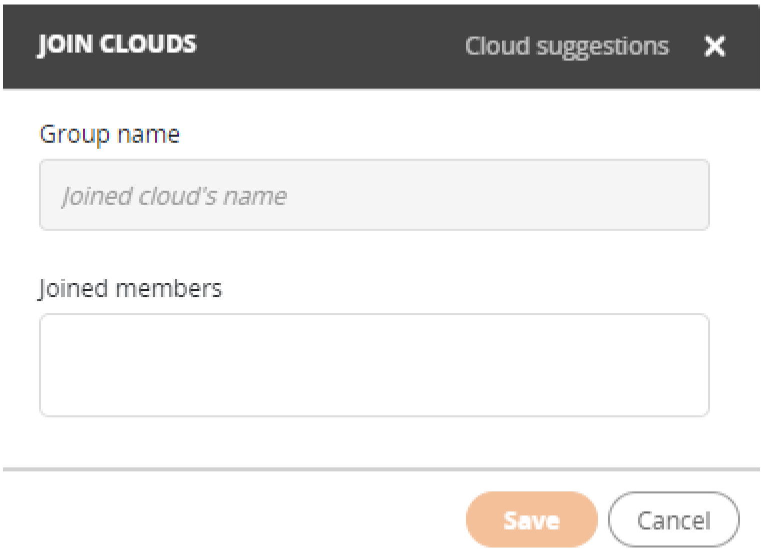
Joining or Splitting Clouds

When you click on a cloud in the map, you see the details of the cloud. The details include the name, status, and IP address of the instance.

You can join clouds together to connect devices through the clouds. For example, if you have two devices that are each connected to a cloud and you know that the clouds connect to each other, you can join the two clouds together. This lets you create a path between two subnets when there are devices in between them that are not monitored by SecureTrack.

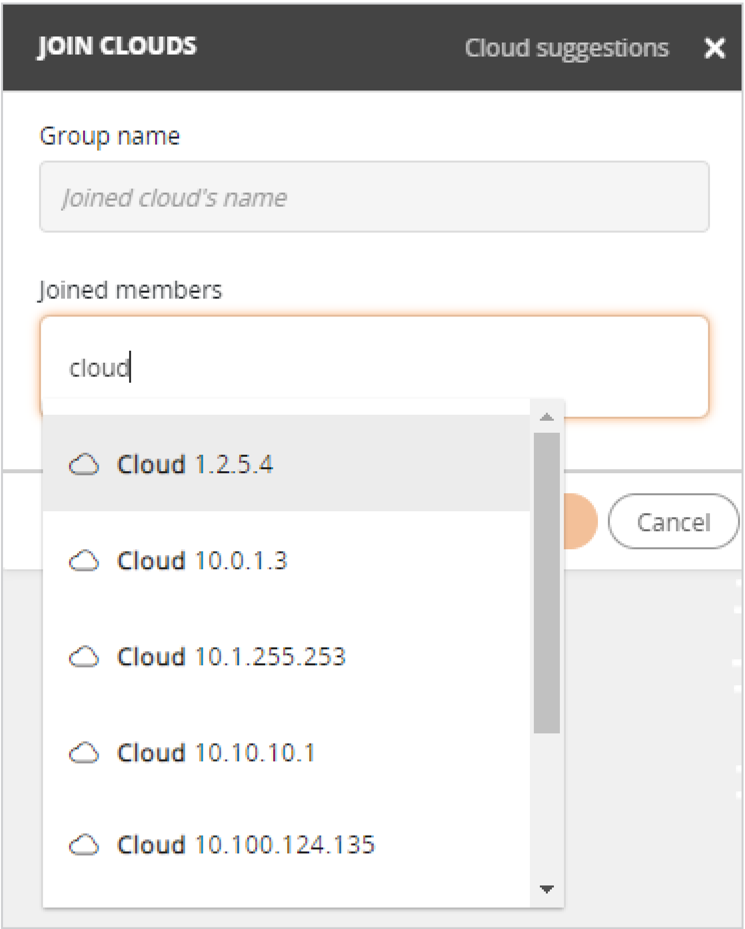
Join clouds

1. In the Interactive Map, click ☁. The **Join Clouds** window appears.



2. Type the desired cloud name and select it.

   Matching clouds appear as you type; select as many clouds as needed.

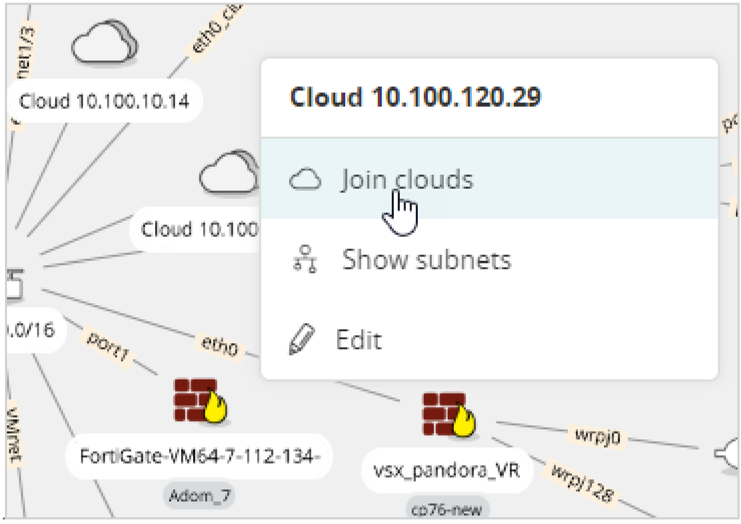


3. If required, in the **Group Name** field, rename the group.
4. Click **Save**.

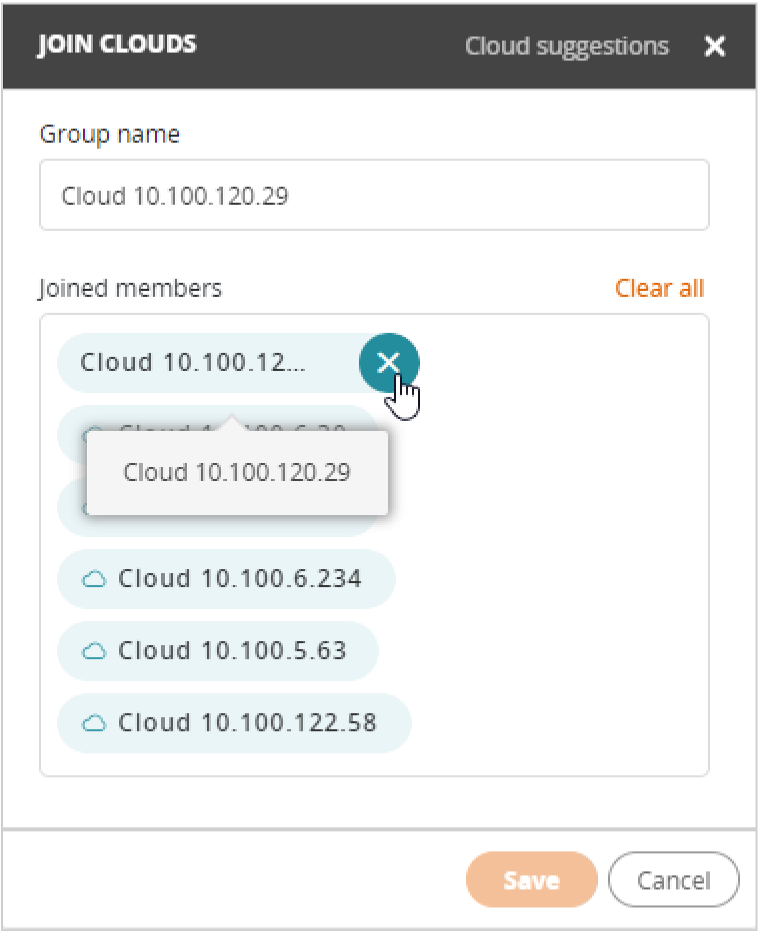
To clear your entries and start over, click **Clear all**.

Split Clouds

1. Right-click a joined cloud and select **Join Clouds**.



2. In the Join Clouds window, hover over a cloud and click ✕ to remove it from the group



Group name

Cloud 10.100.120.29

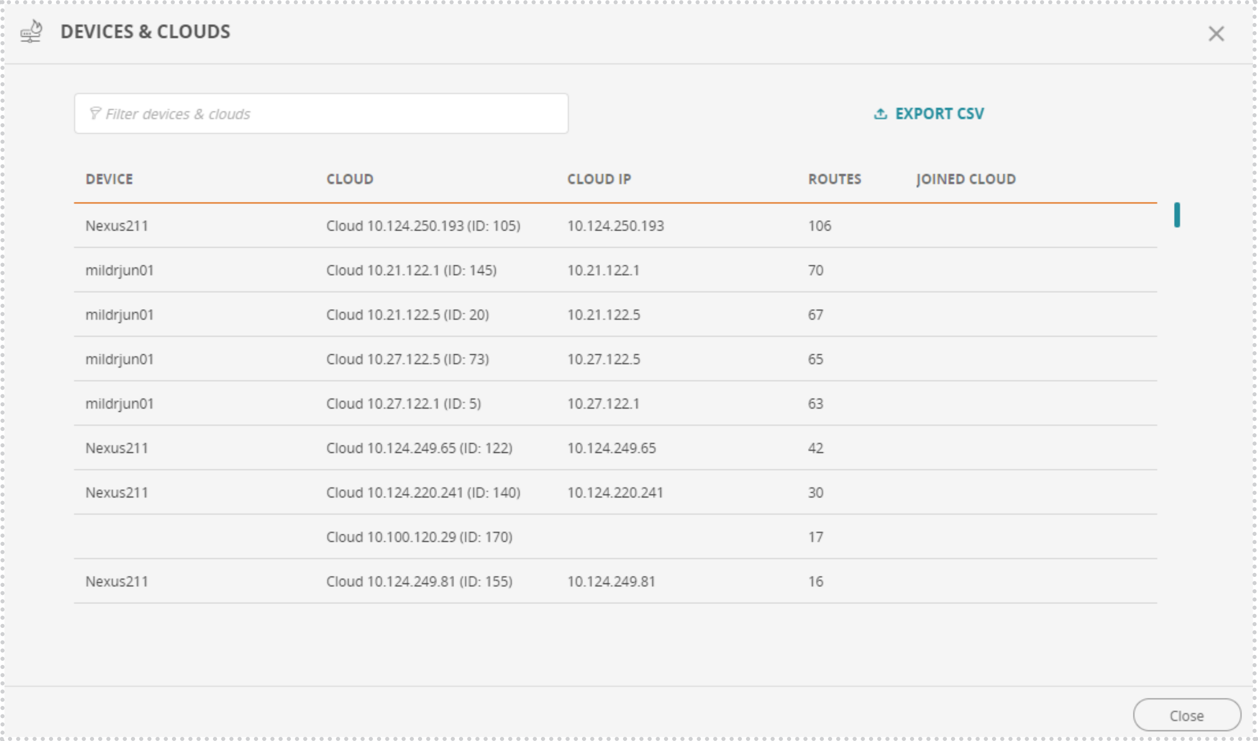
Joined members

- Cloud 10.100.12...
- Cloud 10.100.120.29
- Cloud 10.100.6.234
- Cloud 10.100.5.63
- Cloud 10.100.122.58

3. Click **Save**.

View and Use Cloud Suggestions

The **Cloud Suggestions** link opens all the routes that point to the cloud you select.



DEVICE	CLOUD	CLOUD IP	ROUTES	JOINED CLOUD
Nexus211	Cloud 10.124.250.193 (ID: 105)	10.124.250.193	106	
mildrjun01	Cloud 10.21.122.1 (ID: 145)	10.21.122.1	70	
mildrjun01	Cloud 10.21.122.5 (ID: 20)	10.21.122.5	67	
mildrjun01	Cloud 10.27.122.5 (ID: 73)	10.27.122.5	65	
mildrjun01	Cloud 10.27.122.1 (ID: 5)	10.27.122.1	63	
Nexus211	Cloud 10.124.249.65 (ID: 122)	10.124.249.65	42	
Nexus211	Cloud 10.124.220.241 (ID: 140)	10.124.220.241	30	
	Cloud 10.100.120.29 (ID: 170)		17	
Nexus211	Cloud 10.124.249.81 (ID: 155)	10.124.249.81	16	

You can use the text filter to search for a string and click on a column header to sort the list.

Click **Export CSV** to save the list of cloud suggestions as a `.csv` file.

Refreshing the Map

Click ⟳ Synchronize to display the **Sync Topology Map** panel. The **Sync Topology Map** panel presents the topology sync history and options to start the topology sync process.

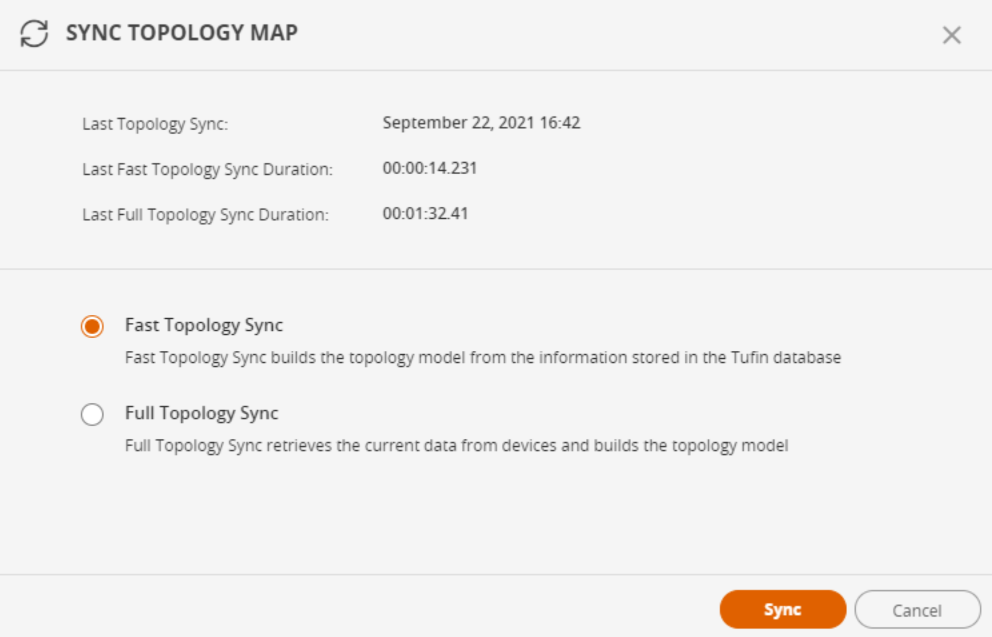
The **Sync Topology Map** panel presents the following information:

- **Last Topology Sync:** Date and time the last sync was performed

  The text is emphasized if more than 25 hours has elapsed since the last sync
- **Last Fast Topology Sync Duration:** The duration of the last fast sync process
- **Last Full Topology Sync Duration:** The duration of the last full sync process

Synchronize Topology

1. To synchronize the Interactive Map, select a Topology Sync option:
   - **Fast Topology Sync:** Fast Topology Sync builds the topology model from the information stored in the Tufin database.
   - **Full Topology Sync:** Full Topology Sync retrieves the current data from devices and builds the topology model.
2. Click **Sync** to update the topology or **Cancel** to return to the Map.



SYNC TOPOLOGY MAP

Last Topology Sync: September 22, 2021 16:42

Last Fast Topology Sync Duration: 00:00:14.231

Last Full Topology Sync Duration: 00:01:32.41

● Fast Topology Sync

Fast Topology Sync builds the topology model from the information stored in the Tufin database

○ Full Topology Sync

Full Topology Sync retrieves the current data from devices and builds the topology model

Adding and Updating a Generic Device

Overview

In the Interactive Map, you can add the interface and routing information for a router that is not monitored by SecureTrack, also called a generic device. When you add a generic device, the topology calculations include the interfaces and routing for the device. The generic device is shown in the Interactive Map and you can click on it to see the interface and routing information for the device.

- Before you add a Cisco generic device, you must run `show ip route` and `show ip interface` from the device's CLI and save the output of both commands to a text file, as shown in the sample file. Also include the `show standby` command in order to include the HSRP information.
- Before you add a non-Cisco generic device, you must prepare a text file with the interface and routing information and save the output in the format shown in the sample file.

When you add the generic device, you upload the prepared file to SecureTrack. Because the generic device is not monitored, if the information changes you must prepare the file again and re-upload it.

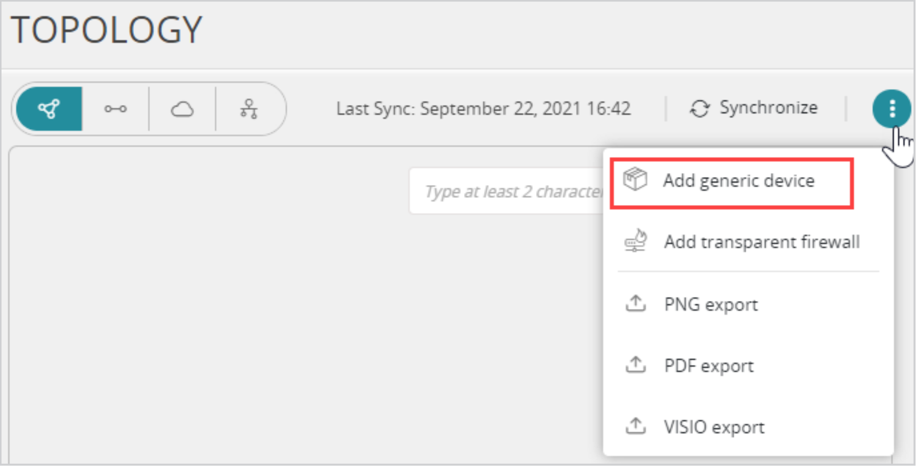
If you have a multi-domain mode enabled:

- **Segregated domains**: each domain has its own Topology Map, and the device should be added to the relevant domain.
- **Interconnected domains**: The device should be added to the Global Topology Map, and then can be added to other domains.

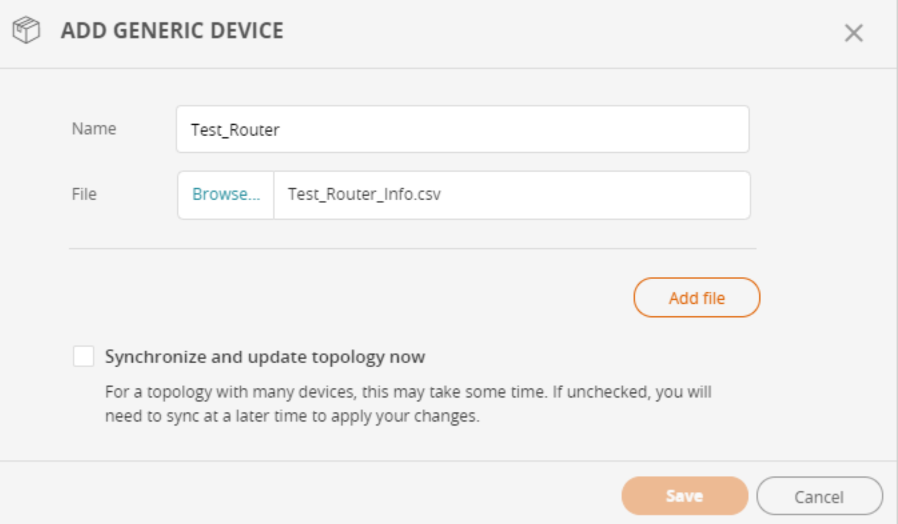
What Can I Do Here?

Add a Generic Device

1. In the Interactive Map, click ⋮ > **Add generic device**.



2. Enter the name of the device.
3. Click **Browse** to select the interface and routing file for the device
4. Click **Add file**.


ADD GENERIC DEVICE

Name: Test_Router

File: Browse... Test_Router_Info.csv

□ Synchronize and update topology now

For a topology with many devices, this may take some time. If unchecked, you will need to sync at a later time to apply your changes.

You can repeat these steps to add multiple devices at one time.

5. (Optional) Select **Synchronize and update topology now** to update the map with the new generic devices.
6. Click **Save**.

   The Interactive Map is recalculated and includes the generic devices.

Update the Name or Interface and Routing File for a Generic Device

1. Click the device in the Interactive Map.
2. Update the device information:
   - Edit the name of the device.
   - Click **Browse** and select the interface and routing file for the device.

3. Click **Save**.

   The new information appears in the Interactive Map.

Delete a Generic Device

1. Click the device in the Interactive Map.
2. Click **Delete**.

   The generic device does not appear in the updated Interactive Map.

How Do I Get Here?

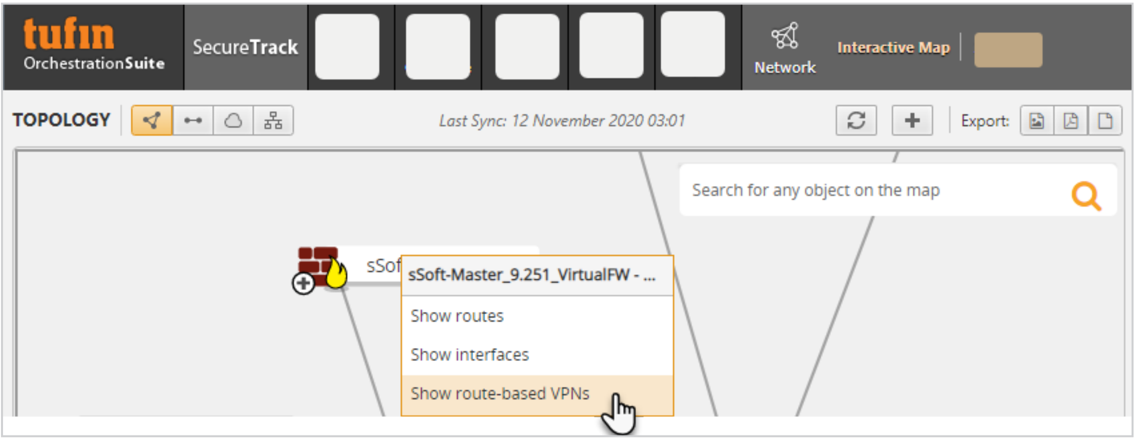
Go to **Network** > **Interactive Map**

Adding Generic Route-Based VPN Connections

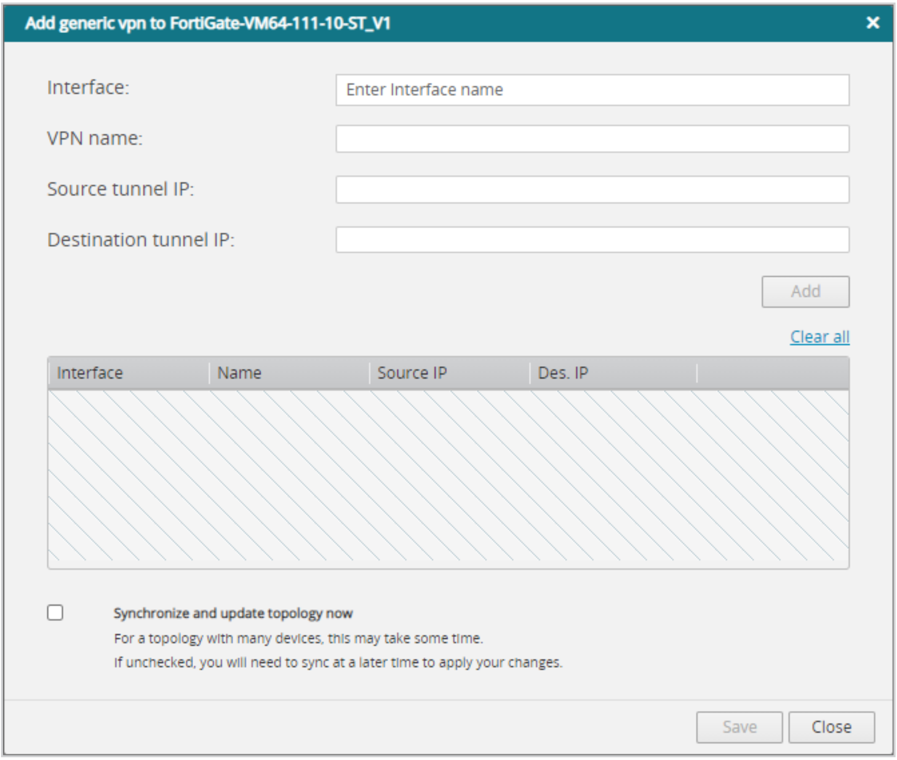
Tufin Orchestration Suite lets you extend the SecureTrack topology model by adding or removing generic route based VPN connections.

Add Generic Route-Based VPN Connections

1. In the Interactive Map, right-click a non-generic device and select **Show route-based VPNs**.



2. Click ➕ to open the Add Generic VPN window.



Add generic vpn to FortiGate-VM64-111-10-ST_V1

Interface: Enter Interface name

VPN name:

Source tunnel IP:

Destination tunnel IP:

□ Synchronize and update topology now

For a topology with many devices, this may take some time.

If unchecked, you will need to sync at a later time to apply your changes.

3. Enter the following information:
   - **Interface name**: Name of the interface on the device
   - **VPN name**: Name of the VPN connection
   - **Source tunnel IP**: Source IP address for the IPsec packet header. The source tunnel IP does not have be the same as the IP address of Interface name.
   - **Destination tunnel IP**: Destination IP address for the IP.
4. Click **Add** and if required enter additional interfaces.
5. Once all the interfaces have been entered, click **Save** to add the VPN to the device.

Use APIs to Add, Delete, and Change Generic Route-Based VPN Connections

See:

- Add generic route-based VPN
- Update generic route-based VPN
- Delete a generic route-based VPN
- Delete generic route-based VPNs

Adding or Removing Generic NAT Information

Overview

Tufin Orchestration Suite (TOS) can retrieve network topology and firewall policy information from devices that are monitored by TOS Classic. NAT rules present a special challenge to this process because a firewall policy must be defined to allow or deny access to traffic based on the correct side of the NAT rule. A firewall rule that uses the incorrect address will not impact the traffic flow as intended.

TOS Classic automatically processes NAT rules for many devices, and it uses that information to correctly analyze the impact of the firewall rules on traffic that is changed using NAT. The information is used in policy analysis and path calculations in TOS Classic and SecureChange, and in connection status and connection analysis on SecureApp.

For devices for which native NAT is not supported, you can compile a file that includes the NAT rules for other vendors, and enter that information directly into TOS Classic using a simple CLI command. This applies to devices monitored by TOS Classic or policies added to TOS Classic as offline devices.

- Generic NAT cannot be used for devices for which native NAT is supported.
- Devices with revisions that do not originate in TOS Classic cannot include Generic NAT.

For a list of devices which support the ability to calculate the impact of NAT rules, see SecureTrack Features by Vendor.

After you add the NAT rules from your device to TOS Classic, you see the impact of the NAT rules in these TOS Classic features:

- TOS Classic - Policy Analysis
- All Tufin features that use path calculation:
    - Automatic Target Suggestion
    - Designer
    - Verifier
    - Connection Status and Connection Analysis
    - Path Finder in the interactive map
    - Path calculation using API

Generic NAT information is not shown in other areas of TOS Classic, including policy comparison and Policy Browser.

About the Generic NAT File

The generic NAT file must contain a CSV file of NAT rules. When you import the CSV file, you specify the device in TOS Classic to which the NAT rules are associated.

This list identifies the fields, in order, in a NAT rule:

- Interface before NAT
- Interface after NAT
- Source before NAT
- Source after NAT
- Destination before NAT
- Destination after NAT
- Service before NAT
- Service after NAT
- Type of NAT (Dynamic or Static)

Examples of NAT Rules

```
any,any,150.10.80.1,60.60.60.1,any,any,any,http,static
```

```
any,any,{150.10.90.0/24;150.10.91.0/24;150.10.92.0/24},60.60.70.1-60.60.70.10,any,any,any,any,dynamic
```

```
any,any,150.10.90.0/24,60.60.70.1-60.60.70.10,any,any,80(tcp),8080(tcp),dynamic
```

Formats for IP Addresses

IP Address Format	Description
`x.x.x.x`	An IP address, assumed to be a single host
`x.x.x.x/y`	An IP subnet with CIDR subnet mask
`x.x.x.x-y.y.y.y`	A range of IP addresses delimited with a dash (-)
`{x.x.x.x;y.y.y.y}`	A combination of IP addresses or subnets in curly brackets ({ }) and delimited with a semi-colon (;)

Formats for Services

Service Format	Description
`x(protocol)`	A port

Service Format	Description
`y-z(protocol)`	A range of ports delimited with a dash (-)
`{x(protocol);y-z(protocol)}`	A combination of ports or port ranges in curly brackets ({ }) and delimited with a semi-colon (;)

Notes:

- Any line that begins with a double-slash (//) or does not contain 8 commas is ignored. You can use "any" as an entry (not case-sensitive) for any field except for the type of NAT.
- Source, destination or service can be either the name of a network object or service already defined in the device, or an IP address or service explicitly defined according to the formats below.
- Any entry that is not recognized as a network object already defined in the device or and explicitly defined IP address or service in a valid format causes the import process to fail.
- Any IP address, subnet, range or service in a NAT rule that does not match an existing object in the device is added to the device with a name that includes the definition of the object. For example: `Host_x.x.x.x`
- For JunOS devices, when you include an object name that does not exist in the device, you must specify to which zone to add the object. The expected format is `object name(zone name)`. For example: `25.1.1.12(External)` or `H_2.2.2.2(Internal)`

Add Generic NAT Information

For devices connected to a remote collector (RC), the generic NAT file needs to be on the RC server and not the central server, and that is where you need to run the commands.

1. To process the generic NAT file, you must copy the file to the TOS Classic server and run this command:

```
/usr/local/st/topology_generic_nat -m <device_id> -f <path>/<NAT_
filename.csv> -o <path>/<xml_filename>
```

where:

`-f` is the path to the generic NAT CSV file.

`-o` is the path to the an xml file, which includes all of the NAT rules from the generic NAT file in XML format (optional).

`-m` is the TOS Classic ID of the device to associate with the NAT rules. The ID must be a TOS Classic ID.

`-l` lists all of the devices that currently have generic NAT information.

Remove Generic NAT Information

To remove the generic NAT information from a device, run this command:

```
/usr/local/st/topology_generic_nat -m <device_id> -d
```

where:

`-m` is the TOS Classic ID of the device to associate with the NAT rules. The ID must be a TOS Classic ID.

`-d` is the option that deletes the NAT information

After you run this command, the NAT rules are associated with the specified device.

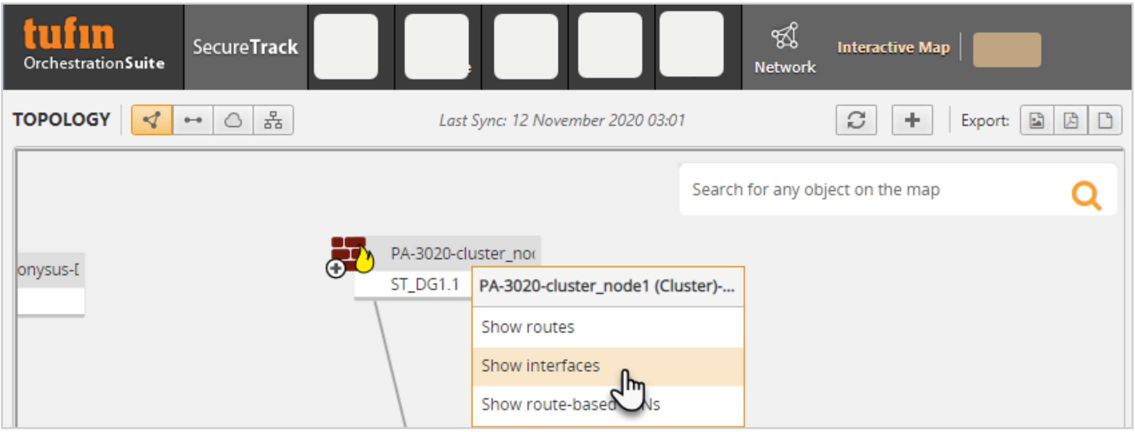
Note that when you run this command for devices that are monitored by an RC, the command will run on the RC as well.

Adding or Removing Generic Interfaces

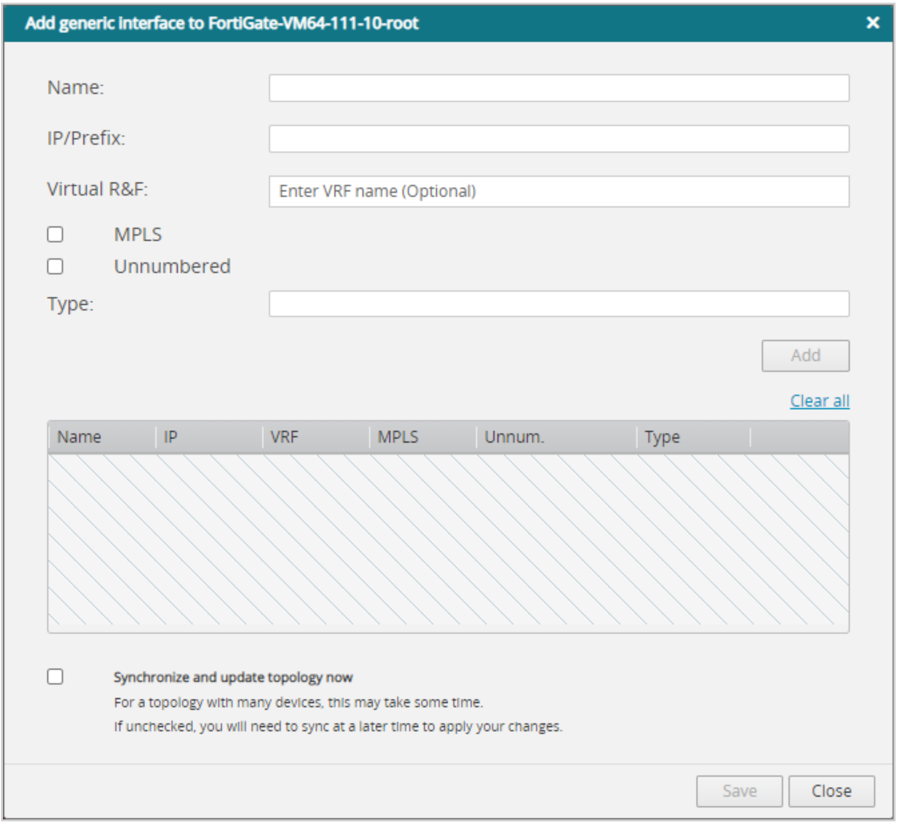
Tufin Orchestration Suite lets you extend the SecureTrack topology model by adding generic interfaces to a device. The generic interfaces you add will automatically appear in the interactive map when SecureTrack syncs the Interactive Map.

Add Generic Interfaces

1. In the Interactive Map, right-click a non-generic device and select **Show interfaces**.



2. Click ➕ to open the Add Generic Interface window.



Add generic interface to FortiGate-VM64-111-10-root

Name:

IP/Prefix:

Virtual R&F: Enter VRF name (Optional)

□ MPLS

□ Unnumbered

Type:

Name	IP	VRF	MPLS	Unnum.	Type

□ Synchronize and update topology now
For a topology with many devices, this may take some time.
If unchecked, you will need to sync at a later time to apply your changes.

3. Enter the following information:
   - **Name** – Display name for the interface
   - **IP/Prefix** – IP adress or prefix of the interface
   - **Virtual R&F** – (optional) The virtual router in which the interface resides; mandatory for AWS
   - **MPLS** – Select if the interface type uses Multi-protocol label switching (MPLS)
   - **Unnumbered** – Select if the interface is unnumbered
   - **Type** – The device type.
4. Click **Add** and if required enter additional interfaces.
5. Once all the interfaces have been entered, click **Save** to add the route to the device.

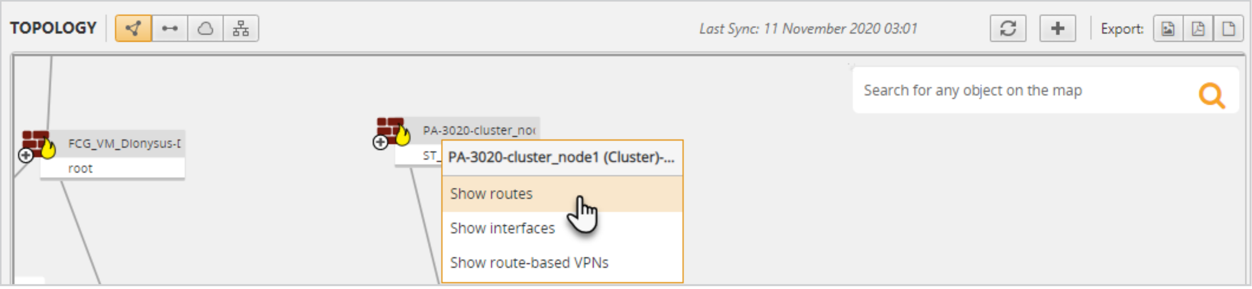
You can also add generic interfaces using API commands.

Adding or Removing Generic Routes

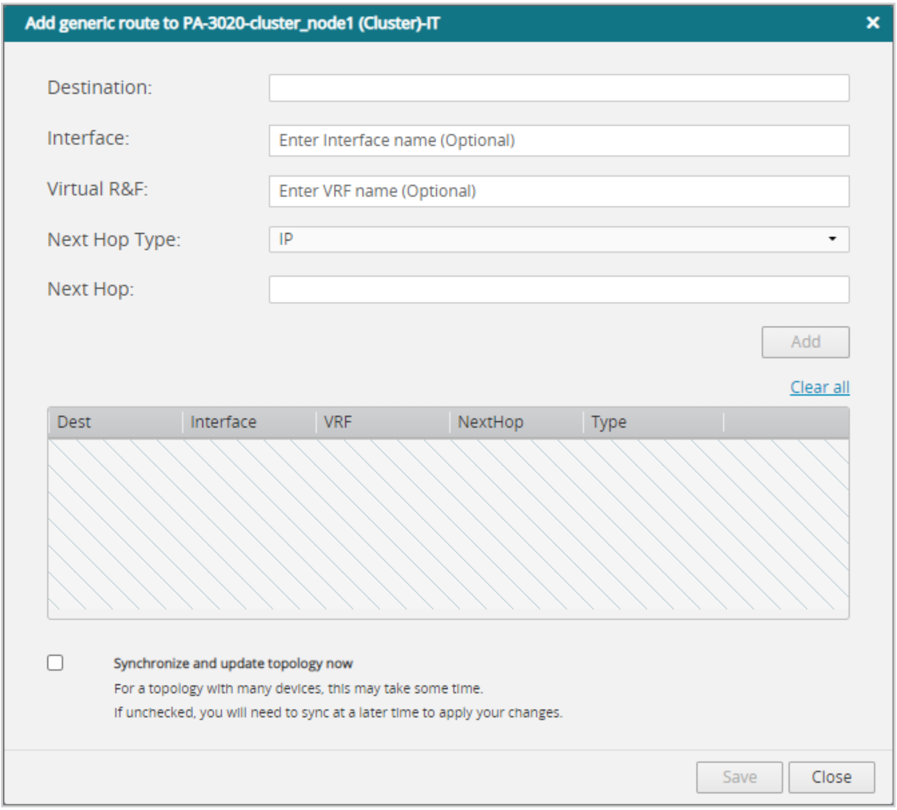
Tufin Orchestration Suite lets you extend the SecureTrack topology model by adding or removing generic routes. The generic routes you add or delete will automatically appear in the interactive map when SecureTrack syncs the topology map.

Add Generic Routes in the Interactive Map

1. In the Interactive Map, right-click a non-generic device and select **Show routes**.



2. Click + to open the Add Generic Route window.


Add generic route to PA-3020-cluster_node1 (Cluster)-IT

Destination:

Interface: Enter Interface name (Optional)

Virtual R&F: Enter VRF name (Optional)

Next Hop Type: IP

Next Hop:

Dest	Interface	VRF	NextHop	Type

☐ Synchronize and update topology now
For a topology with many devices, this may take some time.
If unchecked, you will need to sync at a later time to apply your changes.

3. Enter the following information:
   - **Destination**: Generic route destination IP address
   - **Interface**: (optional) Interface name on the source device
   - **Virtual R&F**: (optional) Name of the VRF on the source device in which the route will be placed. If left blank, the route will be placed in the global routing table.
   - **Next Hop Type:** Select the hop type (IP or VR)
   - **Next Hop**: Next hop for this route, either an IP address or virtual router name
4. Click **Add** and if required enter additional hops.
5. Once all the hops have been entered, click **Save** to add the route to the device.

Use APIs to Add, Delete, and Change Generic Routes

See:

- Add generic route
- Update generic routes
- Delete a generic route
- Delete generic routes

See also:

- All topology APIs
- Delete a generic interface
- Delete generic interfaces

To delete all generic routes using tos CLI:

```
/usr/local/st/topology_generic_routes -d -m <mgmtId>
```

To delete all generic interfaces using tos CLI:

```
/usr/local/st/topology_generic_interfaces -d -m <mgmtId>
```

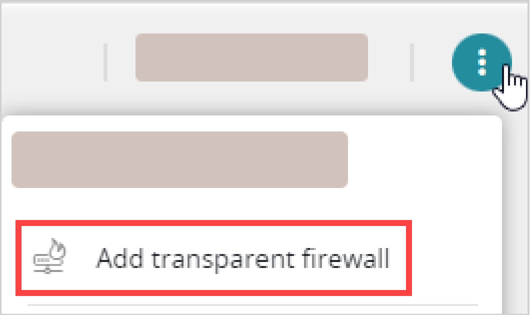
Adding Transparent Devices

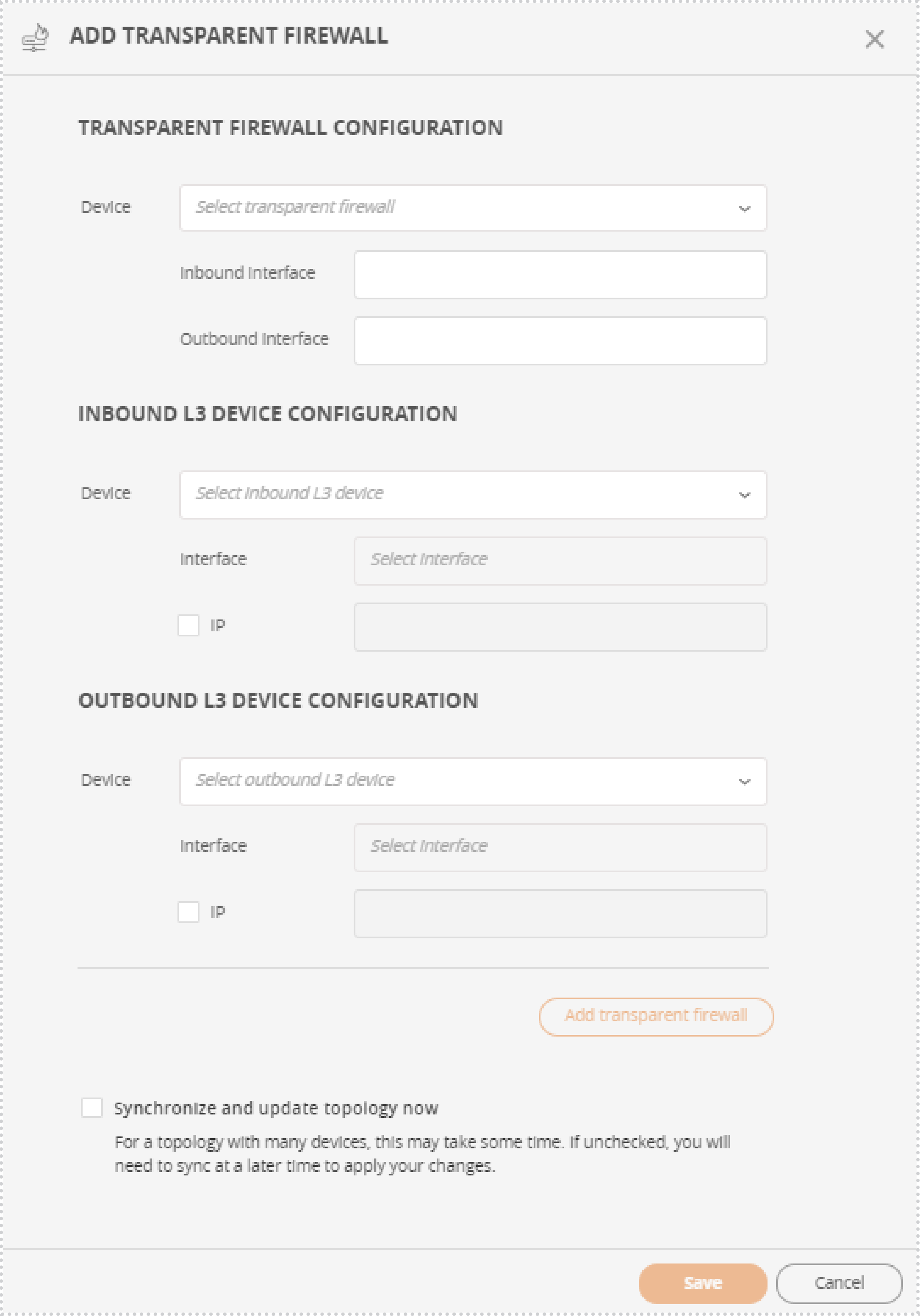
Because firewalls that are configured in transparent mode do not have routing information, these firewall connections are not shown in the Interactive Map by default. After you enter the interface information for the firewall and the two devices that the firewall is connected to, the firewall is included in TOS features that are based on topology calculations.

Firewalls can be entered directly in the Interactive Map, or using the browser-based tool,

Add a Transparent Device in the Interactive Map

1. From the Actions menu, select **Add transparent firewall**.





ADD TRANSPARENT FIREWALL

TRANSPARENT FIREWALL CONFIGURATION

Device: Select transparent firewall

Inbound Interface

Outbound Interface

INBOUND L3 DEVICE CONFIGURATION

Device: Select inbound L3 device

Interface: Select interface

□ IP

OUTBOUND L3 DEVICE CONFIGURATION

Device: Select outbound L3 device

Interface: Select interface

□ IP

□ Synchronize and update topology now

For a topology with many devices, this may take some time. If unchecked, you will need to sync at a later time to apply your changes.

2. Enter or select the following information:
   - **Transparent Firewall Configuration** - Select the name of the layer 2 device and enter the inbound and outbound interfaces.
   - **Inbound L3 Device Configuration** - Select the layer 3 inbound device name and interface. If required, enter an IP address.
   - **Outbound L3 Device Configuration** - Select the layer 3 outbound device name and interface. If required, enter an IP address.
3. Click **Add transparent firewall**.

   You can repeat these steps to add multiple devices at one time.

4. Click **Save**.

   SecureTrack recalculates the Interactive Map to include the transparent devices.

Select the **Sychronize and update topology now** checkbox so that SecureTrack recalculates the Interactive Map to include the transparent devices.

How Do I Get Here?

Go to **Network** > **Interactive Map**

Network Zones

- Overview
- What Can I Do Here?
- How Do I Get Here?

Overview

Network zones are groups of IPv4 or IPv6 network addresses, such as an organization's internal network or DMZ. Zones can include IPv4 or IPv6 subnets with explicit network addresses or security groups. Security groups can be added, changed and deleted through the REST API or by importing a zone list from a CSV file.

There are three predefined zones:

- Internet - This zone represents all addresses that are considered public by SecureTrack, and excludes all addresses that are defined in the other zones. You cannot edit this zone.
- Unassociated Networks - This zone includes all private addresses that are not included in any other defined zone. You cannot edit this zone.

  You can add this zone to any USP matrix and define the behavior of this zone relative to all other zones or to specific zones in the environment.

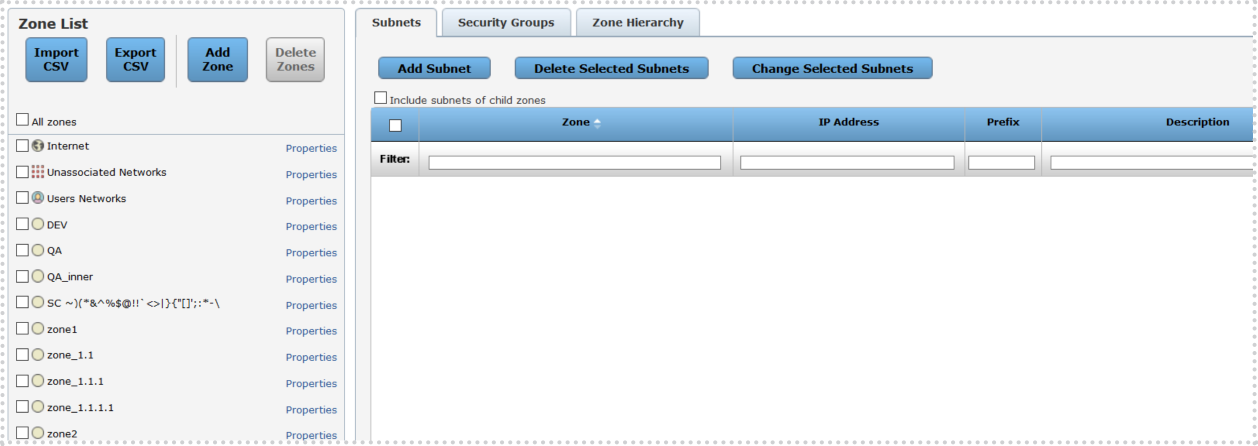
  The Unassociated Networks zone is included in the calculations for Violations in SecureTrack, Risk Analysis in SecureChange, and Compliance checks in SecureApp.

  The Unassociated Networks zone is not available for Policy Analysis, Compliance Policy definition, Business ownership, Risk reports, Configuration of risk security zones (Internal/DMZ/external) or PCI profile definition
- Users Networks - This zone is where you can add the subnets that users use to connect to your network. (Available for devices that support User Identity functionality).

Zones can also include other zones. This allows you to build a zone hierarchy.

You can import zones from CSV format to easily add them to SecureTrack. You can export zones to CSV format, for example to backup the zones.

What can I see?



You can use these zones to define:

- Security zone matrix in Unified Security Policy
- Regulations profiles
- Policy analysis queries

- Compliance policies
- Business ownership reports
- The Internal, External or DMZ network for the security risk report and risky rules

What Can I Do Here?

- Configure the zone list - Add, delete, edit the name, or view zone dependencies.
- Export or Import a zone list - Import a new zone list, or export the zone list to a CSV file.
- Manage the Zone Hierarchy - View and modify the zone hierarchy.
- Manage zone subnets - Add, edit or delete the subnets in a zone.
- Managing the Users Networks Zone - Manage the User Identity functionality.
- Managing Zone Security Groups - View the Security Groups zones.

How Do I Get Here?

Settings > Configuration > Risk > General

,

Configuring the Zone List

You can add, edit, or delete zones. Zones can include IPv4 or IPv6 subnets with explicit network addresses or security groups. Security groups can be added or changed through the REST API or when you import a zone list from a CSV file.

The predefined zones are:

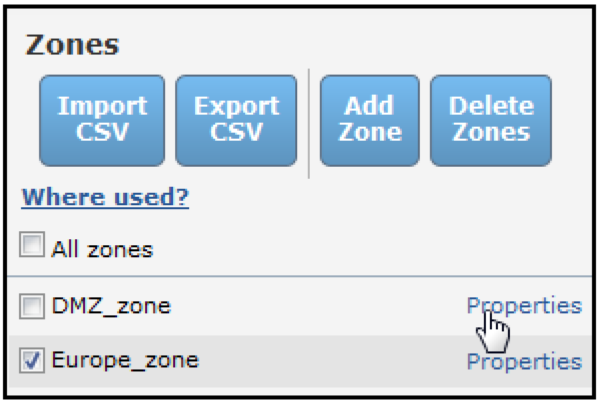
- Internet - This zone represents all addresses that are considered public by SecureTrack, and excludes all addresses that are defined in the other zones. You cannot edit this zone.
- Unassociated Networks - This zone includes all private addresses that are not included in any other defined zone. You cannot edit this zone.

  You can add this zone to any USP matrix and define the behavior of this zone relative to all other zones or to specific zones in the environment.

  The Unassociated Networks zone is included in the calculations for Violations in SecureTrack, Risk Analysis in SecureChange, and Compliance checks in SecureApp.

  The Unassociated Networks zone is not available for Policy Analysis, Compliance Policy definition, Business ownership, Risk reports, Configuration of risk security zones (Internal/DMZ/external) in **Settings > Configuration > Risk > General**, or PCI profile definition
- Users Networks - This zone is where you can add the subnets that users use to connect to your network. (Available for devices that support User Identity functionality).

Zones can also include other zones to build a hierarchy. Network Zone names should not include the ">" character to ensure compatibility across all devices.



When adding or editing zones (via the **Zones** page, REST API, or importing zones from a CSV file) the zone name and description fields are validated.

If you have upgraded from a previous release, the zone fields are not validated. When a zone with an invalid name is edited after the upgrade, a warning message will be displayed.

The following characters are allowed: Characters in all languages, Integers **0-9,** Special characters **+ -_ # @ . , : = ! ^ ( )**

In Multi-Domain deployments:

- Super Admins can view the topology and zones in the Global context. Other users that have access to the Global context see that the Network section of SecureTrack is disabled.
- The types of zones in the zone list are:

Zone Type	Icon	How to Create	Description
Internet	🌐	You cannot add, edit or delete the Internet zone	A default zone that includes public IP addresses, excluding addresses that are defined in other SecureTrack zones. If you do not have SecureTrack zones defined then the Internet zone is treated as ANY. Internet zones exclude all RFC1918 addresses and public subnets defined in other zones.
Unassociated Networks	▦	You cannot add, edit or delete the Unassociated Networks zone	A predefined zone that includes all private IP addresses that are not included in any other defined SecureTrack zones.
Users Networks	👤	You cannot add, edit or delete the Users Networks zone	Predefined zone that is a collection of all the IP addresses used by users. (Available for devices that support User Identity functionality).
Regular	○	• Click **Add Zone** • Enter the zone details • Click **Save**	A zone that can only be used in the domain it is created in. A regular zone includes Subnets and Security Groups. A Super admin in the Global context can only create regular zones and these zones cannot be seen in other domains.
Shared	⋖	• Click **Add Zone** • Enter the zone details • Select **Shared Zone** • Click **Save**	A zone that can be used in any domain, except for the Global context. You cannot share a zone that is a parent of an imported zone.
Imported	⤵	• Click **Add Zone** • Select **Select shared zone** • Select a zone from the list of shared zones from other domains • Click **Save**	A zone that is used in a domain that it was not created in. When you delete an imported zone, the zone is removed from the domain but still exists in the domain it was created in.

What can I do on this page?

- **Add a new zone** - Click **Add Zone**, enter a **Zone Name** and **Description**, and click **Save**.
- **Delete zone** - Select the zones you want to delete and click **Delete Zones**.
- **Change the zone name or description** - Click **Properties.**
- **Check zone usage in SecureTrack reports and queries** - Select the zone and click **Where used**. SecureTrack shows you the dependencies for the selected zones.

How Do I Get Here?

Network > **Zones**

Managing Zone Subnets

Zones can include IPv4 or IPv6 subnets with explicit network addresses or security groups. Security groups can be added or changed through the REST API or when you import a zone list from a CSV file.

The predefined zones are:

- **Internet:** This zone represents all addresses that are considered public by SecureTrack, and excludes all addresses that are defined in the other zones. You cannot edit this zone.
- **Unassociated Networks:** This zone includes all private addresses that are not included in any other defined zone. You cannot edit this zone.

  You can add this zone to any USP matrix and define the behavior of this zone relative to all other zones or to specific zones in the environment.

  The **Unassociated Networks** zone is included in the calculations for Violations in SecureTrack, Risk Analysis in SecureChange, and Compliance checks in SecureApp.

  The **Unassociated Networks** zone is not available for Policy Analysis, Compliance Policy definition, Business ownership, Risk reports, Configuration of risk security zones (Internal/DMZ/external) in Risk Configuration - General, or PCI profile definition.
- **Users Networks:** This zone is where you can add the subnets that users use to connect to your network. (Available for devices that support User Identity functionality).

Zones can also include other zones to build a hierarchy. You can view and manage explicit network addresses in the **Subnets** tab of zones.

All the subnets of all zones selected in the zone list are displayed. For each subnet, the zone it belongs to is displayed. For effective zone content, select **Include subnets of child zones** to recursively display subnets that are indirectly included in the selected zones.

If there are many subnets, you can filter the list by one or more of the four fields: Zone, IP Address, Netmask, and Description. In the **Filter** row, type or select a filter. As you type, SecureTrack only shows you the subnets that match the IP Address and Netmask match the filters and that include the Zone and Description filters. For an IP Address, you can type a network address in CIDR notation (for example: 192.168.0.0/16 or 2001:db8::/32), and only included IP addresses are displayed.

If you change a zone in a way that creates a Compliance Policy violation, SecureTrack does not automatically send an alert. After you make changes to zones, we recommend that you run your Compliance Policy audits.

Upgrade Behavior for 'Unassociated Networks' Zones

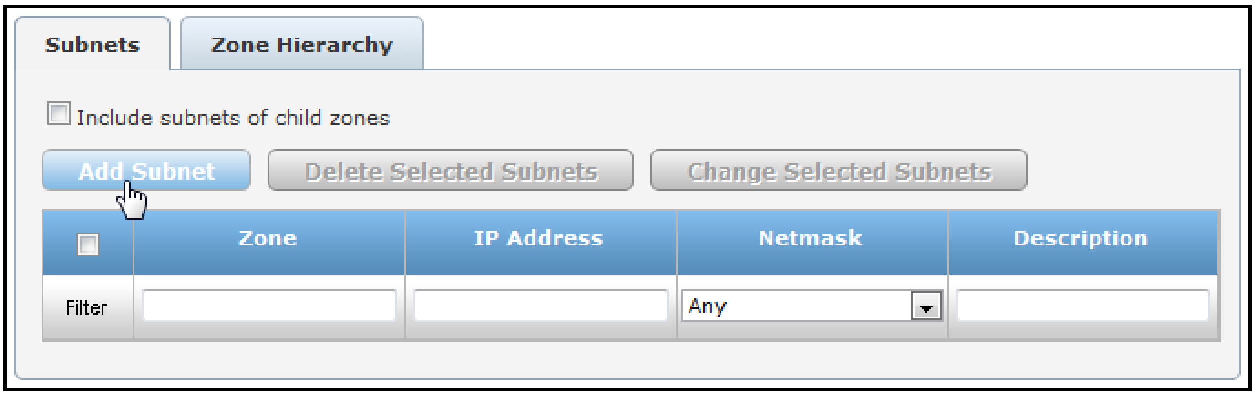
When upgrading Tufin Orchestration Suite, the predefined **Unassociated Networks** zone is added to the Zone Manager during upgrade. If you are upgrading from a system that already contains a zone with the name “Unassociated Networks”, the existing zones are renamed, as follows:

- The existing zones named **Unassociated Networks** will be renamed **copy_of_Unassociated Networks, copy(2)_of_Unassociated Networks**, and so on. For each domain in multidomain/MSSP mode, any existing zone that is named **Unassociated Networks** will also be renamed.
- The existing USP matrices in each domain will be changed to reflect the renamed zones. They will include the name **copy_of_ Unassociated Networks** (and not **Unassociated Networks**).

When you import new matrices after an upgrade, the name of the zone is taken from the CSV without being renamed.

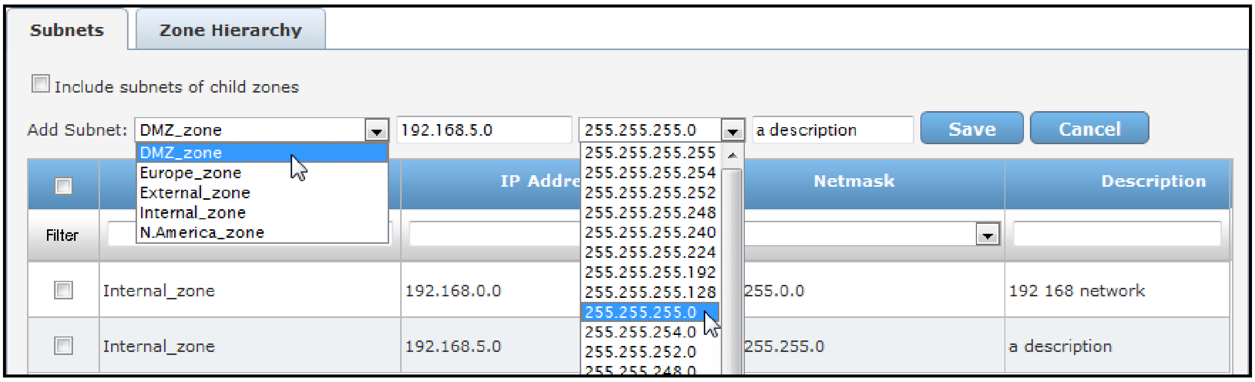
To add a network address to a zone

1. In **Network** > **Zones**, in the **Subnets** tab, click **Add Subnet**:



□	Zone	IP Address	Netmask	Description
Filter			Any	

2. Enter the subnet information.
   1. Select the zone for the subnet.
   2. Enter the network address.
   3. Select the net mask.
   4. Enter a description for the subnet.



□ Include subnets of child zones

Add Subnet: DMZ_zone 192.168.5.0 255.255.255.0 a description

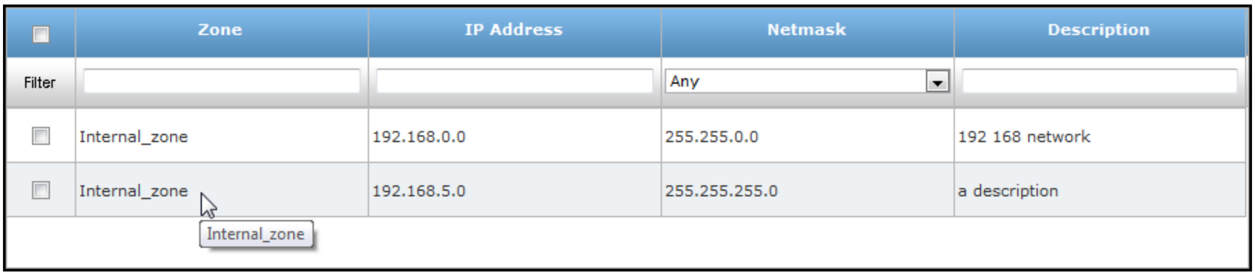
□		IP Addre	Netmask	Description
Filter				
□	Internal_zone	192.168.0.0	255.0.0	192 168 network
□	Internal_zone	192.168.5.0	255.255.0	a description

3. Click **Save**.

To edit an existing subnet

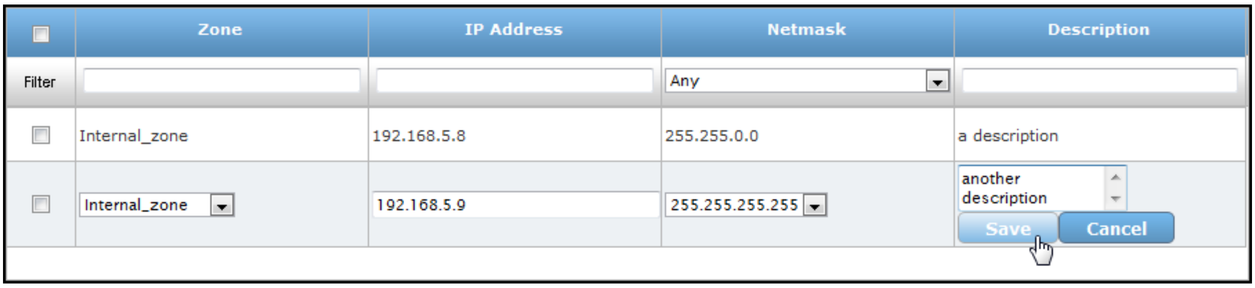
1. Click on one of fields for the subnet.

   For example, if you click on the zone field, you can change the zone for that subnet.



□	Zone	IP Address	Netmask	Description
Filter			Any	
□	Internal_zone	192.168.0.0	255.255.0.0	192 168 network
□	Internal_zone	192.168.5.0	255.255.255.0	a description

2. Edit the fields for the subnet.

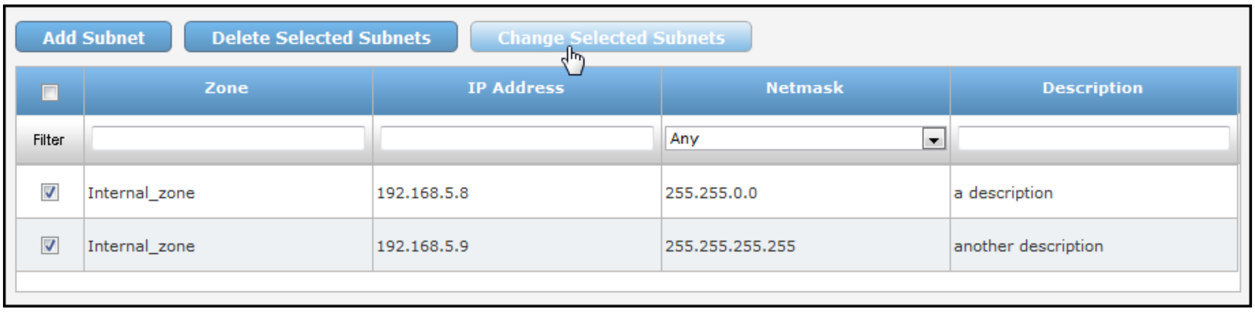


□	Zone	IP Address	Netmask	Description
Filter			Any	
□	Internal_zone	192.168.5.8	255.255.0.0	a description
□	Internal_zone	192.168.5.9	255.255.255.255	another description

3. Click **Save.**

To edit multiple subnets at the same time

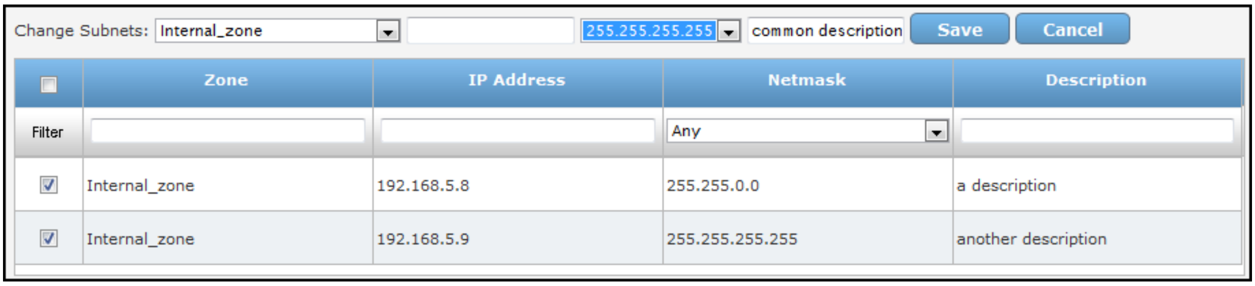
1. Select the subnets, and click **Change Selected Subnets**:



□	Zone	IP Address	Netmask	Description
Filter			Any	
☑	Internal_zone	192.168.5.8	255.255.0.0	a description
☑	Internal_zone	192.168.5.9	255.255.255.255	another description

2. Configure the common fields.

   Only the fields that you change are changed for all subnets. You cannot change all of the fields for the selected subnets because the subnets will all be the same.



Change Subnets: Internal_zone | | 255.255.255.255 | common description | Save | Cancel

☐	Zone	IP Address	Netmask	Description
Filter			Any	
☑	Internal_zone	192.168.5.8	255.255.0.0	a description
☑	Internal_zone	192.168.5.9	255.255.255.255	another description

3. Click **Save**.

To delete one or more subnets, select them and click **Delete Selected Subnets**.

Managing the Users Networks Zone

The Users Networks zone is a predefined zone in SecureTrack where you add all the valid subnets that users are allowed to use when connecting to your network. TOS requires the Users Networks zone when User Identity is used for a device that does not natively support using LDAP groups. (See Using User Identity in TOS.)

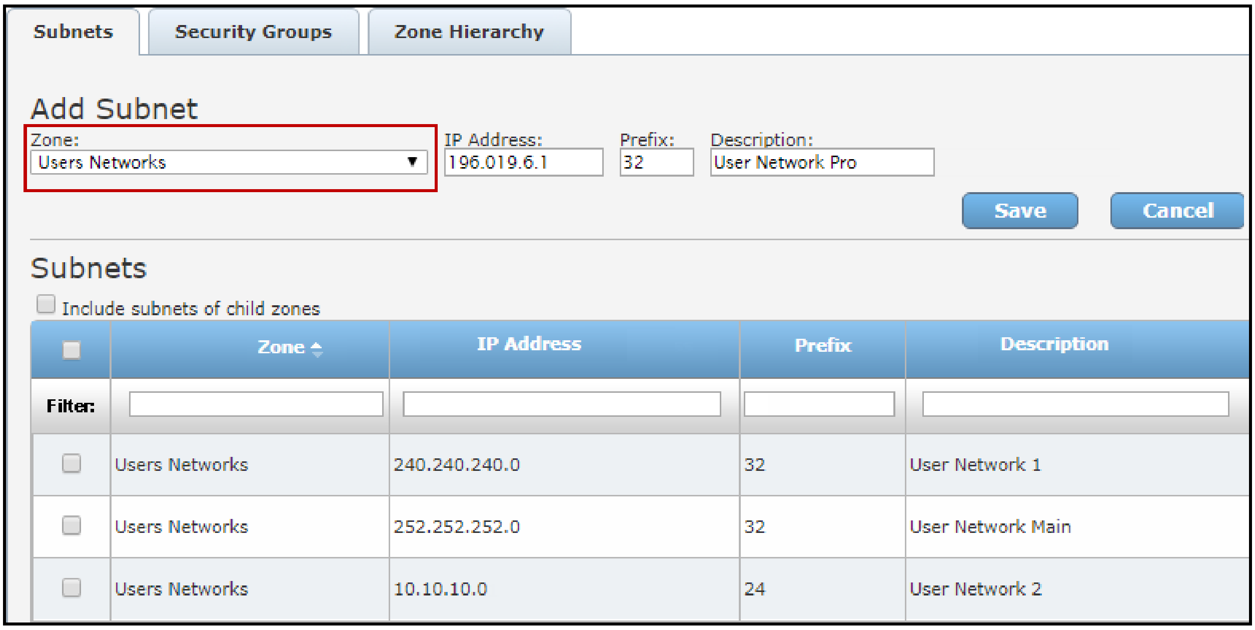
Prerequisites

Configure SecureTrack for LDAP authentication, as described in Configuring User Identity. All users or groups in the LDAP tree listed under the Domain DN field will be authenticated as valid.

Add Subnets to the Users Networks Zone

To add IPv6 subnets to a zone, use the REST API or import the zones using a CSV file.

1. In the Users Networks zone, add all subnets that users are allowed to use when connecting to your network. See Managing Zone Subnets for details.



Add Subnet

Zone: Users Networks
IP Address: 196.019.6.1
Prefix: 32
Description: User Network Pro

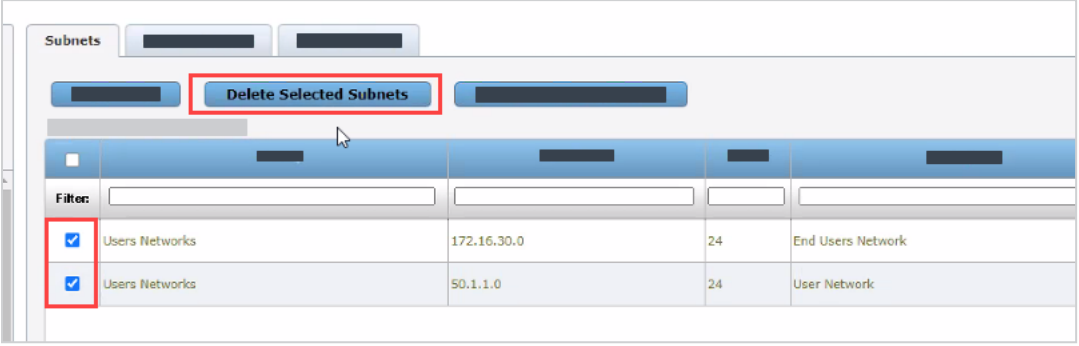
Subnets

☐ Include subnets of child zones

☐	Zone	IP Address	Prefix	Description
Filter:				
☐	Users Networks	240.240.240.0	32	User Network 1
☐	Users Networks	252.252.252.0	32	User Network Main
☐	Users Networks	10.10.10.0	24	User Network 2

Delete Subnets from the User Networks Zone

1. Select the subnets that you want to delete.



□	[redacted]	[redacted]	[redacted]	[redacted]
Filter:				
☑	Users Networks	172.16.30.0	24	End Users Network
☑	Users Networks	50.1.1.0	24	User Network

2. Click **Delete Selected Subnets**.

If one or more IP addresses in the Users Networks zones are removed, we recommend that you create a Rule Modification ticket requesting that all of the deleted subnets be removed from the rules that include them. Removing these subnets from the rules reduces attack surface and improves policy strictness.

Managing Zone Security Groups

A Security Group is a collection of instances that can be used to represent zones for all supported devices. Zones can include IPv4 or IPv6 subnets with explicit network addresses or security groups. Security groups can be added or changed through the REST API or when you import a zone list from a CSV file.

The predefined zones are:

- Internet - This zone represents all addresses that are considered public by SecureTrack, and excludes all addresses that are defined in the other zones. You cannot edit this zone.
- Unassociated Networks - This zone includes all private addresses that are not included in any other defined zone. You cannot edit this zone.

  You can add this zone to any USP matrix and define the behavior of this zone relative to all other zones or to specific zones in the environment.

  The Unassociated Networks zone is included in the calculations for Violations in SecureTrack, Risk Analysis in SecureChange, and Compliance checks in SecureApp.

  The **Unassociated Networks** zone is not available for Policy Analysis, Compliance Policy definition, Business ownership, Risk reports, Configuration of risk security zones (Internal/DMZ/external) in Risk Configuration - General, or PCI profile definition.
- Users Networks - This zone is where you can add the subnets that users use to connect to your network. (Available for devices that support User Identity functionality).

Zones can also include other zones to build a hierarchy.You can view the security groups in each zone in the **Security Groups** tab of zones.

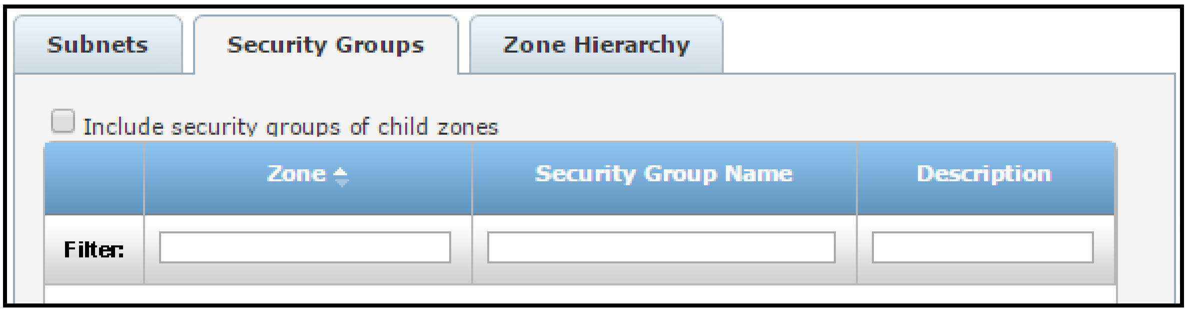
All the security groups of all zones selected in the zone list are displayed. For each security groups , the zone it belongs to is displayed. You can also select to **Include security groups of child zones** to recursively display security groups that are indirectly included in the selected zones.

If there are many security groups, you can filter the list by one or more of these fields: Zone, Security Groups, and Description. In the **Filter** row, type or select a filter. As you type, SecureTrack only shows you the security groups that match the filters.

If you change a zone in a way that creates a Compliance Policy violation, SecureTrack does not automatically send an alert. After you make changes to zones, we recommend that you run your Compliance Policy audits.

To view a security groups zone:

1. In Zones, select the **Security Groups** tab:



□ Include security groups of child zones

	Zone	Security Group Name	Description
Filter:			

2. To filter the results, enter text in the filter area for any of the fields: **Zone**, **Security Group Name**, **Description**. As you type, SecureTrack only shows you the security groups that match the filters.

   When compliance is checked via the Unified Security Policy, any Security Group that contains the name you added to the zone will be a match. For example, if the **Security Group Name** field contains"oursg", all these zone Security Groups will match: "oursg1" , "0oursg2", "a_oursg", and so on.

Managing Zone Hierarchy

Zones can include IPv4 or IPv6 subnets with explicit network addresses or security groups. Security groups can be added or changed through the REST API or when you import a zone list from a CSV file.

The predefined zones are:

- Internet - This zone represents all addresses that are considered public by SecureTrack, and excludes all addresses that are defined in the other zones. You cannot edit this zone.
- Unassociated Networks - This zone includes all private addresses that are not included in any other defined zone. You cannot edit this zone.

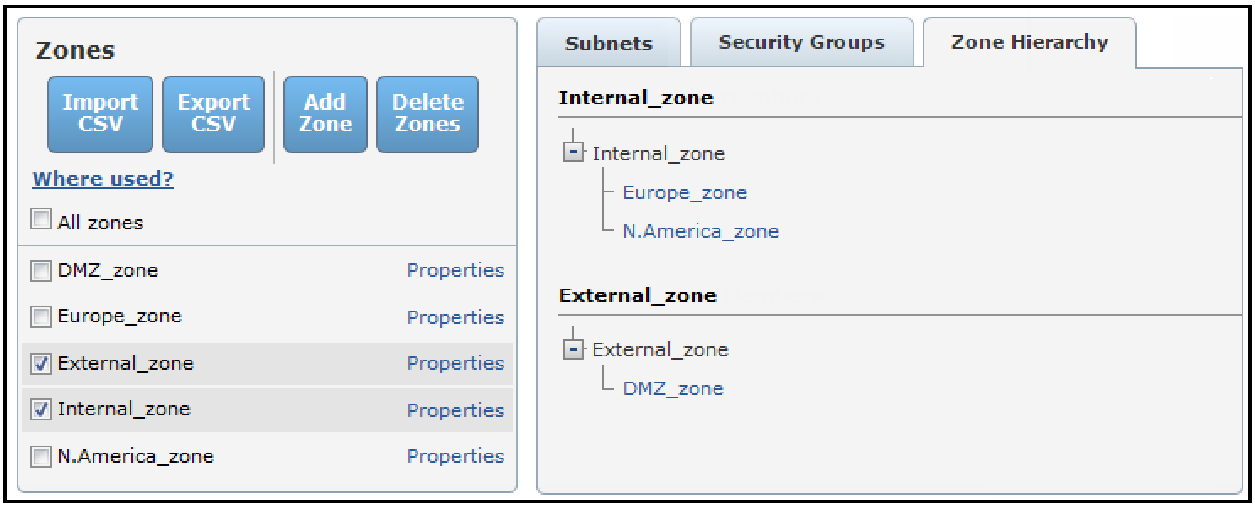
  You can add this zone to any USP matrix and define the behavior of this zone relative to all other zones or to specific zones in the environment.

  The Unassociated Networks zone is included in the calculations for Violations in SecureTrack, Risk Analysis in SecureChange, and Compliance checks in SecureApp.

  The **Unassociated Networks** zone is not available for Policy Analysis, Compliance Policy definition, Business ownership, Risk reports, Configuration of risk security zones (Internal/DMZ/external) in Risk Configuration - General, or PCI profile definition.
- Users Networks - This zone is where you can add the subnets that users use to connect to your network. (Available for devices that support User Identity functionality).

  Zones can also include other zones to build a hierarchy.

In Zones, the **Zone Hierarchy** shows the parent and child zones of the zones that are selected in the zone list:



□ All zones

□ DMZ_zone Properties

□ Europe_zone Properties

☑ External_zone Properties

☑ Internal_zone Properties

□ N.America_zone Properties

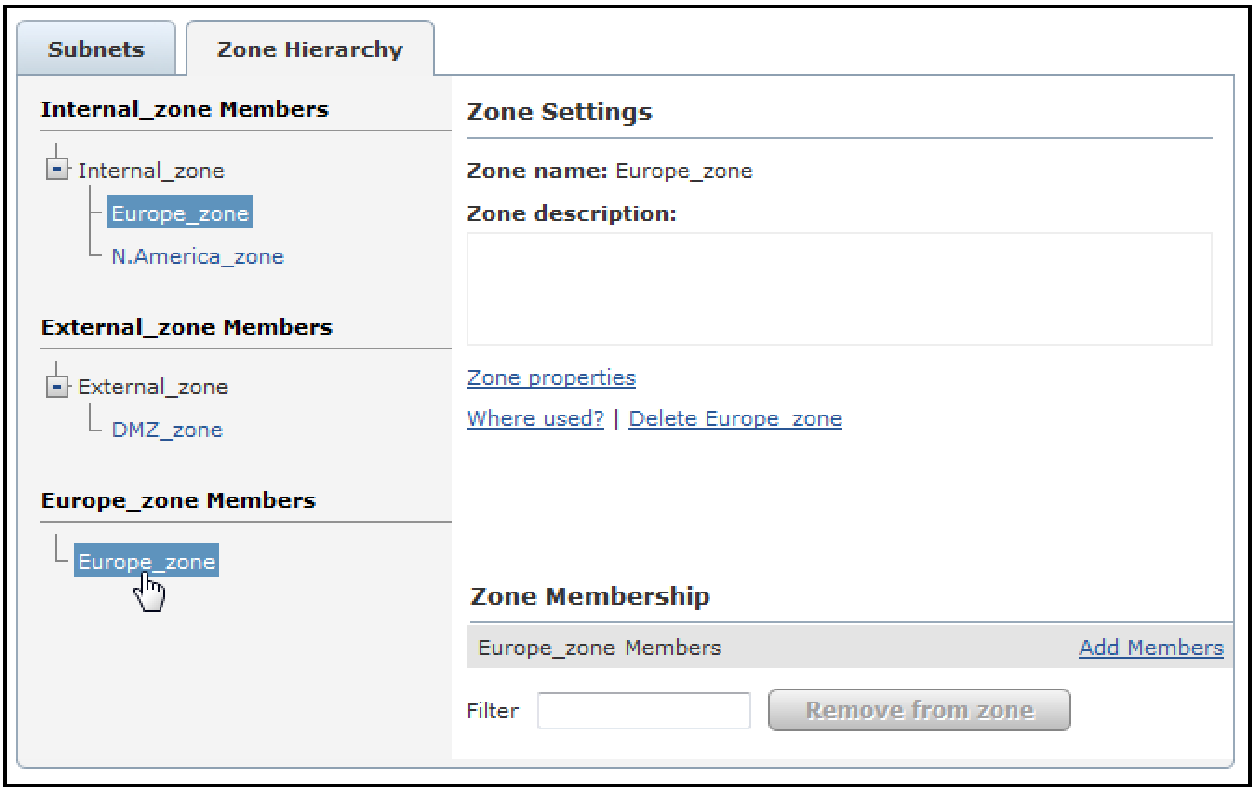
Internal_zone

```
⊟ Internal_zone
   ├ Europe_zone
   └ N.America_zone
```

External_zone

```
⊟ External_zone
   └ DMZ_zone
```

You can select a zone in the hierarchy trees to change it:



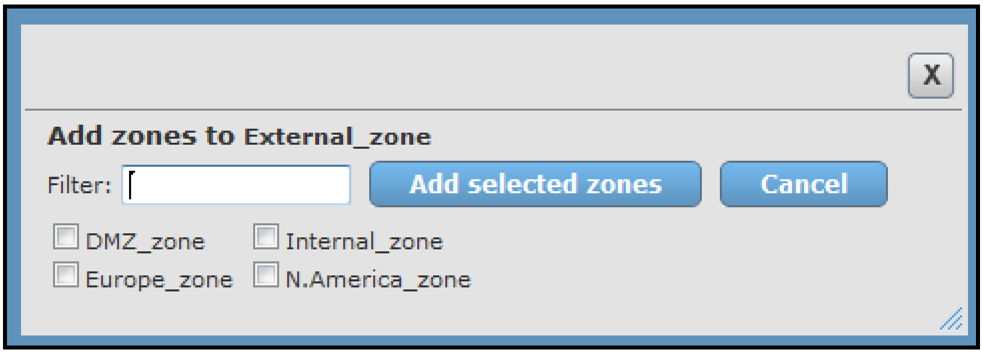
Zone name: Europe_zone

Zone description:

Zone Settings and controls (**Zone properties**, **Where used?**, and **Delete**) are the same as in the Zone List. Under **Zone Membership**, you can do the following:

To add a member to the zone selected in the hierarchy trees:

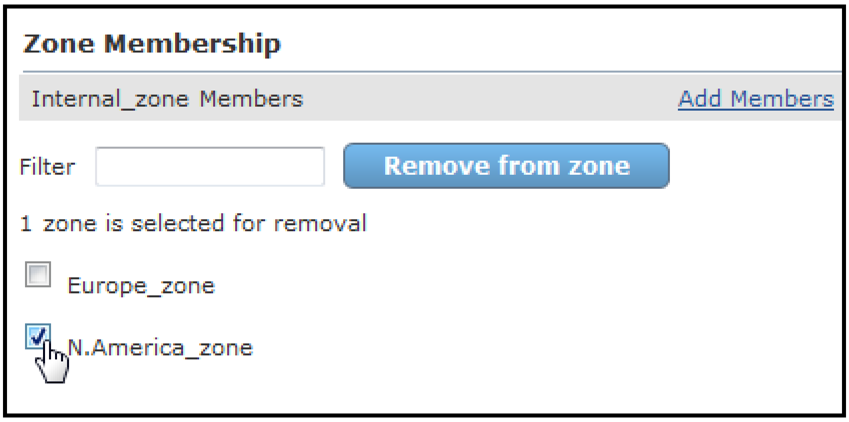
1. Select the parent zone and click **Add Members**.
2. Select the zones to be added, and click **Add selected zones**:



If there are many available zones, you can first filter the list by typing a **Filter** text. As you type, only zones whose names include the filter text are displayed.

To remove members from the zone selected in the hierarchy trees:

1. Below **Zone Membership**, select the zones to be removed:



1 zone is selected for removal

□ Europe_zone

☑ N.America_zone

If there are many available zones, you can first filter the list by typing a **Filter** text. As you type, only zones whose names include the filter text are displayed.

2. Click **Remove from zone**.

Exporting and Importing Zones

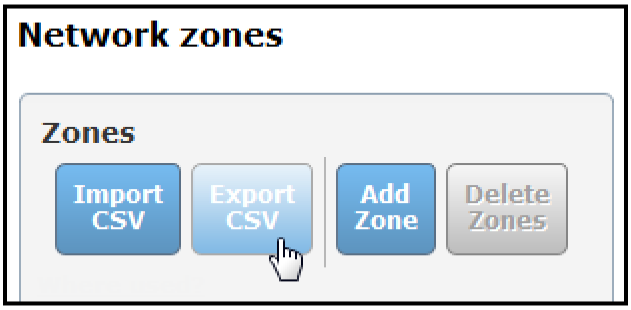
You can import zones from CSV format to easily add them to SecureTrack. You can export zones to CSV format, for example to backup the zones.

When adding or editing zones (via the **Zones** page, REST API, or importing zones from a CSV file) the zone name and description fields are validated.

If you have upgraded from a previous release, the zone fields are not validated. When a zone with an invalid name is edited after the upgrade, a warning message will be displayed.

The following characters are allowed: Characters in all languages, Integers **0-9,** Special characters **+ -_ # @ . , : = ! ^ ( )** and blank spaces.

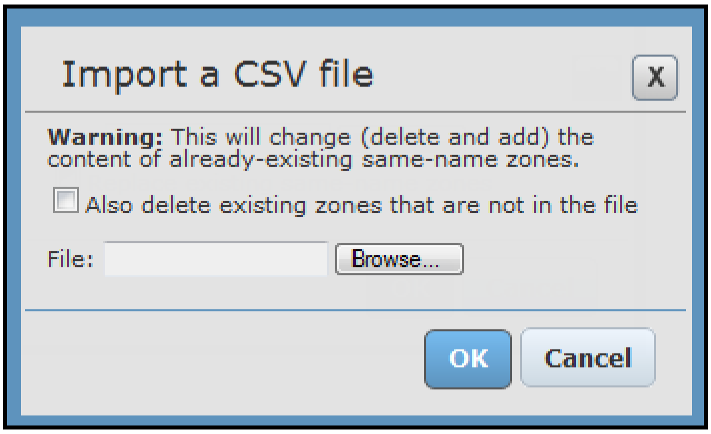
To export the set of configured zones to CSV, in Zones, in the Zone list, click **Export CSV***:*



To prevent a CSV injection attack when exporting zones to a CSV file, if a special character (**= - + @**) appears at the beginning of the zone name or description field, a single quote (') is added before the character.

To import a CSV file to SecureTrack, in the Zone list:

1. Click **Import CSV**. The Import window appears:



Warning: This will change (delete and add) the content of already-existing same-name zones.

□ Also delete existing zones that are not in the file

File:

For zones that already exist in SecureTrack, if they exist in the file by the same name, their contents are completely replaced. If they do not exist in the file, you can select whether to **Also delete existing zones that are not in the file**.

2. **Browse** to the file, and click **OK**.

   When importing a CSV file to SecureTrack, any single quotes (') that were added to the CSV file before a special character (**= - + @**) at the beginning of the zone name or description field are removed.

If you want to manually configure a CSV file for import, you must use the format:

- Each line in the file defines a member for a specified zone.
- The member can be a network address, or an already-defined zone.
- All the members defined for a specific Network Zone name are aggregated to define the Network Zone.

The format for each line in the zone file is:

```
#Zone Properties,,
```

```
zone name,domain, is_shared, description,
```

Where:

- `<Zone name>` is the name of the zone.
- `<domain>` is the domain where the zone was created. (For Multi-Domain deployment only)
- `<is_shared>` is whether the zone is shared for use in other domains. (For Multi-Domain deployment only)
- `<description>` is free text.

```
#Zone Hierarchy,,
```

```
parent,child,
```

Where:

- `<parent>` is the name of the zone above the child in the hierarchy.
- `<child>` is the name of the zone below the parent in the hierarchy.

```
#Zone Subnets,,
```

```
zone name,subnet,description
```

Where:

- `<Zone name>` is the name of a zone defined in the zone properties section.
- `<subnet>` is the IP address or network of the zones in the format `<IP>/<netmask>`

  where:

  - `<IP>` is the IP address of the member network.
  - `<netmask>` is the netmask of the member network, in either IP notation (for example: `255.255.255.0`) or CIDR notation (for example: `24`). For IPv6 addresses you must use CIDR notation
- `<description>` is free text.

  If circular definition occurs (zone A is included in zone B which is included in zone A), the import fails.

```
#Zone Security Groups
```

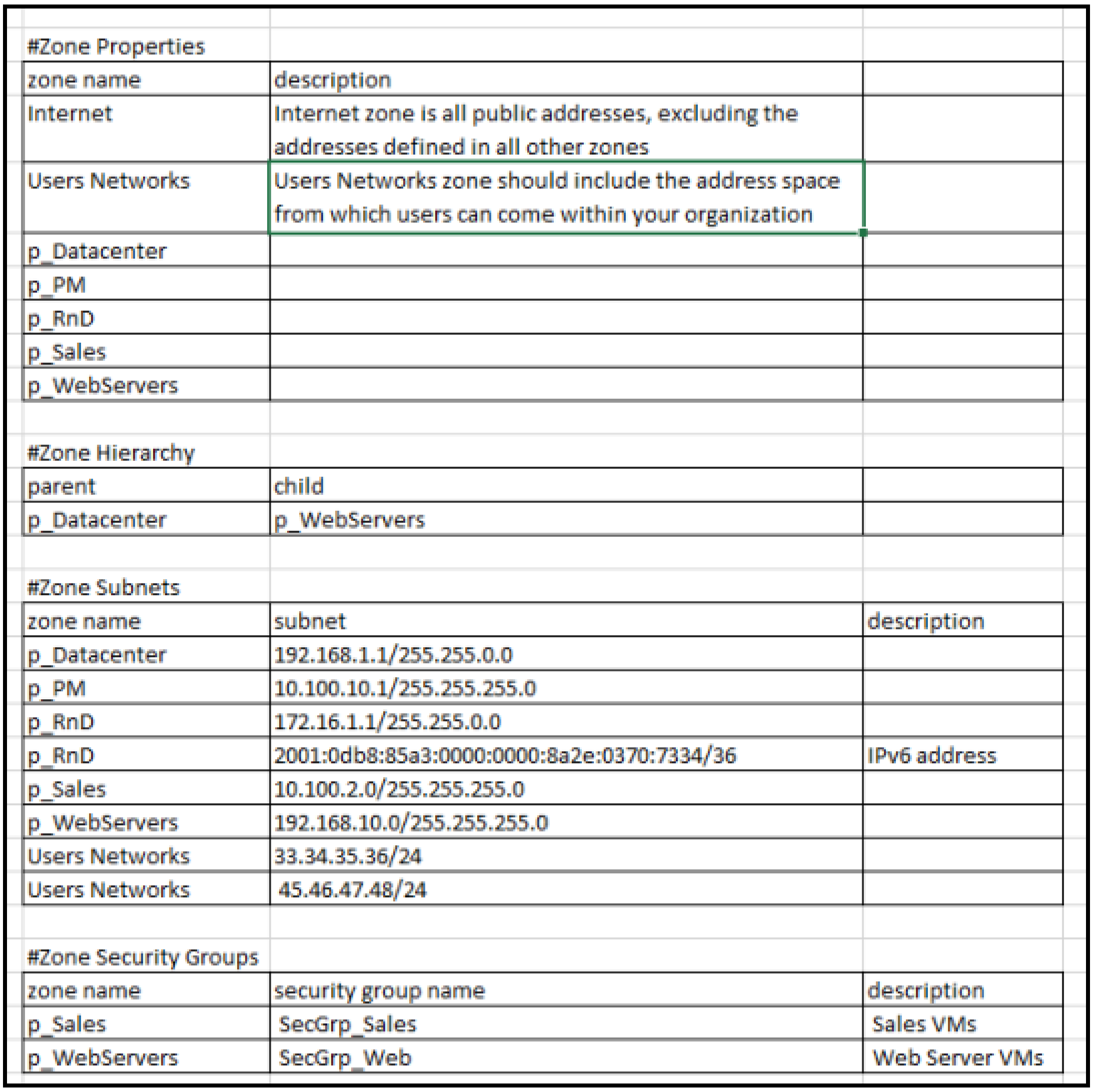
```
zone name,security group name,description
```

Where:

- `<Zone name>` is the name of a zone defined in the zone properties section.
- `<security group name>` is the name of the security group that is associated with this zone.
- `<description>` is free text.

Sample File

Sample as shown in Excel



#Zone Properties

zone name	description	
Internet	Internet zone is all public addresses, excluding the addresses defined in all other zones	
Users Networks	Users Networks zone should include the address space from which users can come within your organization	
p_Datacenter		
p_PM		
p_RnD		
p_Sales		
p_WebServers		

#Zone Hierarchy

parent	child	
p_Datacenter	p_WebServers	

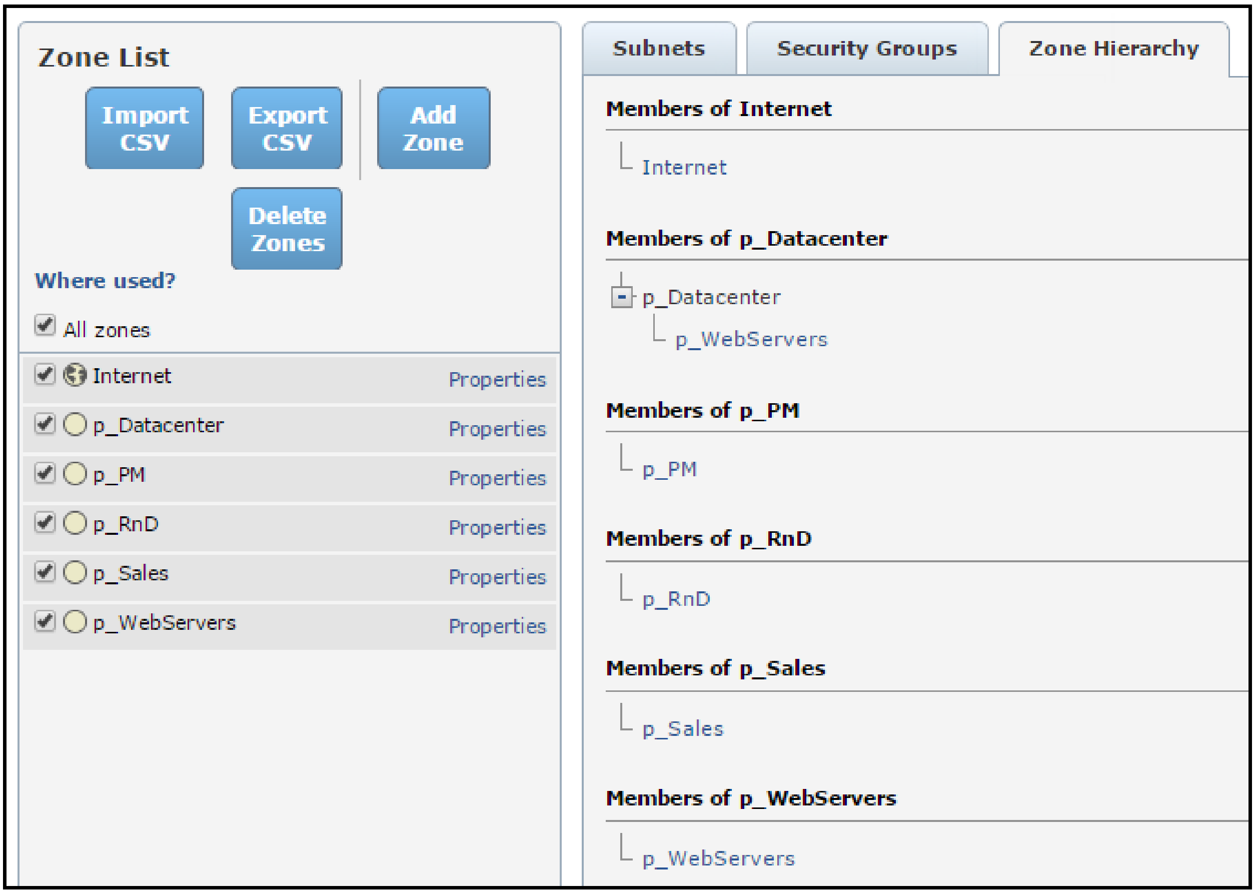
#Zone Subnets

zone name	subnet	description
p_Datacenter	192.168.1.1/255.255.0.0	
p_PM	10.100.10.1/255.255.255.0	
p_RnD	172.16.1.1/255.255.0.0	
p_RnD	2001:0db8:85a3:0000:0000:8a2e:0370:7334/36	IPv6 address
p_Sales	10.100.2.0/255.255.255.0	
p_WebServers	192.168.10.0/255.255.255.0	
Users Networks	33.34.35.36/24	
Users Networks	45.46.47.48/24	

#Zone Security Groups

zone name	security group name	description
p_Sales	SecGrp_Sales	Sales VMs
p_WebServers	SecGrp_Web	Web Server VMs

Sample after import



Security Zone Matrix CSV File

Use a text editor such as Notepad to save this text as a CSV file and import it into Zones to see an example of a list of zones.

```
#Zone Properties,,
zone name,description,
Internet,"Internet zone is all public addresses, excluding the addresses defined in all other zones",
"Users Networks","Users Networks zone should include the address space from which users can come within your organization"
p_Datacenter,,
p_PM,,
p_RnD,,
p_Sales,,
p_WebServers,,

#Zone Hierarchy,,
parent,child,
p_Datacenter,p_WebServers,

#Zone Subnets,,
zone name,subnet,description
p_Datacenter,192.168.1.1/255.255.0.0,
p_PM,10.100.10.1/255.255.255.0,
p_RnD,172.16.1.1/255.255.0.0,
p_RnD,2001:0db8:85a3:0000:0000:8a2e:0370:7334/36,IPv6 address
```

```
p_Sales,10.100.2.0/255.255.255.0,
p_WebServers,192.168.10.0/255.255.255.0,
Users Networks,33.34.35.36/24
Users Networks, 45.46.47.48/24

#Zone Security Groups
zone name,security group name,description
p_Sales, SecGrp_Sales, Sales VMs
p_WebServers, SecGrp_Web, Web Server VMs
```

Configuring SecureTrack Settings

This chapter explains how to configure SecureTrack settings, such as user configuration, notifications and database maintenance.

Only SecureTrack Administrators can see all the pages. Regular Users see only the pages under **Settings** > **My Settings** and then selecting **Display Options**, or **Account Details**. In a Multi-Domain environment, Multi-Domain Administrators in the Global context also see only these pages.

Setting Timing for Monitoring

Here you can configure:

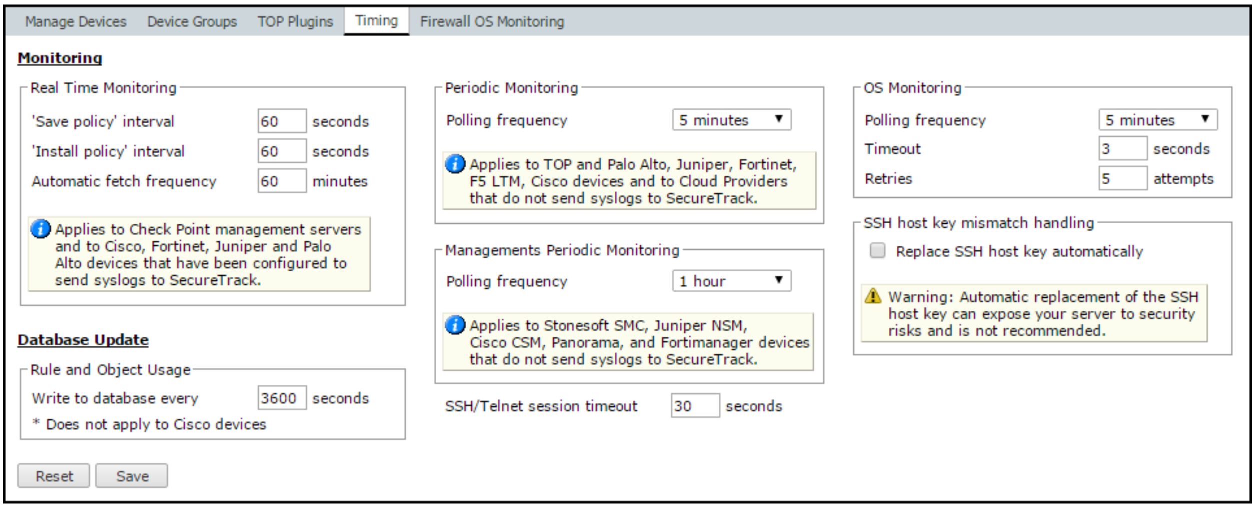
- Timing values for policy retrieval, device polling, and database updating
- SSH host key mismatch handling where you can choose to replace SSH host key automatically when a new SSH host key is detected for a device

  Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.

This page is available only to Administrators. For changes to take effect, you must click **Save**.

By default, the settings on this page affect all devices that are monitored in the relevant monitoring mode (real time, periodic polling, or OS monitoring). The settings can be overridden for each specific monitored device, in the properties for that device (**Settings** > **Monitoring** > **Devices** > select device > **Edit configuration**). In some cases the monitoring mode itself can be set there as well.

Here on the Timing page, the available settings are:



Monitoring

Real Time Monitoring

'Save policy' interval 60 seconds
'Install policy' interval 60 seconds
Automatic fetch frequency 60 minutes

Applies to Check Point management servers and to Cisco, Fortinet, Juniper and Palo Alto devices that have been configured to send syslogs to SecureTrack.

Periodic Monitoring

Polling frequency 5 minutes

Applies to TOP and Palo Alto, Juniper, Fortinet, F5 LTM, Cisco devices and to Cloud Providers that do not send syslogs to SecureTrack.

Managements Periodic Monitoring

Polling frequency 1 hour

Applies to Stonesoft SMC, Juniper NSM, Cisco CSM, Panorama, and Fortimanager devices that do not send syslogs to SecureTrack.

SSH/Telnet session timeout 30 seconds

OS Monitoring

Polling frequency 5 minutes
Timeout 3 seconds
Retries 5 attempts

SSH host key mismatch handling

□ Replace SSH host key automatically

Warning: Automatic replacement of the SSH host key can expose your server to security risks and is not recommended.

Database Update

Rule and Object Usage

Write to database every 3600 seconds
* Does not apply to Cisco devices

- **Real-Time Monitoring**: Applies to Cisco, Fortinet, and Juniper devices that have been configured to send syslogs to SecureTrack (unless in the device's properties real-time monitoring has been disabled), and to Check Point management servers:
  - **'Save policy' interval** (Applies only to Check Point management servers): When a Save Policy event is followed within this time interval by an Install Policy event for the same policy, SecureTrack tries to combine the two events into a single revision. The default value is 60 seconds.
    - **'Install policy' interval**: When two or more Install Policy events for the same policy occur within this time interval, SecureTrack combines the events into a single Install Policy revision (Default: 60 seconds)
  - **Automatic fetch frequency**: Frequency (in minutes) for automatic fetch
- **Periodic Polling**: Applies to TOP and Palo Alto devices, and to Cisco, Fortinet, and Juniper devices that do not send syslogs or that have had real-time monitoring disabled (in the device properties):
  - **Polling frequency**: How often SecureTrack will fetch the configuration from each device. To select an exact time for daily polling, set the polling frequency specifically for each device, in the device's properties.
- **Session timeout**: How long SecureTrack will wait for a response from device before giving up. This setting is used in case a device is down or too busy. Applies to Automatic fetch (for real-time monitored devices) and to periodic polling.
- **OS Monitoring**:
  - **Polling frequency**: How often SecureTrack will fetch the configuration from each device.
  - **Timeout**: Controls how long SecureTrack will wait for a response from device before giving up. This setting is used in case a device is down or too busy.
  - **Retries**: The number of attempts SecureTrack will make.

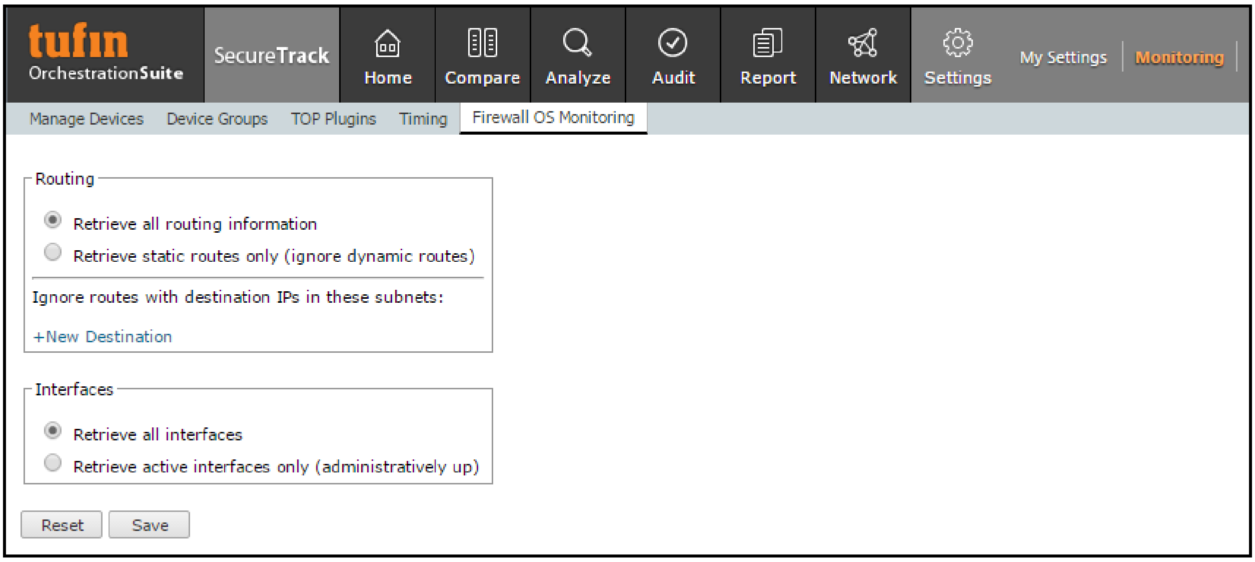
- **Database Update**:
  - **Write to database every**: Dictates the frequency with which SecureTrack updates its database. The default is every 3600 seconds (1 hour), but this can be changed. When you increase this time, you increase the amount of memory used, but have fewer write actions to the database, which in turn means a smaller amount of disk is required to store the same amount of data. Changing the default database update frequency may adversely affect the responsiveness of your system. Contact Tufin Support before making any changes to the default value.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Monitoring** > **Timing**.

Firewall OS Monitoring Settings

The Firewall OS Monitoring tab contains the following settings:



Routing

● Retrieve all routing information

○ Retrieve static routes only (ignore dynamic routes)

Ignore routes with destination IPs in these subnets:

+New Destination

Interfaces

● Retrieve all interfaces

○ Retrieve active interfaces only (administratively up)

Reset Save

- Routing
  - **Retrieve all routing information**: SecureTrack collects and analyzes all routing information, including dynamic routes. Dynamic routes are displayed in the routing tab of Check Point firewall modules. Firewall OS Monitoring is performance-intensive and causes SecureTrack to collect many revisions.
  - **Retrieve static routes only (ignore dynamic routes)**: SecureTrack does not fetch dynamic routes.
  - **Ignore routes with destination IPs in these subnets**: Click **new destination** to configure destination subnets to be ignored by SecureTrack.
- Interfaces
  - **Retrieve all interfaces**: SecureTrack fetches and analyzes information on all interfaces, including stopped interfaces.
  - **Retrieve active interfaces only (administratively up)**: SecureTrack fetches information only on interfaces that are configured as up (regardless of hardware state).

Change Windows

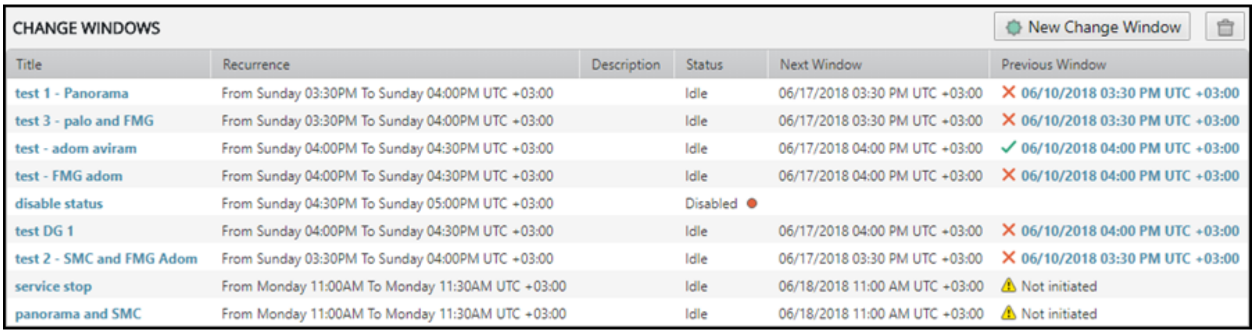
What are Change Windows?

Change windows are recurring time slots that you configure to commit policy changes which have been provisioned to management devices. The change window automatically commits the changes to the managed firewalls according to the schedule you created. See What is Provisioning and Commit Policy Changes in SecureChange for more information.

Change windows let you:

- Aggregate network policy changes for management devices–such as Panorama Advanced mode, FortiManager Advanced mode, and Check Point R80.x CMA and MDS devices–and then automatically commit those changes.
- Schedule change commit windows for off hours.
- Monitor the success or failure of the policy commit processes in real time for the current, next, and last policy commit processes.

What am I looking at?



CHANGE WINDOWS

Title	Recurrence	Description	Status	Next Window	Previous Window
test 1 - Panorama	From Sunday 03:30PM To Sunday 04:00PM UTC +03:00		Idle	06/17/2018 03:30 PM UTC +03:00	✗ 06/10/2018 03:30 PM UTC +03:00
test 3 - palo and FMG	From Sunday 03:30PM To Sunday 04:00PM UTC +03:00		Idle	06/17/2018 03:30 PM UTC +03:00	✗ 06/10/2018 03:30 PM UTC +03:00
test - adom aviram	From Sunday 04:00PM To Sunday 04:30PM UTC +03:00		Idle	06/17/2018 04:00 PM UTC +03:00	✓ 06/10/2018 04:00 PM UTC +03:00
test - FMG adom	From Sunday 04:00PM To Sunday 04:30PM UTC +03:00		Idle	06/17/2018 04:00 PM UTC +03:00	✗ 06/10/2018 04:00 PM UTC +03:00
disable status	From Sunday 04:30PM To Sunday 05:00PM UTC +03:00		Disabled ●		
test DG 1	From Sunday 04:00PM To Sunday 04:30PM UTC +03:00		Idle	06/17/2018 04:00 PM UTC +03:00	✗ 06/10/2018 04:00 PM UTC +03:00
test 2 - SMC and FMG Adom	From Sunday 03:30PM To Sunday 04:00PM UTC +03:00		Idle	06/17/2018 03:30 PM UTC +03:00	✗ 06/10/2018 03:30 PM UTC +03:00
service stop	From Monday 11:00AM To Monday 11:30AM UTC +03:00		Idle	06/18/2018 11:00 AM UTC +03:00	⚠ Not initiated
panorama and SMC	From Monday 11:00AM To Monday 11:30AM UTC +03:00		Idle	06/18/2018 11:00 AM UTC +03:00	⚠ Not initiated

This page displays a list of all your change windows for committing changes. The table lists the **Recurrence**, **Status**, **Next** and **Previous Window** for each change window. If available, a link is displayed for a report on the status, next scheduled window, and results of the previous window. The following information is displayed in the **Change Windows** table for each change window:

Change Window field	Description
Title	Name of the configured change window Click the link to edit the change window fields
Domain	For multi-domain environments, displays the domain name
Recurrence	The day and time the change window is configured to run
Description	Optional text
Status	• **Idle** - The change window is not currently running • Disabled ● - The change window is not available for scheduling • **Commit in progress** - Click the link to view the **Change Window Progress Report** for the change window • ✗ - Errors encountered: Some actions failed during the commit process
Next Window	Date and time for the next configured change window - Click the link to view the **Next Change Window Report** for the change window
Previous Window	For the previous change window, displays the date and time and summarizes the execution results • ✓ - All policies successfully installed on the selected firewalls • ✗ - Some actions not completed • ⚠ Not initiated - Did not start or timed out Click the link to view the **Commit Status Report** for the change window

Prerequisites

To access the **Change Windows** tab, you must have the following licenses and user privileges/roles defined:

- Licenses for SecureTrack, SecureChange, and Provisioning for all relevant devices
- User privileges/roles:
  - Non-managed security service provider (non-MSSP) mode: administrator user
  - MSSP mode:
    - SecureTrack super admin (can create change windows in any domain)
    - multi-domain admin privileges (can create change windows in specified domains)

What can I do on this page

- Create a change window - Click New Change Window.

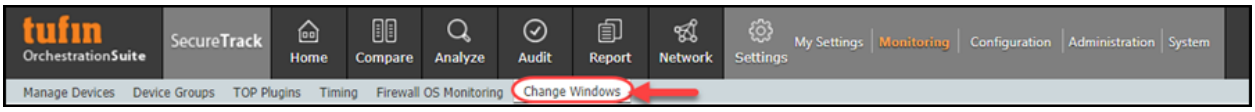
  You must add at least one device, enter a title, and configure at least a single recurrence for the change window.
- View/update a change window - View a change window and update the configured **Status** (**Enable/Disable**), **Devices**,and **Settings**.
- Delete a change window - Select the change window in the **Change Windows** table, click 🗑, and click **OK** to confirm the **DELETE CHANGE WINDOW** action.
- View change window reports - View the progress of a running change window, the details of the next configured change window, and the results of the last change window.

The reports include information such as the change window title, start and end date/time, relevant manufacturer and device names, status, warnings, errors, and elapsed time.

The details shown in the **Commit Status Report** display the returned results exactly as received from the vendor, including the status, warning, error data, duplicated object names, and so on. Duplicated results or unexpected names may be caused by specific vendor limitations.

How Do I Get Here?

To go to the Change Windows tab:



1. In SecureTrack, go to **Settings** > **Monitoring**.
2. Select the **Change Windows** tab.

View and Update a Change Window

During the configured change window, Tufin automatically commits the saved policies on the relevant firewalls. Each change window can be configured for multiple devices and a device can be configured in multiple change windows. The commit process only occurs for devices that are online, enabled, and running within the change window.

Support for automatic policy commit is provided for the following management systems/devices:

- Panorama Advanced mode (includes Device Groups at any level)
- FortiManager Advanced mode (ADOMs)
- Check Point R80.x CMA and MDS devices

When a change window runs, the latest policy version of each device is committed on the relevant firewalls:

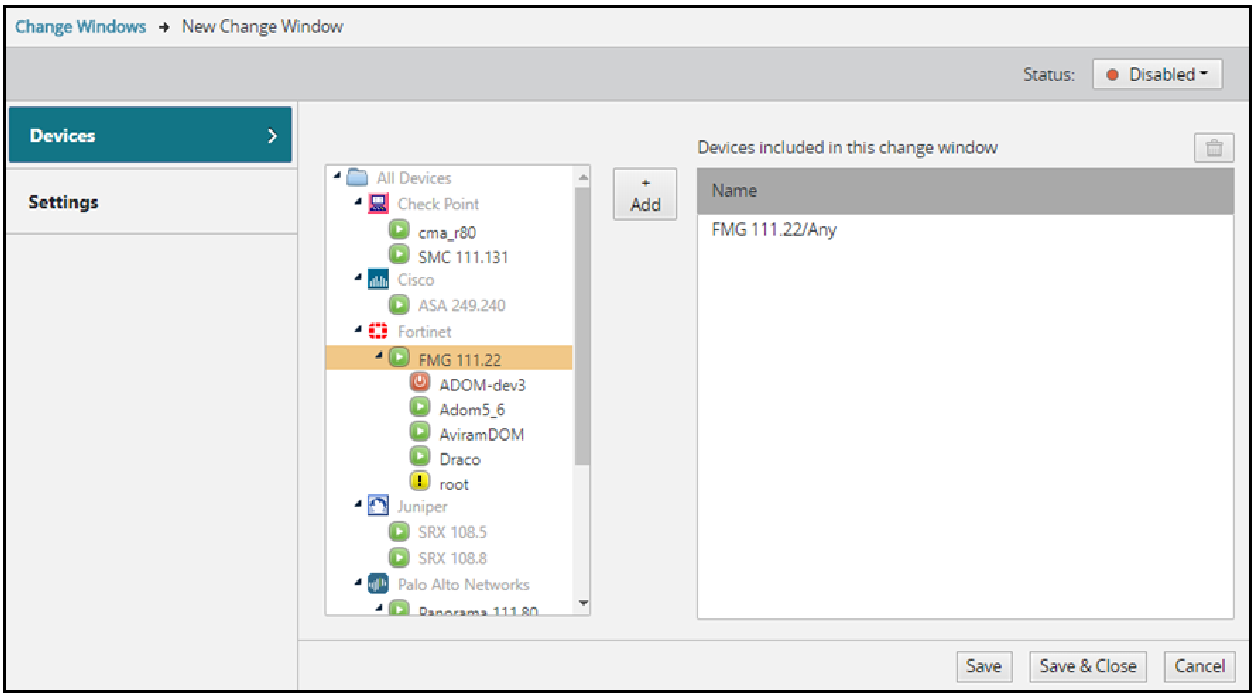
- For a selected Device Group, the policy is installed on all the firewalls associated with that Device Group.
- For a selected management device-for example, a FortiManager device in Advanced mode-all of an ADOM's policies are installed on all the firewalls associated with that policy.
- For a selected CMA device, its policies are installed on all the firewalls associated with each policy.

Best Practices

Change window creation date and recurrence

Change window duration

What am I looking at



What can I do on this page

Configure a change window for a firewall management console or per specific device:

1. Select devices to add or remove them from a change window.
2. Configure the **Settings** for a change window - **Title**, **Description**, and **Recurrence.**
3. Configure the **Status** - **Enable** or **Disable** a change window.

To Update a Change Window

1. In **Devices**, add or remove devices:

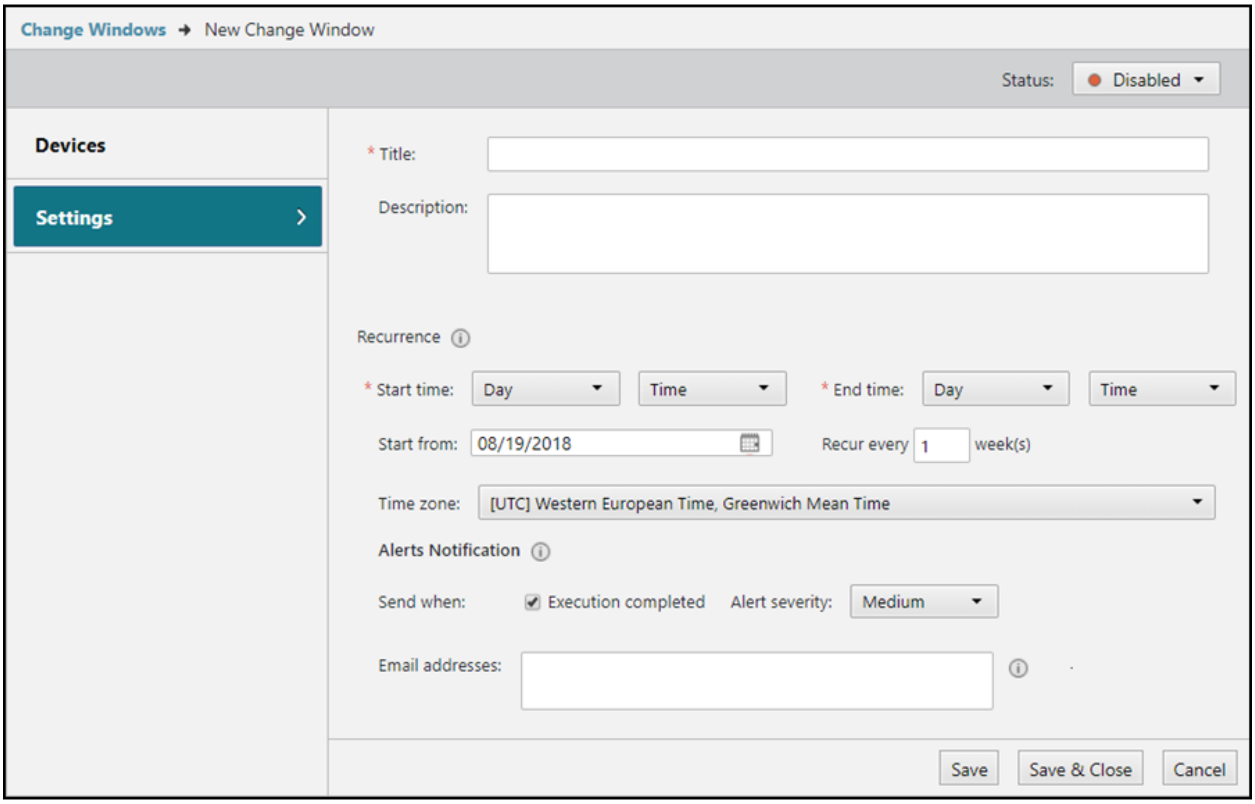
    - To add a device, select an available device for the Change Window and click + Add to move it to the list of **Devices included in this change window**.
    - To remove a device from the list of **Devices included in this change window**, select the device and click 🗑.

    In MSSP mode, select a **Domain** and then add the relevant devices.

    Use **Ctrl + Shift** to select multiple devices.

2. In **Settings**, configure the following parameters:

Change Window field	Description
Title	Mandatory text for the change window name
Description	Optional text
Recurrence	The change window will recur on the selected days of the week. A week is defined as Monday-Sunday.
Start time and End time	Recurrence: The day(s) of the week and time to start and end the change window execution
Day	The day(s) of the week to start or end the change window
Time	The time of day to start or end the change window
Start from	The starting date for the change window
Recur every_week (s)	Configure (in weeks) how frequently to run the change window
Time zone	Select the UTC time zone for the change window
Alerts Notification	Alerts are sent when the execution is completed and include a link to the SecureTrack report
Send when	Select **Execution completed** to enable email notifications
Alert severity	Select the severity for the alert: Low, Medium (default), High
Email addresses	Only SecureTrack users are allowed to access the link provided in the alert email Only valid email addresses are accepted



Change Windows ➔ New Change Window

Status: ● Disabled

Devices

Settings

* Title:

Description:

Recurrence ⓘ

* Start time: Day Time * End time: Day Time

Start from: 08/19/2018 Recur every 1 week(s)

Time zone: [UTC] Western European Time, Greenwich Mean Time

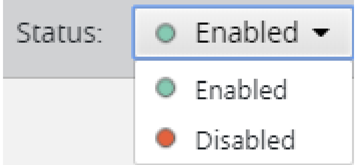
Alerts Notification ⓘ

Send when: ☑ Execution completed Alert severity: Medium

Email addresses: ⓘ

Save | Save & Close | Cancel

3. **Status**: Select **Enabled** or **Disabled** (default option) when you finish creating the new change window.
   - **Enabled** - The change window is active and will be executed at the relevant date and time
   - **Disabled** - The change window is not active and will not be executed

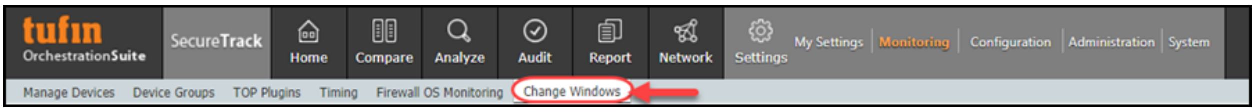


4. Click Save or Save & Close to save your changes.

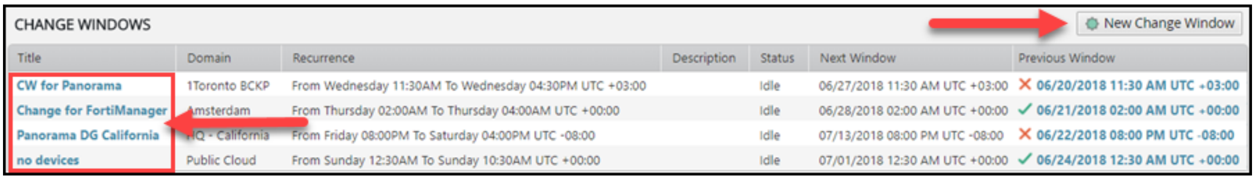
The change window is displayed as a row in the **Change Windows** table.

How Do I Get Here?

To navigate to a specific change window:



1. In SecureTrack, navigate to **Settings** > **Monitoring**.
2. Select the **Change Windows** tab.
3. Click New Change Window or click the **Title** of an existing change window.



CHANGE WINDOWS

New Change Window

Title	Domain	Recurrence	Description	Status	Next Window	Previous Window
CW for Panorama	1Toronto BCKP	From Wednesday 11:30AM To Wednesday 04:30PM UTC +03:00		Idle	06/27/2018 11:30 AM UTC +03:00	✗ 06/20/2018 11:30 AM UTC +03:00
Change for FortiManager	Amsterdam	From Thursday 02:00AM To Thursday 04:00AM UTC +00:00		Idle	06/28/2018 02:00 AM UTC +00:00	✓ 06/21/2018 02:00 AM UTC +00:00
Panorama DG California	HQ - California	From Friday 08:00PM To Saturday 04:00PM UTC -08:00		Idle	07/13/2018 08:00 PM UTC -08:00	✗ 06/22/2018 08:00 PM UTC -08:00
no devices	Public Cloud	From Sunday 12:30AM To Sunday 10:30AM UTC +00:00		Idle	07/01/2018 12:30 AM UTC +00:00	✓ 06/24/2018 12:30 AM UTC +00:00

Change Window Creation Date and Recurrence

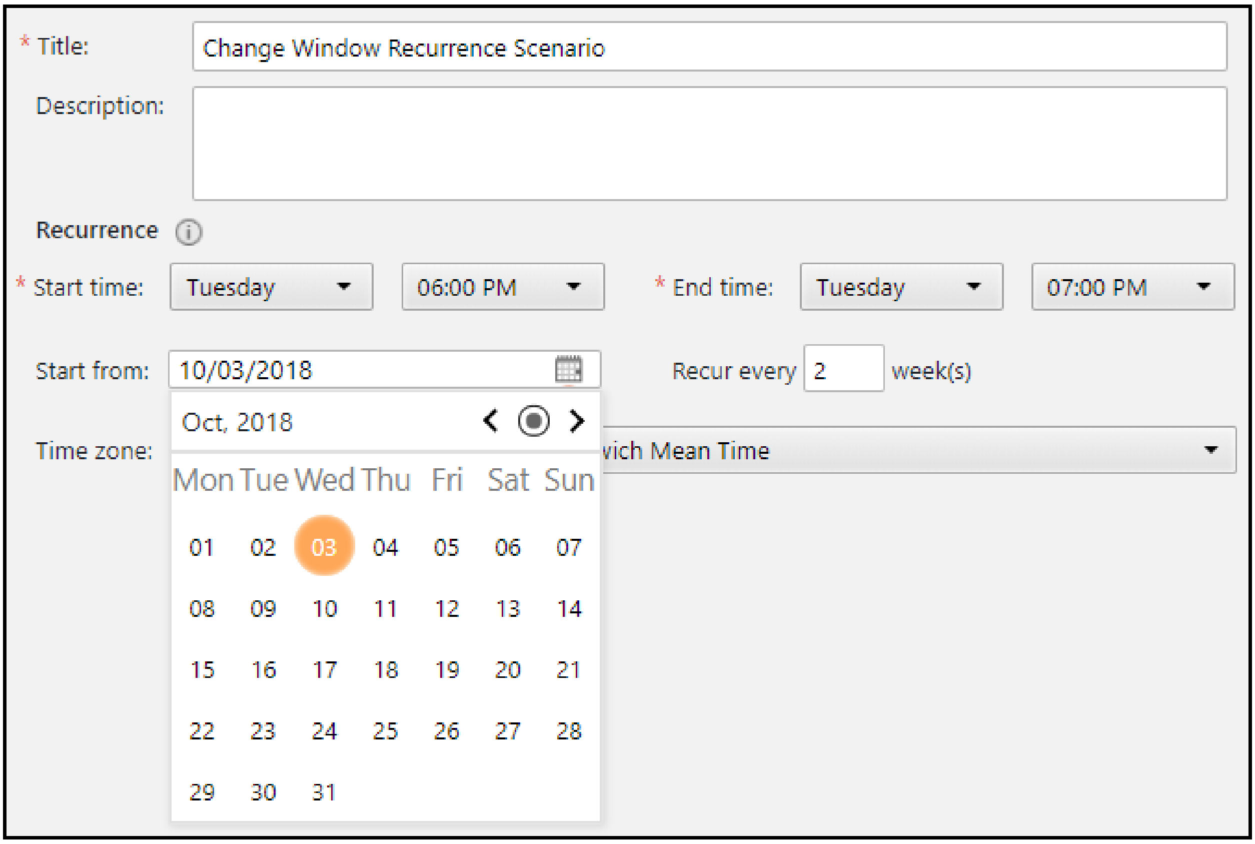
Change Window Creation Date and Recurrence Schedule

The day and date on which you create a change window affects the recurrence logic.

The first instance of a change window is assumed to be the day and time you set in **Start time**, during the work week (Monday through Sunday) of the **Start from** date. The **Next Window** instance is the day (and time) in **Start time**, according to the number of weeks you configured.

For example, consider a change window that is configured for Fridays at 6 pm, beginning October 3rd 2018, and recurring every three weeks: The change window runs for the first time on Friday, October 5th. The **Next Window** after that will be Friday, October 26th.

Consider a change window that is configured to start on a day of the week that occurs **before** the starting date. In the example below, the change window is configured for Tuesdays at 6 pm, beginning October 3rd 2018, and recurring every two weeks:



* Title: Change Window Recurrence Scenario

Description:

Recurrence

* Start time: Tuesday 06:00 PM * End time: Tuesday 07:00 PM

Start from: 10/03/2018 Recur every 2 week(s)

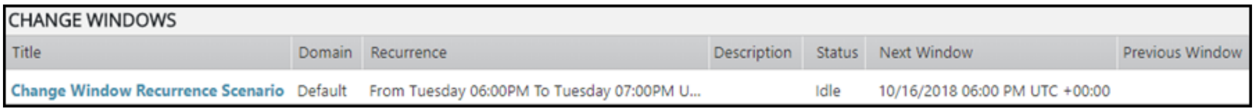
Time zone: wich Mean Time

Oct, 2018

Mon	Tue	Wed	Thu	Fri	Sat	Sun
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Even though the **Start from** date falls on Wednesday, the change window is calculated from the Tuesday of that week (October 2nd).

Therefore, the **Next Window** (and the first time the change window actually runs) occurs two weeks after the calculated starting day, on Tuesday, October 16th:



CHANGE WINDOWS

Title	Domain	Recurrence	Description	Status	Next Window	Previous Window
Change Window Recurrence Scenario	Default	From Tuesday 06:00PM To Tuesday 07:00PM U...		Idle	10/16/2018 06:00 PM UTC +00:00	

Change Window Duration

Change window duration

If the policy commit processes running in the change window exceed the allotted time, the processes that are currently in progress run to completion, and the policy commit processes that did not start are not performed. The policy commit processes will restart for all the selected devices during the next scheduled change window.

If the change window period is too short for all the processes to complete, we recommend that you edit the change window to do one of the following:

- Increase the allotted time in the **Settings**
- Split the original change window into several change windows, with fewer devices included in each change window

System Configuration

You can:

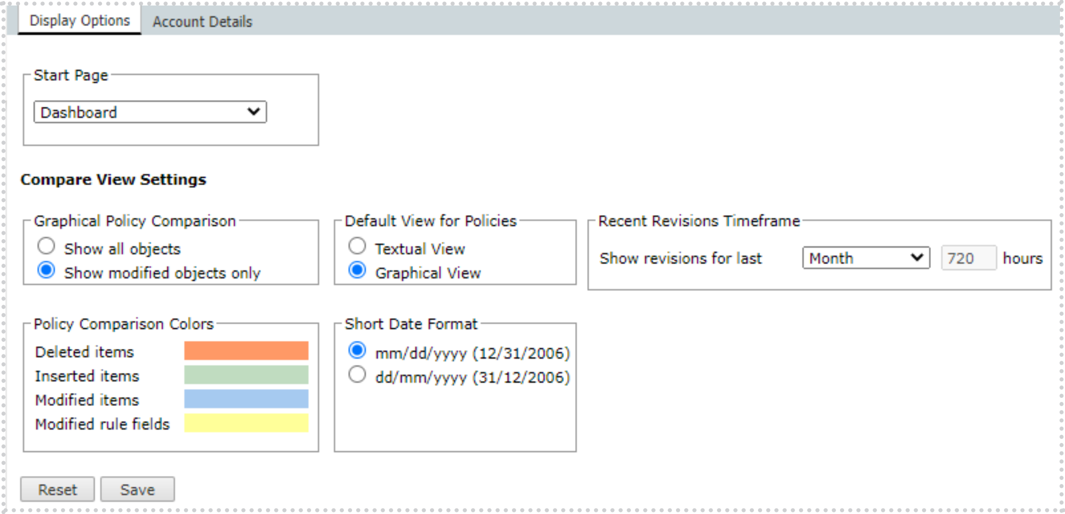
- Manage SecureTrack user authentication and notifications
- Manage data segragation by domains
- Configure linking to ticketing systems

How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration**.

Display Options

Overview



Start Page: Dashboard

Compare View Settings

Graphical Policy Comparison
○ Show all objects
● Show modified objects only

Default View for Policies
○ Textual View
● Graphical View

Recent Revisions Timeframe
Show revisions for last Month 720 hours

Policy Comparison Colors

Deleted items	🟧
Inserted items	🟩
Modified items	🟦
Modified rule fields	🟨

Short Date Format
● mm/dd/yyyy (12/31/2006)
○ dd/mm/yyyy (31/12/2006)

The **Display Options** page enables SecureTrack users to customize their viewing preferences. The settings in this page are user specific.

For changes to take effect, you must click **Save**.

What Can I Do?

Using the **Display Options** page, you can customize your viewing preferences as follows:

- Define the SecureTrack start page
- Customize which objects are displayed in policy comparison
- Customize the policy comparison colors
- Customize the time period used to determine recent revisions
- Customize the default view for non-Check Point policies
- Customize the short date format

Define the SecureTrack Start Page

- In the **Start Page** drop-down menu, select which page you want to appear when logging into SecureTrack:
  - **Compare**
  - **Policy Analysis**
  - **Compliance Alerts**
  - **General Reports**
  - **Reports Repository**

Customize Which Options are Displayed in Policy Comparison

- In the **Graphical Policy** section, select one of the following:
  - **Show all objects**: All objects in the policy are shown.
  - **Show modified objects only**: Only added, deleted or modified objects are shown.

    This setting does not affect the display of rule bases, which are always fully displayed. All rules are shown, including those that were not modified.

Customize the Policy Comparison Colors

In policy comparison, SecureTrack displays graphical differences between policy revisions by marking the changed rules and objects using different colors.

To customize the colors:

- In the **Policy Comparison Colors** section, choose custom colors for **Deleted items**, **Inserted items**, **Modified items** and **Modified rule fields**.

Customize The Time Period for Determining Recent Revisions

Because SecureTrack can store policy revisions back for several years, the revisions list can become quite large, while SecureTrack users are usually interested in examining the most recent policy changes.

The revisions list displayed for each device shows only the recent revisions, and uses the setting **Show revisions for last...** to filter recent revisions from older revisions. The default period is 72 hours.

To customize this time period:

- In **Recent Revisions Timeframe** > **Show revisions for last**, select the time period to be used for determining recent revisions.

> **Compare View** has its own filter settings, which override the settings here. To revert to the settings here, in **Compare View**, click **Reset filter**.

Customize The Default View for Non-Check Point Policies

Many firewall administrators are more accustomed to viewing firewall configuration in textual format (raw access lists) rather than in a graphical rulebase format. SecureTrack displays non-Check Point policies in both textual and graphical views. You can customize which view is used by default when logging into SecureTrack.

To customize the default view for non-Check Point policies:

- In the **Default View for Policies** section, select one of the following:
  - **Textual View**
  - **Graphical View**

Customize The Short Date Format

In the **Short Date Format** section, select one of the following:

- **mm/dd/yyyy**
- **dd/mm/yyyy**

How Do I Get Here?

User Display Options are located in: **Settings** > **My Settings** > **Display Options**.

Managing TOS Classic Users

- Overview
- What Can I Do Here?
- How Do I Get Here?

Overview

All users can change their own account details. Only administrators can add, change and delete other user accounts.

Types of User - Single Domain

By default, all users and devices belong to a single domain. there are two types of users:

- **Administrator**
- **User**

All users can manage policy revisions, and configure and run queries, audits, and reports, for their assigned devices.

The following actions are available only to administrators:

- Configure system-level settings such as users and Network zones.
- Add or configure monitored devices.
- Assign Users specific devices in the organization's deployment.
- Administrative supervision over other users' queries, audits and reports.

Types of User - Multi-Domain

If you have configured your system for multi-domains, the two types of user are replaced by four different types of users:

- **Super Administrator**
- **Multi-Domain Administrator**
- **Multi-Domain User**
- **Domain User**

After the first additional (non-default) Domain is defined, existing administrators become Super Administrators and existing users become Multi-Domain Users. The scope of each is shown below.

		Permitted actions (within permission scope)		
	Permission scope	**System-level configuration, and Unified Security Policy**	**Users Devices Zones Edit Topology View Topology**	**Policy Mgmt Auditing Analysis Reporting**
Super Administrator	All	✓	✓	✓
Multi-Domain Administrator	One or more domains	✓ Configure/Create intra-domain USPs only.	✓ Configure Domain Users only. For default Domain, only edit Topology.	✓
Multi-Domain User	One or more domains			✓
Domain User	One domain			✓

- Super Administrator - Full permissions, for all Domains, and for all SecureTrack actions including system-level configuration and Unified Security Policy.
- Multi-Domain Administrator - Defined by Super Administrator and given permission for one or more specified Domains (including any devices to be added in the future to the Domain), including (optionally) the default Domain. For devices in any of these Domains, can perform policy management, analysis, auditing, and reporting, and can view and modify the Topology. For any of these Domains except the default Domain, can configure device monitoring, Domain Users, and Network zones.
- Multi-Domain User - Defined by Super Administrator and given permission for one or more specified monitored devices (group-selectable by Domain, but applying only to currently configured devices). For these devices, can perform policy management, analysis, auditing, and reporting.
- Domain User - Defined by Administrator (Super or Multi-Domain) and given permission for one specified Domain (not the default Domain). For this Domain, can perform policy management, analysis, auditing, and reporting.

Administrators have administrative supervision over other users' reports, queries, and audits.

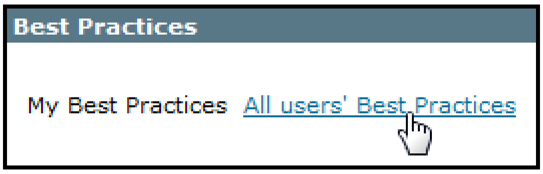
Managing Users in a Multi-Domain Environment

In a Multi-Domain environment, a Multi-Domain Administrator who wants to add or configure a Domain User must be in the context for that Domain. A Super Administrator who wants to add or configure a Multi-Domain Administrator for more than one Domain, or a Multi-Domain User, or another Super Administrator, must be in the Global context (All Domains).

Administrative Supervision

SecureTrack Administrators can manage reports, queries, audits, and alerts that were created by Users and by other Administrators. This includes viewing, running, and editing the output (scheduling and recipients). Regular Users can only see reports that they themselves created.

In the various reports, analysis, and audit pages in SecureTrack, logged-in Administrators can select only reports, queries, or alerts that they created, or all available ones. For example:



Best Practices

My Best Practices All users' Best Practices

If you have configured your system for managing multi-domains, reports (configured and generated), queries, audits, and alerts are only available for the domains in which they were created. Super Administrators can manage any reports (in the domain contexts in which they were created). Multi-Domain Administrators have administrative supervision only in Domain contexts for which they have permissions (but not in the Global context), over reports created by other Multi-Domain Administrators and by Domain Users (but not over reports created by Super Administrators or by Multi-Domain Users).

What Can I Do Here?

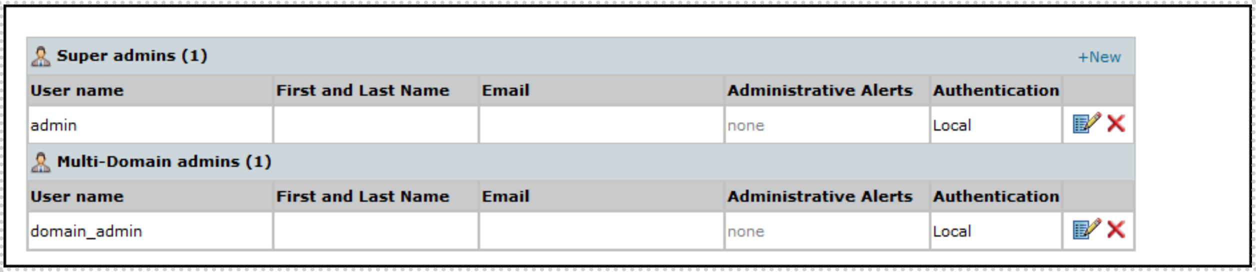
- Manage your own account
- Add a new user
- Edit a user
- Add an administrator using st_add_user

Manage Your Own Account

You can change some details of your own user account, including your name, email address, enable or disable administrative alerts, and your password.

Add a New User

Existing users are listed. From the list, you can Edit (📝) a user's properties, or Delete (✗) a user:



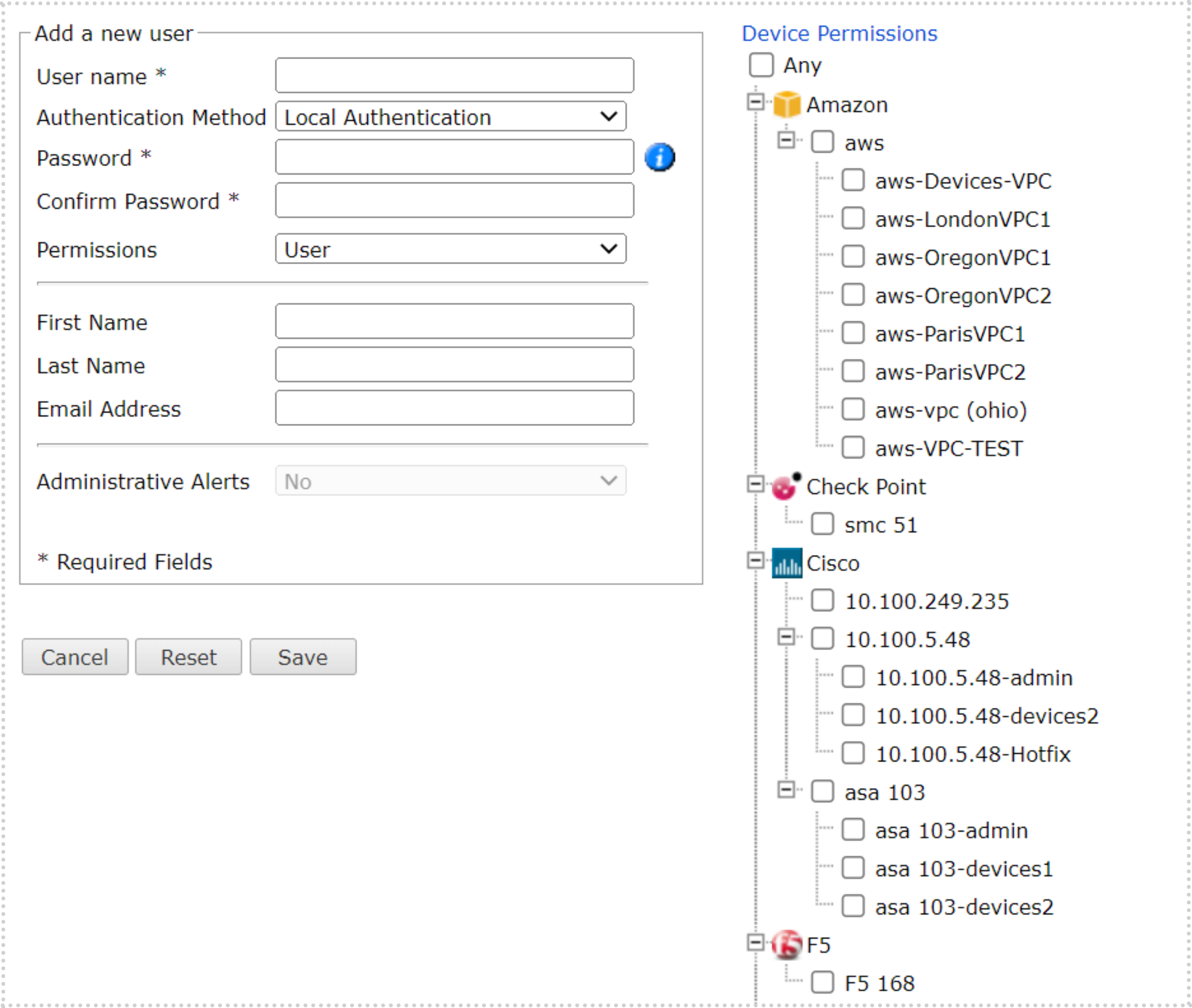
Super admins (1) +New

User name	First and Last Name	Email	Administrative Alerts	Authentication	
admin			none	Local	📝 ✗

Multi-Domain admins (1)

User name	First and Last Name	Email	Administrative Alerts	Authentication	
domain_admin			none	Local	📝 ✗

To add a user, click **New**. The new user's properties appear:



Add a new user

User name *	
Authentication Method	Local Authentication
Password *	
Confirm Password *	
Permissions	User
First Name	
Last Name	
Email Address	
Administrative Alerts	No

* Required Fields

Device Permissions

- ☐ Any
- Amazon
  - ☐ aws
    - ☐ aws-Devices-VPC
    - ☐ aws-LondonVPC1
    - ☐ aws-OregonVPC1
    - ☐ aws-OregonVPC2
    - ☐ aws-ParisVPC1
    - ☐ aws-ParisVPC2
    - ☐ aws-vpc (ohio)
    - ☐ aws-VPC-TEST
- Check Point
  - ☐ smc 51
- Cisco
  - ☐ 10.100.249.235
  - ☐ 10.100.5.48
    - ☐ 10.100.5.48-admin
    - ☐ 10.100.5.48-devices2
    - ☐ 10.100.5.48-Hotfix
  - ☐ asa 103
    - ☐ asa 103-admin
    - ☐ asa 103-devices1
    - ☐ asa 103-devices2
- F5
  - ☐ F5 168

Available options under **Device Permissions** depend on the selected user type (**Permissions**) and, in a Multi-Domain environment, on the current context.

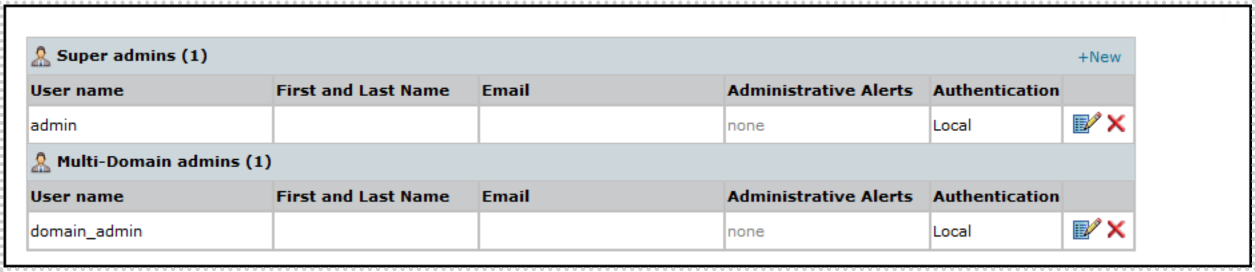
In a Multi-Domain environment, when adding or configuring a Multi-Domain User, devices are categorized and selectable by Domain, but the actual permissions are defined by device. Even when a whole Domain is selected, permissions are not automatically applied to devices added in the future.

- In the First Name and Last Name fields, the following characters are allowed: Characters in all languages, integers **0-9**, special characters **+ -_ # @ . , : = ! ^ ( )** and blank spaces.
- **Authentication Method** is either **Local** (the password is defined here), **SSO Authentication** , **RADIUS** or **TACACS+**. If you select RADIUS or TACACS+, make sure the user's name here exactly matches the name in the RADIUS or TACACS+ server.
- **Permissions** define the user type. Available options depend on whether or not multi-domain is configured, on the current domain context (Global or selected domain) and on the type of the logged-in user.
- An **Email Address** is required for notifications, alerts, and reports. The Email field must be in the standard email format
- **Administrative Alerts** can also be enabled from the **Notifications** page.

Click **Save** to add the user. The new user will be prompted to reset the password when logging in to the TOS Classic UI for the first time and must do so before performing other functions such as running REST APIs and connecting from SecureChange.

Edit a User

All existing users are displayed. Click to Edit (✎) a user's properties, or Delete (✗) a user:



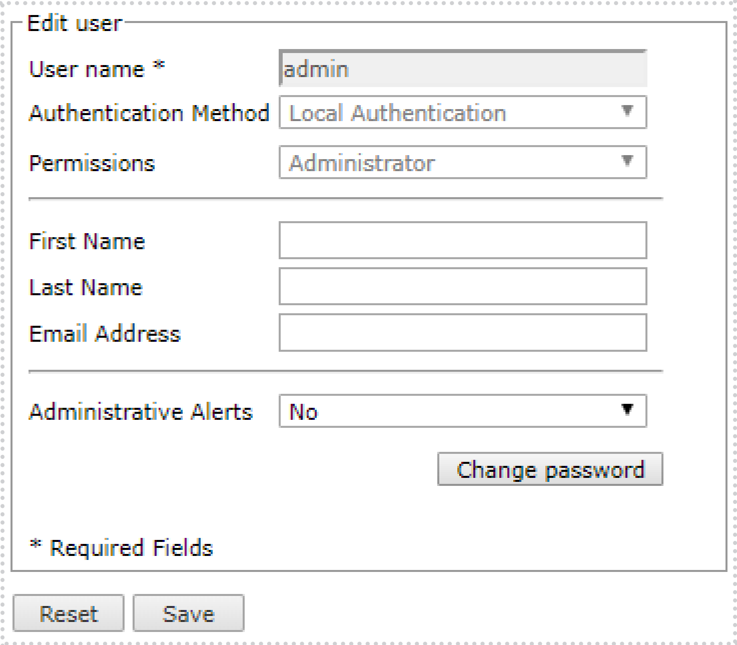
Super admins (1) +New

User name	First and Last Name	Email	Administrative Alerts	Authentication	
admin			none	Local	

Multi-Domain admins (1)

User name	First and Last Name	Email	Administrative Alerts	Authentication	
domain_admin			none	Local	

User details:



Edit user

User name *	admin
Authentication Method	Local Authentication
Permissions	Administrator
First Name	
Last Name	
Email Address	
Administrative Alerts	No

Make changes and click **Save** to update the user. If you change the password, the user will be prompted to reset the password when next logging in to the TOS Classic UI and must do so before performing other functions such as running REST APIs and connecting from SecureChange.

How Do I Get Here?

To manage other user accounts: In TOS Classic, go to **Settings** > **Configuration** > **Users**.

To manage your own account: In TOS Classic, go to **Settings** > **My Settings** > **Account Details**.

Create a New SecureTrack Administrator Username

The original SecureTrack administrator username and password created when the initial setup wizard was run is required for certain configuration settings. If you do not know the username or password, you can create a new administrator username.

To create a new administrator username

1. Connect to the remote server via SSH.
2. Run the `st_add_user` command and follow the instructions in the wizard.

   [root@TufinOS ~]# **st_add_user**

   Username: **<username>**

   Password: **<pwd>**

   Confirm Password: **<pwd>**

   Admin user <username> is added.

User Authentication

Overview

TOS Classic supports these methods of user authentication (in the following order):

- Local (the password is defined in TOS Classic)
- External server:
  - LDAP (Active Directory)
  - TACACS+
  - RADIUS
- SSO Authentication Service:
  - SAML (Contact Support for setup assistance)

TOS Classic users do not need to use the same authentication methods because TOS Classic recognizes different authentication methods for different users.

For authentication methods, Local, TACAS+ and RADIUS, usernames can contain all alphanumeric characters and these special characters: **@ - + . _**

When TOS Classic is configured to use LDAP, TOS Classic users defined in the LDAP are automatically imported to TOS Classic, and use only LDAP authentication. Their permission types (Administrator or User) are also defined by their LDAP groups. Device permissions for Users are defined in TOS Classic.

Other users are defined locally in TOS Classic. For these users, you can define whether their authentication method is **Local**, **RADIUS** or **TACACS+**, as part of the user's configuration. Their permission types (Administrator or User) are defined in TOS Classic, not in RADIUS or TACACS+.

Use External LDAP Authentication

Configure TOS Classic to use Active Directory for LDAP Authentication, and use the automatically imported LDAP users

Create and Configure a Custom LDAP for External Authentication of TOS Classic Users

See the Tech Note Configuring a new LDAP vendor for TOS Classic.

Use External RADIUS or TACACS+ Authentication

Configure TOS Classic to use RADIUS or TACACS+, and define users in TOS Classic with the authentication method set to RADIUS or TACACS+.

Use SSO Authentication Service

Contact Support to configure TOS Classic to use SSO Authentication, and define users in TOS Classic with the authentication method set to SSO Authentication.

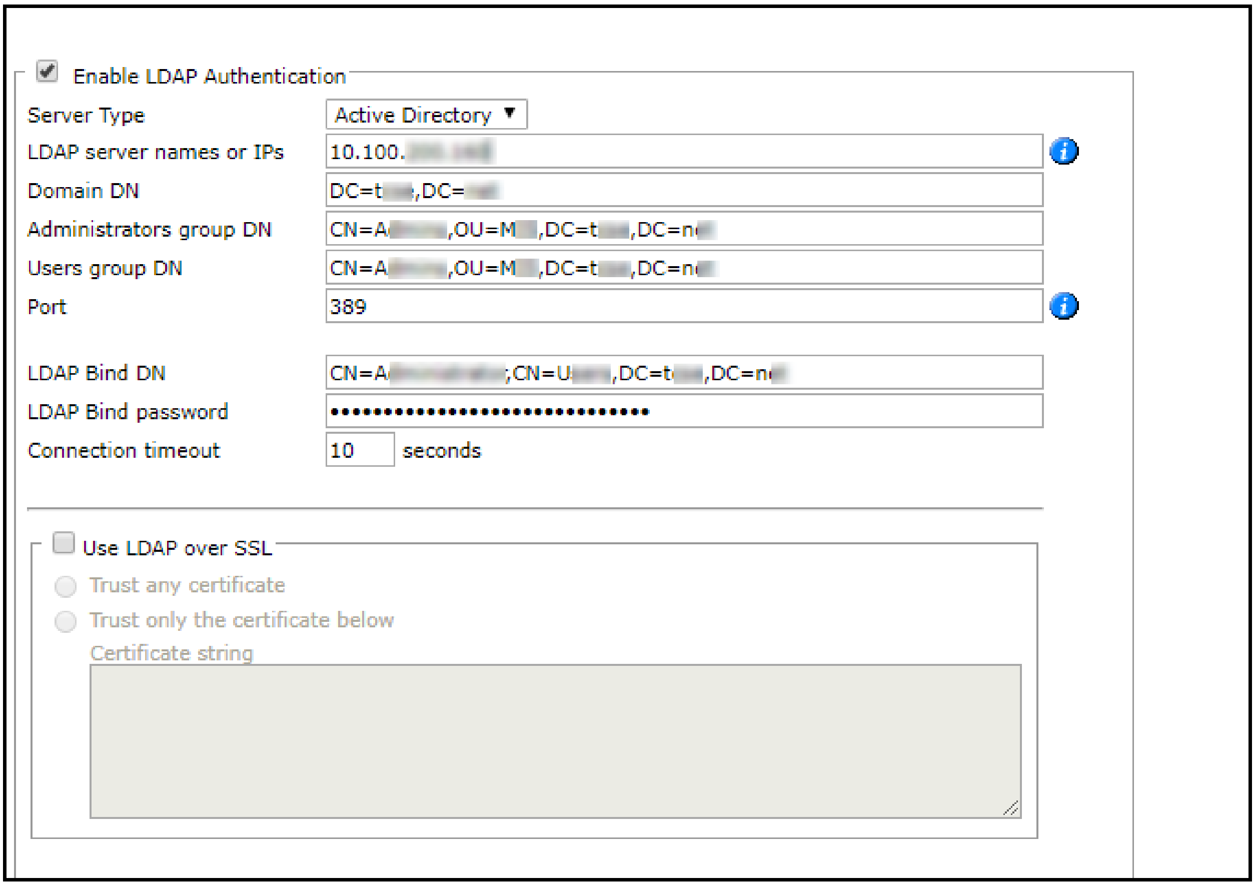
Configuring LDAP (Active Directory) Authentication

SecureTrack supports LDAP external authentication of users, when installed on Red Hat or CentOS Linux, or on TufinOS (Tufin appliance). Microsoft Active Directory 2000, 2003, 2008,2008, 2012, and 2016 are supported. SecureTrack uses TLS 1.2, 1.1, and 1.0 to negotiate SSL/TLS with the LDAPS server for authentication, and uses LDAP version 3 as the protocol to perform administrative binds and retrieve attributes.

To configure SecureTrack to use Active Directory

1. In Active Directory, configure two groups: One for SecureTrack Administrators, and the other for SecureTrack Users.
2. Add the relevant Active Directory users to each group: users who should receive Administrative permissions for SecureTrack - to the Administrators group, and other users - to the Users group.

   If you have configured your system for managing multi-domains, users in the SecureTrack Administrators group will initially be Super Administrators; they can subsequently be changed in the Users page to Multi-Domain Administrators. Users in the SecureTrack Users group will initially be Multi-Domain Users; they can subsequently be changed in the Users page to Domain Users.
3. In **Settings** view, select the **Configuration** tab.
4. Select **External Authentication**, and select **Enable LDAP Authentication**:



☑ Enable LDAP Authentication

Server Type	Active Directory ▼
LDAP server names or IPs	10.100.[redacted]
Domain DN	DC=t[redacted],DC=[redacted]
Administrators group DN	CN=A[redacted],OU=M[redacted],DC=t[redacted],DC=n[redacted]
Users group DN	CN=A[redacted],OU=M[redacted],DC=t[redacted],DC=n[redacted]
Port	389
LDAP Bind DN	CN=A[redacted];CN=U[redacted],DC=t[redacted],DC=n[redacted]
LDAP Bind password	••••••••••••••••••••••••••••••
Connection timeout	10 seconds

☐ Use LDAP over SSL

○ Trust any certificate

○ Trust only the certificate below

Certificate string

5. Configure the following values:
   - **LDAP server names or IP**: Resolvable hostname or address of the Active Directory server.

     When you use LDAP over SSL, enter the name the value from the 'Issued To' field of the server certificate.
     For LDAP server redundancy, enter multiple server names or IP addresses separated by a space or a comma.
   - **Domain DN**: The domain's Distinguished Name (also known as Base DN). Make sure to use the DN of the desired Domain DN root.
   - **Administrators group DN**: The Distinguished Name (DN) of the SecureTrack Administrators group on the Active Directory.
   - **Users group DN**: The Distinguished Name (DN) of the SecureTrack Users group on the Active Directory.
   - The **Port** used by Active Directory, according to the following table:

Active Directory Configuration	Regular LDAP (no SSL)	Encrypted LDAP (SSL)
Standalone	389	636
Global Catalog	3268	3269

   - **LDAP Bind DN**: LDAP user that has permission to read all LDAP objects and attributes that exist in the LDAP base DN.

     This field should always contain a value.
   - **LDAP Bind password**: Password of the LDAP Bind DN.
   - **Connection timeout**: The number of minutes that the authenticated connection is available before it must re-authenticate.
6. To use LDAP over SSL, select **Use LDAP over SSL** and select either:
   - **Trust any certificate** - Automatically accept the certificate presented by the Active Directory server, such as a self-signed certificate.
   - **Trust only the certificate below** - In the **Certificate string** box, paste the public key (certificate) from the Active Directory server.
7. Click **Save**.

When each LDAP user logs in for the first time, SecureTrack automatically generates a matching local user account with default settings according to user type (Domain admin or User) as set by group membership. For Users, default settings include no device permissions. An Administrator (in the Multi-Domain scheme: a Super Administrator) must then assign permissions for the domains.

How Do I Get Here?

In SecureTrack, go to **Admin** ⚙ **> External Authentication**.

Configuring a new SecureTrack LDAP Vendor

You can create a custom LDAP for external authentication of users by adding and editing the desired LDAP server attributes:

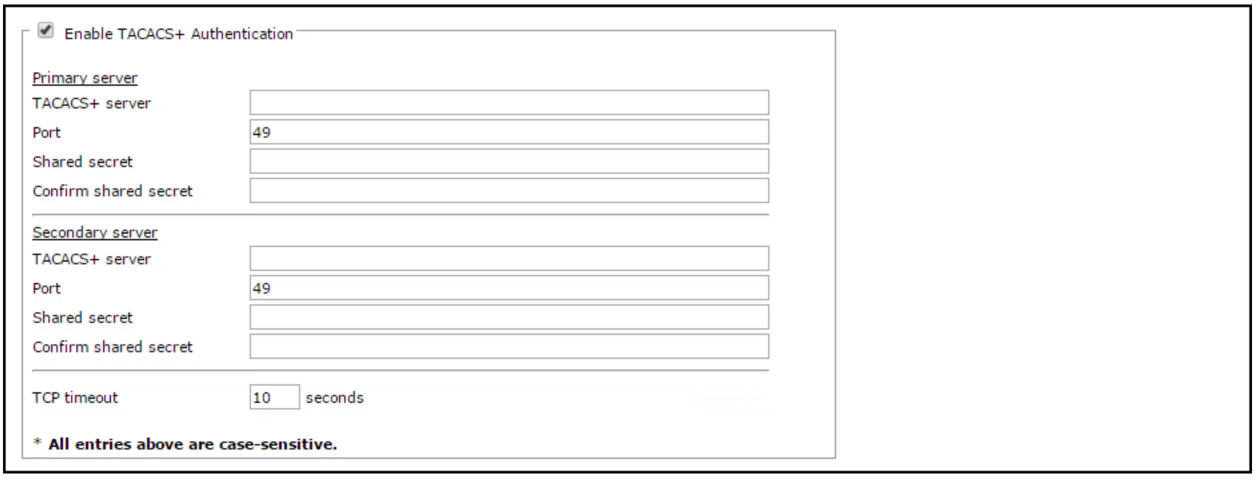
1. Retrieve the configuration for all available LDAPs or for a specific LDAP.
2. Configure the LDAP vendor attributes.

Configuring TACACS+ Authentication

SecureTrack supports TACACS+ external authentication of users.

To configure SecureTrack to use TACACS+ authentication:

1. Select **Enable TACACS+ Authentication**:



☑ Enable TACACS+ Authentication

Primary server

TACACS+ server	
Port	49
Shared secret	
Confirm shared secret	

Secondary server

TACACS+ server	
Port	49
Shared secret	
Confirm shared secret	

TCP timeout 10 seconds

* **All entries above are case-sensitive.**

2. For each TACACS+ server in the organization (**Primary** and **Secondary**), enter the server details that you get from your organizational RADIUS administrator:
   - **TACACS+ server**: The resolvable name or IP address of the TACACS+ server.
   - **Port** number
   - **Shared secret**: The password for SecureTrack to access the TACACS+ server.
3. Define the **TCP timeout**: The number of seconds SecureTrack tries to connect to the TACACS+ server before giving up.
4. Click **Save**.

Users that are configured to use TACACS+ authentication can login.

How Do I Get Here?

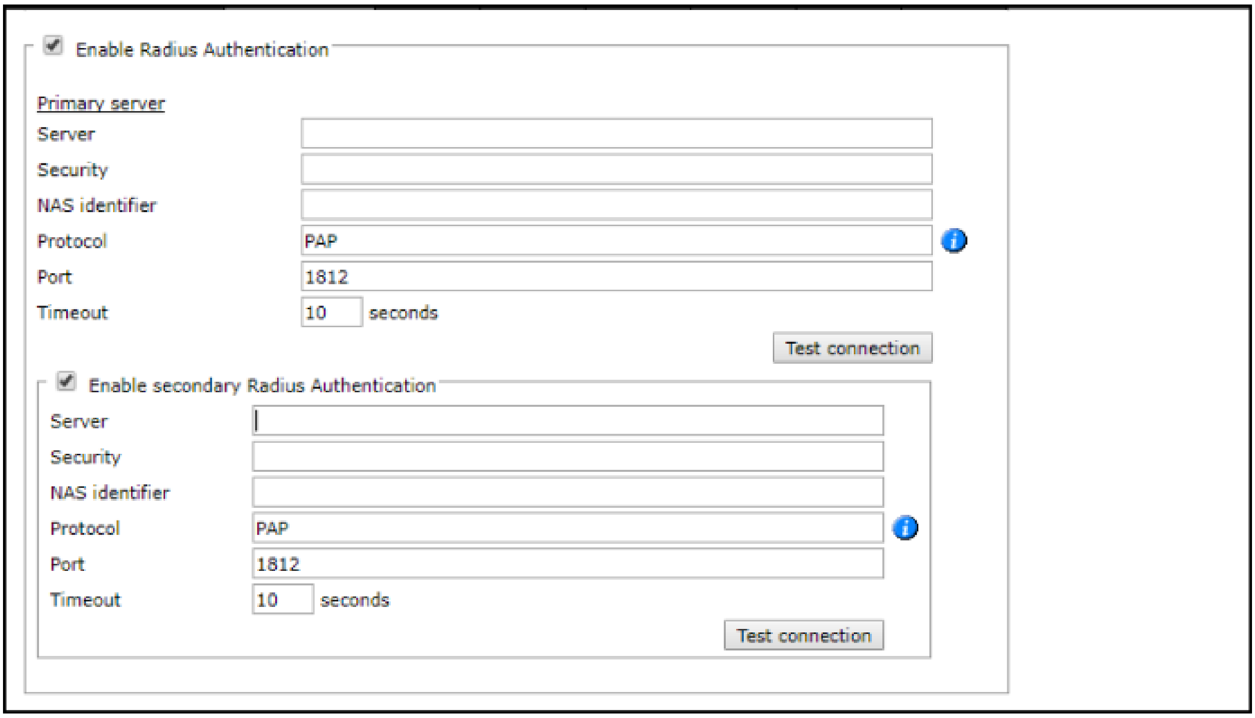
In SecureTrack, go to **Settings** > **Configuration > External Authentication**.

Configuring RADIUS Authentication

SecureTrack supports RADIUS external authentication of users.

To configure SecureTrack to use RADIUS authentication:

1. Select **Enable RADIUS Authentication**:



☑ Enable Radius Authentication

Primary server

Server	
Security	
NAS identifier	
Protocol	PAP
Port	1812
Timeout	10 seconds

☑ Enable secondary Radius Authentication

Server	
Security	
NAS identifier	
Protocol	PAP
Port	1812
Timeout	10 seconds

2. For each RADIUS server in the organization (**Primary** and **Secondary**), enter the server details that you get from your organizational RADIUS administrator:
   - **Server**: The resolvable name or IP address of the RADIUS server.
   - **Security**: The password for SecureTrack to access the RADIUS server.
   - **NAS identifier**: Identifier configured on the RADIUS server, which will be included with all user authentication requests. If empty, the IP address of the SecureTrack will be used.
   - **Protocol**: Enter one of the following supported values: PAP, CHAP, EAPMD5, EAPMSCHAPv2, MSCHAPv1, or MSCHAPv2
   - **Port**: Port number
   - **Timeout**: The number of seconds SecureTrack tries to connect to the RADIUS server before giving up.
3. Click **Test Connection** to make sure that SecureTrack successfully connects to the RADIUS server.
4. Click **Save**.

Users that are configured to use RADIUS authentication can login.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration > External Authentication**.

SSH to RADIUS Configuration

You can enable RADIUS authentication for SSH in TufinOS (version 2.8 or higher), so that SSH users authenticate with an existing Radius server. With RADIUS authentication enabled, you can add RADIUS users to TufinOS.

To allow these users to run Tufin commands, configure Sudo for the TufinOS users.

Prerequisites

- You must have a correctly configured RADIUS server
- In your /etc/hosts file, your host name must be specified with the correct interface IP

Configuration

1. To edit the SSH authentication configuration, enter:

```
vi /etc/pam.d/sshd
```

2. After the line auth required pam_sepermit.so, add the following line:

   ```
   auth sufficient pam_radius_auth.so
   ```

   The result file will be as showing below:

   ```
   #%PAM-1.0
   auth required pam_sepermit.so
   auth sufficient pam_radius_auth.so
   ```

3. To add the Radius server IP address and secret, enter:

   ```
   vi /etc/raddb/server
   ```

   If the file /etc/raddb/server does not exist, create the file and change the permissions with the following command:

   ```
   chmod 0600 /etc/raddb/server
   ```

4. Add the following line to the file /etc/raddb/server:

   ```
   <radius_ip> <secret> 3
   ```

5. To restart the SSHD service, enter:

   ```
   systemctl restart sshd
   ```

6. Run this command for each RADIUS user:

   ```
   useradd <username>
   ```

Sudo Setup and Configuration Instructions

Configuration of sudo lets a non-root user run Tufin commands with root privileges. This lets you to keep the root password secret and lets you audit TufinOS commands.

Important Security Warning: Each user that is configured in sudo can run any command with root privileges.

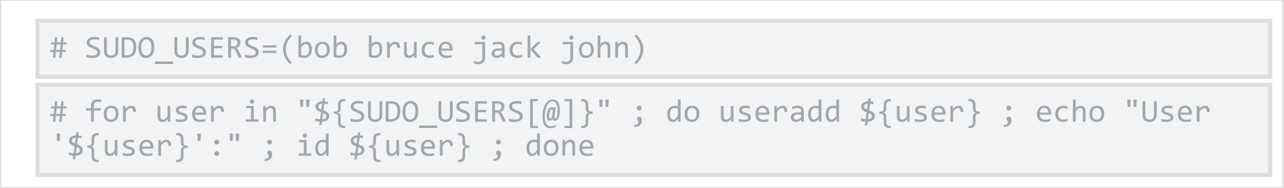
We recommend that you configure users to run Tufin commands only.

sudo commands will require a user password. In case a root-related command is being executed, you will be prompted for the root password.

Preparation

1. Login as root user to a machine with installed TOS.
2. Add RADIUS users without passwords that will use sudo:

   The username MUST NOT contain the strings: 'tufin', 'st', 'tomcat', 'jboss'
3. To give the users rights for sudo, run this command with the names of the users:

   ```
   # SUDO_USERS=(bob bruce jack john)
   ```

   ```
   # for user in "${SUDO_USERS[@]}" ; do useradd ${user} ; echo "User
   '${user}':" ; id ${user} ; done
   ```
4. Extract the archive file `sudo_tufin.tgz` located in:

/opt/tufin/share/docs/examples/sudo_configuration/:

```
# cd /opt/tufin/share/docs/examples/sudo_configuration/
# tar xvzf sudo_tufin.tgz --directory /etc/sudoers.d/
```

5. Check the correctness of sudo syntax:

```
# visudo -c
```

   You should get "parsed OK" for each sudo file.

Usage

1. Pre-configured users:
   - 'bob', 'bruce' are in one group (file: /etc/sudoers.d/tufin_commands ; group: LIMITED_FOR_TUFIN_CMD) to only run Tufin-defined commands as root user.
   - 'jack', 'john' are in one group (file: /etc/sudoers.d/all_commands ; group: USERS_FOR_ALL_CMD) to run all commands as root user.
2. Two methods to login:
   - (Preferred method) Login as one of the users in different terminal (the user shell should be parent shell for all subshells) and run commands with sudo.
   - (Alternative method) If you are logged in as root, then you can login any user from same terminal with the following command:

```
# su - user
```

3. Using of sudo command:

```
sudo <command> [command parameter]
```

4. To track a user that runs sudo commands, login as root in another terminal and run:

```
# tail -f /var/log/secure
```

   The output is shown in this format:

```
Feb 3 14:07:19 ha-test1 sudo: bob : TTY=pts/0 ; PWD=/home/bob ; USER=root ;
COMMAND=/usr/sbin/st stat
Feb 3 14:07:28 ha-test1 sudo: bob : command not allowed ; TTY=pts/0 ; PWD=/home/bob ; USER=root
; COMMAND=/sbin/fdisk -l
```

Configuring sudo

Always edit sudo files with 'visudo' editor to prevent mistakes in sudo syntax.

1. Configuring all commands (Note: It is already pre-configured for users: 'jack', 'john'):
   a. To add an existing Linux user to sudo, add the new user to /etc/sudoers.d/all_commands file:

```
# visudo -f /etc/sudoers.d/all_commands
User_Alias USERS_FOR_ALL_CMD = jack, john, new_user
```

   b. Allow the user to run all commands as root user:

```
# visudo -f /etc/sudoers.d/all_commands
USERS_FOR_ALL_CMD ALL=(ALL) NOPASSWD: ALL
```

2. Configuring Tufin-defined commands only (Note: It is already pre-configured for users: 'bob', 'bruce'):

    a. To add an existing Linux user to sudo, add the new user to `/etc/sudoers.d/tufin_commands` file:

    ```
    # visudo -f /etc/sudoers.d/tufin_commands
    User_Alias LIMITED_FOR_TUFIN_CMD = bob, bruce, new_user
    ```

    b. Add specific commands to run as root user (The pre-configured example to run: tos, tss, hactl, st and scw commands):

    ```
    # visudo -f /etc/sudoers.d/tufin_commands
    Cmnd_Alias TUFIN_CMD = /usr/sbin/t?s [[\:alpha\:]-]*,
    /usr/sbin/hactl [[\:alpha\:]-]*, /usr/sbin/st [[\:alpha\:]-]*,
    /usr/sbin/scw [[\:alpha\:]-]*
    /bin/sh /opt/tufin/securitysuite/scripts/set_disclaimer.sh --*
    *, \
    /bin/sh /opt/tufin/securitysuite/scripts/manage_ldap_vendor_
    configuration.sh --* *, \
    /usr/sbin/st_add_user
    LIMITED_FOR_TUFIN_CMD ALL=(root:root) NOPASSWD: TUFIN_CMD
    ```

    You can customize the examples in these pre-configured sudo files:

    ```
    /etc/sudoers.d/all_commands
    ```

    ```
    /etc/sudoers.d/tufin_commands
    ```

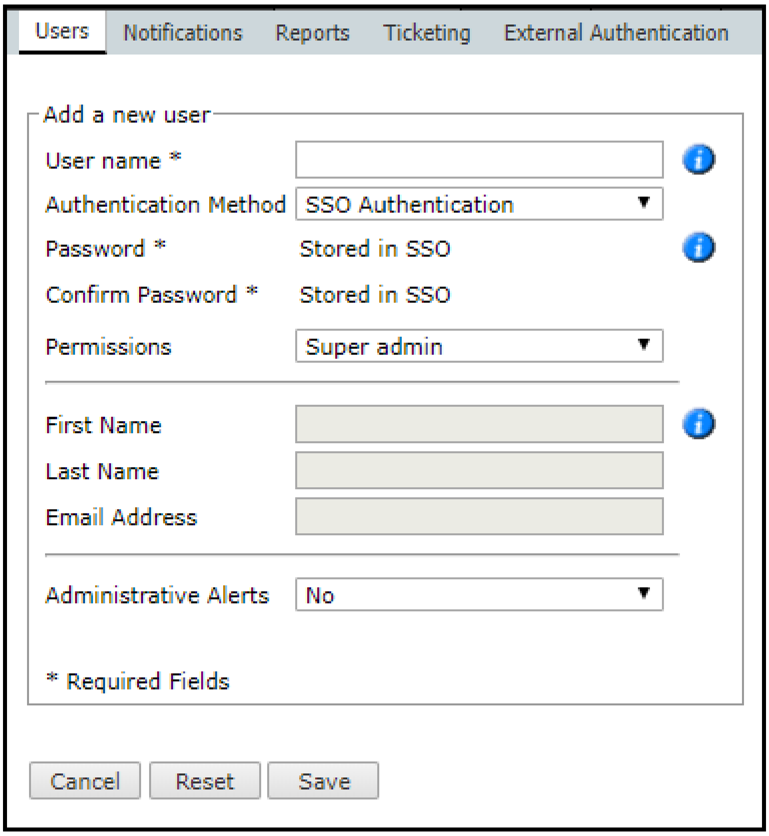
Configuring SSO Authentication Service

To have SSO Authentication service configured, please see Configuring Tufin Orchestration Suite for Single Sign On (SSO) - Okta and Azure.

Once the SSO Authentication service is configured you can add users to have SSO Authentication. Upon authentication, data is imported into SecureTrack from the SSO Authentication service.

Create Users Manually

1. To add a local user, click **New**. The new user's properties is displayed.



Add a new user

User name *

Authentication Method: SSO Authentication

Password *: Stored in SSO

Confirm Password *: Stored in SSO

Permissions: Super admin

First Name

Last Name

Email Address

Administrative Alerts: No

* Required Fields

For a general explanation of the fields see Managing SecureTrack Users.

Note the following regarding the field entries:

- **User name**: User names in SSO authentication are case-insensitive and are saved as lower case. The user name entered here must be the same as the user name stored in the SSO Authentication service, otherwise the login will fail.
- **First Name**, **Last Name**, **Email Address**: These fields are populated into SecureTrack from the SSO Authentication service upon authentication.
- **Administrative Alerts**: This field can only be configured after a user is authenticated.

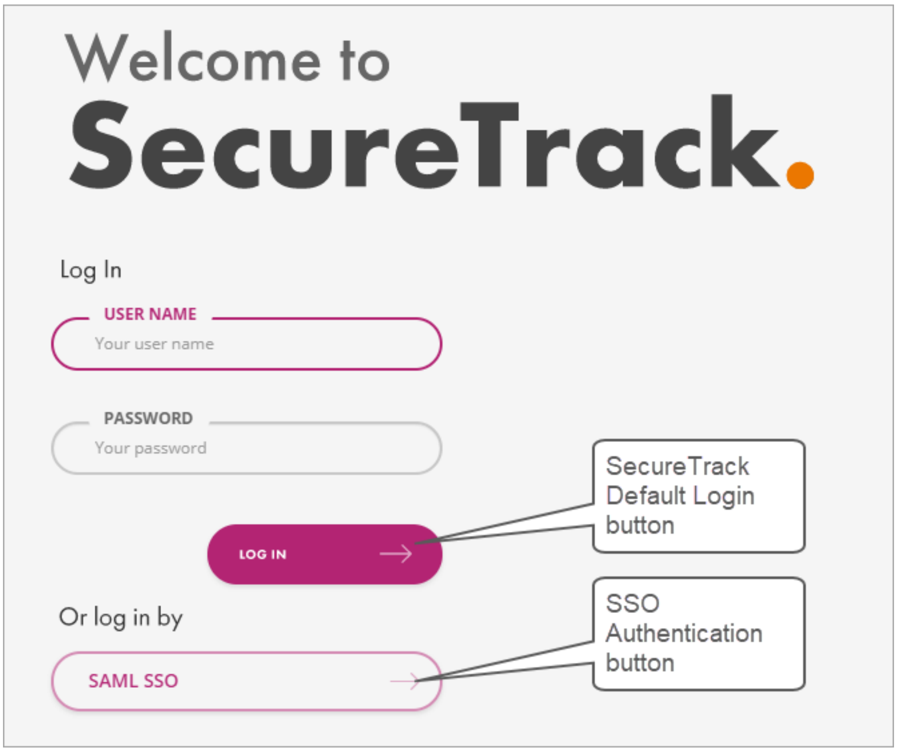
Create Users Automatically after Successful SSO Authentication

When each SSO user logs in for the first time (after clicking the SSO Authentication service button in the SecureTrack login screen), SecureTrack automatically generates a matching local user account. User names are saved as lower case since user names in SSO authentication are case insensitive. The default settings for users do not have device or administrative permissions.

SecureTrack Login Screen Authentication Buttons

When TOS is configured to work with the SSO Authentication service, the SecureTrack login screen displays two buttons:

- SecureTrack default login button: Directs the user to local or external servers. This is the existing default button for SecureTrack login.
- SSO authentication button: Directs the user to SSO authentication. The label of this button can be customized.



How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration** > **Users**

Configuring User Identity

Overview

LDAP of user groups for User Identity is available only with an Active Directory LDAP server.

For supported devices only, the User Identity feature is available by configuring LDAP. User groups are validated from the Domain DN (Base DN) tree of the LDAP server.

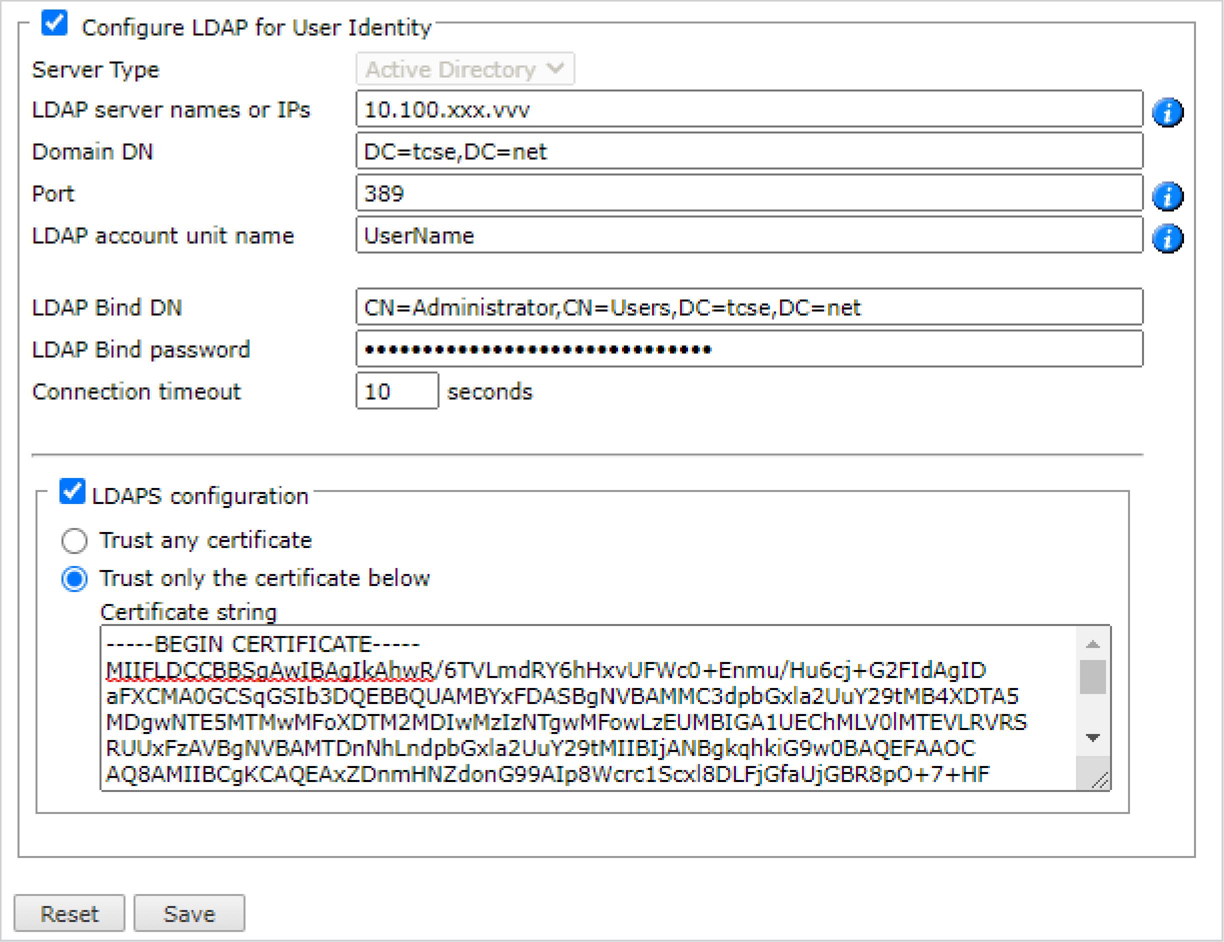
Prerequisites

If you require a LDAP generated certificate, you should retrieve the certificate before configuring the user identity and open the certificate in a text editor. The certificate is in the following format:

```
-----BEGIN CERTIFICATE-----
MIIFLDCCBBSgAwIBAgIkAhwR/6TVLmdRY6hHxvUFWc0+Enmu/Hu6cj+G2FIdAgID
aFXCMA0GCSqGSIb3DQEBBQUAMBYxFDASBgNVBAMMC3dpbGxla2UuY29tMB4XDTA5
....
....
-----END CERTIFICATE-----
```

Configure User Identity

1. Select **Settings** > **Configuration** > **User Identity**
2. Select **Configure LDAP for User Identity**:



☑ Configure LDAP for User Identity

Server Type: Active Directory

LDAP server names or IPs: 10.100.xxx.vvv

Domain DN: DC=tcse,DC=net

Port: 389

LDAP account unit name: UserName

LDAP Bind DN: CN=Administrator,CN=Users,DC=tcse,DC=net

LDAP Bind password: ••••••••••••••••••••••••••••••

Connection timeout: 10 seconds

☑ LDAPS configuration

○ Trust any certificate

● Trust only the certificate below

Certificate string

```
-----BEGIN CERTIFICATE-----
MIIFLDCCBBSgAwIBAgIkAhwR/6TVLmdRY6hHxvUFWc0+Enmu/Hu6cj+G2FIdAgID
aFXCMA0GCSqGSIb3DQEBBQUAMBYxFDASBgNVBAMMC3dpbGxla2UuY29tMB4XDTA5
MDgwNTE5MTMwMFoXDTM2MDIwMzIzNTgwMFowLzEUMBIGA1UEChMLV0lMTEVLRVRS
RUUxFzAVBgNVBAMTDnNhLndpbGxla2UuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAxZDnmHNZdonG99AIp8Wcrc1Scxl8DLFjGfaUjGBR8pO+7+HF
```

3. Configure the following fields:

   - **Server Type:** SecureTrack currently supports Active Directory.
   - **LDAP server names or IPs:** Resolvable hostname or address of the Active Directory server.

     When you use LDAP over SSL, enter the name the value from the 'Issued To' field of the server certificate.

     For LDAP server redundancy, enter multiple server names or IP addresses separated by a space or a comma.
   - **Domain DN:**: The domain's Distinguished Name (also known as Base DN). You cannot use the DN "root".
   - The **Port** used by Active Directory, according to the following table:

Active Directory Configuration	Regular LDAP (no SSL)	Encrypted LDAP (SSL)
Standalone	389	636
Global Catalog	3268	3269

   - **LDAP account unit name:** For Check Point devices, the LPAD account must be set. Enter the LDAP account unit name configured in the MDA/CMA/SMC.
   - **LDAP Bind DN:** LDAP user that has permission to read all LDAP objects and attributes that exist in the LDAP base DN.

     This field must contain a value.
   - **LDAP Bind password:** Password of the LDAP Bind DN.
   - **Connection timeout:** The number of seconds that the authenticated connection is available before it must re-authenticate.

4. For LDAP over SSL, select **LDAPS configuration** and select one of the following:

   - **Trust any certificate:** Automatically accept the certificate presented by the Active Directory server, such as a self-signed certificate.
   - **Trust only the certificate below**: Copy the certificate generated in LDAP and paste it in the **Certificate string** field.

The certificate starts with

```
-----BEGIN CERTIFICATE-----
```

and ends with

```
-----END CERTIFICATE-----.
```

5. Click **Save**.

Update the Name of an LDAP Server Field

- See the Tech Note Configure LDAP Vendor Attributes for User Identity.

How Do I Get Here?

In SecureTrack, go to: **Settings** > **Configuration** > **User Identity**

Creating Custom LDAP Vendors

If you use an LDAP server that is not natively supported in Tufin Orchestration Suite (TOS), you can create your own custom LDAP for:

- External authentication of SecureTrack users
- External authentication of SecureChange users
- LDAP of user groups for User Identity (available only with an Active Directory LDAP server)

When you create a custom LDAP, add the required attributes described in the LDAP Server Attributes list.

LDAP servers must support LDAPv3 protocol.

LDAP Server Attributes

This is the list of LDAP server attributes required for any custom LDAP configuration:

attr_objective	attr_name (Example)	Attribute Description	Required/ Optional
userIdAttributeNames	cn	The username field of a user account (Can include multiple values; Separate with comma or space)	Required
mailAttributeName	mail	The email address field of a user account	Required
firstNameAttributeName	givenName	The first name field of a user account	Required
lastNameAttributeName	sn	The last name field of a user account	Required
objectClassAttributeName	objectClass	The name of the LDAP attribute that contains the object class	Required
userObjectSearchAttributeNames	cn	The name of the LDAP attribute that is used to search for users (Can include multiple values; Separate with comma or space)	Required
userObjectClassAttributeNames	organizationalPerson	The name of the LDAP class that contains users (Can include multiple values; Separate with comma or space)	Required
userObjectCustomLdapQuery	(sAMAccountType=805306368)	The custom LDAP query that is used to search for the LDAP Class of users (Overrides	Optional

attr_objective	attr_name (Example)	Attribute Description	Required/ Optional
		userObjectClassAttributeNames)	
commonNameAttributeName	cn	The common name field of a user account	Required
displayNameAttributeName	cn	The display name field of a user account	Required
userManagerDnAttributeName	manager	The name of LDAP attribute of a user account that contains a manager DN	Required
groupMembersAttributeName	uniqueMember	The name of the LDAP attribute that contains members of group	Required
groupObjectSearchAttributeNames	cn	The name of the LDAP attribute that is used to search for groups (Can include multiple values; Separate with comma or space)	Required
groupObjectClassAttributeNames	orclGroup	The name of the LDAP class that contains groups (Can include multiple values; Separate with comma or space)	Required
groupObjectCustomLdapQuery		The custom LDAP query that is used to search for the LDAP Class of groups (Overrides groupObjectClassAttributeNames)	Optional
groupMailAttributeName	mail	The email address field of a group	Required
groupCommonNameAttributeName	cn	The common name field of a group	Required
groupDisplayNameAttributeName	cn	The display name field of a group	Required
ouObjectSearchAttributeNames	cn	The name of the LDAP attribute that is used to search for organizational units (Can include multiple values; Separate with comma or space)	Required
ouObjectClassAttributeNames	orclContainer, orclSubscriber, orclContext	The name of the LDAP class that contains organization units (Can include multiple values; Separate with comma or space)	Required
ouObjectCustomLdapQuery		The custom LDAP query that is used to search for the LDAP Class of organizational units (Overrides ouObjectClassAttributeNames)	Optional
ouMailAttributeName	mail	The email address field of a organization unit	Required
ouCommonNameAttributeName	cn	The common name field of a organization unit	Required
ouDisplayNameAttributeName	cn	The display name field of a organization unit	Required
uniqueIdAttributeName	cn	Unique identifier attribute for the user (Do not change the unique identifier attribute after the LDAP server support	Required

attr_objective	attr_name (Example)	Attribute Description	Required/ Optional
		is added) Note: Ignored if isSupportsQueryById is False	
isSupportsBrowsing	true	False - Results are not shown in the LDAP browser (Cannot search for objects in LDAP) True - Results are shown in the LDAP browser	Required
isSupportsPaging	true	False - Results in the LDAP browser are not shown in paged groups True - Results in the LDAP browser are shown in paged groups	Required
isSupportsQueryById	false	False - Do not query for results by UID True - Query for results by UID (Requires value for uniqueIdAttributeName)	Required

Configuring a new LDAP Vendor for SecureTrack

You can create a custom LDAP for external authentication of users by adding and editing the desired LDAP server attributes:

1. Retrieve the configuration for all available LDAPs or for a specific LDAP.
2. Configure the LDAP vendor attributes.

Retrieve LDAP Vendor Configuration

The `get_ldap_vendor_configuration` script retrieves the configuration for all available LDAPs or for the specified LDAP.

Syntax

```
/opt/tufin/securitysuite/scripts/get_ldap_vendor_configuration.sh [--vendor '<vendor_name>']
```

Supported arguments

`--vendor '<vendor_name>'`	(Optional) Returns the configuration details for the specified vendor

Sample code

Returns the configuration for all LDAP vendors:

```
/opt/tufin/securitysuite/scripts/get_ldap_vendor_configuration.sh
```

Returns the configuration for Active Directory:

```
/opt/tufin/securitysuite/scripts/get_ldap_vendor_configuration.sh --vendor 'Active Directory'
```

Configure LDAP Vendor Attributes for SecureTrack

The `configure_ldap_vendor_configuration` script (located in `/opt/tufin/securitysuite/scripts/)` is used to configure the LDAP vendor attributes.

You can:

- Create a new vendor and add the relevant attributes.
- Customize the attributes for an existing LDAP vendor.

You can create a shell file with a list of commands, where each command configures a different attribute. Sample script files to create custom LDAPs can be found in: `/opt/tufin/share/docs/examples/ldap_vendors/`

Syntax

The `add_or_update` action:

- Creates the specified vendor if it does not exist and adds the specified attribute.
- Creates the specified attribute for an existing vendor.
- Updates a value for an existing vendor.

```
configure_ldap_vendor_configuration.sh --action add_or_update --vendor '<vendor_name>' --attr_
objective '<attr_objective>' --attr_name '<attr_name>' --attr_type '<attr_type>'
```

Supported arguments

`--action add_or_update`
`--action delete`
	`add_or_update:` Adds a new value or updates an existing value
	`delete:` Deletes an existing value

`--vendor '<vendor_name>'`	The vendor name that is displayed in SecureTrack: **Settings** > **Configuration** > **External Authentication** > **LDAP Authentication** > **Server Type**
`--attr_objective '<attr_objective>'`	An attribute from the list of LDAP server attributes
`--attr_name '<attr_name>'`	The name of the LDAP server field that corresponds to the attr_objective
`--attr_type '<attr_type>'`	Supported attribute types: • `string` • `binary`

Sample code

- For the Active Directory vendor, update the mail attribute name to the string "mail":

```
configure_ldap_vendor_configuration.sh --action add_or_update --vendor 'Active Directory' --
attr_objective 'mailAttributeName' --attr_name 'mail' --attr_type 'string'
```

Delete LDAP Vendor for SecureTrack

The `configure_ldap_vendor_configuration` script (located in `/opt/tufin/securitysuite/scripts/)` is used to delete the LDAP vendor attributes. You can delete specific vendor attributes. To remove a specific vendor, remove all the attributes for that vendor.

Syntax

The `delete` action removes the attribute value.

```
configure_ldap_vendor_configuration.sh --action delete --vendor '<vendor_name>' --attr_objective
'<attr_objective>'
```

Supported arguments

`--action delete`	`delete:` Deletes an existing value
`--vendor '<vendor_name>'`	The vendor name that is displayed in SecureTrack: **Settings** > **Configuration** > **External Authentication** > **LDAP Authentication** > **Server Type**
`--attr_objective '<attr_objective>'`	An attribute from the list of LDAP server attributes

Sample code

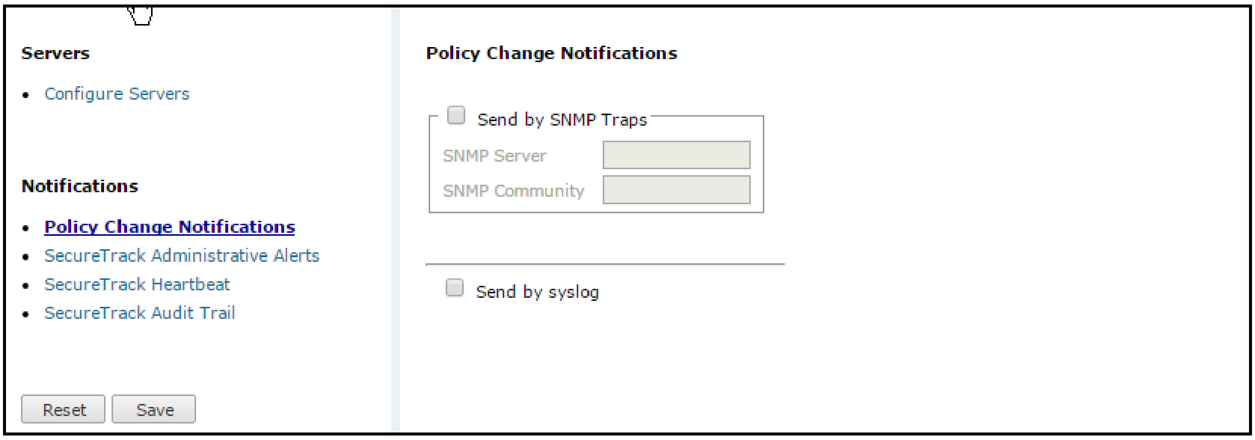
For the Active Directory vendor, deletes the "mail" attribute:

```
configure_ldap_vendor_configuration.sh --action delete --vendor 'Active Directory' --attr_objective
'mail'
```

Configure LDAP Vendor Attributes for SecureTrack

Please contact Tufin Support and ask about **Additional LDAP Customizations**.

Configuring Notifications



Servers

- Configure Servers

Notifications

- **Policy Change Notifications**
- SecureTrack Administrative Alerts
- SecureTrack Heartbeat
- SecureTrack Audit Trail

Policy Change Notifications

□ Send by SNMP Traps

SNMP Server

SNMP Community

□ Send by syslog

In this page you can set how SecureTrack sends change notifications and alerts, and whether an ongoing syslog audit trail is maintained. The supported notification and audit trail mechanisms are:

	Syslog	SNMP Traps	Email
Policy change notifications	✓	✓	
Administrative alerts	✓		✓
Heartbeat notifications		✓	
Audit trail	✓		

Click here to view the full list of SecureTrack SNMP notifications.

This page is available only to Administrators.

What can I do on this page?

- Configure servers - Configure the SMTP and syslog server.
- Configure notifications - Enable/disable audit trail and notifications for policy changes, SecureTrack administrative changes, Heartbeat notifications, and audit trail.

How Do I Get Here?

To go to the Notifications page:

1. In SecureTrack, click **Settings** > **Configuration**.
2. Select the **Notifications** tab.

Configuring Servers (SMTP and Syslog)

Overview

For SecureTrack to send email and syslog notifications, you must configure the server information.

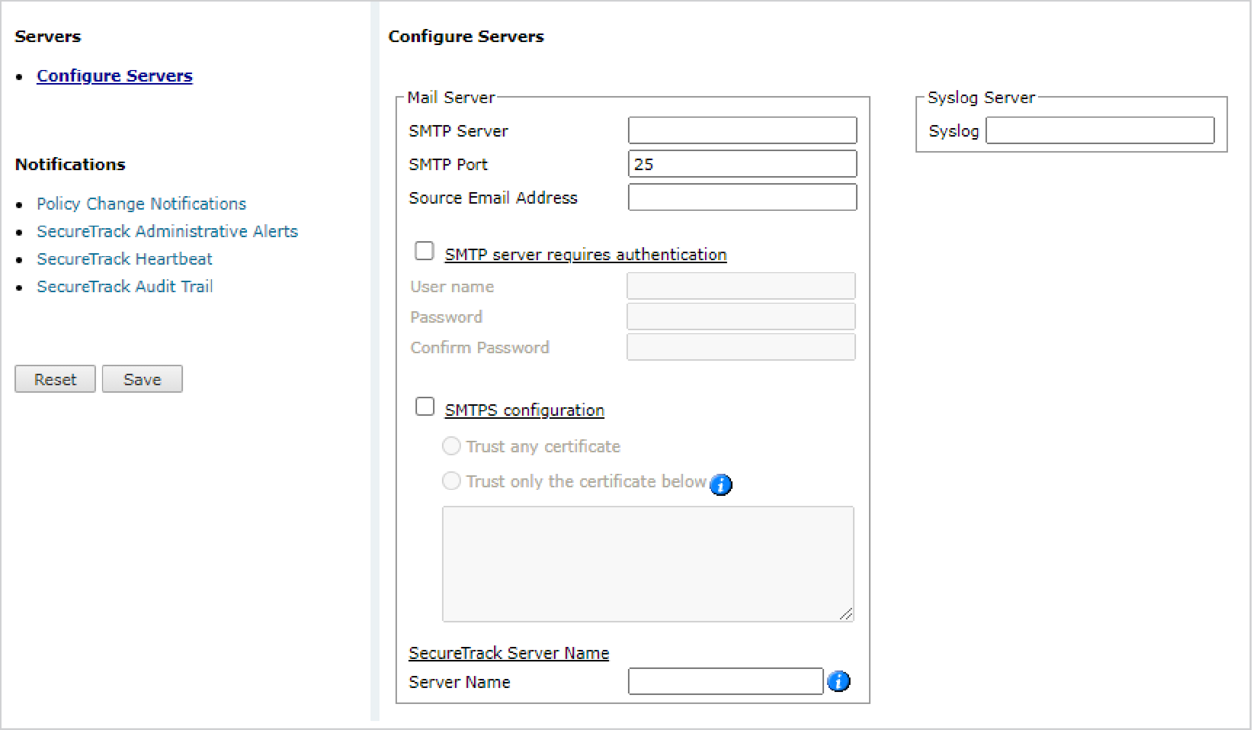
The email, Syslog and SNMP settings are used for Policy Change notifications, scheduled reports performance alerts and real-time Organizational Policy Audit messages.

This page is available only to Administrators.

What Can I Do Here?

Configure a Mail Server for SecureTrack

1. Go to **Admin** > **Notifications**.



Servers

- Configure Servers

Notifications

- Policy Change Notifications
- SecureTrack Administrative Alerts
- SecureTrack Heartbeat
- SecureTrack Audit Trail

Reset Save

Configure Servers

Mail Server

SMTP Server

SMTP Port 25

Source Email Address

□ SMTP server requires authentication

User name

Password

Confirm Password

□ SMTPS configuration

○ Trust any certificate

○ Trust only the certificate below

SecureTrack Server Name

Server Name

Syslog Server

Syslog

2. Enter SMTP information for:
   - **SMTP Server**: SecureTrack can send email notifications and alerts directly (using its SMTP engine), or act as an email client, and send emails to an organizational SMTP server. In order to send emails to an SMTP server, configure its IP address in this option. The default setting for the SMTP Mail Server is localhost, which sends emails directly.
   - **SMTP Port**: The port used by your SMTP server.
   - **Source Email Address**: The email address chosen by SecureTrack in the SMTP email messages sent (for example: securetrack@yourcompany.com). This can be used for easy identifications of email messages coming from SecureTrack.
   - **SMTP server requires authentication**: Select this if your SMTP server requires authentication for sending email, and type the username and password that will be used by SecureTrack to communicate with the SMTP server.
   - **Enable SMTP over SSL**: Select if your SMTP requires certificate encryption when sending and receiving emails. If you require encryption then select to trust all certificates or list specified certificates.

     The option **Trust only the certificate below**. For non-TufinOS users, this option requires PHP version 5.6 or above.
3. Click **Save**.

Configure a DNS or IP Address

The DNS or IP address is used by SecureTrack in URLs that appear in email notifications and reports.

1. Go to **Admin** > **Notifications**.
2. In **SecureTrack Server Name** area, enter the DNS or IP address for the SecureTrack server
3. Click **Save**.

Configure SecureTrack to Send Alerts to a Syslog Server

To configure SecureTrack to send Syslog alerts to a syslog server, if enabled under Notifications

1. Go to **Admin** > **Notifications**.
2. In the **Syslog Server area**, enter the DNS or IP address for the Syslog server
3. Click **Save**.

   To encrypt the syslog messages, contact Tufin Support for assistance.

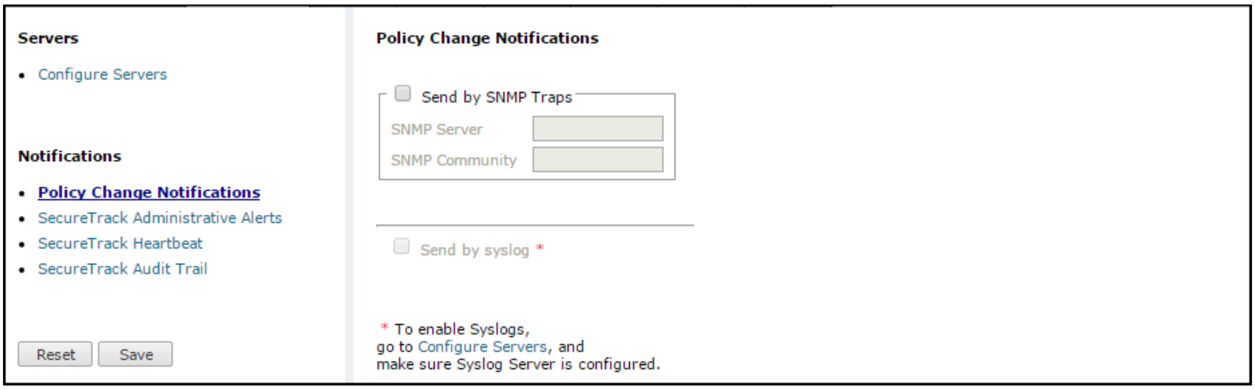
How Do I Get Here?

In SecureTrack, go to: **Settings** > **Configuration** > **Notifications**

Policy Change, Administrative, Heartbeat, Audit Trail

The notifications you can configure are:

- **Policy Change Notifications** provide real-time information on changes to monitored firewall policies, similar to the information provided in the New Revision report.



Servers

- Configure Servers

Notifications

- **Policy Change Notifications**
- SecureTrack Administrative Alerts
- SecureTrack Heartbeat
- SecureTrack Audit Trail

Policy Change Notifications

□ Send by SNMP Traps

SNMP Server

SNMP Community

□ Send by syslog *

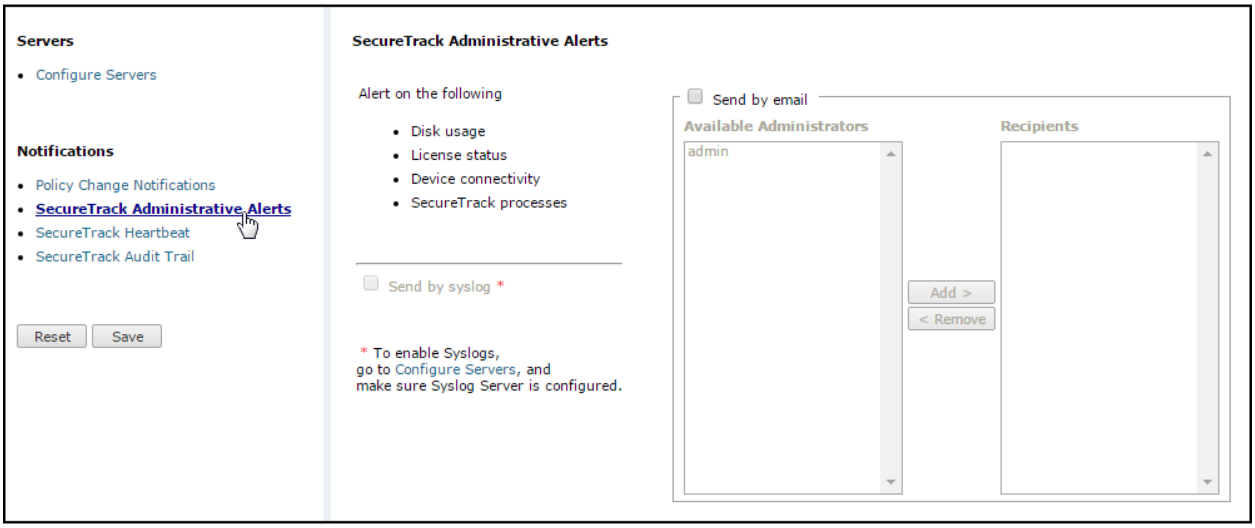
* To enable Syslogs,
go to Configure Servers, and
make sure Syslog Server is configured.

Policy Change Notifications can be sent in the following ways:

- **Send by SNMP Traps**: SNMP Notifications are sent to the SNMP Server configured here:
    - **SNMP Server**: Configure the IP address of the SNMP server which SecureTrack should send Policy Change SNMP Traps to.
    - **SNMP Community**: Choose the SNMP Community string, which will be used in the Policy Change SNMP traps. The community string is often used as a method of easy identification and classification of different SNMP traps.
- **Send by syslog**: Policy Change Notifications are sent to the server configured under **Configuring Servers**.

- **SecureTrack Administrative Alerts** notify administrators of the following types of problems with the SecureTrack server or appliance:
    - Disk usage
    - License status
    - Device connectivity
    - SecureTrack processes

Administrative Alerts can be sent the following ways:



Servers

- Configure Servers

Notifications

- Policy Change Notifications
- **SecureTrack Administrative Alerts**
- SecureTrack Heartbeat
- SecureTrack Audit Trail

SecureTrack Administrative Alerts

Alert on the following

- Disk usage
- License status
- Device connectivity
- SecureTrack processes

□ Send by syslog *

* To enable Syslogs,
go to Configure Servers, and
make sure Syslog Server is configured.

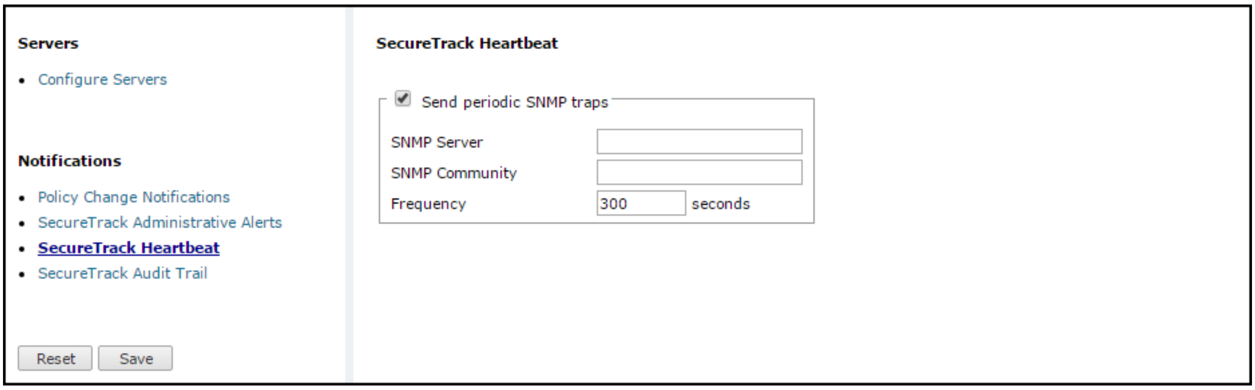
□ Send by email

Available Administrators: admin

Recipients

- **Send by syslog**: The alerts are sent to the syslog server configured under **Configuring Servers**.
- **Send by email**: The alerts are sent to the **Recipients** configured here (SecureTrack Administrators only), using the SMTP server configured under **Configuring Servers**.

- **SecureTrack Heartbeat**: Periodically sent SNMP Notifications indicating the monitoring statuses of monitoring processes, for Check Point management servers only. To enable the SecureTrack Heartbeat, select **Send periodic SNMP traps**, and configure the following:



Servers

- Configure Servers

Notifications

- Policy Change Notifications
- SecureTrack Administrative Alerts
- **SecureTrack Heartbeat**
- SecureTrack Audit Trail

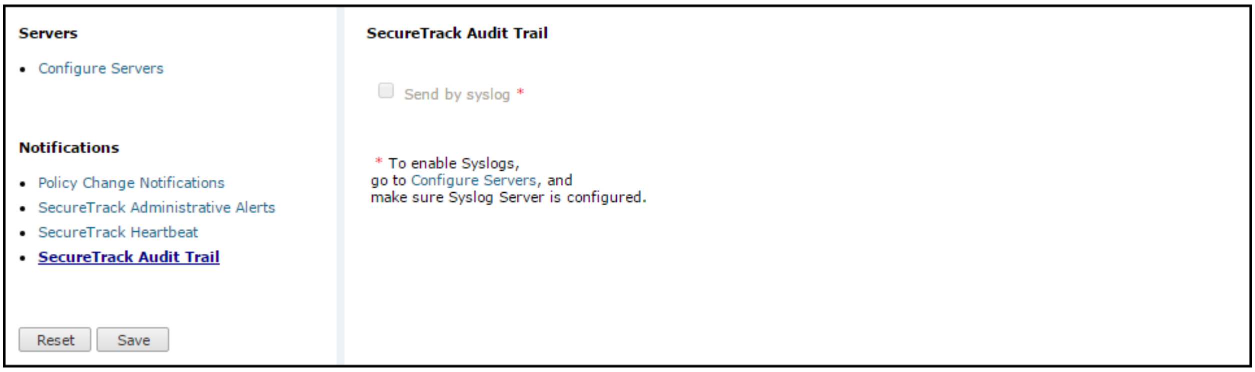
Reset Save

SecureTrack Heartbeat

☑ Send periodic SNMP traps

SNMP Server	
SNMP Community	
Frequency	300 seconds

  - **SNMP Server**: The IP address of the SNMP server to which SecureTrack should send Hearbeat SNMP Traps.
  - **SNMP Community**: The SNMP Community string, which will be used in the Heartbeat SNMP traps. The community string is often used as a method of easy identification and classification of different SNMP traps.
  - **Frequency**: The Heartbeat SNMP trap frequency (in seconds).
- **SecureTrack Audit Trail**: When you select **Send by syslog**, SecureTrack sends syslog messages to the configured syslog server with the username and time for the events listed in the audit trail.



Servers

- Configure Servers

Notifications

- Policy Change Notifications
- SecureTrack Administrative Alerts
- SecureTrack Heartbeat
- **SecureTrack Audit Trail**

Reset Save

SecureTrack Audit Trail

□ Send by syslog *

* To enable Syslogs,
go to Configure Servers, and
make sure Syslog Server is configured.

The areas of SecureTrack that are audited are:

System Configuration	Device Monitoring, Analysis and Reporting
- User authentication	- Policy comparison
- Device management	- Revision and rules metadata
- License management	- Topology management
- Plugin and domain management	- Zone management
- System configuration	- Automatic policy generator jobs
- User management	- Report configuration and generation
	- Repository

Each action is listed with:

- The date and time of the action
- The username of the user that did the action
- The IP address of the host from which the action was done (automatic actions, such as scheduled reports, are listed without a user IP address)
- The category or feature area that the action belongs to
- The type of action, such as add, remove, modify, or generate report
- The type of object and object name to which the action was done
- A description of the action

SecureTrack SNMP Notifications

SecureTrack uses SNMP version 2c traps to send Policy change and heartbeat notifications. The traps are generated using the Tufin MIB. For details of the Tufin SNMP MIBs, see Tufin Orchestration Suite MIB Definitions.

Identifying SecureTrack SNMP Messages

Tufin Technologies has been assigned the Private Enterprise Number 21834 by IANA. If you would like to provide special handling for SecureTrack's SNMP messages, you can either:

- Copy the SNMP MIB file, located on the SecureTrack machine at `/usr/local/st/mibs/TUFIN-MIB.txt` to your SNMP server, and use it to uniquely identify SecureTrack SNMP messages
- Parse SNMP messages arriving at your SNMP server - the first element in SecureTrack's SNMP message will be TUFIN-MIB::stEvent.0.

Tufin SNMP Policy Change and Periodic Change Messages

The following tables summarizes the different elements contained in SecureTrack's SNMP messages, their meaning and possible values.

nodeDiskPartitionFilesystemUsageTrap

SNMP trap element	Meaning	Possible values
TUFIN-MIB::stEvent.0	Policy change type	Install, Save, Automatic
TUFIN-MIB::stManagementName.0	Check Point: Management name Others: Device name	String (0-256 characters)
TUFIN-MIB::stAdmin.0	Administrator name*	String (0-256 characters)
TUFIN-MIB::stEventPriority.0	Priority	Info, Low, Medium, High, Critical
TUFIN-MIB::stCustomMsg.0	Custom message configured for this SNMP event	String (0-1024 characters)
TUFIN-MIB::stAdditionalInfo.0	Additional information	String (0-1024 characters)

* Admin name is not included in SNMP traps for JunOS, Fortinet and Palo Alto

The following table summarizes the different elements contained in SecureTrack's Periodic Status notification SNMP messages, their meaning and possible values:

SNMP trap element	Meaning	Possible values
TUFIN-MIB::stEvent.0	Policy change type	Install, Save, Automatic
TUFIN-MIB::stManagementName.0	Check Point management friendly name	String (0-256 characters)
TUFIN-MIB:: stManagementIP.0	Check Point management IP address	String (0-256 characters)
TUFIN-MIB:: stManagementPeriodicStatus.0	Periodic status message	String (0-1024 characters)

The following periodic status messages can be expected in the trap element TUFIN-MIB:: stManagementPeriodicStatus.0:

- **Starting SecureTrack Server**: the SecureTrack process monitoring this management server was started.
- **LEA session was established**: SecureTrack successfully established an OPSEC connection with the management server. This status message is expected a few seconds after the previous one (Starting SecureTrack Server).
- **Stopping SecureTrack Server**: The SecureTrack process monitoring this management server was stopped.
- **LEA session was closed**: The OPSEC connection between SecureTrack and the management server was closed. If this message is immediately followed by the "Stopping SecureTrack Server" message, the product was stopped (via "st stop"), otherwise the connection was reset for some other reason (e.g., network connection down, management server was stopped, etc).
- **Disk space is low. <x>% free**: Disk capacity warning, with an indication of the amount of free disk space (as a percentage). This message is sent daily to all administrators when the disk usage exceeds 80%. When disk usage exceeds 90%, rule and object usage collection is stopped. When disk usage exceeds 95%, all SecureTrack processes are stopped.
- **No valid license found**: Indicates that SecureTrack does not have a license installed, or that the Check Point configuration does not match the licensed configuration. This message will usually be followed by the "Stopping SecureTrack Server" message.

Tufin Orchestration Suite MIB Definitions

You can use the MIB definitions below to help you work with SNMP messages that are sent from TOS and SecureTrack, or using SNMP get/walk. The correct version of the file depends on whether you use SMIv1 or SMIv2 format in your monitoring management system.

Tufin MIB File (SMIv2 Format)

MIB file for SMIv2 format

```
TUFIN-MIB DEFINITIONS ::= BEGIN

-- SecureTrack:
-- SUBTREE: 1.3.6.1.4.1.21834.1.1
-- iso.org.dod.internet.private.enterprises.tufin.tos.securetrack

-- Securitysuite:
-- SUBTREE: 1.3.6.1.4.1.21834.1.2
-- iso.org.dod.internet.private.enterprises.tufin.tos.securitysuite

IMPORTS
--enterprises
--FROM RFC1155-SMI
--TRAP-TYPE
--FROM RFC-1215
OBJECT-TYPE, NOTIFICATION-TYPE, enterprises
FROM SNMPv2-SMI;

-- textual conventions

DisplayString ::= OCTET STRING

tufin OBJECT IDENTIFIER ::= { enterprises 21834 }
tos OBJECT IDENTIFIER ::= { tufin 1 }
securitysuite OBJECT IDENTIFIER ::= { tos 2 }

```

```
-- #########[ SECURETRACK GROUP ]#########

securetrack NOTIFICATION-TYPE
    OBJECTS {
        stManagementName, stAdmin, stCustomMsg, stEventPriority, stEvent, stAdditionalInfo, stManagementIP, stManagementPeriodicStatus
        }
    STATUS      current
    DESCRIPTION
       "SecureTrack issues"
    ::= { tos 1 }


stManagementName OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS not-accesible
STATUS mandatory
DESCRIPTION
"Firewall Management name"
::= { securetrack 1 }

stAdmin OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS not-accesible
STATUS mandatory
DESCRIPTION
"Security Administrator"
::= { securetrack 2 }

```

```
stCustomMsg OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS not-accesible
STATUS mandatory
DESCRIPTION
"Custom message describing the event watch"
::= { securetrack 3 }

stEventPriority OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS not-accesible
STATUS mandatory
DESCRIPTION
"Event Priority"
::= { securetrack 4 }

stEvent OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..1024))
MAX-ACCESS not-accesible
STATUS mandatory
DESCRIPTION
"The event monitored by SecureTrack"
::= { securetrack 5 }

stAdditionalInfo OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..1024))
MAX-ACCESS not-accesible
STATUS mandatory
DESCRIPTION
```

```
"Additional info"
::= { securetrack 6 }

stManagementIP OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..15))
MAX-ACCESS not-accesible
STATUS mandatory
DESCRIPTION
"Management IP"
::= { securetrack 7 }

stManagementPeriodicStatus OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS not-accesible
STATUS mandatory
DESCRIPTION
"Management Periodic Status"
::= { securetrack 8 }

-- #########[ SECURITYSUITE GROUP ]#########

-- os SUBTREE: 1.3.6.1.4.1.21834.1.2.1
os       OBJECT IDENTIFIER ::= { securitysuite 1 }

-- #########################################

-- groups in os
-- cpu SUBTREE: 1.3.6.1.4.1.21834.1.2.1.1
cpu                   OBJECT IDENTIFIER ::= { os 1 }
```

```
-- disk SUBTREE: 1.3.6.1.4.1.21834.1.2.1.2
disk                  OBJECT IDENTIFIER ::= { os 2 }
-- memory SUBTREE: 1.3.6.1.4.1.21834.1.2.1.3
memory                OBJECT IDENTIFIER ::= { os 3 }
-- services SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4
services              OBJECT IDENTIFIER ::= { os 4 }

-- #########################################

-- groups in cpu
-- cpuUsage SUBTREE: 1.3.6.1.4.1.21834.1.2.1.1.1
cpuUsage NOTIFICATION-TYPE
    OBJECTS {
        cpuUsageDescription, cpuUsageValue, cpuUsageThreshold, cpuUsageSeverity
        }
    STATUS      current
    DESCRIPTION
       "CPU usage issues"
    ::= { cpu 1 }

-- groups in disk
-- diskUsage SUBTREE: 1.3.6.1.4.1.21834.1.2.1.2.1
diskUsage NOTIFICATION-TYPE
    OBJECTS {
        diskUsageDescription, diskUsageValue, diskUsageThreshold, diskUsageSeverity
        }
    STATUS      current
    DESCRIPTION
       "Disk usage issues"
    ::= { disk 1 }

-- groups in memory
-- memoryUsage SUBTREE: 1.3.6.1.4.1.21834.1.2.1.3.1
memoryUsage NOTIFICATION-TYPE
    OBJECTS {
        memoryUsageDescription, memoryUsageValue, memoryUsageThreshold,
memoryUsageSeverity
        }
    STATUS      current
    DESCRIPTION
       "Memory usage issues"
    ::= { memory 1 }

-- groups in services
-- webServer SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.1
webServer NOTIFICATION-TYPE
    OBJECTS {
        webServerDescription, webServerStatus
        }
    STATUS      current
    DESCRIPTION
       "Web server status issues"
    ::= { services 1 }

-- database SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.2
database NOTIFICATION-TYPE
```

```
    OBJECTS {
        databaseDescription, databaseStatus
        }
    STATUS      current
    DESCRIPTION
       "Webserver status issues"
    ::= { services 2 }

-- applicationServer SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.3
applicationServer NOTIFICATION-TYPE
    OBJECTS {
        applicationServerDescription, applicationServerStatus
        }
    STATUS      current
    DESCRIPTION
       "Application server status issues"
    ::= { services 3 }

-- syslog SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.4
syslog NOTIFICATION-TYPE
    OBJECTS {
        syslogDescription, syslogStatus
        }
    STATUS      current
    DESCRIPTION
       "Syslog status issues"
    ::= { services 4 }

```

```
-- cron SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.5
cron NOTIFICATION-TYPE
    OBJECTS {
        cronDescription, cronStatus
        }
    STATUS      current
    DESCRIPTION
       "Cron status issues"
    ::= { services 5 }

-- stunnel SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.6
stunnel NOTIFICATION-TYPE
    OBJECTS {
        stunnelDescription, stunnelStatus
        }
    STATUS      current
    DESCRIPTION
       "Stunnel status issues"
    ::= { services 6 }

-- jmsTunnel SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.7
jmsTunnel NOTIFICATION-TYPE
    OBJECTS {
        jmsTunnelDescription, jmsTunnelStatus
        }
    STATUS      current
    DESCRIPTION
       "JmsTunnel status issues"
    ::= { services 7 }
```

```

-- ######################################

-- objects in cpuUsage
cpuUsageDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The CPU usage description."
::= { cpuUsage 1 }

cpuUsageValue OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The percentage of CPU time spent processing system-level code,
calculated over the last minute."
::= { cpuUsage 2 }

cpuUsageThreshold OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The CPU usage threshold."
::= { cpuUsage 3 }

```

```
cpuUsageSeverity OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The CPU usage severity."
::= { cpuUsage 4 }

-- ########################################

-- objects in diskUsage
diskUsageDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The disk usage description."
::= { diskUsage 1 }


diskUsageValue OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Used space on the disk.
For large heavily-used disks (>2Tb), this value will latch at INT32_MAX
(2147483647)."
::= { diskUsage 2 }
```

```

diskUsageThreshold OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The disk usage threshold."
::= { diskUsage 3 }

diskUsageSeverity OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The disk usage severity."
::= { diskUsage 4 }

-- ##########################################

-- objects in memoryUsage
memoryUsageDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The memory usage description."
::= { memoryUsage 1 }

memoryUsageValue OBJECT-TYPE
```

```
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The amount of real/physical memory currently being used."
::= { memoryUsage 2 }

memoryUsageThreshold OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The memory usage threshold."
::= { memoryUsage 3 }

memoryUsageSeverity OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The memory usage severity."
::= { memoryUsage 4 }

-- #########################################

-- objects in webServer .1
webServerDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
```

```
STATUS current
DESCRIPTION
"The Web Server init service description."
::= { webServer 1 }

webServerStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Web Server init service status."
::= { webServer 2 }

-- objects in database .2
databaseDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Database init service description."
::= { database 1 }

databaseStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Database init service status."
::= { database 2 }
```

```

-- objects in applicationServer .3
applicationServerDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Application Server init service description."
::= { applicationServer 1 }

applicationServerStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Application Server init service status."
::= { applicationServer 2 }

-- objects in syslog .4
syslogDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Syslog init service description."
::= { syslog 1 }

syslogStatus OBJECT-TYPE
SYNTAX Integer32
```

```
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Syslog init service status."
::= { syslog 2 }

-- objects in cron .5
cronDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Cron init service description."
::= { cron 1 }

cronStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Cron init service status."
::= { cron 2 }

-- objects in stunnel .6
stunnelDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
```

```
DESCRIPTION
"The Stunnel init service description."
::= { stunnel 1 }

stunnelStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Stunnel init service status."
::= { stunnel 2 }

-- objects in jmsTunnel .7
jmsTunnelDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The JmsTunnel init service description."
::= { jmsTunnel 1 }

jmsTunnelStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The JmsTunnel init service status."
::= { jmsTunnel 2 }
```

```

END
```

Tufin MIB File (SMIv1 Format)

MIB file for SMIv1 format

```
TUFIN-MIB DEFINITIONS ::= BEGIN
-- SecureTrack:
-- SUBTREE: 1.3.6.1.4.1.21834.1.1
-- iso.org.dod.internet.private.enterprises.tufin.tos.securetrack
-- Securitysuite:
-- SUBTREE: 1.3.6.1.4.1.21834.1.2
-- iso.org.dod.internet.private.enterprises.tufin.tos.securitysuite
IMPORTS
enterprises
FROM RFC1155-SMI
TRAP-TYPE
FROM RFC-1215
OBJECT-TYPE
FROM RFC-1212;
-- textual conventions
DisplayString ::= OCTET STRING
tufin OBJECT IDENTIFIER ::= { enterprises 21834 }
tos OBJECT IDENTIFIER ::= { tufin 1 }
securetrack OBJECT IDENTIFIER ::= { tos 1 }
securitysuite OBJECT IDENTIFIER ::= { tos 2 }
-- #########[ SECURETRACK GROUP ]#########
stManagementName OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
```

```
STATUS mandatory
DESCRIPTION
"Firewall Management name"
::= { securetrack 1 }
stAdmin OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Security Administrator"
::= { securetrack 2 }
stCustomMsg OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Custom message describing the event watch"
::= { securetrack 3 }
stEventPriority OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Event Priority"
::= { securetrack 4 }
stEvent OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..1024))
ACCESS read-only
STATUS mandatory
```

```
DESCRIPTION
"The event monitored by SecureTrack"
::= { securetrack 5 }
stAdditionalInfo OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..1024))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Additional info"
::= { securetrack 6 }
stManagementIP OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..15))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Management IP"
::= { securetrack 7 }
stManagementPeriodicStatus OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"Management Periodic Status"
::= { securetrack 8 }
-- #########[ SECURITYSUITE GROUP ]#########
-- os SUBTREE: 1.3.6.1.4.1.21834.1.2.1
os OBJECT IDENTIFIER ::= { securitysuite 1 }
-- #########################################
-- groups in os
-- cpu SUBTREE: 1.3.6.1.4.1.21834.1.2.1.1
cpu OBJECT IDENTIFIER ::= { os 1 }
-- disk SUBTREE: 1.3.6.1.4.1.21834.1.2.1.2
disk OBJECT IDENTIFIER ::= { os 2 }
-- memory SUBTREE: 1.3.6.1.4.1.21834.1.2.1.3
memory OBJECT IDENTIFIER ::= { os 3 }
-- services SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4
services OBJECT IDENTIFIER ::= { os 4 }
-- #########################################
-- groups in cpu
-- cpuUsage SUBTREE: 1.3.6.1.4.1.21834.1.2.1.1.1
cpuUsage OBJECT IDENTIFIER ::= { cpu 1 }
-- groups in disk
-- diskUsage SUBTREE: 1.3.6.1.4.1.21834.1.2.1.2.1
diskUsage OBJECT IDENTIFIER ::= { disk 1 }
-- groups in memory
-- memoryUsage SUBTREE: 1.3.6.1.4.1.21834.1.2.1.3.1
memoryUsage OBJECT IDENTIFIER ::= { memory 1 }
-- groups in services
-- webServer SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.1
webServer OBJECT IDENTIFIER ::= { services 1 }
-- database SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.2
database OBJECT IDENTIFIER ::= { services 2 }
-- applicationServer SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.3
applicationServer OBJECT IDENTIFIER ::= { services 3 }
-- syslog SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.4
syslog OBJECT IDENTIFIER ::= { services 4 }
```

```
-- cron SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.5
cron OBJECT IDENTIFIER ::= { services 5 }
-- stunnel SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.6
stunnel OBJECT IDENTIFIER ::= { services 6 }
-- jmsTunnel SUBTREE: 1.3.6.1.4.1.21834.1.2.1.4.1.7
jmsTunnel OBJECT IDENTIFIER ::= { services 7 }
-- #########################################
-- objects in cpuUsage
cpuUsageDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The CPU usage description."
::= { cpuUsage 1 }
cpuUsageValue OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The percentage of CPU time spent processing system-level code,
calculated over the last minute."
::= { cpuUsage 2 }
cpuUsageThreshold OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The CPU usage threshold."
```

```
::= { cpuUsage 3 }
cpuUsageSeverity OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The CPU usage severity."
::= { cpuUsage 4 }
-- #########################################
-- objects in diskUsage
diskUsageDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The disk usage description."
::= { diskUsage 1 }
diskUsageValue OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Used space on the disk.
For large heavily-used disks (>2Tb), this value will latch at INT32_MAX
(2147483647)."
::= { diskUsage 2 }
diskUsageThreshold OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
```

```
STATUS current
DESCRIPTION
"The disk usage threshold."
::= { diskUsage 3 }
diskUsageSeverity OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The disk usage severity."
::= { diskUsage 4 }
-- #########################################
-- objects in memoryUsage
memoryUsageDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The memory usage description."
::= { memoryUsage 1 }
memoryUsageValue OBJECT-TYPE
SYNTAX Integer32
UNITS "kB"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The amount of real/physical memory currently being used."
::= { memoryUsage 2 }
memoryUsageThreshold OBJECT-TYPE
```

```
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The memory usage threshold."
::= { memoryUsage 3 }
memoryUsageSeverity OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The memory usage severity."
::= { memoryUsage 4 }
-- #########################################
-- objects in webServer .1
webServerDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Web Server init service description."
::= { webServer 1 }
webServerStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Web Server init service status."
::= { webServer 2 }
```

```
-- objects in database .2
databaseDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Database init service description."
::= { database 1 }
databaseStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Database init service status."
::= { database 2 }
-- objects in applicationServer .3
applicationServerDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Application Server init service description."
::= { applicationServer 1 }
applicationServerStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
```

```
"The Application Server init service status."
::= { applicationServer 2 }
-- objects in syslog .4
syslogDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Syslog init service description."
::= { syslog 1 }
syslogStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Syslog init service status."
::= { syslog 2 }
-- objects in cron .5
cronDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Cron init service description."
::= { cron 1 }
cronStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
```

```
DESCRIPTION
"The Cron init service status."
::= { cron 2 }
-- objects in stunnel .6
stunnelDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Stunnel init service description."
::= { stunnel 1 }
stunnelStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The Stunnel init service status."
::= { stunnel 2 }
-- objects in jmsTunnel .7
jmsTunnelDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The JmsTunnel init service description."
::= { jmsTunnel 1 }
jmsTunnelStatus OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
```

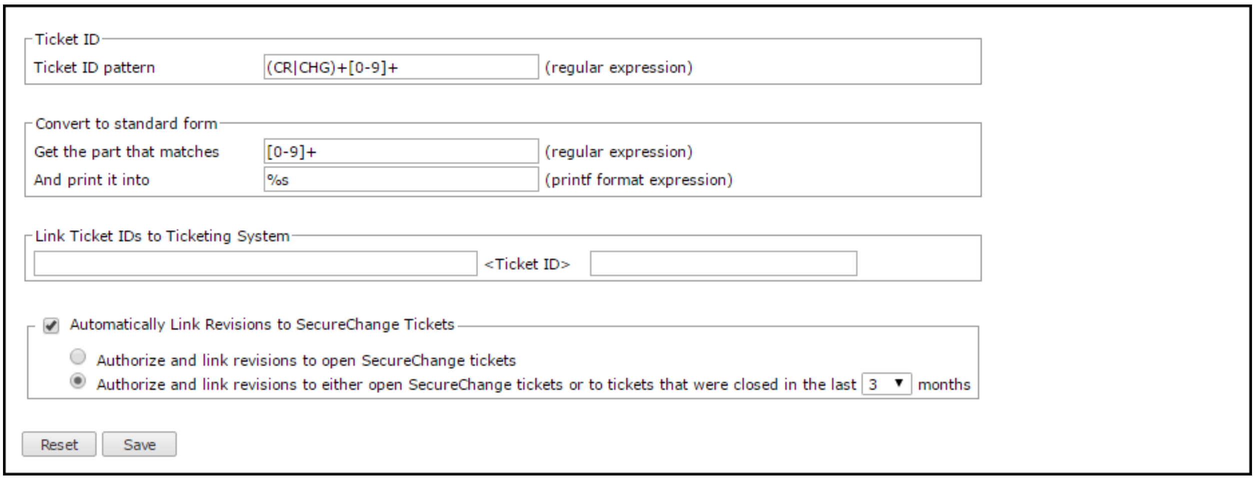
```
STATUS current
DESCRIPTION
"The JmsTunnel init service status."
::= { jmsTunnel 2 }
END
```

Linking to Ticketing Systems

You can see the link between your revisions and the tickets in your ticketing system with either:

- Display ticket ID from an external ticketing system
- Revision authorization based on SecureChange tickets

This option is only available to users with administrator permissions.



Ticket ID

Ticket ID pattern: (CR|CHG)+[0-9]+ (regular expression)

Convert to standard form

Get the part that matches: [0-9]+ (regular expression)

And print it into: %s (printf format expression)

Link Ticket IDs to Ticketing System

<Ticket ID>

☑ Automatically Link Revisions to SecureChange Tickets

○ Authorize and link revisions to open SecureChange tickets

● Authorize and link revisions to either open SecureChange tickets or to tickets that were closed in the last 3 months

Display Ticket ID

SecureTrack can link to web-based ticket systems such as Tufin SecureChange, BMC Remedy AR System, HP Service Center, CA Service Desk Manager, or home-grown systems. When a ticket ID is included in the rules or objects in security policies monitored by SecureTrack, SecureTrack recognizes it in all policy views, including report results. SecureTrack shows the ticket ID as a hyperlink according to the ticket ID pattern configured in this page. When there is a revision that includes a new ticket ID, SecureTrack also adds a hyperlink for the new ticket ID.

SecureTrack looks for the ticket ID in these fields:

Vendor	Ticket Field
Check Point	comment
Cisco	access rule description
Fortinet	security policy comment
Juniper	
JunOS SRX, J-series	security policy name
JunOS M, MX	firewall term name
Netscreen	security policy name
Palo Alto	security policy rule name, security policy rule description

To display the ticket ID in a revision, configure:

- **Ticket ID Pattern** (regular expression): You can enter case-sensitive regular expressions to match your ticket ID. For a complete reference on the syntax of supported regular expressions, please visit this page:.

- **Convert to Standard Form**: Select this to normalize ticket IDs and change them from one format to another. This is achieved by configuring an additional regular expression which will match part of the ticket ID, and creating a modified form of the ticket ID using a "C/C++" printf-like expression.
- **Link Ticket IDs to Ticketing System**: Enter a URL pattern that can be used to view a specific ticket's details. Ticket IDs in rule Name and Comment fields will appear as URLs in displayed revisions. This setting is relevant only if the ticketing system has a web interface which can be accessed through a known URL.

  For SecureChange, the URL pattern is:

  `https://<IP_or_hostname>/securechangeworkflow/pages/reports/viewTicket.seam?ticket=`**<Ticket ID>**

Click **Save** after you make changes to these options.

Example 1: Ticket ID with a hyperlink to the Ticketing System

My company's ticket ID format is "CR" followed by several digits. The URL to my Ticketing System for viewing a specific ticket is: https://1.2.3.4/remedy/<ticket ID>

The following configuration should be used in this case:

- **Ticket ID Pattern**: CR[0-9]+
- **Convert to Standard Form**: leave all values empty
- **Link Ticket IDs to Ticketing System**: http://1.2.3.4/remedy/

Example 2: Multiple Ticket ID patterns with a hyperlink to the Ticketing System

My company's ticket ID formats are "CR or CHG followed by several digits". The URL to my Ticketing System for viewing a specific ticket is: https://1.2.3.4/remedy/ticket=<ticket ID digits without leading characters>

The following configuration should be used in this case:

- **Ticket ID Pattern**: (CR|CHG)+[0-9]+
- **Convert to Standard Form**:
  - **Get the part that matches**: [0-9]+
  - **And print it to**: %s
- **Link Ticket IDs to Ticketing System**: http://1.2.3.4/remedy/ticket=

Revision Authorization

If you use SecureChange, SecureTrack can also automatically look for authorized SecureChange tickets that match all of the new allowed traffic in a revision to mark the revisions as **Authorized**. SecureTrack automatically associates a SecureChange ticket with the revision if:

- The ticket has an access request that at least partially matches the traffic changes in the revision
- The target of the access request is **Any** with Topology disabled, or the same as the device from which the revision was received
- The ticket is open (You can also configure authorization to include tickets that were closed within the last 3, 6, 9 or 12 months.)
- The ticket is authorized, meaning that it either:
  - Has at least one step with the Approve/Decline field and the final step with this field is Approved
  - Does not have any steps with the Approve/Decline field but the ticket has passed to the last step of the workflow

SecureTrack automatically marks each revision as, either:

- **Authorized** without tickets - There are no rule changes in the revision or there is a rule change that does not impact network traffic, such as a change to a rule comment
- **Authorized** with tickets - All of the changed traffic matches at least one associated SecureChange ticket
- **Unauthorized** with tickets - Tickets are associated with the revision, but not all of the changed traffic matches at least one associated SecureChange ticket
- **Unauthorized** without tickets - No tickets are associated with the changed traffic in the revision

How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration** > **Ticketing**.

Administrative Maintenance

You can:

- Check the status of device monitoring and licensing
- Do system maintenance tasks

- Audit the actions that are performed by SecureTrack users

How Do I Get Here?

In SecureTrack, go to **Settings** > **Administration**.

Monitoring Server and Device Status

The **Status** page is available only to Administrators.

In the **Status** page, it is possible to see the status of each SecureTrack server (Central server, Distribution servers, and Remote Collectors), and of each monitored device. With management devices, the status is taken from the managed firewalls, which on other words means that if there is at least one managed firewall with the status "**Expired**", the management device will also have the status **Expired**, and will be disabled.

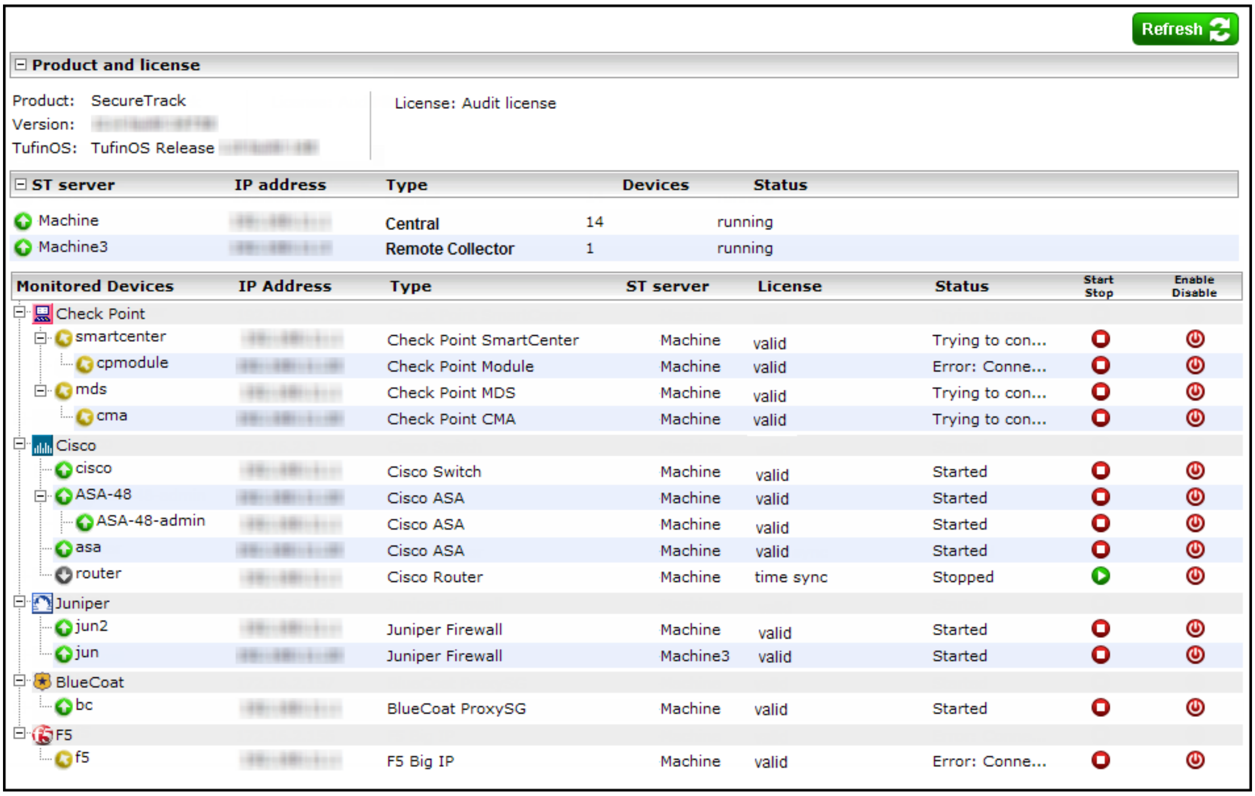
To activate the management devices:

- Ensure that a valid license is attached to all managed firewalls
- Disable the unlicensed firewalls
- Remove the unlicensed firewalls from SecureTrack

> After a new revision is pulled from the expired device, the entire device tree will be disabled

What Can I Do Here?

- Stop or start the SecureTrack process for any monitored device.
- Disable a device to make its license available to another device. After disabling the first device, restart the second to see the license applied to it.
- Hover over the device status to see details of the status of the device



Product and license

Product: SecureTrack
Version: [redacted]
TufinOS: TufinOS Release [redacted]

License: Audit license

ST server	IP address	Type	Devices	Status
Machine	[redacted]	Central	14	running
Machine3	[redacted]	Remote Collector	1	running

Monitored Devices	IP Address	Type	ST server	License	Status	Start Stop	Enable Disable
Check Point							
smartcenter	[redacted]	Check Point SmartCenter	Machine	valid	Trying to con...	⏹	⏻
cpmodule	[redacted]	Check Point Module	Machine	valid	Error: Conne...	⏹	⏻
mds	[redacted]	Check Point MDS	Machine	valid	Trying to con...	⏹	⏻
cma	[redacted]	Check Point CMA	Machine	valid	Trying to con...	⏹	⏻
Cisco							
cisco	[redacted]	Cisco Switch	Machine	valid	Started	⏹	⏻
ASA-48	[redacted]	Cisco ASA	Machine	valid	Started	⏹	⏻
ASA-48-admin	[redacted]	Cisco ASA	Machine	valid	Started	⏹	⏻
asa	[redacted]	Cisco ASA	Machine	valid	Started	⏹	⏻
router	[redacted]	Cisco Router	Machine	time sync	Stopped	▶	⏻
Juniper							
jun2	[redacted]	Juniper Firewall	Machine	valid	Started	⏹	⏻
jun	[redacted]	Juniper Firewall	Machine3	valid	Started	⏹	⏻
BlueCoat							
bc	[redacted]	BlueCoat ProxySG	Machine	valid	Started	⏹	⏻
F5							
f5	[redacted]	F5 Big IP	Machine	valid	Error: Conne...	⏹	⏻

How Do I Get Here?

In SecureTrack, go to **Settings** > **Administration** > **Status**.

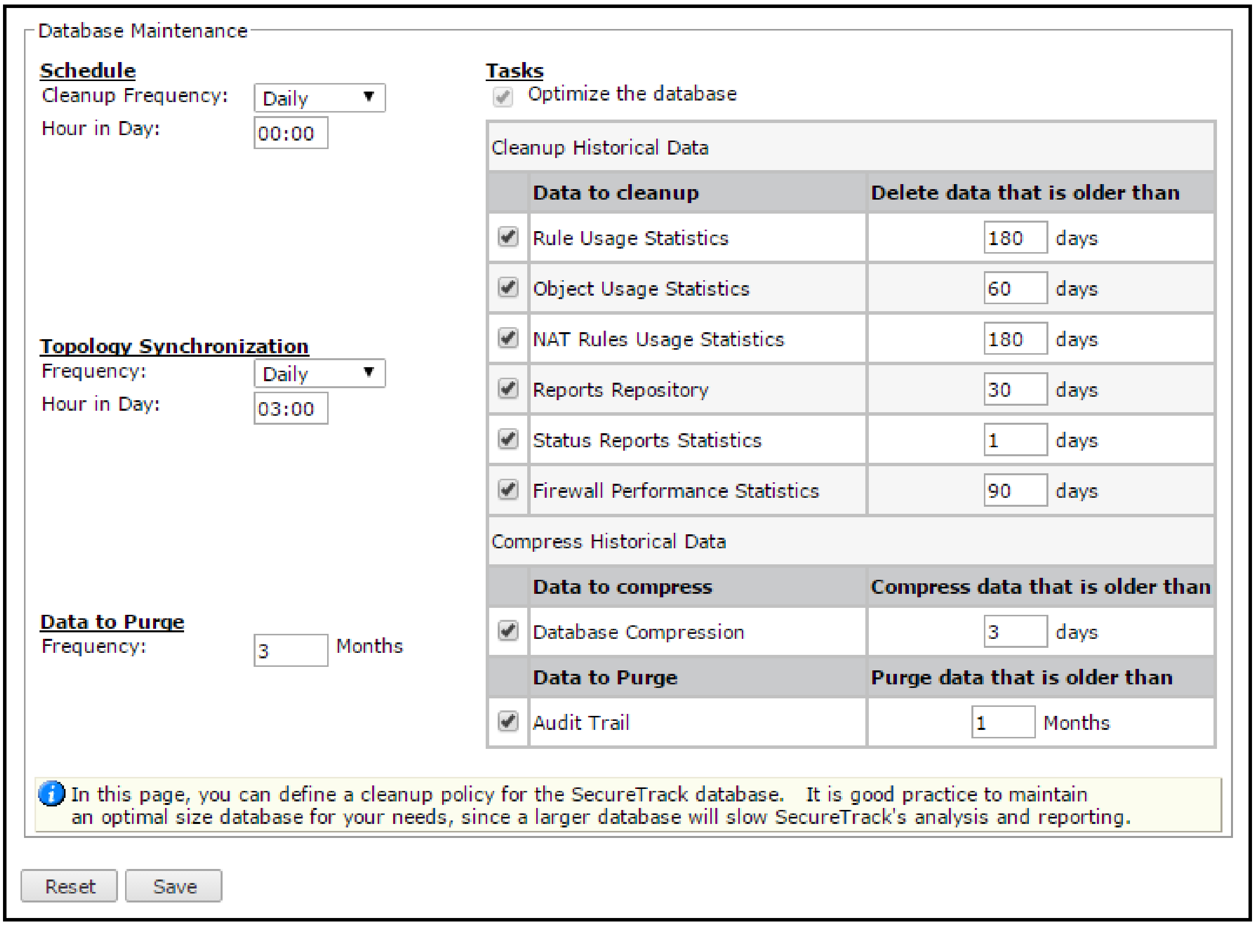
Database Maintenance

Includes:

- Database compression - Every time the cleanup process runs, it compresses all data that is older than the configured number of days
- Audit Trail purge - According to the configured frequency of purge, the audit trail logs that are older than the configured number of months are purged from the audit trail.

Here you can define a cleanup policy for the SecureTrack database. It is good practice to maintain an optimally-sized database for your needs. A large database will slow SecureTrack's analysis and reporting. This page is available only to SecureTrack Administrators.

After you make changes, click **Save**.



Database Maintenance

Schedule

Cleanup Frequency: Daily ▼

Hour in Day: 00:00

Topology Synchronization

Frequency: Daily ▼

Hour in Day: 03:00

Data to Purge

Frequency: 3 Months

Tasks

☑ Optimize the database

Cleanup Historical Data		
	Data to cleanup	**Delete data that is older than**
☑	Rule Usage Statistics	180 days
☑	Object Usage Statistics	60 days
☑	NAT Rules Usage Statistics	180 days
☑	Reports Repository	30 days
☑	Status Reports Statistics	1 days
☑	Firewall Performance Statistics	90 days
Compress Historical Data		
	Data to compress	**Compress data that is older than**
☑	Database Compression	3 days
	Data to Purge	**Purge data that is older than**
☑	Audit Trail	1 Months

ⓘ In this page, you can define a cleanup policy for the SecureTrack database. It is good practice to maintain an optimal size database for your needs, since a larger database will slow SecureTrack's analysis and reporting.

With the maintenance tasks you can:

- **Schedule**: The frequency and time of day that the maintenance tasks are run.

  Tasks: Delete historical data of the selected types, according to the specified retention periods

  - **Optimize the database**: Automatically optimize the database
  - **Rule Usage Statistics**: Data collected from device logs that shows the rules that receive traffic hits
  - **Object Usage Statistics**: Data collected from device logs that shows the objects that receive traffic hits
  - **NAT Rules Usage Statistics**: Data collected from device logs that shows the NAT rules that receive traffic hits
  - **Reports Repository**: Reports that are stored in the Reports Repository
  - **Status Reports Statistics**: Records of all the statuses of all devices on all servers
  - **Firewall Performance Statistics**: Performance data collected for Check Point devices
- , including:
  - Database compression - Every time the cleanup process runs, it compresses all data that is older than the configured number of days
  - Audit Trail purge - According to the configured frequency of purge, the audit trail logs that are older than the configured number of months are purged from the audit trail.
- **Topology Synchronization**: The time each day that SecureTrack collects topology information from enabled devices

  The default setting is to run the cleanup every day at midnight, and to run the topology synchronization every morning at 3am.

The backup and topology synchronization processes should not run at the same time. To prevent these processes from running at the same time:

a. Before backing up your database, check that the topology synchronization is not also running.

b. Schedule the Backup and Topology Synchronization to run at different times in which there will be no overlap between the two processes.

Data to Purge: Compress historical data to reduce the size of the database but keep access to the historical data

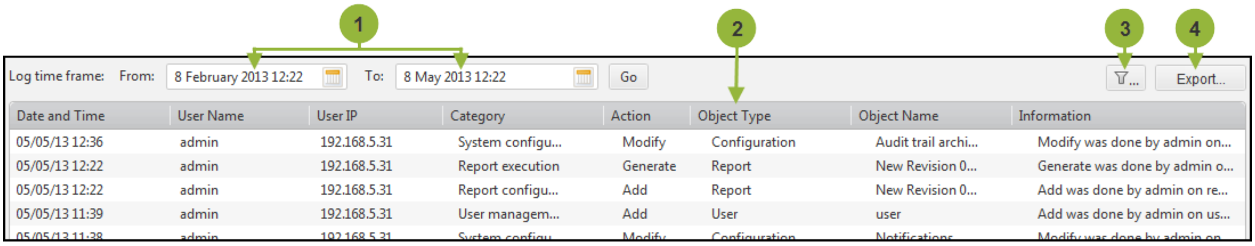
Compressed rule and object usage data is stored in the resolution of 1 day. If you run a Rule and Object Usage report on historical data that includes part of a day, the report time period is changed to include the data available.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Administration** > **Maintenance**.

SecureTrack Audit Trail

Every action that a SecureTrack user does in SecureTrack is recorded to give you complete accountability.



Log time frame: From: 8 February 2013 12:22 To: 8 May 2013 12:22

Date and Time	User Name	User IP	Category	Action	Object Type	Object Name	Information
05/05/13 12:36	admin	192.168.5.31	System configu...	Modify	Configuration	Audit trail archi...	Modify was done by admin on...
05/05/13 12:22	admin	192.168.5.31	Report execution	Generate	Report	New Revision 0...	Generate was done by admin o...
05/05/13 12:22	admin	192.168.5.31	Report configu...	Add	Report	New Revision 0...	Add was done by admin on re...
05/05/13 11:39	admin	192.168.5.31	User managem...	Add	User	user	Add was done by admin on us...
05/05/13 11:38	admin	192.168.5.31	System configu...	Modify	Configuration	Notifications...	Modify was done by admin on...

In the Audit Trail, you can:

1. Specify the start and end dates of the records that you want to see
2. See the list of the audit trail records
3. Filter the audit trail records based on any of the fields
4. Export the unfiltered or filtered results to a PDF file

You can also configure SecureTrack to send the actions to a syslog server.

The areas of SecureTrack that are audited are:

System Configuration	Device Monitoring, Analysis and Reporting
• User authentication	• Policy comparison
• Device management	• Revision and rules metadata
• License management	• Topology management
• Plugin and domain management	• Zone management
• System configuration	• Automatic policy generator jobs
• User management	• Report configuration and generation
	• Repository

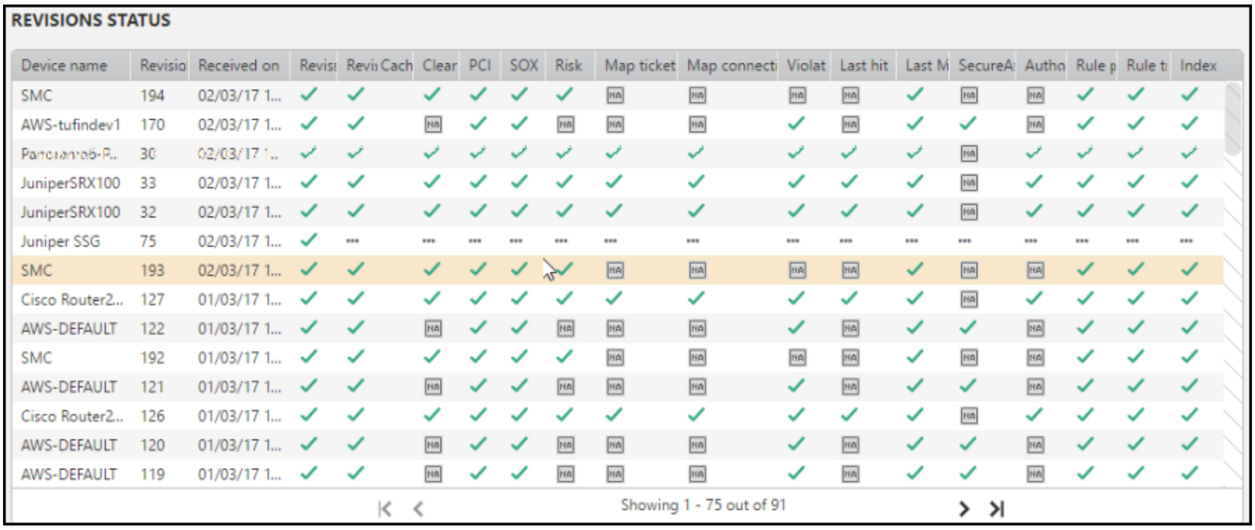
Each action is listed with:

- The date and time of the action
- The username of the user that did the action
- The IP address of the host from which the action was done (automatic actions, such as scheduled reports, are listed without a user IP address)
- The category or feature area that the action belongs to
- The type of action, such as add, remove, modify, or generate report
- The type of object and object name to which the action was done
- A description of the action

How Do I Get Here?

In SecureTrack, go to **Settings** > **Administration** > **Audit Trail**.

Revisions Status



REVISIONS STATUS

Device name	Revisio	Received on	Revis	Revi Cach	Clear	PCI	SOX	Risk	Map ticket	Map connecti	Violat	Last hit	Last M	SecureA	Autho	Rule p	Rule t	Index
SMC	194	02/03/17 1...	✓	✓	✓	✓	✓	✓	NA	NA	NA	NA	✓	NA	NA	✓	✓	✓
AWS-tufindev1	170	02/03/17 1...	✓	✓	NA	✓	✓	NA	NA	NA	✓	NA	✓	✓	NA	✓	✓	✓
Panorama6-P..	30	02/03/17 1...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	NA	✓	✓	✓	✓
JuniperSRX100	33	02/03/17 1...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	NA	✓	✓	✓	✓
JuniperSRX100	32	02/03/17 1...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	NA	✓	✓	✓	✓
Juniper SSG	75	02/03/17 1...	✓	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••	•••
SMC	193	02/03/17 1...	✓	✓	✓	✓	✓	✓	NA	NA	NA	NA	✓	NA	NA	✓	✓	✓
Cisco Router2...	127	01/03/17 1...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	NA	✓	✓	✓	✓
AWS-DEFAULT	122	01/03/17 1...	✓	✓	NA	✓	✓	NA	NA	NA	✓	NA	✓	✓	NA	✓	✓	✓
SMC	192	01/03/17 1...	✓	✓	✓	✓	✓	✓	NA	NA	NA	NA	✓	NA	NA	✓	✓	✓
AWS-DEFAULT	121	01/03/17 1...	✓	✓	NA	✓	✓	NA	NA	NA	✓	NA	✓	✓	NA	✓	✓	✓
Cisco Router2...	126	01/03/17 1...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	NA	✓	✓	✓	✓
AWS-DEFAULT	120	01/03/17 1...	✓	✓	NA	✓	✓	NA	NA	NA	✓	NA	✓	✓	NA	✓	✓	✓
AWS-DEFAULT	119	01/03/17 1...	✓	✓	NA	✓	✓	NA	NA	NA	✓	NA	✓	✓	NA	✓	✓	✓

Showing 1 - 75 out of 91

The Revisions Status page displays revision collection status information for every device monitored by SecureTrack. Each column identifies one of the processing steps taken by TOS when a new revision is received. The processing steps represented by the columns are:

- Device name - name of the device
- Revision number - number of the last revision received
- Received on - date and time the revision was received
- Revision retrieval - data received has been parsed
- Revision Caching - revision data has been cached to the TOS database
- Cleanup - rule cleanup actions have been completed
- PCI - PCI compliance has been calculated
- SOX - SOX compliance has been calculated
- Risk - Risk information for the Risk Browser has been calculated
- Map tickets - Ticket ID has been mapped to SecureChange for relevant rules in this policy revision
- Map connections - SecureApp applications have been mapped to the device rules
- Violations -Violations have been calculated
- Last hit - Last hit information has been calculated
- Last Modified - Last modified date has been calculated
- SecureApp metadata - Metadata for AWS objects and SecureApp has been cached
- Authorization - SecureChange authorization has been calculated
- Rule permissiveness - Rule permissiveness has been calculated
- Rule traffic - Changes in rules have been identified for unused objects cleanup calculation
- Index - Revision index for the search capability in Policy Browser and object lookup has been calculated

Hover over an icon to display a tooltip describing the specific status for that cell. Use the pagination controls (|< < > >|) to page through the devices displayed.

The icons identify the following status:

Icon	Description
✓	Completed successfully
✗	Failed to complete
NA	Not applicable for this device
•••	Pending
⟳	In progress

How Do I Get Here?

In SecureTrack, click on **Settings** > **Administration** > **Revisions Status**.

Customizing the Disclaimer

Overview

On the server, use the `set_disclaimer` script to modify the disclaimer text displayed on the SecureTrack login screen. You can add plain text or formatted text in HTML format.

What Can I Do Here?

Add a simple text disclaimer

1. Connect to the server CLI
2. Run the following:

```
/opt/tufin/securitysuite/scripts/set_disclaimer.sh --content "<text>"
```

Add a complex disclaimer from a file in HTML format

1. Connect to the server CLI
2. Run the following:

```
/opt/tufin/securitysuite/scripts/set_disclaimer.sh --full_path_to_content_file <file name>
```

Delete the disclaimer:

1. Connect to the server CLI
2. Run the following:

```
/opt/tufin/securitysuite/scripts/set_disclaimer.sh --content ""
```

Displaying the Navigation Menus in Japanese

You can configure SecureTrack to display the navigation menus in Japanese. The displayed language is determined in the file `/var/www/html/menuTranslations.js`. If this file does not exist, menus are displayed in English.

After each TOS upgrade, you need to repeat this process to ensure that any menu navigation changes are displayed correctly.

To display navigation menus in Japanese:

1. Connect to the SecureTrack server.
2. In the directory `/var/www/html/`, copy the provided menu language file:

```
# cd /var/www/html/

# cp menuTranslations.jp.js menuTranslations.js
```

For a High Availability (HA) deployment, repeat this process on each server.

To restore the navigation menus to English:

1. Connect to the SecureTrack server.
2. In the directory `/var/www/html/`, delete the file `menuTranslations.js`:

```
# cd /var/www/html/

# rm menuTranslations.js
```

For a High Availability (HA) deployment, repeat this process on each server.

Brute Force Protection

A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. SecureTrack provides the following brute force protection policy for SecureTrack users:

- REST API: 5 minute lockout after 2 failed login attempts within 1 second
- SecureTrack users: 45 minute lockout after 20 failed attempts within 12 hours

Use the `brute_force_protection.sh` script to enable or disable the policy. By default, brute force protection is enabled.

- View current status

  ```
  /opt/tufin/securitysuite/scripts/brute_force_protection.sh status
  ```

- Enable

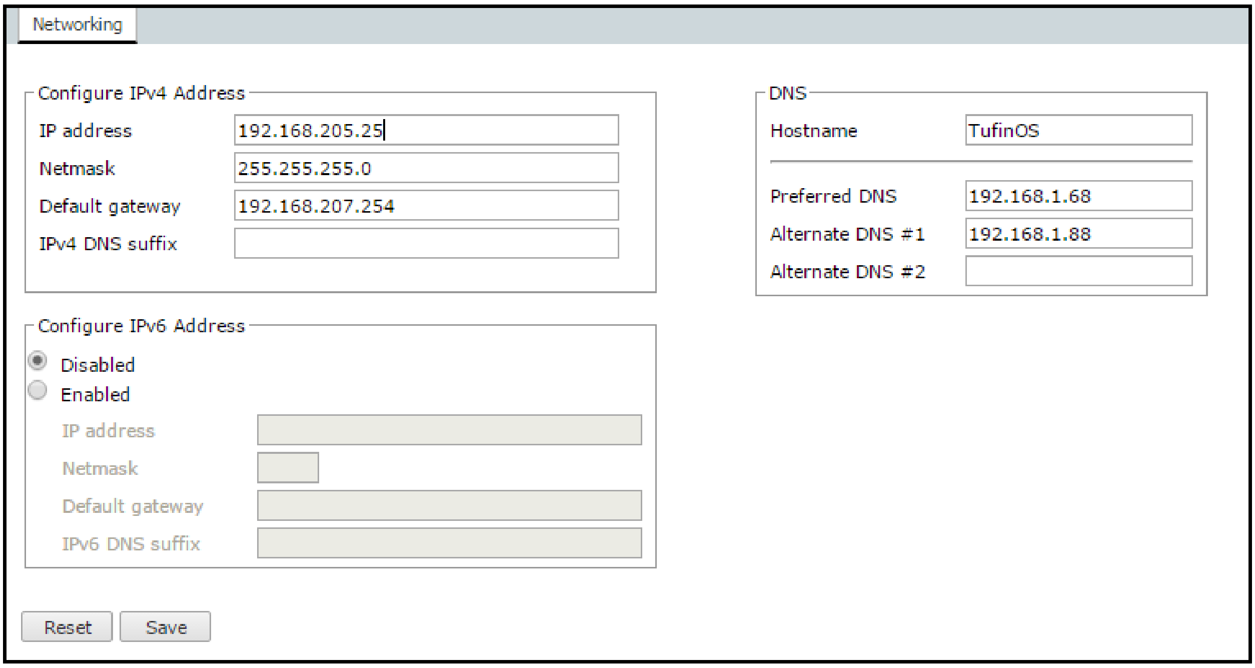
  ```
  /opt/tufin/securitysuite/scripts/brute_force_protection.sh enable
  ```

- Disable

  ```
  /opt/tufin/securitysuite/scripts/brute_force_protection.sh disable
  ```

Tufin Appliance Network Configuration

This page is available only to Administrators, and only for a Tufin SecureTrack appliance.



Configure IPv4 Address

IP address	192.168.205.25
Netmask	255.255.255.0
Default gateway	192.168.207.254
IPv4 DNS suffix	

Configure IPv6 Address

● Disabled

○ Enabled

IP address	
Netmask	
Default gateway	
IPv6 DNS suffix	

DNS

Hostname	TufinOS
Preferred DNS	192.168.1.68
Alternate DNS #1	192.168.1.88
Alternate DNS #2	

Here you can change:

- IPv4 networking - IP address, Netmask, Default gateway, IPv4 DNS suffix
- IPv6 networking - IP address, Netmask, Default gateway, IPv6 DNS suffix
- DNS - Hostname, DNS servers

How Do I Get Here?

In SecureTrack, go to **Settings** > **Configuration**.

Command Line Reference

The SecureTrack processes can be managed from the command line with these commands:

SecureTrack

```
st_add_user
```

Adds a SecureTrack Administrator; In a Multi-Domain environment, adds a Super Administrator. This command is useful if the Administrator's SecureTrack password has been forgotten.

The command initiates a series of prompts, for username, password, full name, and options for the new Administrator.

```
st info
```

If you encounter a problem that cannot be easily resolved, Tufin Support may ask you to send additional information. The "st info" command line collects SecureTrack logs and additional information, and places it in a file named st_info.tgz.

"st info" does not collect any part of the security policy (rules, objects, etc) or your organization's security configuration.

SecureTrack's web interface has an equivalent action.

```
st reconf [IP]
```

Notifies SecureTrack processes of an updated configuration.

To notify a specific connection, specify the device IP address as an additional parameter.

```
st restart [IP]
```

Stops and restarts all running connections to all devices.

To restart a specific connection, specify the device IP address as an additional parameter.

SecureTrack's web interface has an equivalent action.

```
st start [-s] [IP]
```

Starts the connections with all of the devices that are configured in SecureTrack.

To start a specific connection, specify the device IP address as an additional parameter.

Use the -s flag for stealth mode: does not provide feedback.

SecureTrack's web interface has an equivalent action.

```
st stat
```

Prints status information about the monitored devices, SecureTrack processes, and license and version information.

The command returns this information for each device:

- Management - Management server name or device name
- IP - IP address
- ID - SecureTrack ID# for the device
- Type - Device type
- PID - SecureTrack Process ID
- License - License status
- Status - Connection status

The command returns the status of these processes:

- Web server - the TOS web server
- Database - the TOS database
- Syslog processes - the SecureTrack processes that handle syslogs
- Job queue server - the server that handles TOS jobs such as reports
- Tufin Jobs service - the service that handles calculations for the dashboard browsers
- Tomcat server - the dynamic server that renders certain features in TOS
- DS connection - the service used for communication between servers in Distributed Architecture

For example:

```
         15465                 Valid           Connected
ADMIN_CMA        192.168.1.4          9          CMA            26374      Valid            Trying
Cisco_ext        192.168.1.5          10         Cisco          -          Evaluation       Started
Juniper_VPN      192.168.1.9          8          Netscreen      -          Evaluation       Started
 Web server: running
 Database: running
 Syslog ipc: running
 Syslog server: running
 Syslog bookkeeper: running
 Syslog message handlers: running
 Syslog traffic manager: running
 Syslog revision manager: running
 Job queue server: running
 Tufin Jobs service: running
 Tomcat server: running
 DS Tunnel: stopped
29 days left on evaluation license issued for: user
SecureTrack version: XX-X build XXXXX
```

If Check Point Customer Log Modules (CLMs) are being monitored for Rule Usage reports, the process monitoring each CLM will be displayed as well, and its type will be listed as CLM.

You can also see some of this information in SecureTrack in **Settings** > **Administration** > **Status**.

st stop [IP]

Stops all running connections to the devices.

To stop a specific connection, add the device IP address.

SecureTrack's web interface has an equivalent action.

`st version`

Displays the product version and build number. This information is also displayed in "st stat".

`tos conf`

Displays status of Tufin Orchestration Suite products, and prompts to change these settings.

`tos version`

Displays TufinOS and TOS versions currently installed.

`tos backup [--st] [--conf-only] [--stop-all] [--scw] <backup_file>`

Creates a backup of Tufin Orchestration Suite's current configuration and databases for restore and disaster recovery purposes. The backup includes all files necessary to restore a TOS server, but does not include files that are part of the operating system, such as `postgresql.conf`.

`--st` - Makes a backup of the SecureTrack database and configuration only

`--conf-only` - Makes a partial backup that includes only SecureTrack configuration information. You must use `--conf-only` with `--st` only.

`--stop-all` - Stops all SecureTrack and SecureChange processes before performing the backup. Use this option only if you need to make sure that revisions from after the time the backup is run are not included in the backup.

When `--stop-all` is used, some traffic usage information may be lost.

`--scw` - Makes a backup the SecureChange and SecureApp database and configuration only

`--sa` - Include Suite Administration backup data

`<backup_file>` - the name of the backup file. The file is compressed in TGZ format.

By default, the backup operation is performed while SecureTrack monitoring processes are active. A database locking mechanism makes sure the database maintains integrity.

When the Tufin databases take up most of the hard drive's disk space, this command may fail if the backup is made to a local (non-NFS) file.

`tos restore [--st] [--scw] <backup_file>`

Restores from a backup file to an existing TOS installation.

`--st` - Restores the SecureTrack database and configuration

`--scw` - Restores the SecureChange and SecureApp database and configuration

`-- sa` - Restores the Suite Administration backup data

The restore completely replaces the existing configuration and database of the TOS products specified by `--st`, `--scw`, `--sa` or any combination of them.

The target restore server must have the same TOS version and the same amount of installed RAM as the source backup server.

Deprecated Commands

You can use SecureTrack's web interface to add, delete and edit devices. As a result of this change, the following CLI commands have become obsolete:

st mgmt add

st mgmt edit

st mgmt delete

st device add

st device delete

st lic request <request file>

st lic add <license file>

Topology of a Generic Device: Sample File

This is an example of a file that you can use to create a generic device in Topology:

Generic device

```
Router2801#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.100.0.1 to network 0.0.0.0

     172.16.10.0/24 is subnetted, 1 subnets
C 172.16.2.0 is directly connected, FastEthernet0/1
```

```
     10.100.0.0/16 is subnetted, 1 subnets
C 10.100.0.0 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 172.16.10.10

Router2801#show ip interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 10.100.0.1/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  Output features: Post-Ingress-NetFlow
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
FastEthernet0/1 is up, line protocol is up
  Internet address is 172.16.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 101
  Inbound access list is 101
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: Ingress-NetFlow, Access List, MCI Check
  Output features: Post-Ingress-NetFlow, Access List
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
Router2801#
```

Topology of a non-Cisco Generic Device: Sample File

This is an example of a file that you can use to create a generic device in Topology for a non-Cisco device:

```
Name, Ip, Mask, Vrf
```

```
interface1, 1.1.1.1, 255.255.255.0
interface1, 1.1.2.1, 255.255.255.0
interface2, 1.1.1.1, 255.255.255.0, vrf1
interface2, 1.1.3.1, 255.255.255.0, vrf1
interface3, 2.2.2.2, 255.255.255.0, vrf2

Destination, Mask, Interface, Next-Hop, Vrf
5.5.5.5, 255.255.0.0, , 1.1.1.3
6.6.6.6, 255.255.0.0, interface2, 1.1.1.3, vrf1
6.6.6.6, 255.255.0.0, , 2.2.2.3, vrf1
0.0.0.0, 0.0.0.0, interface2, 1.1.1.4
```

Topology of Generic MPLS VPN Device: Sample File

This is an example of a file that you can use to create a generic MPLS VPN device in Topology:

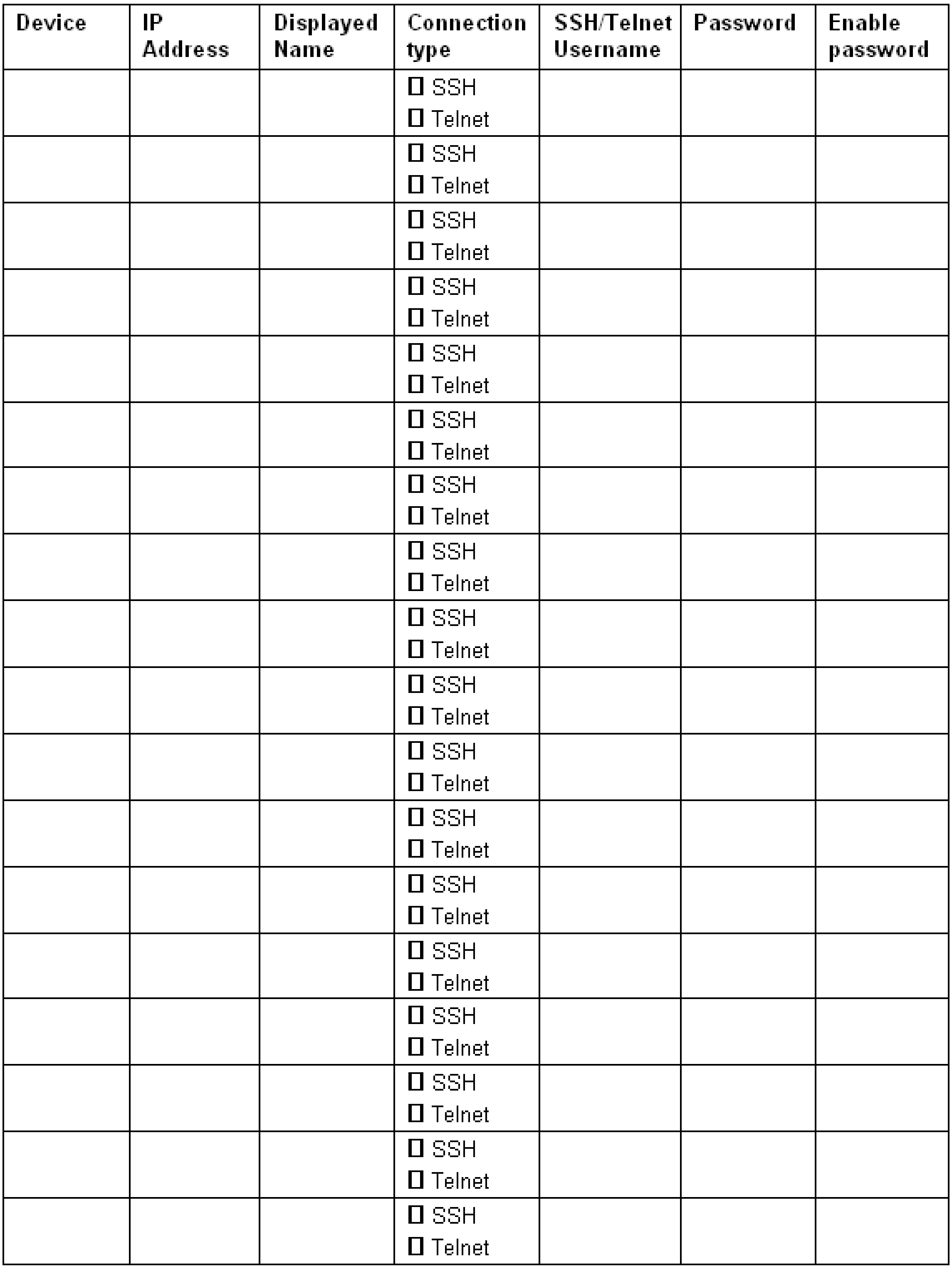
generic non-Cisco MPLS VPN device

```
Name, Ip, Mask, Vrf, IsMPLS
FastEthernet0/0, 70.19.19.1, 255.255.255.255, , true
FastEthernet0/1, 10.19.19.0, 255.255.255.0, VRF_A
FastEthernet0/1, 20.19.19.0, 255.255.255.0, VRF_B

Destination, Mask, Interface, Next-Hop, Vrf
10.17.17.0, 255.255.255.0, ,70.17.17.1, VRF_A
20.17.17.0, 255.255.255.0, ,70.15.15.1, VRF_B

Destination, Mask, Next-Hop, InLabel, OutLabel, Vrf
10.17.17.0, 255.255.255.0, 70.17.17.1, , 80, VRF_A
10.19.19.0, 255.255.255.0, 0.0.0.0, 50, , VRF_A
20.17.17.0, 255.255.255.0, 70.15.15.1, , 85, VRF_B
20.19.19.0, 255.255.255.0, 0.0.0.0, 55, , VRF_B
```

Worksheets

Check Point Device Information Worksheet

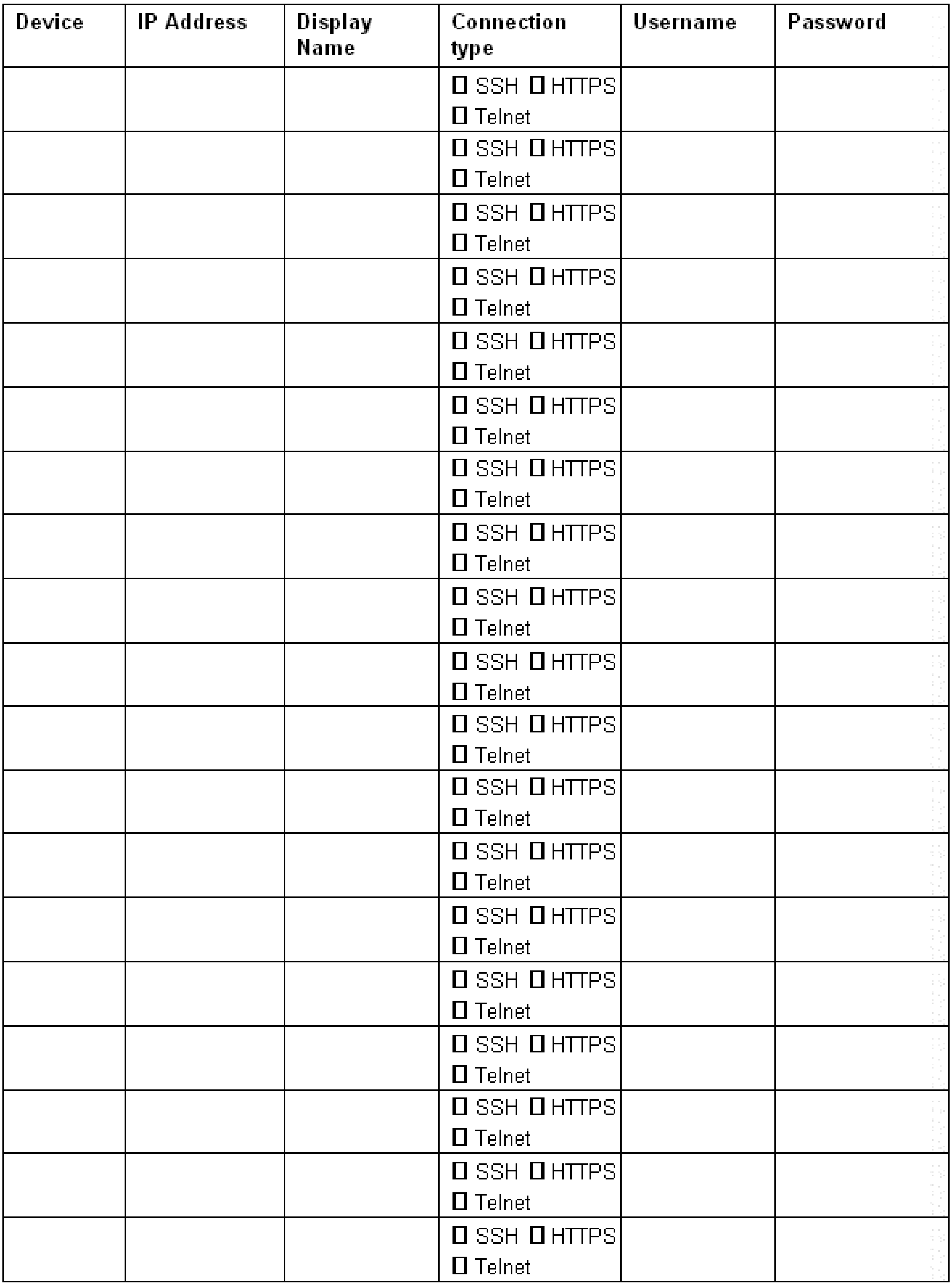
Cisco/TOP Device Information Worksheet



Device	IP Address	Displayed Name	Connection type	SSH/Telnet Username	Password	Enable password
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			
			□ SSH □ Telnet			

Juniper/Fortinet/Palo Alto Device Information Worksheet

Juniper, Fortinet, McAfee devices - either SSH or Telnet; Palo Alto devices - HTTPS



Device	IP Address	Display Name	Connection type	Username	Password
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		
			□ SSH □ HTTPS □ Telnet		

Troubleshooting SecureTrack

Database Disk Space is Low Alert

You may receive an automatic email from SecureTrack that the database directory's partition is running low on disk space. Consider doing one or more of the following:

- Allocating additional disk space for the partition.
- Removing older object usage statistics and policy analysis data. To configure the clean-up settings, go to **Configure** > **Administration** > **Maintenance**.

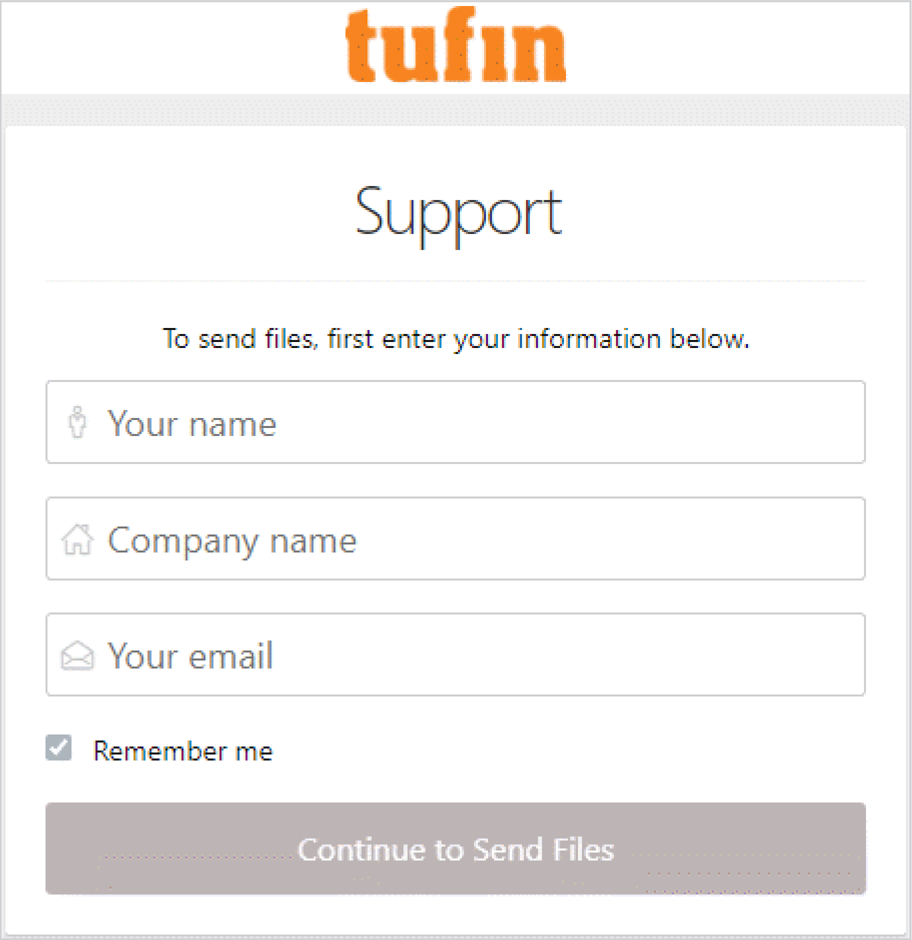
Sending Files to Tufin Support

Overview

Tufin’s Filer lets you securely send files to Tufin Support in a fast and secure manner via our SSL encrypted website https://transfer.tufin.com/u/support. The upload process sends a verification email to the address you enter, which includes a unique link to the file upload web page. Files uploaded to the Tufin Filer are deleted after two weeks.

Uploading a File

1. Go to https://transfer.tufin.com/u/support



tufin

Support

To send files, first enter your information below.

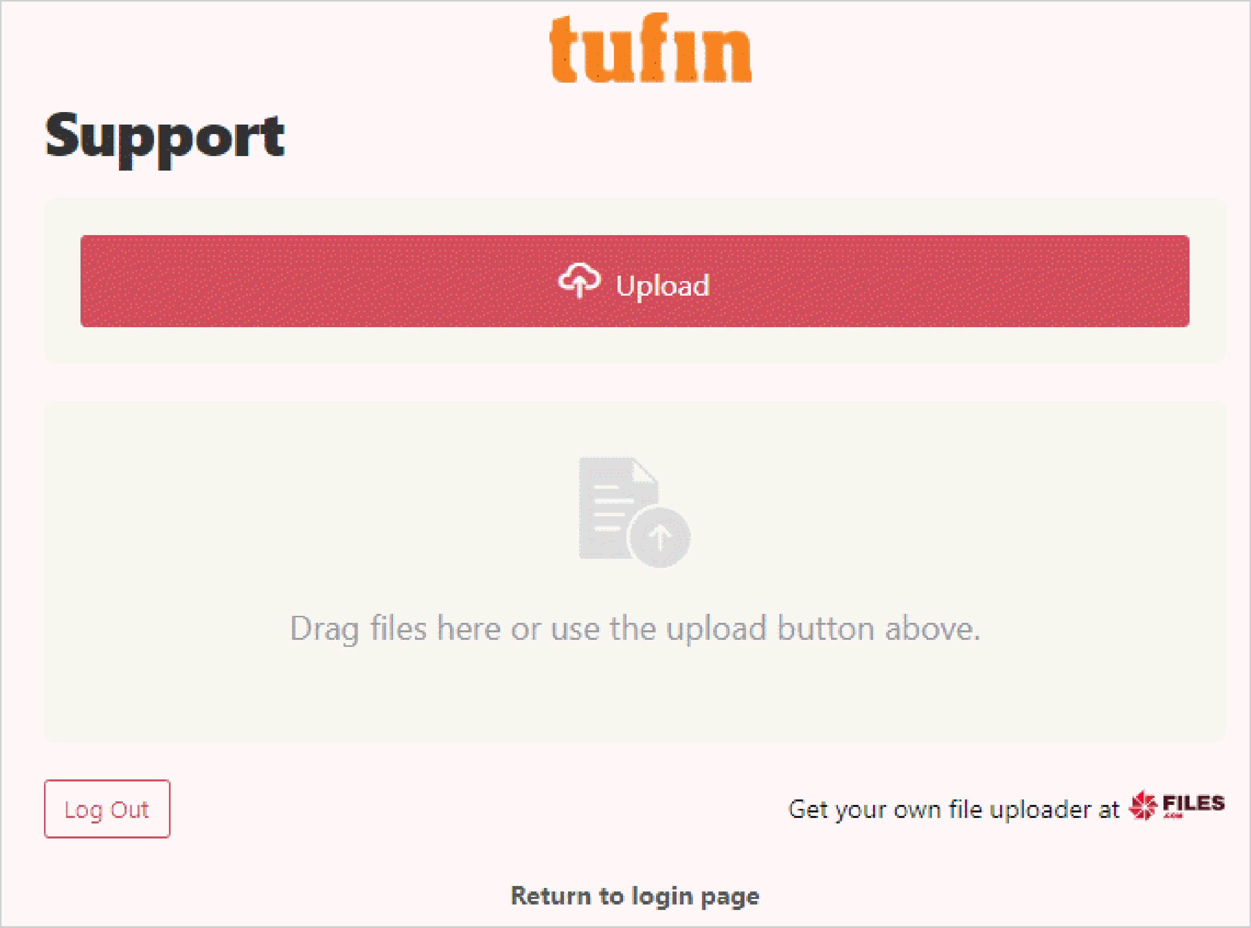
Your name

Company name

Your email

☑ Remember me

2. Enter you name, company name, and email address and click **Continue to Send Files**.



tufin
Support
Upload
Drag files here or use the upload button above.
Log Out
Get your own file uploader at FILES
Return to login page

Troubleshooting Network Connectivity

If a network connectivity problem is suspected, try the following solutions, in the order that they appear. After trying each solution, check whether the problem persists. If so, continue on to the next solution.

1. Try to connect from the SecureTrack host to the monitored device (for example, with the ping command). If unsuccessful, make sure that your network and routing is properly configured.
2. Make sure that there is connectivity between the two hosts over the required ports, by using telnet:

   ```
   telnet <IP> <port#>
   ```

   If a port is closed, configure organizational firewalls to open the port.
3. For a non-Check Point monitored device, make sure that the device configuration allows authenticated Telnet/SSH connections.

Troubleshooting OPSEC Connectivity

To monitor Check Point management servers, SecureTrack requires OPSEC connectivity. If there is a problem with connectivity with the monitored device, and you have eliminated other causes, try the following solutions, in the order that they appear. After trying each solution, check whether the problem persists. If so, continue on to the next solution.

1. In SmartDashboard, make sure there is an OPSEC object for SecureTrack.
2. In SmartDashboard, open the OPSEC object, and make sure that the following settings are correct:
   a. In the **General** tab, under **Client Entities**, **LEA** and **CPMI** should both be selected.
   b. In the **CPMI Permissions** tab, there should be a read-only Permissions Profile.
   c. In the **General** tab, click **Communication**, and make sure that the trust state is either **Communicating** or **Trust Established**.

- If the trust state is **Initialized but trust not established** and you know the Activation Key that was configured in the OPSEC object, then after performing **Install Database**, in SecureTrack, edit the monitored device and establish trust by typing the **Activation Key** and clicking **Retrieve Certificate**.
- If the trust state is **Uninitialized**, or it is **Initialized but trust not established** and you do not know the Activation Key that was configured in the OPSEC object, set an **Activation Key** and click **Initialize**. After performing **Install Database**, in SecureTrack, edit the monitored device and establish trust by typing the **Activation Key** and clicking **Retrieve Certificate**.

d. In SmartDashboard, from the Policy menu, select **Install Database** (even if you did not make any changes, in case this step was previously forgotten). Make sure you receive a confirmation message: **Database Installation succeeded**.

3. Stop and then start the device in SecureTrack. Check whether the problem has been resolved.
4. On the Check Point management server, using vi or any other text editor, edit the following file:

   ```
   $FWDIR/conf/fwopsec.conf
   ```

   In Provider-1, before opening the file, set the shell to the correct CMA (with `mdsenv <cma>`).

   - The line containing `cpmi_server auth_port` should either be commented out (with `#`, this is the default setting), or uncommented, but with the default port number 18190.
   - The line containing `lea_server auth_port` should either be commented out (with `#`, this is the default setting), or uncommented, but with the default port number 18184.
   - If you made any changes to the file, on the management server, run: `cpstop` , and then: `cpstart` (in Provider-1: `mdsstop <cma>`, and then: `mdsstart <cma>`).
5. On the Check Point management server, using vi or any other text editor, edit the following file:

   ```
   $CPDIR/conf/sic_policy.conf
   ```

   In Provider-1, before opening the file, set the shell to the correct CMA (with `mdsenv <cma>`).

   - Search for the line containing: `LEA_clients` in the following form:

     ```
     ANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_comp
     ```

     This line should be active (without: `#`), and should contain: `sslca` .
   - Right below the previous line, you should see a line containing `CPMI_clients`, in similar form:

     ```
     ANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp
     ```

     This line should also be active (without: `#`), and should contain: `sslca` .
   - If you made any changes to the file, on the management server, run: `cpstop` , and then: `cpstart` (in Provider-1: `mdsstop <cma>` , and then: `mdsstart <cma>`).
6. Stop and then start the device in SecureTrack. Check whether the problem has been resolved.

Usage Report Error: Waiting for initial policy installation

If the Rule and Object Usage report produces this error message, it is because SecureTrack needs to receive a policy revision with an Install Policy action for each Check Point management server. Once this has occurred, run the Usage report again.

Wrong Policy Packages are Compared

If a Comparison Report compares the wrong Check Point Policy Packages to each other, this may be because the installation target gateways have not been defined on the Check Point management server (SmartServer or CMA).

To define installation target gateways for Policy Packages, for each Policy Package do the following:

1. In SmartDashboard, from the **Policy** menu, select **Policy Installation Targets**.
2. Select the relevant Policy Package.

3. Select **Specific Modules**.
4. Add and Remove installation target gateways so that only the relevant gateways appear under **In Installation Targets**.
5. Click **OK**.

SecureTrack should now compare the correct Policy Packages in Comparison Reports. These will also be the default Policy Packages shown when comparing policy revisions within SecureTrack.

TOS Maintenance and Configuration

Tufin Orchestration Suite (TOS) includes SecureTrack, SecureChange, and SecureApp.

Licensing TOS

License Types

TOS Classic uses the following types of license types:

- **Evaluation** - Obtained from Tufin resellers and installed on SecureTrack via SecureTrack's web interface. An Evaluation license provides full feature functionality, for a limited period, for example of 30 days.
- **Subscription** - License for a limited period that needs to be renewed periodically.
- **Perpetual** - License for an unlimited period of time.
- **Audit** - License which is used by Tufin partners to perform firewall audits for their customers.

The same license file can be used for both perpetual and subscription licenses, and it is possible to upscale by adding subscription licenses to the already existing perpetual licenses on the same file.

A license can include the following properties:

- **Attachable** - Attachable licenses are associated with a device as follows:
  - **SecureTrack** - SecureTrack can monitor revisions on the device.
  - **SecureChange** - You can include the device as a target on SecureChange tickets, excluding provisioning.
  - **Provisioning** - You can provision changes in the device,
  - **OS Monitoring**
- **Global** - License for the entire system, for example a license for a base component, or an HA license.

There are also licenses for SecureApp and Cloud installations.

License Expiration, Renewal, and Maintenance

Software License Expiration and Renewal

Tufin offers both perpetual and subscription licenses that can be attached to devices. The same license file can contain perpetual and subscription components (SKUs). Each SKU, includes the number of devices of each type that can be attached using that component.

Perpetual Licenses

Devices attached to a perpetual SKU will never expire.

If you increase the number of gateways managed by a monitored management server, inform your Tufin partner or Tufin, so that you can purchase an extension license. You can request and use a temporary evaluation license to ensure continuous service until Tufin generates an extended permanent license.

When importing and reinstalling a new license file, all devices attached to a perpetual SKU will continue to be attached to a perpetual SKU.

Subscription Licenses

Subscription licenses have an expiration date. Shortly (45 days by default) before a subscription expires, a notification is sent to your SecureTrack administrator listing the SKUs that are going to expire, and the devices covered by those SKUs. This information is also visible in the SecureTrack Licenses page.

Once a subscription license expires, the attached devices are considered **Unlicensed**. If you want to continue using these devices in TOS, you will need to attach them to available SKUs.

To renew your subscription, you will need to contact Tufin and purchase a new license file. You will then need to import the license file into the system. SecureTrack will then proceed to attach the **Expired** and **Plug and Play** devices, if there are enough available SKUs on the imported license file. If there are any **Unlicensed** devices, or devices with a **License about to be expired**, you will need to manually attach them to available SKUs.

Later expiration dates are attached to devices before earlier expiration dates to ensure that the device is covered for as long as possible. If there are not enough available SKUs, the devices will be considered **Unlicensed**.

> For **Plug and Play** devices (devices added beyond the license limit and monitored by SecureTrack for 30 days), SecureTrack will first attempt to attach them to a perpetual license SKU. If there are no available perpetual SKUs, SecureTrack will attach them to a subscription SKU, starting from the latest expiration date. If there is no available subscription license, the devices will remain plug and play until the renewal period expires.

Annual Maintenance and Support

In addition to the product component, a typical Tufin sale includes an annual Maintenance and Support component. Tufin Technologies issues a License Certificate (in PDF format) for each purchase, which details the expiration of the Maintenance and Support rights, before which the contract should be renewed.

Managing License Allocation

All devices need to be attached to a license component (SKU). When you import a license file into SecureTrack SKUs (perpetual and subscription) and activate it, the SKUs you purchased from Tufin become available for use, and can be attached to enabled devices.

If a device appears in the License page or in the Status page as **Unlicensed**, **Evaluation**, **Expired**, **About to be Expired**, or **Plug-and-Pla**y, then it either is not or soon will not be licensed. You can resolve this issue by attaching an available SKU to the device.

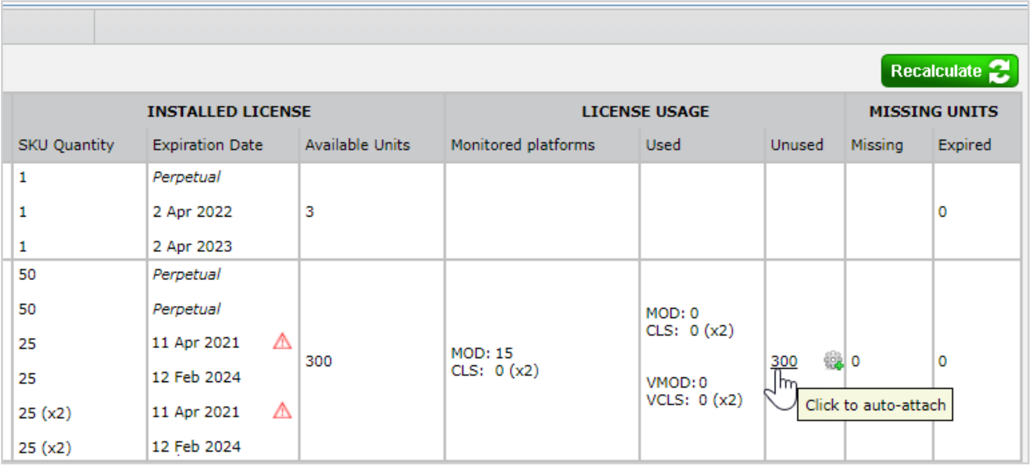
There are three options for attaching SKUs to devices:

- Automatically attach all unused SKUs
- Manually attach a device to a specific SKU
- Detach a device that does not need monitoring, and then attach its SKU to a different device.

After attaching the licenses, you will need to apply the change in the **Licenses** page for the changes to take effect

To Automatically Attach All Unused SKUs to Devices

1. Go to **Settings > Administration** > **Licenses.**
2. In the **Status** table, in the **Unused** column, click on the number of unused licenses to automatically attach them to devices.



INSTALLED LICENSE			LICENSE USAGE			MISSING UNITS	
SKU Quantity	Expiration Date	Available Units	Monitored platforms	Used	Unused	Missing	Expired
1 1 1	*Perpetual* 2 Apr 2022 2 Apr 2023	3					0
50 50 25 25 25 (x2) 25 (x2)	*Perpetual* *Perpetual* 11 Apr 2021 ⚠ 12 Feb 2024 11 Apr 2021 ⚠ 12 Feb 2024	300	MOD: 15 CLS: 0 (x2)	MOD: 0 CLS: 0 (x2) VMOD: 0 VCLS: 0 (x2)	300	0	0

When clicking on the link, SecureTrack attaches devices to the unused SKUs in the following order:

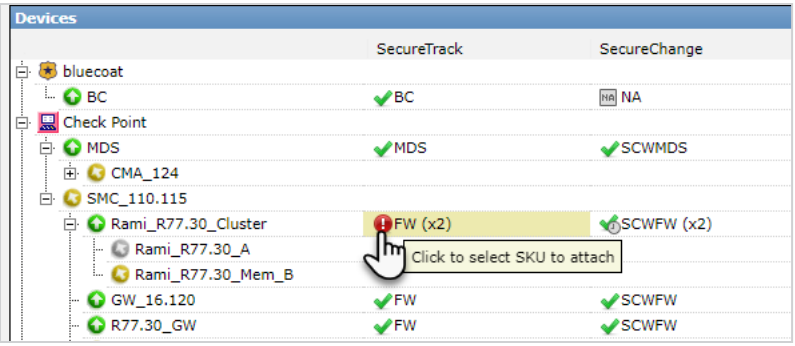
1. Expired devices
2. Unlicensed devices
3. Plug and Play devices
4. All other statuses

Expired devices are attached only to subscription licenses. For all other statuses, SecureTrack uses available perpetual licenses first, and then subscription licenses. When attaching a device to a subscription license, SecureTrack chooses the license with the latest expiration date, which will result in the device remaining monitored for the longest possible time period.

For physical firewall licenses, the licenses are first attached to the appropriate physical firewalls. If there are any remaining unused licenses, while there are not enough virtual licenses to cover all virtual devices, the unused licenses for physical firewalls will be automatically attached to virtual firewalls that require a license. With perpetual firewall licenses, this mechanism is applied from 21-3 HF2 and above.

To Manually Attach A Device to An SKU

1. Go to **Settings > Administration** > **Licenses.**
2. In the **Devices** license tree, click on the icon of a device that needs to be attached to an SKU.

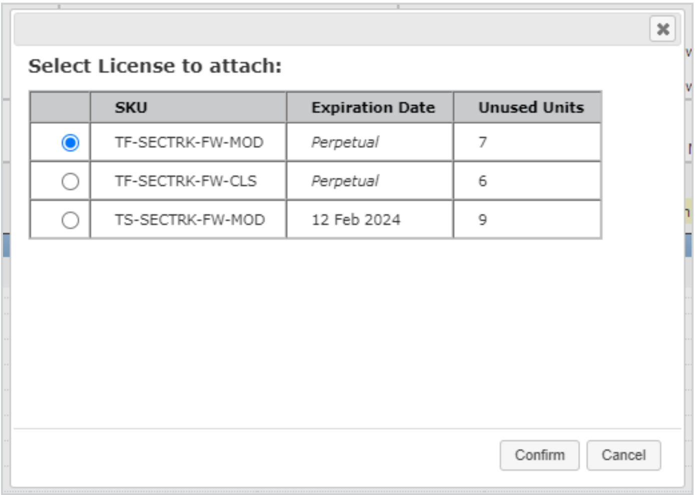


Devices

	SecureTrack	SecureChange
bluecoat		
BC	✓BC	NA
Check Point		
MDS	✓MDS	✓SCWMDS
CMA_124		
SMC_110.115		
Rami_R77.30_Cluster	FW (x2)	✓SCWFW (x2)
Rami_R77.30_A		
Rami_R77.30_Mem_B		
GW_16.120	✓FW	✓SCWFW
R77.30_GW	✓FW	✓SCWFW

Click to select SKU to attach

If there is only one relevant SKU, it is automatically attached to the device. If there are multiple types of available SKUs, a dialog box appears.



Select License to attach:

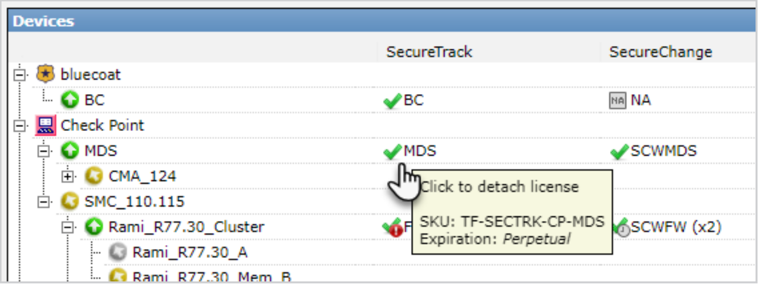
	SKU	Expiration Date	Unused Units
●	TF-SECTRK-FW-MOD	*Perpetual*	7
○	TF-SECTRK-FW-CLS	*Perpetual*	6
○	TS-SECTRK-FW-MOD	12 Feb 2024	9

3. Select the SKU to attach, and click **Confirm**.

   You can attach virtual firewalls to licenses for physical firewalls. For perpetual licenses, starting from 21-3 HF2 and above.

To Detach A Device From an SKU

1. Go to **Settings > Administration** > **Licenses.**
2. In the **Devices** license tree, click on the license status icon of the device you want to detach.



Devices

	SecureTrack	SecureChange
bluecoat		
BC	✓BC	NA
Check Point		
MDS	✓MDS	✓SCWMDS
CMA_124		
SMC_110.115		
Rami_R77.30_Cluster	✓F	✓SCWFW (x2)
Rami_R77.30_A		
Rami_R77.30_Mem_B		

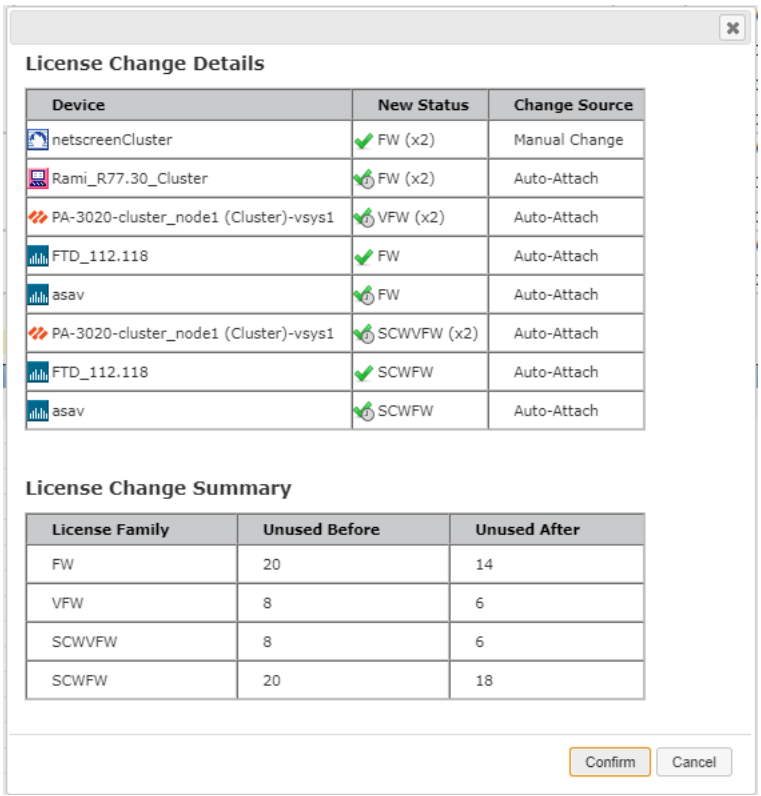
Click to detach license

SKU: TF-SECTRK-CP-MDS
Expiration: *Perpetual*

To Apply Changes Made to SKU Allocations

1. In the **Licenses** page, click **Apply**.

   A list of changes appears, with the net effects on license component availability:



License Change Details

Device	New Status	Change Source
netscreenCluster	✓ FW (x2)	Manual Change
Rami_R77.30_Cluster	✓ FW (x2)	Auto-Attach
PA-3020-cluster_node1 (Cluster)-vsys1	✓ VFW (x2)	Auto-Attach
FTD_112.118	✓ FW	Auto-Attach
asav	✓ FW	Auto-Attach
PA-3020-cluster_node1 (Cluster)-vsys1	✓ SCWVFW (x2)	Auto-Attach
FTD_112.118	✓ SCWFW	Auto-Attach
asav	✓ SCWFW	Auto-Attach

License Change Summary

License Family	Unused Before	Unused After
FW	20	14
VFW	8	6
SCWVFW	8	6
SCWFW	20	18

Changes that were made from the license table are marked as **Auto-Attach**; changes made from the device tree are marked as **Manual Change**.

2. Click **Confirm**.
3. If you still need additional licensing, purchase a Tufin license or license extension.

Additional Notes

- For Server Decommission and Clone Server Policy workflows, SecureChange license enforcement is based on a list of targets calculated by the ticket's tools. For these workflows a ticket handler cannot manage the target list or remove specific devices from a ticket, therefore the whole ticket is put on hold if an unlicensed device exists. After the appropriate SecureChange license is assigned to the device, the ticket will continue.
- The license status of management devices (such as Checkpoint CMA, Palo Alto Device Groups, and Fortinet ADOMs) is determined according to the accumulated license statuses of their managed firewalls. As a result, if there is at least one managed firewall with the license status **Expired** or **Unlicensed**, the management device will also have the license status **Expired** or **Unlicensed**.

  To resolve this, you can:

  - Ensure that a valid license is attached to all managed firewalls.
  - Disable the unlicensed firewalls (not supported for Check Point devices).
  - Remove the unlicensed firewalls from SecureTrack monitoring.

Licensing SecureTrack

Tufin's Simplified Licensing lets you manage your licenses easily with:

- Vendor-neutral licenses - For example, a license component purchased for a Check Point virtual cluster can be moved to be used for a Cisco virtual cluster.
- Per-gateway licenses - All vendors' firewall devices, including Check Point, licensing is per managed gateway and not by management server (CMA or SmartCenter). For example, you can license a subset of gateways managed by one Check Point management server.
- Simple tracking of license status - In SecureTrack (**Settings > Administration** > **Licenses**), you can see a clear view of license usage and device license statuses
  - SecureTrack and SecureChange - Easily move license components between devices
  - SecureApp - Quickly see how many licenses you have for applications and how they are allocated

Adding Licenses in SecureTrack

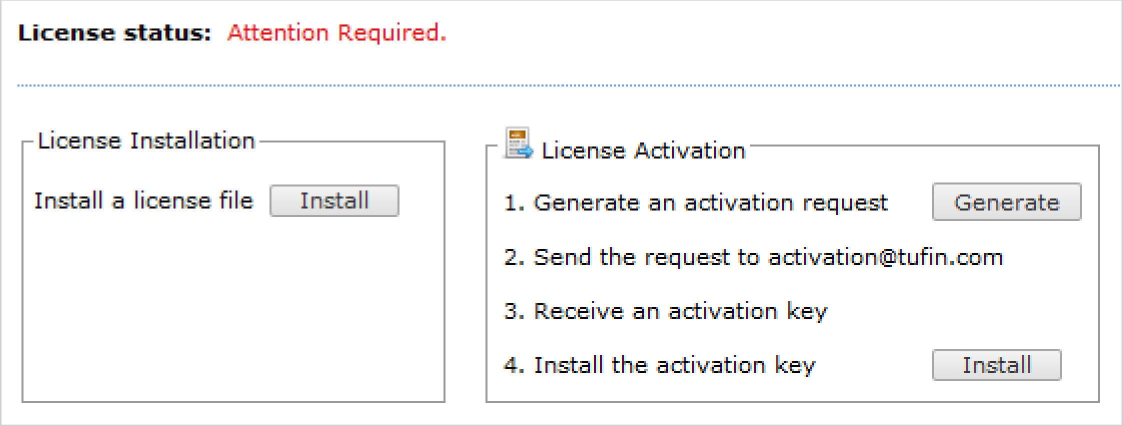
Use the following process to add licenses to SecureTrack.

Step 1: Download and Install Product

Download the software and documentation from the Tufin download center, and install the product on a supported platform.

Step 2 (Optional): Evaluate

1. Obtain an evaluation license from your Tufin partner or reseller, who has previously downloaded it from the Evaluation page.
2. Select **Settings** > **Administration** > **Licenses** and under **License Installation**, click **Install**:



License status: Attention Required.

License Installation

Install a license file

License Activation

1. Generate an activation request
2. Send the request to activation@tufin.com
3. Receive an activation key
4. Install the activation key

3. Navigate to the license file and click **Open**.

Step 3: Purchase Order (PO) and Permanent License

1. Send a PO, specifying optional features and the number of monitored devices of each type, to your Tufin partner or reseller. You will then receive an invoice and a permanent license file.
2. Under **License Installation**, click **Install**. Navigate to the license file and click **Open**.

Once the permanent license is installed, SecureTrack is fully functional.

Step 4: Activate License

To enable subsequent upgrades, the license needs to be activated:

1. Click **Generate**.
2. Save the generated file, and then email it to the Tufin activation team.
3. Tufin sends back an Activation Key. Normally, this takes about 3-5 business days.
4. Under **Activation**, click **Install**. Locate the license file and click **Open**.

Step 5: Attach Devices to SKUs

See Managing License Allocation.

How Do I Get Here?

In SecureTrack, go to **Settings** > **Administration** > **Licenses**.

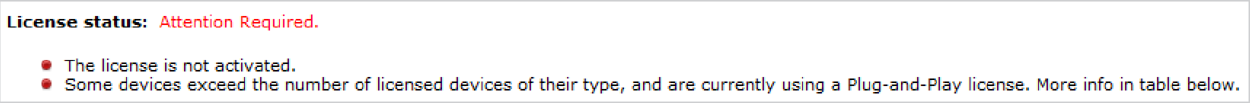
Viewing License Status

Detailed licensing statuses for the entire SecureTrack system, by license component and by device, are displayed in the **License** page, available to Administrators.

The **License** page contains the following information:

- **License Status messages:** messages related to the license status
- **License Status table:** The status of all installed licenses ordered by license component and by device
- **Devices License Tree:** The license status of each monitored device

License Status Messages



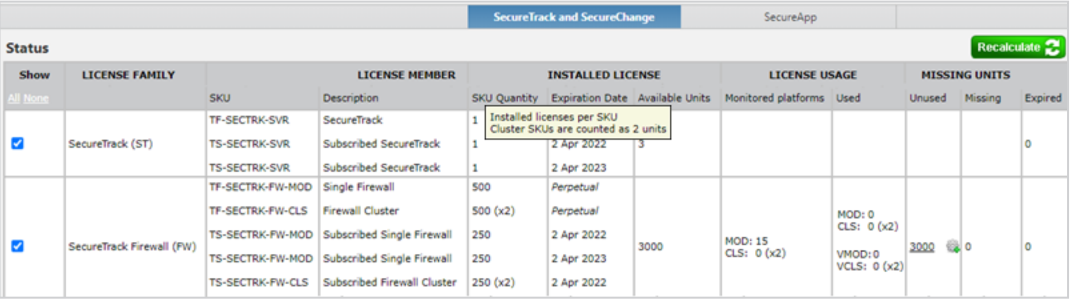
License status: Attention Required.

- The license is not activated.
- Some devices exceed the number of licensed devices of their type, and are currently using a Plug-and-Play license. More info in table below.

This section lists messages related to the status of your licenses. If there are issues with the licenses, **Attention Required** appears and lists the issues that need to be addressed.

After addressing the issues, it may take a few minutes for the updated status to appear.

License Status Table



Show	LICENSE FAMILY	LICENSE MEMBER		INSTALLED LICENSE			LICENSE USAGE		MISSING UNITS		
All None		SKU	Description	SKU Quantity	Expiration Date	Available Units	Monitored platforms	Used	Unused	Missing	Expired
☑	SecureTrack (ST)	TF-SECTRK-SVR	SecureTrack	1		3					0
		TS-SECTRK-SVR	Subscribed SecureTrack	1	2 Apr 2022						
		TS-SECTRK-SVR	Subscribed SecureTrack	1	2 Apr 2023						
☑	SecureTrack Firewall (FW)	TF-SECTRK-FW-MOD	Single Firewall	500	*Perpetual*	3000	MOD: 15 CLS: 0 (x2)	MOD: 0 CLS: 0 (x2) VMOD: 0 VCLS: 0 (x2)	3000	0	0
		TF-SECTRK-FW-CLS	Firewall Cluster	500 (x2)	*Perpetual*						
		TS-SECTRK-FW-MOD	Subscribed Single Firewall	250	2 Apr 2022						
		TS-SECTRK-FW-MOD	Subscribed Single Firewall	250	2 Apr 2023						
		TS-SECTRK-FW-CLS	Subscribed Firewall Cluster	250 (x2)	2 Apr 2022						

Installed licenses per SKU
Cluster SKUs are counted as 2 units

The table shows the complete list of licenses installed, as well as how they are allocated and used by your devices. If the **Missing Licenses** column is greater than 0, then you need to purchase the relevant SKU to be compliant with Tufin licensing requirements.

A license SKU may include one or two units depending on the type of SKU - single device or cluster. Cluster SKUs (physical and virtual) include two units, and cluster firewalls consume two units. In the table these are indicated as "(x2)", and you should multiply the number accordingly. For example, 250 (x2) = 500 units, which can be applied to 250 firewall clusters.

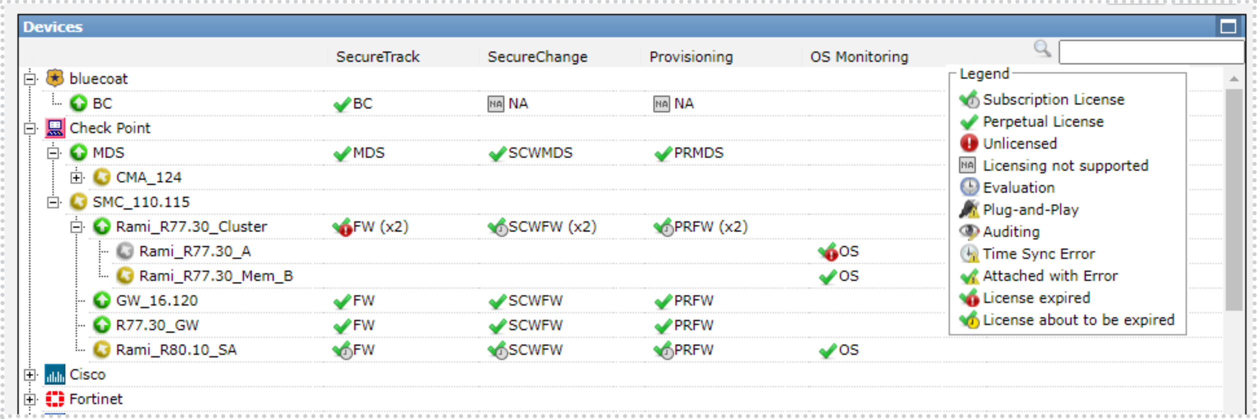
For each License Family, the **License Status** table displays:

- **License Family:** Name of the license family
- **License Member:** SKUs included in the installed license file, and their description.
- **Installed License:**
  - SKU Quantity - Installed licenses per SKU.
  - Expiration Date - The expiration date of each SKU. Perpetual SKUs are marked as **Perpetual**.
  - Available Units - The total number of available units per license family.
- **License Usage:**
  - Monitored Platforms - The number of platforms monitored by SecureTrack. For firewall devices, this column indicates how many single firewall module (MOD) and firewall cluster (CLS) devices require licenses.
  - Used - The number of platforms with an attached license. For firewall devices, this column indicates how many licenses have been allocated to single firewall module (MOD) and firewall cluster (CLS) devices. If a physical license is attached to both physical and virtual devices, the column will display how many licenses are attached to each device type.
  - Unused - The number of SKUs which have not been attached to a platform.
- **Missing Units:**
  - Missing - The total number of missing SKUs including expired SKUs. This is the number of additional SKUs needed to cover all monitored platforms
  - Expired - The number of SKUs that have expired

> For many columns, this information is also displayed in the tooltips.

If there are available SKUs in the **Unused** column, you can automatically attach them to devices by clicking on the link.

Devices License Tree



Devices

	SecureTrack	SecureChange	Provisioning	OS Monitoring
bluecoat				
BC	✓BC	NA	NA	
Check Point				
MDS	✓MDS	✓SCWMDS	✓PRMDS	
CMA_124				
SMC_110.115				
Rami_R77.30_Cluster	FW (x2)	SCWFW (x2)	PRFW (x2)	
Rami_R77.30_A				OS
Rami_R77.30_Mem_B				✓OS
GW_16.120	✓FW	✓SCWFW	✓PRFW	
R77.30_GW	✓FW	✓SCWFW	✓PRFW	
Rami_R80.10_SA	FW	SCWFW	PRFW	✓OS
Cisco				
Fortinet				

Legend
- Subscription License
- Perpetual License
- Unlicensed
- Licensing not supported
- Evaluation
- Plug-and-Play
- Auditing
- Time Sync Error
- Attached with Error
- License expired
- License about to be expired

Licenses are identified with the following icons:

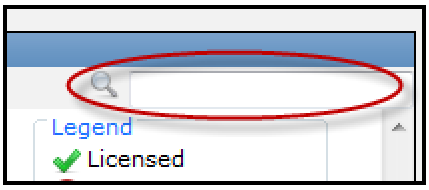
- **Subscription License** - License for a limited period that needs to be renewed periodically.
- **Perpetual License** - License for an unlimited period of time
- **Unlicensed** - Device does not have a license. If there are available licenses, when clicking on the icon, SecureTrack will attach the device to a license. If there are multiple relevant license files SecureTrack will prompt you to select which license to attach to the device.
- **Licensing not supported** - License is not supported for the device type
- **Evaluation** - Temporary license received form a Tufin reseller.
- **Plug-and-Play** - Device was added beyond the licensed limit, SecureTrack will monitors the device for 30 days. During this time you need to obtain an extended license.
- **Auditing** - License used by Tufin partners to perform firewall audits for their customers.
- **Time Sync Error** - The timestamp in the device is outside of the evaluation license validity. This occurs if the SecureTrack timestamp is not synchronized with the device timestamp, and the system is currently unable to determine the license status for the device.
- **Attached with Error** - The license was not correctly attached to the device or a parent or child in the device hierarchy was not licensed or it was disabled
- **License expired** - The License has expired and needs to be renewed.
- **License about to be expired** - The license will expire at the end of a defined period, by default 45 days.

To attach a device to an available **Perpetual** or **Subscription** license, click on the license icon. If there are multiple relevant licenses, you will be prompted to choose which one to attach.

The license status of individual switches and routers may be missing from the list because these devices are not displayed in the devices list. Switches and routers being monitored can be viewed on the Dashboard, and can be configured from **Settings** > **Monitoring** > **Manage Devices**.

You can filter the device tree in the following ways:

- To view only devices that require attention, select **Show only elements without permanent licenses**.
- To view only specific device types, select their corresponding check boxes in the license table above.
- To filter by device name, use the search box. Only devices with names including the search term, case-sensitive, are displayed.



Legend
✓ Licensed

How Do I Get Here?

In SecureTrack, go to **Settings > Administration** > **Licenses**.

SecureTrack License Components (SKUs)

This topic provides a general overview of the various SecureTrack license components offered by Tufin. For more detailed information, including support and pricing information, contact your Tufin partner or email us at salesops@tufin.com

Tufin licenses define the licensed components (SKUs), including the number of devices of each type that can be monitored. When you issue a purchase order to Tufin, you need to specify the SKUs, and when you add to the number of monitored devices of a particular type, or want to extend other functionality, you need to purchase an extended license.

Licenses can be purchased as perpetual licenses or on a subscription basis. Each SecureTrack installation requires a single SecureTrack base component with **TF-SECTRK-SVR** (perpetual) or **TS-SECTRK-SVR** (subscription) license. Subscription licenses for physical firewalls can be attached to virtual firewalls. High Availability requires an additional SKU.

SecureTrack for public cloud accounts (AWS, Azure) are only available as an annual subscription license.

Additional SKUs enable management and monitoring of different types and quantities of devices. Each component type requires a specific SecureTrack SKU. It is possible to combine both perpetual and subscription licenses for the different components. There are also various bundle options.

SecureTrack Audit SKUs are available for all supported devices.

Device	License Type	Examples
Check Point, Cisco, Juniper Networks, Fortinet, Palo Alto Networks, and Forcepoint firewalls and firewall clusters - physical and virtual	Firewall module /physical cluster/virtual context firewall/virtual cluster license - depends on how the firewall is configured	• **PA-VM:** Firewall license • **Check Point VSX:** Virtual context FW license • **Fortinet cluster with VDOMs:** virtual firewall cluster license
Check Point Provider-1 MDS Servers (Licenses for HA servers need to be purchased separately)	MDS license	
F5 BIG-IP LTMs	F5 BIG-IP LTMs license	
Blue Coat Proxy SG	Blue Coat Proxy SG license	
Cisco ACI (per ACI leaf)	Cisco ACI license	
Cisco Routers, switches, Juniper Networks M/MX routers	Router/Switch license	• **Juniper MX router:** Router/switch license • **Cisco Nexus switch:** Router/switch license
VMware NSX (per CPU)	NSX CPU license	
Azure, AWS (per account)	Public Cloud license	

Licensing SecureChange

Tufin licenses define the licensed components (SKUs), including the number of devices of each type that can be used as a target in a SecureChange ticket.

SecureChange requires a SecureTrack installation and the licensed SecureChange base component. Additional license components enable change management for different types and quantities of devices.

A SecureChange license entitles you to use all of the SecureChange features except for provisioning.

Provisioning

Tufin's provisioning license entitles you to:

- Let handlers update devices and policies directly from the Designer
- Let the Designer update devices and policies automatically in an auto step
- View any syntax-based change instructions using the Commands feature of Designer on supported devices

Adding SecureChange Licenses

The SecureChange licensing components are included in the SecureTrack license file. To obtain a license, please contact your Tufin partner or reseller. Once you have the license file, install it in SecureTrack's **Licenses** page, and update the license in SecureChange. After you install the license, you need to manually refresh the license status in SecureChange.

In addition, licenses automatically synchronize once a day around midnight.

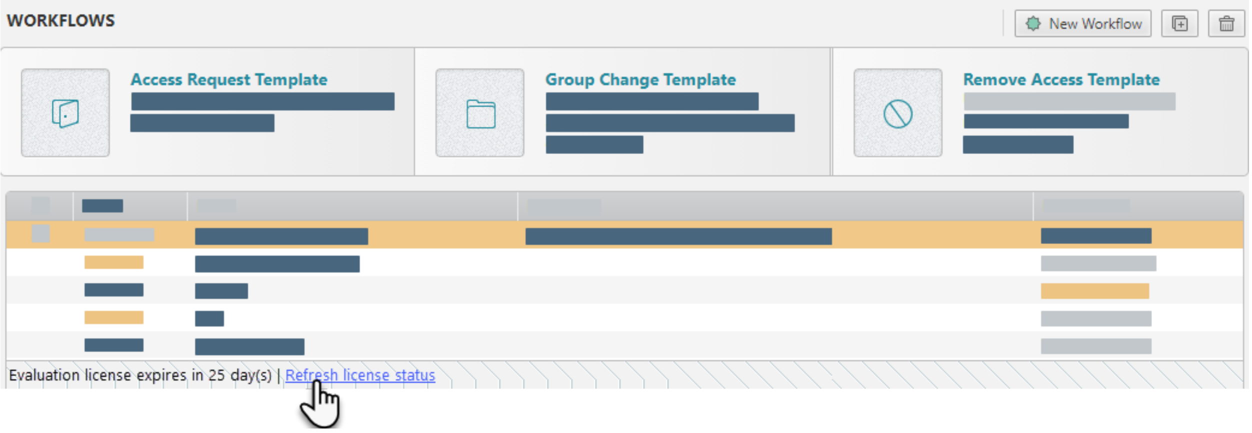
The license status is not visible to Requesters. (Users who can only submit requests.)

To Install a License

See Adding a License in SecureTrack.

To Manually Update The License Status in SecureChange

- In SecureChange, click **Refresh license status** at the bottom of the SecureChange window



Evaluation license expires in 25 day(s) | Refresh license status

SecureChange License Components (SKUs)

This topic provides a general overview of the various SecureChange license components offered by Tufin. For more detailed information, including support and pricing information, contact your Tufin partner or email us at salesops@tufin.com

Tufin licenses define the licensed components (SKUs), including the number of devices of each type that can be used as a target in SecureChange. When you issue a purchase order to Tufin, you need to specify the license components, and when you add to the number of monitored devices of a particular type, or want to extend other functionality, you need to purchase an extended license.

Licenses can be purchased as perpetual licenses or on a subscription basis. Each SecureChange installation requires a single SecureChange base component with **TF-SCWF-SVR** (perpetual) or **TS-SCWF-SVR** (subscription) license. This entitles you to use all SecureChange Network Change Automation features, except provisioning. **Change provisioning requires a separate SKU.**

Subscription licenses for physical firewalls can be attached to virtual firewalls. High Availability requires an additional SKU.

SecureChange for public cloud accounts (AWS, Azure) are only available as an annual subscription license.

You can purchase Network Change Automation and separate Change provisioning SKUs for the following devices:

Device	License Type	Examples
Check Point, Cisco ASA, Juniper Networks, Fortinet, Palo Alto Networks, and Forcepoint firewalls and firewall clusters - physical and virtual	Firewall module/physical cluster/virtual context firewall/virtual cluster license - depends on how the firewall is configured	- **PA-VM:** Firewall license - **Check Point VSX:** Virtual context FW license - **Fortinet cluster with VDOMs:** virtual firewall cluster license
Cisco IOS Router or Switch	Router/Switch license	
Cisco ACI (per ACI leaf)	Cisco ACI license	
Check Point Provider-1 MDS Servers	MDS license	
VMware NSX (per CPU)	NSX CPU license	
Azure, AWS (per account)	Public Cloud license	

Licensing SecureApp

A SecureTrack license grants you a SecureApp Basic license, allowing you to access up to three SecureApp applications (the first three you created in the system, in chronological order). Any additional application you want to create or access requires a separate license, which is installed through the SecureTrack licensing mechanism.

SecureApp gives unlicensed applications a temporary Plug-and-Play status, which is a 30-day grace period during which you can continue to access these applications while you purchase any additional license you require. After 30 days, the status of **Plug-and-Play** applications changes to **Unlicensed**, and their content becomes inaccessible.

SecureChange integration with SecureApp

SecureChange Basic is the version of SecureChange that is included when you purchase SecureTrack. SecureChange Basic lets you use the pre-defined workflows to manage network requests for your organization with all of the SecureChange features, except workflow customization. All other workflows and the SecureChange provisioning capabilities are only available for fully licensed SecureChange users.

When you purchase **SecureChange** and install the license, you can customize the workflows to match the processes that your organization uses to handle network requests, including conditional workflows and automatic actions. SecureChange is then integrated with SecureApp so that you can open change requests directly from SecureApp with the precise access requests to implement the SecureApp connections.

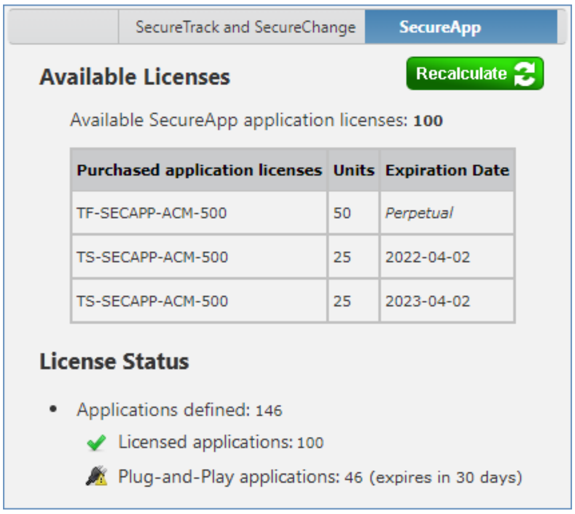
To Install a License

See Adding a License in SecureTrack.

To View The SecureApp License Status

1. In SecureTrack, go to **Settings** > **Administration** > **Licensing** and click on the **SecureApp** tab to view the license details:
    - **Available Licenses** shows the number of licenses you have and their names.
    - **License Status** shows the total number of applications you have, and specifies the sub-total number of applications in each

status: **Licensed**, **Plug-and-Play** and **Unlicensed**.



Available Licenses

Available SecureApp application licenses: **100**

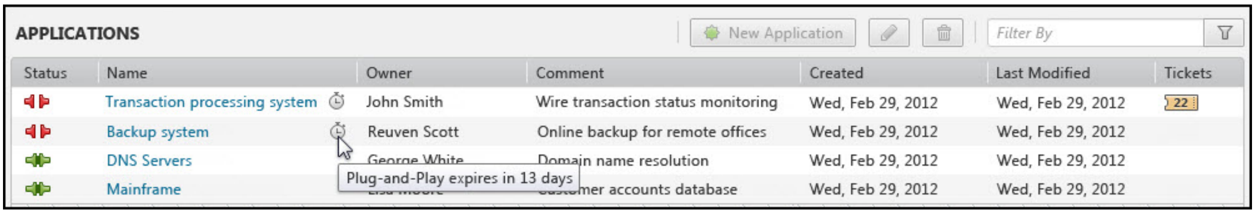
Purchased application licenses	Units	Expiration Date
TF-SECAPP-ACM-500	50	*Perpetual*
TS-SECAPP-ACM-500	25	2022-04-02
TS-SECAPP-ACM-500	25	2023-04-02

License Status

- Applications defined: 146
  - ✓ Licensed applications: 100
  - Plug-and-Play applications: 46 (expires in 30 days)

2. In SecureApp, go to the **Applications** view to see the license status in the applications list:

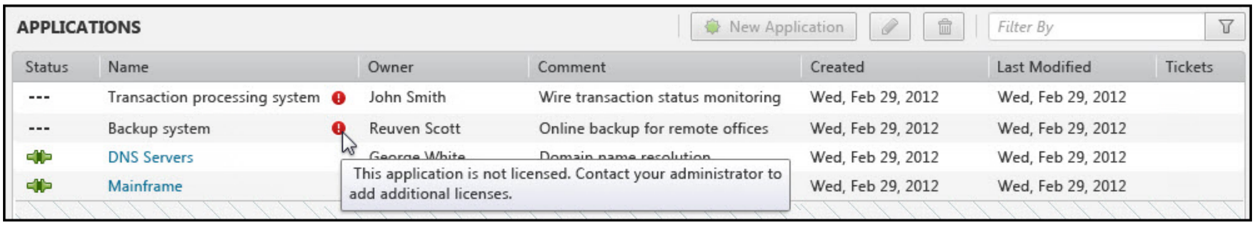
   - Plug-and-Play applications are indicated by the ⏱ icon:



Status	Name	Owner	Comment	Created	Last Modified	Tickets
	Transaction processing system ⏱	John Smith	Wire transaction status monitoring	Wed, Feb 29, 2012	Wed, Feb 29, 2012	22
	Backup system ⏱	Reuven Scott	Online backup for remote offices	Wed, Feb 29, 2012	Wed, Feb 29, 2012	
	DNS Servers	George White	Domain name resolution	Wed, Feb 29, 2012	Wed, Feb 29, 2012	
	Mainframe		...mer accounts database	Wed, Feb 29, 2012	Wed, Feb 29, 2012	

Plug-and-Play expires in 13 days

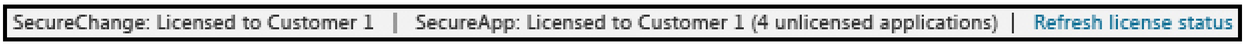
   - After 30 days, the status of these Plug-and-Play application changes to unlicensed, as indicated by the ❗ icon. The application content can no longer be accessed, so the application Name appears as text instead of a link:



Status	Name	Owner	Comment	Created	Last Modified	Tickets
---	Transaction processing system ❗	John Smith	Wire transaction status monitoring	Wed, Feb 29, 2012	Wed, Feb 29, 2012	
---	Backup system ❗	Reuven Scott	Online backup for remote offices	Wed, Feb 29, 2012	Wed, Feb 29, 2012	
	DNS Servers	George White	Domain name resolution	Wed, Feb 29, 2012	Wed, Feb 29, 2012	
	Mainframe			Wed, Feb 29, 2012	Wed, Feb 29, 2012	

This application is not licensed. Contact your administrator to add additional licenses.

   - The bottom left status bar indicates your license status. After you install a new license in SecureTrack, go to SecureApp's status bar and click **Refresh license status** to retrieve the updated data.



SecureChange: Licensed to Customer 1 | SecureApp: Licensed to Customer 1 (4 unlicensed applications) | Refresh license status

Deployment

TOS is designed for scalability, and can be used in businesses ranging small offices to large enterprises as well as Managed Security Service Providers (MSSP).

For large environments, you can deploy TOS with:

- High Availability - Uses multiple TOS servers to provide redundancy and disaster recovery.
- Distributed Architecture - Uses additional SecureTrack servers to collect revisions and send them to a central SecureTrack server for comparison, analysis and reporting.
- Multi-Domain Management - Lets you divide your devices into domains and manage access to the network information in SecureTrack and SecureChange with user and group permissions.

High Availability

High Availability (HA) provides minimal downtime and data loss in the event of a server failure, site failure, or scheduled maintenance. TOS data is automatically synchronized from an active TOS server to a standby TOS server to maintain maximum data integrity and continuity during the failover process. The standby TOS server can be on-site or at a remote disaster-recovery location.

In TOS HA, the active TOS server runs TOS and sends database updates to the standby server in real-time. The database updates include all configuration and policy changes. On the standby server, TOS is installed but is not enabled. The active server also sends write-ahead logs to reduce the possibility of lost database transactions. During a failover, TOS becomes enabled on the standby server and can receive connections from clients and devices.

High Availability Requirements

Each HA server, both appliance and VM, requires the following:

- **Memory and CPU requirements** - Each HA server must have the recommended memory and security requirements, based on your specific needs, as described in Hardware Requirements. When using virtual machines, each server requires dedicated memory and CPU.
- **Disk Space** - Each HA server requires storage of the same size. We recommend SSD for better performance. When using virtual machines, the storage disks on each virtual machine should be dedicated only to the HA server.
- **Network** - When using virtual machines, each virtual interface requires a corresponding dedicated physical interface, minimum 1Gb, on an ESX host.
- For automatic failover, when using virtual machines, all ESX servers which host HA servers must be on the same network

These requirements must be dedicated for each HA server and not shared with any other virtual machines.

To deploy TOS HA:

1. Install the same version of TufinOS and TOS on two servers.

   The servers can use any combination of platforms which are supported for TufinOS.
2. Setup the interfaces for the servers, especially the heartbeat interfaces, according to one of the HA deployment configurations.
3. Run the HA setup command to configure the management, database replication and heartbeat interfaces on the servers.

High Availability Scenarios

During the HA setup you can configure interfaces for these functions:

- **Management** - One or two interfaces of the servers that are each assigned a virtual IP address. Monitored devices send all communication to the virtual IP address and users connect to the virtual IP address to use the TOS products. When there is a failure on the active server, the virtual IP address directs connections from users and devices to the standby server. The failover is transparent to the users and devices. Then the administrator can resolve the cause of the failover and do a recovery to restore high availability.
  While the option to use a single management interface is available, Tufin's best practice recommendation is to use two management interfaces.
- **Database synchronization** - By default, the database synchronization is passed over the management interfaces. You can also dedicate an eth0 interface in each server for database synchronization traffic.
- **Heartbeat** - Two interfaces that maintain a heartbeat connection between the servers. The heartbeat process on the standby server sends keep-alive packets to the heartbeat interface on the active server to know when the management interface on the active server is down or when the active server is down.

  You can choose either unicast or multicast for the heartbeat communication within your HA cluster. The default (and Tufin's best practice recommendation) is unicast mode.

  The heartbeat interfaces of the two servers must be either **directly connected with a crossover cable**, **locally connected where each heartbeat pair is connected to a separate local switch**, or **remotely connected over a highly reliable, transparent layer-2 connection over VPN**. The 2 interfaces of each heartbeat link must be in the same network. A highly reliable heartbeat connection is critical to proper HA functioning. Disconnection of the heartbeat interfaces while the Active server is running causes a split-brain state, which can cause overload of device and network resources.

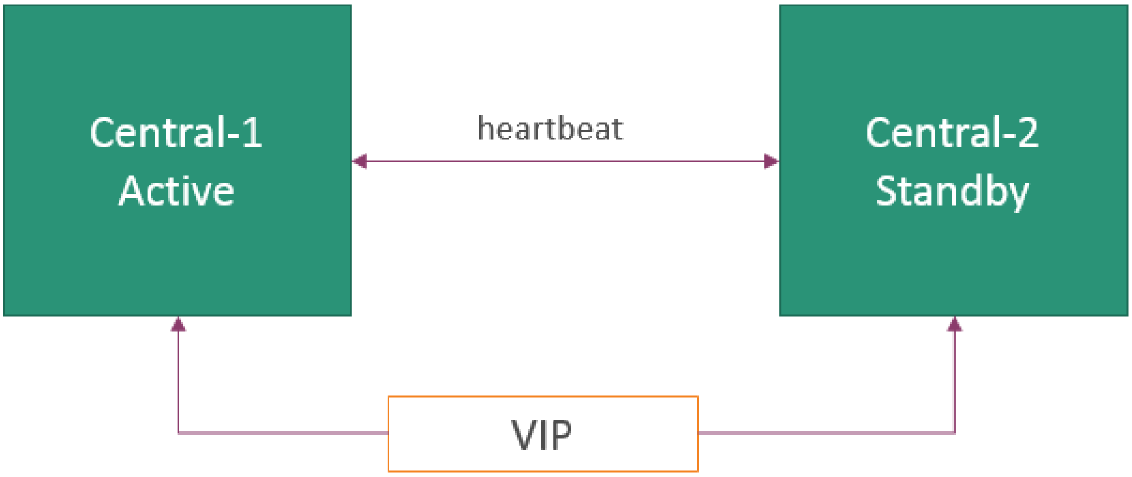
Single Server

In a standard installation of Tufin Orchestration Suite, all the applications (SecureTrack and SecureChange/SecureApp) are installed on a single server. In an HA deployment, you must install Tufin Orchestration Suite on a second server. One server is the active server, and one server is the standby server.

The two servers use the heartbeat interface to check the status of each other. When communication fails on the heartbeat connection, the standby server becomes the new active server.

The servers must be configured to use a VIP address, to allow traffic to be redirected to the currently active HA server. All communication to TOS will use the VIP address, ensuring that traffic is always directed to the currently active HA server.

The operating system on the servers needs to maintain an accurate date and time. Use chrony to automatically configure the server to self-synchronize with an NTP server.



Separate Servers for SecureTrack and SecureApp/SecureChange

If the volume of traffic for SecureTrack is expected to be high, you may want to have one server dedicated for SecureTrack, and a second server dedicated to SecureChange and SecureApp. In this scenario, implementing HA requires a total of four servers:

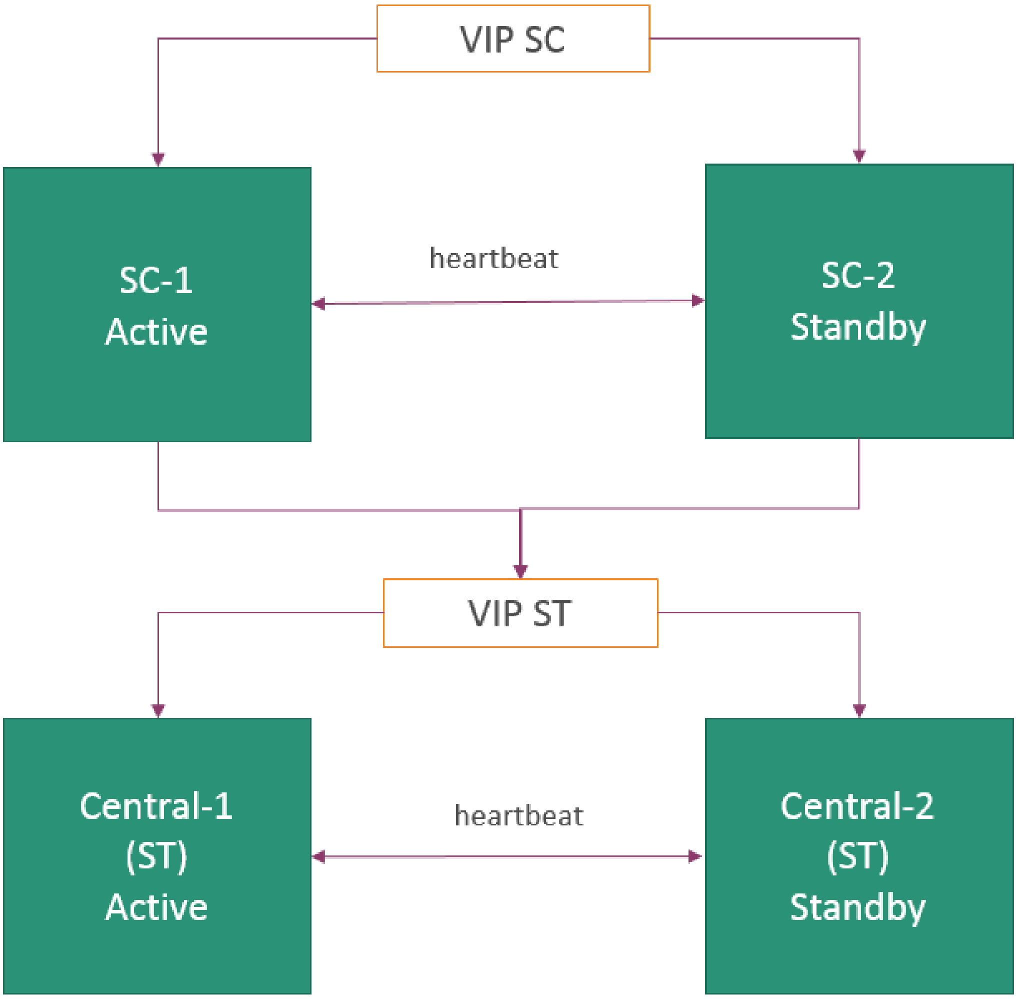
- Active SecureTrack server
- Standby SecureTrack server
- Active SecureChange/SecureApp server
- Standby SecureChange/SecureApp server

A heartbeat interface is configured between the active and standby SecureTrack servers, to determine liveness between the two SecureTrack servers. Another heartbeat interface is configured between the active and standby SecureChange servers, to determine liveness between the active and standby SecureChange/SecureApp servers. When the liveness check on the heartbeat interface determines that the active server is down, the appropriate standby server becomes the new active HA server.

The two SecureTrack HA servers must be configured to use a VIP address, to allow traffic to be redirected to the currently active SecureTrack HA server. The two SecureChange/SecureApp HA servers must be configured to use a VIP address as well, to allow traffic to be redirected to the currently active SecureChange/SecureApp HA server.

This architecture ensures high availability for both SecureTrack and for SecureChange/SecureApp.

The operating system on the servers needs to maintain an accurate date and time. Use chrony to automatically configure the server to self-synchronize with an NTP server.



Distributed Architecture with Distribution Servers

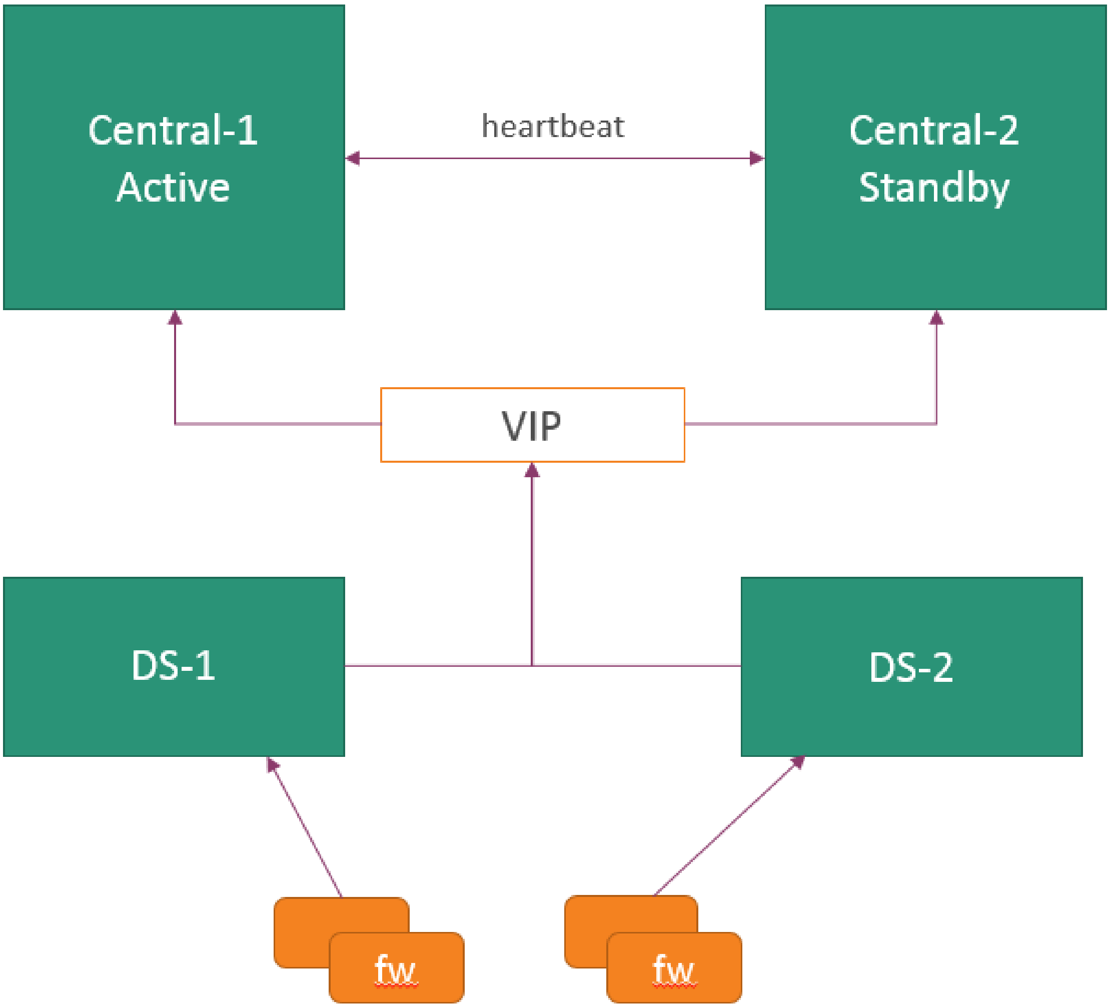
In a distributed architecture using distribution servers, you can also implement HA for the central server. (See Distributed Architecture for a detailed description of distributed architecture.) All TOS applications run on the active central server. A second central server is set up as the standby central server.

The two central servers use the heartbeat interface to determine the liveness of the other server. When communication fails on the heartbeat connection, the standby central server becomes the new active central server.

The central servers must be configured to use a VIP address, to allow traffic to be redirected to the currently active HA server. All communication from the distribution servers to the central server will use the VIP address, ensuring that traffic is always directed to the currently active HA central server.

The central server can be set up for HA. The distribution servers cannot be set up for HA.

> The operating system on the servers needs to maintain an accurate date and time. Use chrony to automatically configure the server to self-synchronize with an NTP server.



Distributed Architecture with Remote Collectors

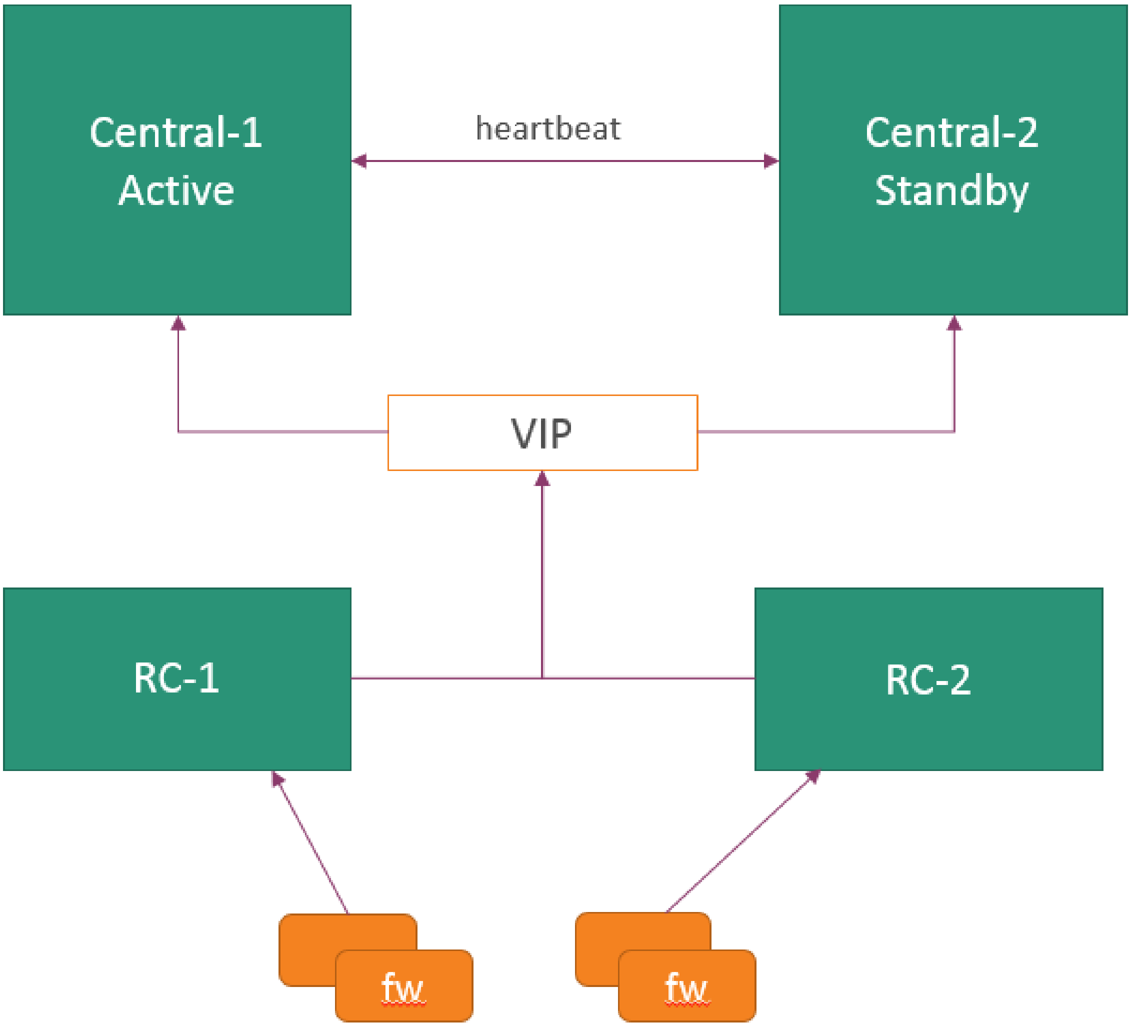
In a distributed architecture using remote collectors, you can also implement HA for the central server. (See Distributed Architecture for a detailed description of distributed architecture.) All TOS applications run on the active central server. A second central server is set up as the standby central server.

The two central servers use the heartbeat interface to determine the liveness of the other server. When communication fails on the heartbeat connection, the standby central server becomes the new active central server.

The central servers must be configured to use a VIP address, to allow traffic to be redirected to the currently active HA server. All communication from the remote collectors to the central server will use the VIP address, ensuring that traffic is always directed to the currently active HA central server.

The central server can be set up for HA. The remote collectors cannot be set up for HA.

The operating system on the servers needs to maintain an accurate date and time. Use chrony to automatically configure the server to self-synchronize with an NTP server.



High Availability Deployment Configurations

Automatic Failover

When configuring for automatic HA failover, both HA servers must be on the same network.

To support automatic failover, your servers must meet these minimum requirements:

1. More than one network interface on both servers
2. Heartbeat interfaces for each heartbeat link must be in the same network
3. At least one management network interface configured

For a list of the network ports that must be opened for bidirectional communication between the two HA servers, refer to the table of High Availability SecureTrack Ports and Services for Automatic Failover.

Manual Failover

When configuring for manual HA failover, each HA server can be on a different network. You must ensure that the required ports are open for bidirectional communication between the two servers.

To support manual failover, your servers must meet these minimum requirements:

- One management network interface configured

For a list of the network ports that must be opened for bidirectional communication between the two HA servers, refer to the table of High Availability SecureTrack Ports and Services for Manual Failover.

If HA is deployed on virtual machines, each virtual interface requires a corresponding dedicated physical interface, minimum 1Gb, on an ESX host. For HA system requirements, see High Availability

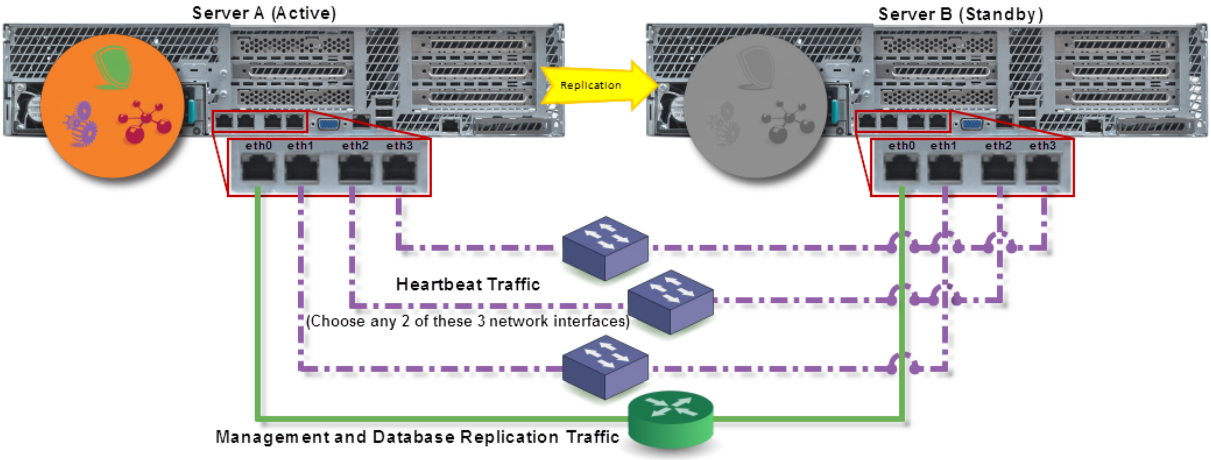
Single Management with Dual Heartbeat

The active and standby servers must have at least 3 network interfaces:

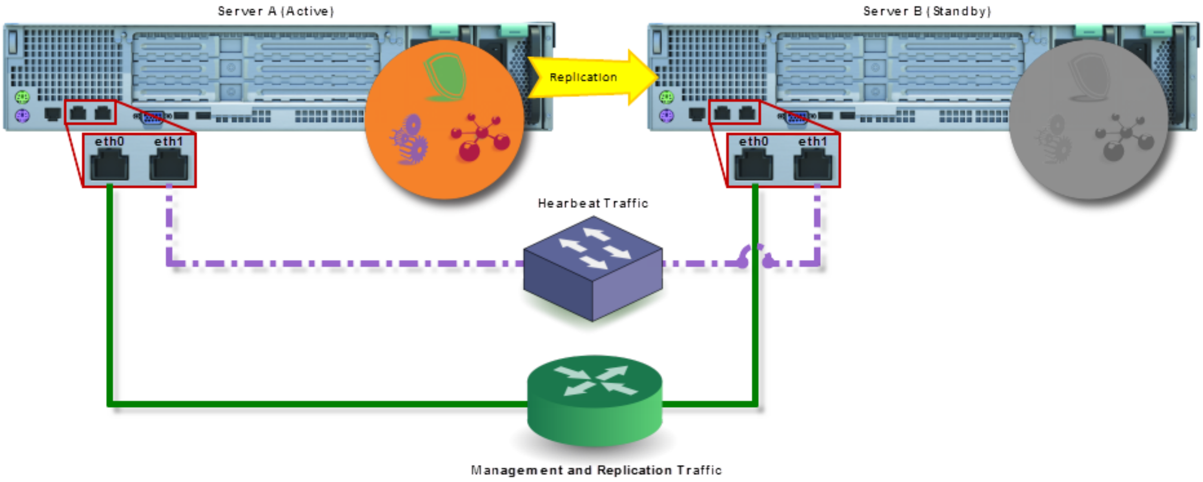
- 1 interface for device monitoring, TOS management and database replication
- 2 interfaces for the heartbeat

  The heartbeat interfaces can be configured on any two of the network interfaces, except for eth0 that is used for management traffic.

For T-1100/XL appliances, the connections are:



T-1000/XL appliances are supported with 2 network adapters, 1 for the heartbeat and 1 for device monitoring:



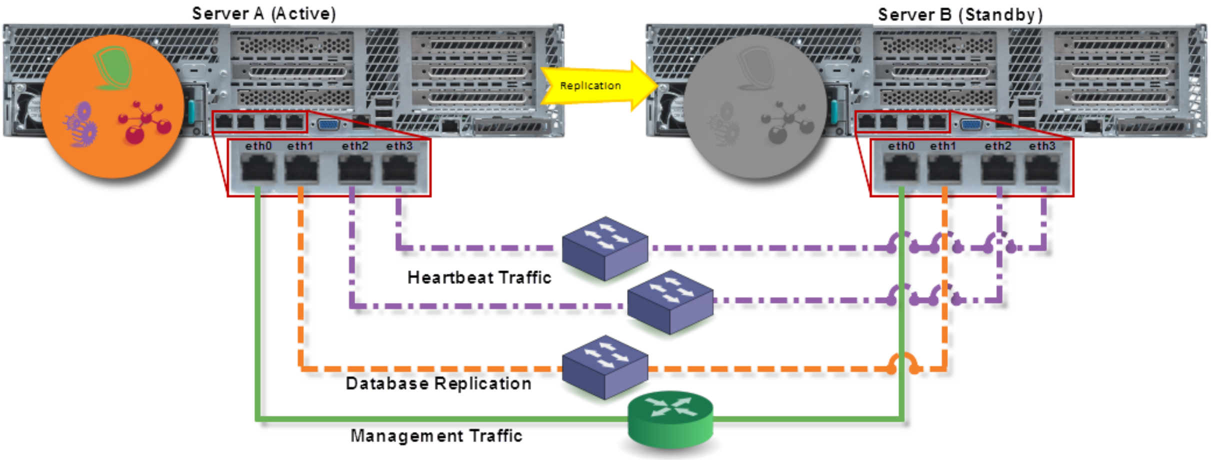
Single Management with Dual Heartbeat and Dedicated Database Sync

For improved performance, you can move the database replication traffic to a dedicated interface so that you use:

- 1 interface for device monitoring and TOS management
- 1 interface for database replication

  In this case, the database replication interfaces on the active and standby servers must be configured with IP addresses on the same network.

- 2 interfaces for the heartbeat



Dual Management with Dual Heartbeat

To allow for access to the server over more than one interface, you can configure two management interfaces so that you use:

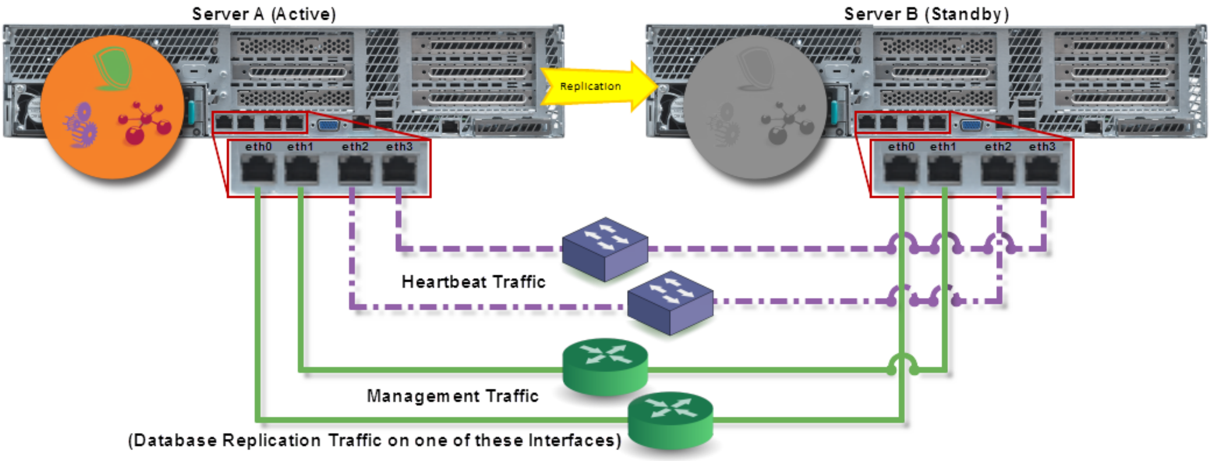
- 2 interfaces for device monitoring and TOS management

  You can select either of these interfaces for the database replication traffic.

  If you have networks that must communicate with a management interface and these networks are not in the scope of the default gateway route, then you must add a static route to the management interface to allow communication with these networks. For more about configuring static routes, see: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-networkscripts-static-routes.html

  If you configure database replication on eth1, the database replication interfaces on the active and standby servers must be configured with IP addresses on the same network.

- 2 interfaces for the heartbeat



Dual Management with Single Heartbeat and Dedicated Database Sync

To allow for access to the server over more than one management interface and segregation between management and database traffic, you can configure two management interfaces and a dedicated interface for database replication. However, in this configuration there can only be one heartbeat interface, which **increases the risk for a split-brain state**. The configuration includes:

- 2 interfaces for device monitoring and TOS management

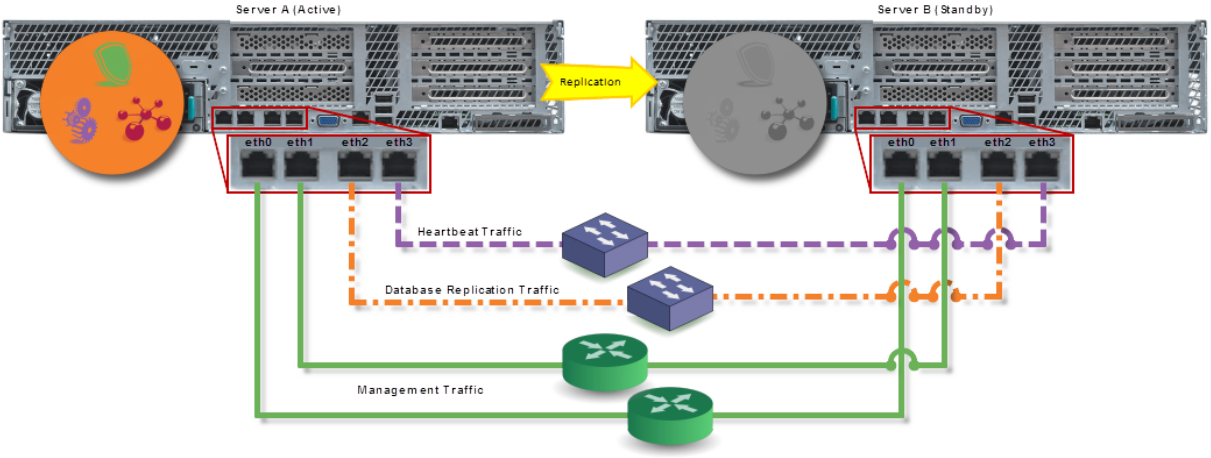
  If you have networks that must communicate with a management interface and these networks are not in the scope of the default gateway route, then you must add a static route to the management interface to allow communication with these networks. For more about configuring static routes, see: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-networkscripts-static-routes.html

- 1 interface for database replication

  In this case, the database replication interfaces on the active and standby servers must be configured with IP addresses on the same network.

- 1 interface for the heartbeat

  Disconnection of the heartbeat interfaces while the Active server is running causes a split-brain state, which can cause overload of device and network resources.



Setting Up High Availability

High Availability on SecureChange servers requires additional configuration. For more information, contact Tufin Support.

High Availability (HA) triggers an **automatic and transparent failover** when a failure is detected, or you can do a manual failover.

In the event of a failover, the virtual IP address directs connections from users and devices to the standby server and TOS sends a notification to SecureTrack administrators that shows the cause of the failover.

TOS becomes enabled on the standby server, and the standby server receives all user and device connections. Then the administrator can resolve the cause of the failover and do a recovery to restore high availability.

An administrator can also do a manual failover, which can be useful in the case of a gradual upgrade of TOS on the active and standby servers.

To restore the HA connection between the two servers, you must do a recovery. After the recovery, the server that was originally the standby remains the active server, and the server that was originally the active server is set up to become the standby server.

You can choose either unicast or multicast for heartbeat communication within your HA cluster. The default (and Tufin's best practice recommendation) is unicast mode.

- Unicast: If you enter 37.37.37.80/30 for the first network and 37.37.37.84/30 for the second network, then the IP addresses will be:

	Network Address	Heartbeat 1	Heartbeat 2
Active	37.37.37.80	37.37.37.81	37.37.37.85
Standby	37.37.37.84	37.37.37.82	37.37.37.86

- Multicast: The recommended multicast addresses are in the ranges: 226.0.0.0/8, 234.0.0.0/8, or 239.0.0.0/8: The default address for the first and second heartbeat connections are 226.94.1.1 and 226.94.1.2, respectively.

  Use the /29 or /30 network addresses for the first and second pairs of heartbeat interfaces: The first interface on each server has an IP address in a /29 or /30 network, and the second interface on each server has an IP address in a different /29 or /30network. IP addresses will be assigned to heartbeat interfaces on each cluster node from these networks.

  For example, if you enter 10.1.1.0 for the first network and 10.1.2.0 for the second network, then the IP addresses will be:

	Network Address	Heartbeat 1	Heartbeat 2
Active	10.1.1.0	10.1.1.1	10.1.2.1
Standby	10.1.2.0	10.1.1.2	10.1.2.2

  If the active server cannot send the database updates to the standby server, the database update files are stored on the active server and **may cause high disk usage**. To prevent this, repair the connection to the standby server or uninstall HA until connectivity is repaired.

  You must not do these actions when High Availability automatic failover is configured. Any of these actions can cause malfunction in HA automatic failover configuration.

- Changes in server configuration, for example: HA configuration, networking configuration, date
- Do not run CLI operations on any services that impact HA configuration, for example:

  ```
  systemctl restart network
  ifdown ethX
  systemctl stop pacemaker
  ```

⚠ WARNING: Manual reboot or shutdown can cause unexpected failover.

Prerequisites

This procedure can take many hours to complete, depending on the size and health of your database and your hardware resources.

To prepare two servers (any combination of platforms which are supported for TufinOS) for High Availability (HA) deployment:

1. On both servers:
   a. To make sure that all of the network adapters that you want to use are enabled in the BIOS of each server, run: `ifconfig -a`

      If you do not see all of the network adapters shown in the results, enter the BIOS and enable the adapters.

   b. To make sure that the heartbeat interfaces that you plan to use are enabled.
      i. Edit `ifcfg-ethX` file in `/etc/sysconfig/network-scripts/` on both the active and standby server for each heartbeat interface (for example, ifcfg-eth2 and ifcfg-eth3).
      ii. Change the `ONBOOT` value from no to `yes`, but do not configure the IP addresses.
      iii. Change the `BOOTPROTO` value from dhcp to `none`.
      iv. Restart the network service:

          ```
          systemctl restart network
          ```

   c. For the interfaces on both servers that you plan to use for management (you can use eth0 or both eth0 and eth1), configure the IP address and Netmask for those interfaces. The management interfaces do not need to be on the same network.

      If the system requires a default gateway, then the default gateway must be on either management interface 1 (eth0) or management interface 2 (eth1). Make sure that the devices and TOS servers that the server communicates with are connected to the interface that has the default gateway. TOS servers can include: SecureChange, Remote Collectors, and Distributions servers

   d. If you do not plan to use `eth0` for dedicated database synchronization, configure the IP address and Netmask for the database synchronization interface. The interfaces for dedicated database synchronization on both servers must be on the same network.

2. If you already have a TOS server that you want to use as the active server, continue with step 3.

   When the active server establishes a connection to the standby server, the existing ST and SC data on the standby server is deleted. Make sure you back up data stored on the standby server before you set up HA.

   If you do not already have a TOS server that you want to use as the active server, on the new active server:

   a. Install TOS.
   b. Log into SecureTrack.
      The first time you log in, you see the SecureTrack Setup Wizard.
   c. Follow the instructions in the setup wizard.

3. On the standby server:
   a. Install TOS.

      You must have the same version of TufinOS installed on both servers.

   b. Log into SecureTrack.

      The first time you login, you see the SecureTrack Setup Wizard.

   c. Follow the instructions in the setup wizard.
   d. Create a secret token from the CLI:

i. Run: `/usr/local/st/ha_secret_token.sh create`

ii. Enter a character string of at least 8 characters that you will also enter as the secret token when you configure HA on the active server. The string can include numbers (0-9) or letters (a-z).

iii. Store the secret token in a safe place so you can enter it during the HA configuration.

We recommend that you create the secret token for the primary server also, because in order to run a failover from the primary or standby, you must have the secret token of the other server.

e. If the `max_connections` value (default: 1024) postgresql.conf file of the active server in `/var/lib/pgsql/<postgresql version>/data/postgresql.conf` was changed, you must make the same change to the same file in the standby server and restart the PostgreSQL service with the command:

```
systemctl restart postgresql-<postgresql version>
```

4. Prepare the following information:

- **Management IP address of standby server:** The management interface address is the IP address that devices connect to for sending syslogs and that users connect to for using TOS products. On failover, the same IP address is used for these purposes, but the traffic is received by the standby server.

- **User name and password for ST administrator on standby server:** To log in as the ST administrator, you need the original SecureTrack administrator username, which is created when the initial setup wizard runs. If you do not know the username or password, Create a New SecureTrack Administrator Username.

  For manual failover, you need to know the SecureTrack admin username and password for the standby server.

- **Secret token for standby server:** See the prerequisites.

- **Operation mode for cluster configuration:** Select the failover and heartbeat mechanisms (based on the minimum requirements for automatic failover and the desired failover mechanism).

  Heartbeat monitoring is supported for both Unicast and Multicast. Failover mode can be automatic or manual. Without manual failover, the servers do replicate database changes, but you must manually perform the failover from the active to the standby server.

  After the failover, you must connect to the management IP address of the standby server to use the TOS products.

  The script prompts you to select one of the following options:

  - `Unicast (Automatic Failover)`
  - `Multicast (Automatic Failover)`
  - `Backup Mode (Manual Failover)`

  The default is Unicast (Automatic Failover)

- **IP addresses for HA clusters:** The HA cluster IP address is the VIP address for the active and standby servers. The VIP address must be on the same network as the IP address configured for Management Traffic.

  An optional second HA cluster can be configured. If you configure a Second HA cluster, you will be prompted for the additional relevant information.

- **IP addresses for Heartbeat Traffic:** The addresses used by the active and standby servers, to monitor each other's health.

- **Network interfaces**: Select network interfaces for the following traffic based on your desired High Availability Deployment Configuration:

  - Management Traffic: eth0 is reserved for Tufin Orchestration Suite Management Traffic.
  - Database Replication Traffic: If you change the "Database Replication Traffic" interface, you will be prompted for the additional relevant information.
  - Heartbeat Traffic: Network interfaces available for Heartbeat Traffic are eth1, eth2, and eth3.

The following example shows a unicast automatic failover, single management with dual heartbeat HA deployment configuration:

Active server IP	192.168.1.208
Standby Management IP	192.168.1.209
SecureTrack username/pw	admin/password
Secret token	<token>
Operation mode	Unicast (Automatic Failover)
HA cluster IP address (Virtual IP)	192.168.1.210

Network interfaces	Management traffic: eth0 Database replication: eth0 Heartbeat traffic: eth2, eth3
Heartbeat networks (assumed subnet /29 or /30)	37.37.37.80 37.37.37.84

Set up the HA cluster

Before running the SecureChange cluster installation make sure that SecureTrack is installed.

Use the screen command to make sure that the hactl command runs to completion.

The sudo command is not supported for HA configurations. Run `$ su -` to become root (see below).

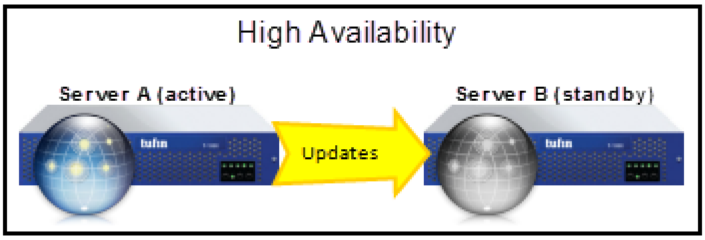
1. On the active server, run:

```
$ su -
hactl configure
```

2. Answer the prompts. Sample hactl script
3. Configure the VIP in SecureTrack: In SecureTrack, go to **Settings** > **Configuration** > **Notifications** and enter the IP address or DNS name for the VIP address in the SecureTrack server name field so that any links in notifications sent from SecureTrack include the VIP address.
4. In Distributed Architecture (DA) deployments, to update the Distribution Server and Remote Collector servers to point to the central SecureTrack VIP address, run: `/usr/local/st/da_remote_configuration.sh update`

When you finish entering the network settings for the HA servers, TOS copies the database and configuration files from the active server to the standby server and then the HA deployment is complete.

In the event of a failover, perform a recovery to restore high availability.



Sample hactl script

This example script presents the setup of the standby server for HA, configured with unicast heartbeats:

[root@192.168.1.208 ~]# **hactl configure**

...

Enter the IP address of the standby server: **192.168.1.209**

Warning: remote machine's web server certificate fingerprint is 30:CA:16:EB:D1:4D:DA:84:F7:7A:3E:54:40:5F:B0:05:CC:DA:B4:99.

Do you want to establish a connection (yes/no)? **yes**

Warning: All SecureTrack and SecureChange data on 192.168.1.209 will be lost!

Are you sure you want to continue (yes/no)? [no]: **yes**

Enter username for SecureTrack's administrator user on 192.168.1.209 [admin]: **<Enter>**

Enter password for admin: **<password>**

Note: The standby server (192.168.1.209) must have a secret token. Run the command '/usr/local/st/ha_secret_token.sh create' on the standby server to create a secret token.

Enter the secret token: **<token>**

Establishing connection with remote server (192.168.1.209)...

You can configure the HA active server to automatically failover to the standby server to control your cluster's health check or implement

Backup mode (Manual Failover).

```
HA with automatic fail-over is supported for both Multicast and Unicast communication for monitoring the heartbeat.
(1) Unicast (Automatic Failover)
(2) Multicast (Automatic Failover)
(3) Backup Mode Manual Failover)
Which operation mode should be used for the cluster configuration? [default: 1]: <Enter>
Generating SSH keys...
Establishing secure connection...
Enter the first HA cluster IP address: 192.168.1.210
Enter the second HA cluster IP address or press ENTER to skip: <Enter>
The default interface for the database synchronization is eth0.
Note: eth0 is reserved for Tufin Orchestration Suite management traffic.
Do you want to change the network interface for the DB sync (yes/no)? [no]: <Enter>
Each server has two heartbeat interfaces. The first and second interface on each server needs
an IP address in a /30 network.
List of available network interfaces:
(1) eth1
(2) eth2
(3) eth3
Enter the numbers of the interfaces to use for heartbeat traffic separated by space or press ENTER [default: 2 3]: <Enter>
Enter the network IP address for the first heartbeat interface: 37.37.37.80
Enter the network IP address for the second heartbeat interface: 37.37.37.84

IP addresses are assigned to heartbeat interfaces on each cluster node.

Settings for HA Cluster with Automatic Failover
==============================================

Active server IP: 192.168.1.208
(1) Standby server IP: 192.168.1.209
(2) First HA cluster IP: 192.168.1.210
(3) Second HA cluster IP: Not Defined
(4) DB sync network interface: [eth0]
(5) First heartbeat network: 37.37.37.80 /30
Node 1 first IP: 37.37.37.81
Node 2 first IP: 37.37.37.82
(6) Second heartbeat network: 37.37.37.84 /30
Node 1 second IP: 37.37.37.85
Node 2 second IP: 37.37.37.86
(7) Network adapters: [eth2, eth3]

Note: If you change the "Second HA cluster IP" or the "DB sync network interface"
you must also reconfigure the settings that follow them.
To change the settings, enter the item number to change.
To exit the wizard and discard changes, enter q
To apply changes and continue, enter c

> c

...

Done.

[root@192.168.1.208 ~]#
```

Managing High Availability

After you setup your servers in a High Availability deployment, you can use these commands to manage the deployment.

If the active server cannot send the database updates to the standby server, the database update files are stored on the active server and **may cause high disk usage**. To prevent this, repair the connection to the standby server or uninstall HA until connectivity is repaired.

You must not do these actions when High Availability automatic failover is configured. Any of these actions can cause malfunction in HA automatic failover configuration.
- Changes in server configuration, for example: HA configuration, networking configuration, date
- You must not run CLI operations on any services that impact HA configuration, for example: `service network restart`, `ifdown ethX`, `service pacemaker stop`

WARNING: Manual reboot or shutdown can cause unexpected failover.

View Status

The `hactl status` command displays the current HA status information, including

- Heartbeat monitoring, virtual IP information, and HA resource processes

  ```
  Last updated: Mon Jul 6 11:57:13 2015

  Last change: Sun Jul 5 15:56:28 2015 via crmd on node2-eth2

  Stack: cman

  Current DC: node2-eth2 - partition with quorum

  Version: 1.1.11-97629de

  2 Nodes configured

  3 Resources configured


  Online: [ node1-eth2 node2-eth2 ]


  Full list of resources:


  ClusterIP-Mgmt-1 (ocf::heartbeat:IPaddr2): Started node1-eth2

  TssAgent (ocf::heartbeat:TufinTssAgent): Started node1-eth2

  LinkMon-Mgmt-1 (ocf::heartbeat:TufinLinkMonMgmt1): Started node1-eth2


  Daemon Status:

  cman: active/disabled

  corosync: active/disabled

  pacemaker: active/enabled

  pcsd: inactive/disabled
  ```

  - Current DC - The node that the heartbeat monitor sees as being active.
  - [Online] / [Offline] - The number of nodes seen by the heartbeat monitor.

    The heartbeat monitor is usually configured to run on a separate connection, so this does not reflect the database replication status.
  - resources - The processes used by HA.

    - Daemon Status - the status of the HA-related daemons.

      The pacemaker daemon will be enabled. The other daemons will be disabled.

- TufinOS HA information

  HA server status: active

  HA cluster IP for Mgmt-1: 192.168.1.210

  DB sync interface: eth0

  -> Node name: node1-eth2

  Heartbeat network status: normal

  Database replication status: normal

    - HA Server Status: Status of this node (active, standby)
    - HA cluster IP: IP address of the HA cluster
    - DB sync interface: Network interface used for database synchronization
    - Node name: Name of this node. This is not displayed when HA is configured for manual failover mode.
    - Heartbeat network status: Communication errors will be displayed here if the status is not normal.
    - Database replication status: Database replication errors will be displayed here if the status is not normal. (normal, stopped, or a warning)

      Warning: If the status command returns an error, do not initiate a failover until the error is resolved.

Sample Command Output

The sample output shows HA configured with 2 nodes, node1-eth2 and node2-eth2.

Status when HA is running, node1-eth2 the active server.

```
[node1-eth2] # hactl status

...

Current DC: node1-eth2 - partition with quorum

...

2 Nodes configured

...

Online: [ node1-eth2 node2-eth2 ]

...

HA server status: active

HA cluster IP for Mgmt-1: 192.168.1.210

DB sync interface: eth0

-> Node name: node1-eth2

Heartbeat network status: normal

Database replication status: normal
```

```
[node2-eth2]# hactl status

...

Current DC: node1-eth2 - partition with quorum

...

2 Nodes configured

...

Online: [ node1-eth2 node2-eth2 ]

...

HA server status: standby

HA cluster IP for Mgmt-1: 192.168.1.210
```

```
DB sync interface: eth0

-> Node name: node2-eth2

Heartbeat network status: normal

Database replication status: normal
```

Status after an automatic failover occurred because of an internal server problem on the original active HA node.

```
[node1-eth2] # hactl status

...

Current DC: node2-eth2 - partition with quorum

...

2 Nodes configured

...

Online: [ node1-eth2 node2-eth2 ]

...

HA server status: standby

HA cluster IP for Mgmt-1: 192.168.1.210

DB sync interface: eth0

-> Node name: node1-eth2

Heartbeat network status: normal

Warning: Failover has been performed on this server.

Database replication is stopped.

To resume database replication please run 'hactl recovery' on the remote server at: 192.168.1.209
```

Status of HA nodes when a communication error was detected on the heartbeat network. The active HA node when the communication error occurred was node1-eth2, and node2-eth2 automatically became the active node.

```
[node1-eth2]# hactl status

...

Current DC: node2-eth2 - partition with quorum

...

2 Nodes configured

...

Online: [ node2-eth2 ]

OFFLINE: [ node1-eth2 ]

...

HA server status: active

HA cluster IP for Mgmt-1: 192.168.1.210

DB sync interface: eth0

-> Node name: node2-eth2

Warning: Heartbeat network failed on (eth3) network adapter.

Warning: Failover has been performed on this server.

Database replication is stopped.

To resume database replication please run 'hactl recovery'
```

```
[node1-eth1]# hactl status

...

Current DC: node2-eth2 - partition with quorum

2 Nodes configured
```

```
...
Online: [ node1-eth2 node2-eth2 ]
...
HA server status: standby
HA cluster IP for Mgmt-1: 192.168.1.210
DB sync interface: eth0
-> Node name: node1-eth2
Warning: Heartbeat network failed on (eth3) network adapter.
Warning: Failover has been performed on this server.
Database replication is stopped.
To resume database replication please run 'hactl recovery' on the remote server at: 192.168.1.209
```

Force Failover

Before you do a failover, run `hactl status` and make sure that the status of the MongoDB database replication is **normal**. If the database is replicating, wait for the replication to complete and then do a failover.

Use the screen command to ensure that the hactl command runs to completion.

To force a failover when configured for automatic failover

- On either the active server (Server A) or the standby server (Server B), run: `hactl failover`

  The automatic failover process includes:

  1. On the active server (Server A), the HA resources stop and cause the TOS services to stop.
  2. On the standby server (Server B), the HA resources start and cause the TOS services to start as the active server.

  The database includes all of the updates that it received from the server that was active before the failover (Server A). No database updates are sent between the servers after the failover. All network devices and TOS servers continue to connect to the virtual IP address for the HA servers.

To force a failover on servers when configured for manual failover

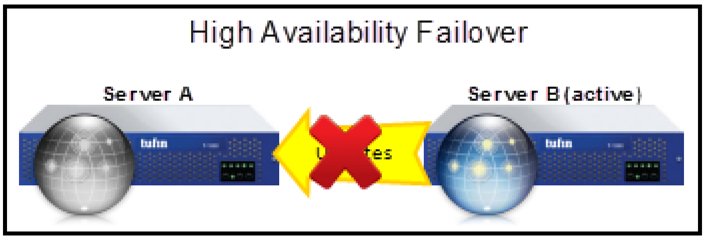
1. On the active server (Server A), run: `hactl failover`

   The TOS services on the active server are stopped.

2. On the standby server (Server B), run: `hactl failover`

   The TOS services on the standby server (Server B) are started as the active server and the database includes all of the updates that it received from the server that was active before the failover (Server A). No database updates are sent between the servers.

   In a Distributed Architecture deployment that is configured for manual failover, after you do a failover or recovery you must also update the Distribution Servers and Remote Collectors with the IP address of the new active server.



If the failover command is being run on a HA SecureChange server, it may take up to 10 minutes for the newly active SecureChange server to find the devices from SecureTrack after the failover has completed.

Sample Code Output

Failover command run on the standby server, when configured for manual failover

```
[node1-eth2] # hactl status
HA server status: standby
Database replication status: normal
```

```
[node1-eth2] # hactl failover
Checking HA license...
Checking HA configuration...
Creating postgresql trigger file...
Removing HA configuration...
Restoring external authentication configuration...
Re-starting PostgreSQL...
Stopping postgresql-11.0 service: [ OK ]
Starting postgresql-11.0 service: [ OK ]
Starting ST services... 100%
Changing Tomcat configuration...
Starting JMS services:

Starting ActiveMQ server: [ OK ]
Starting policy collector: [ OK ]
Starting log collector: [ OK ]
Starting status collector: [ OK ]
Starting APG results collector: [ OK ]
Starting Tufin Jobs service...
Starting tufin-jobs: ............ [ OK ]
Starting Tomcat service...
Done.
[root@TufinOS ~]# hactl status
HA server status: active
Warning: Failover has been performed on this server.
Database replication is stopped.
To resume database replication please run 'hactl recovery'
```

Recovery

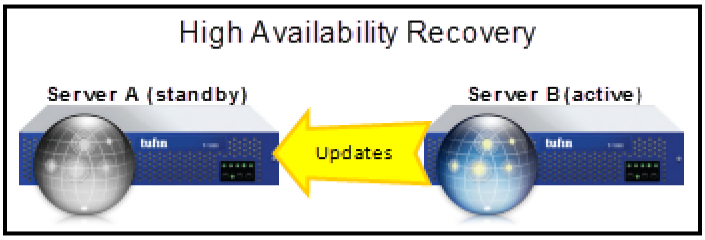
After a failover event, you must make sure both servers and their network connections are functioning properly before you do a recovery. You must do a recovery so that the HA servers are configured properly for another failover.

Use the screen command to ensure that the hactl command runs to completion.

To recover the HA configuration with the same servers:

1. On the current standby server (Server A), create a secret token:
   1. Run: `/usr/local/st/ha_secret_token.sh create`
   2. Enter a character string of at least 8 characters that you will also enter as the secret token when you configure HA on the active server. The string can include numbers (0-9) or letters (a-z).
   3. Store the secret token in a safe place so you can enter it during the HA configuration.
2. On the current active server (Server B), run: `hactl recovery`
3. The standby server's web server certificate fingerprint is shown so you can verify that it is the correct server.
4. If you verify that the remote server is correct, enter: `yes`
5. To confirm that you want to **erase all data** from the database on the standby server, enter: `yes`
6. Enter the username and password for SecureTrack administrator on the remote server.
7. Enter the secret token that you entered on the standby server.

   After you do a recovery, Server A becomes the standby server with TOS services disabled, and it receives database updates from Server B.



If your servers have the same hardware specifications, there is no reason to return the servers to their original state. But, if you want to return the servers back to the original HA configuration:

If your HA is configured for Automatic Failover:

1. Run failover on the active server (Server B): `hactl failover`, and wait for the failover to complete.
2. Resume HA replication from the active server (Server A) to the standby server (Server B): `hactl recovery`

   Server A is the active server and Server B is the standby server, with ongoing database and TOS configuration replication. In a Distributed Architecture deployment that is configured for manual failover, after you do a failover or recovery you must also update the Distribution Servers and Remote Collectors with the IP address of the new active server.

If your HA is configured for Manual Failover:

1. Run failover on the active server (Server B): `hactl failover`, and wait for the failover to complete.
2. Run failover on the standby server (Server A) and make it active, run: `hactl failover`, and wait for the failover to complete.
3. Resume HA replication from the active server (Server A) to the standby server (Server B): `hactl recovery`

   Server A is the active server and Server B is the standby server, with ongoing database and TOS configuration replication. In a Distributed Architecture deployment that is configured for manual failover, after you do a failover or recovery you must also update the Distribution Servers and Remote Collectors with the IP address of the new active server.

Sample Code Output

First create the secret token on the standby server.

```
[StandbyServer]# /usr/local/st/ha_secret_token.sh create

Enter the secret token (at least 8 characters): <secret token>

Secret token created.
```

Then initiate the recovery.

```
[ActiveServer]# hactl recovery

Checking HA license...

Warning: remote machine's web server certificate fingerprint is 2F:76:79:B9:AA:00:D1:5B:EB:AB:9B:0A:17:22:76:C0:F8:07:37:75.

Do you want to establish connection (yes/no)? yes

Enter username for SecureTrack administrator on 192.168.1.208 [admin]: <username>

Enter password for admin: <password>

Note: The standby server must have secret token, please initiate by running '/usr/local/st/ha_secret_token.sh create' on the
standby server

Enter the secret token: <standby server secret token>

Establishing connection with remote server (192.168.1.208)...

Generating SSH keys...

Establishing secure connection...

Removing standby server configuration...

Updating database configuration...

Updating MongoDB configuration...

Performing base backup of database files...

0% [ ]

....

Base backup completed.
```

```
Copying TOP plugins...
Copying configuration files...
Establishing connection with remote server (192.168.1.208)...
Updating remote server HA configuration...
Starting ST services...
Creating MongoDB HA cluster...
Updating local server HA configuration...
Done.
```

Disable High Availability

To remove the HA configuration:

Use the screen command to ensure that the hactl command runs to completion.

- On both servers, run: `hactl uninstall`
  - If HA is configured for automatic failover, you must first Remove HA on the active server, and then Remove HA on the standby server.
  - If you run `uninstall` after you configure or recover High Availability, the active server has the TOS services enabled and the standby server has the TOS services disabled.
  - If you run `uninstall` after you do a failover, the previous active server has the TOS services disabled and the new standby server has the TOS services enabled.

Secret Token

To authenticate a server as an HA standby, you must enter the secret token of the server during the HA setup process.

Create a token on the standby server

1. Run: `/usr/local/st/ha_secret_token.sh create`
2. Enter a character string of at least 8 characters that you will enter as the secret token when you configure HA on the active server. The string can include numbers (0-9) or letters (a-z).
3. Store the secret token in a safe place so you can enter it during the HA configuration of the active server.

Change the secret token on the standby server

1. Run: `/usr/local/st/ha_secret_token.sh reset`
2. Enter a character string of at least 8 characters that you will also enter as the secret token when you configure HA on the active server. The string can include numbers (0-9), letters (a-z), or special characters.

Remove the secret token from the standby server

1. Run: `/usr/local/st/ha_secret_token.sh remove`

Sample Command Output

Create secret token

```
[StandbyServer]# /usr/local/st/ha_secret_token.sh create
Enter the secret token (at least 8 characters): <secret token>
Secret token created.
```

Distributed Architecture

For increased scalability, SecureTrack's Distributed Architecture enables multiple SecureTrack servers to perform device monitoring and processing. Each distributed component can receive revisions and traffic logs. All management, revision viewing, and reporting is done on the SecureTrack central server.

When you use SecureChange with SecureTrack in Distributed Architecture:

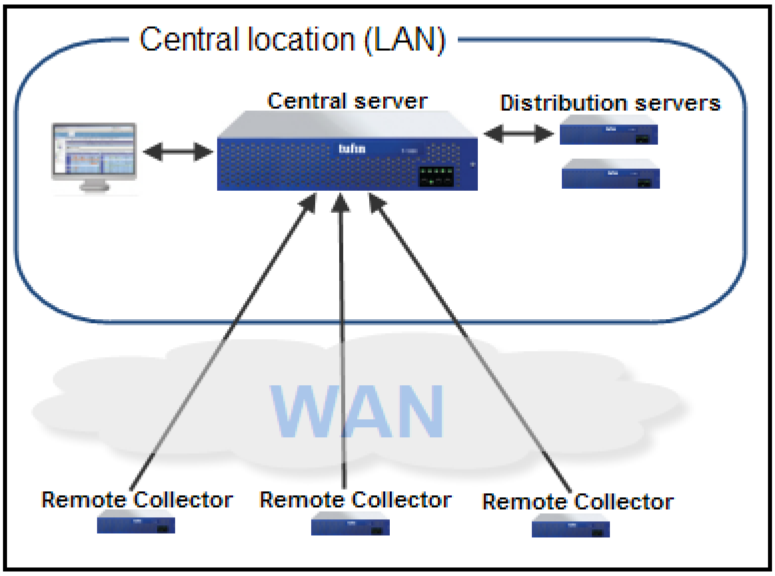
- If SecureChange and SecureTrack are on the same server, SecureChange is only installed on the SecureTrack central server. SecureChange does not use the other Distributed Architecture components.
- If SecureChange and SecureTrack are on different servers, the SecureChange server must connect to the SecureTrack central server.
- The operating system on the servers needs to maintain an accurate date and time. Use chrony to automatically configure the server to self-synchronize with an NTP server.

How Distributed Architecture Works

Distributed Architecture lets you do:

- **Remote monitoring**: Monitored devices may be located in remote locations, so that traffic to SecureTrack's location is across a WAN. Direct monitoring produces heavy traffic, and regular (non-distributed) monitoring across a WAN may result in significant delays and data loss.
- **Load distribution**: In environments producing large quantities of policy and usage data, data retrieval and post-retrieval policy analysis and reporting tasks may consume the CPU resources of a single server. For effective performance, the load may need to be distributed among multiple servers.

To provide solutions to these needs, two kinds of distributed components are available, each of which is in communication only with the single SecureTrack Central server:



- **SecureTrack Remote Collectors**: Remote Collectors perform monitoring (revision and usage retrieval) and basic usage analysis. Using incrementalization, aggregation and data compression, Remote Collectors conserve bandwidth when sending information to the SecureTrack Central server. Remote Collectors store temporary data in a local database until successful delivery is confirmed, so no data is lost when the WAN connection is down.
- **SecureTrack Distribution servers**: Distribution servers exist in a local group with the SecureTrack Central server, connected to it via a LAN-quality connection. In addition to the same kind of monitoring and basic usage analysis performed by Remote Collectors, Distribution servers also perform full post-retrieval policy analysis and on-event reporting for the devices they monitor, and share these tasks with the SecureTrack Central server for devices monitored by the Remote Collectors. So, while Distribution servers cannot perform remote (WAN) monitoring, they contribute more to load distribution than the Remote Collectors do.

All management tasks, revision viewing, and reporting, are centralized and performed on the single SecureTrack Central server's web interface. On-event reports and real-time notifications are sent directly from Distribution servers; scheduled reports are sent from the Central server.

You assign a device to be monitored by a specific SecureTrack server (Central, Distribution, or Remote Collector) when you add the device in SecureTrack's web interface. You can also subsequently manage monitoring throughout the deployment.

Communication between the Distribution servers and Central server is via HTTPS, stunnel, and JMS, over a connection which must be of LAN quality. Communication between the SecureTrack Remote Collectors and the SecureTrack Central server is via HTTPS and JMS. All communications between all components are encrypted and secured.

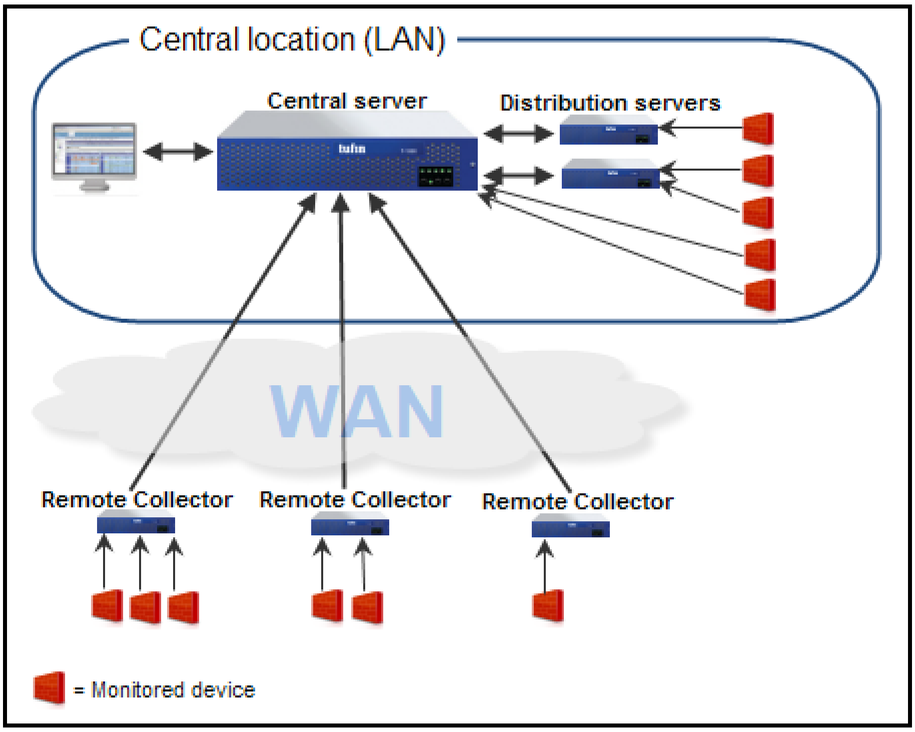
All SecureTrack distributed components must be synchronized with the correct date and time.

Distributed Architecture is currently supported only on TufinOS appliances and VMware virtual machines.

Planning a Distributed Deployment

Plan your distributed deployment as follows:

SecureTrack licensing is dependent only on the number and types of monitored devices, not on the SecureTrack deployment size or configuration.



1. Identify devices that need to be monitored by the SecureTrack deployment, and their locations.
2. The single SecureTrack Central server should be installed in a central location that is easily accessible via HTTPS by administrators, and with LAN connectivity close to as many monitored devices as possible.
3. In each location remote (trans-WAN) from the SecureTrack Central server's location (for example, in each NOC), place one SecureTrack Remote Collector, to monitor the devices in its location.

   SecureTrack Distribution servers cannot be located across a WAN from the SecureTrack Central server.
4. If you need further load distribution in a remote location, add one or more Remote Collectors in that location, and manually distribute the monitored devices among them (by editing each monitored device's properties, in **Settings** > **Administration** > **Devices**).
5. While Distribution servers cannot perform remote (WAN) monitoring, they contribute more to load distribution than Remote Collectors do. So, if there are many devices in the central location to be monitored, and you need load distribution in the central location, add one or more SecureTrack Distribution servers. Each Distribution server must have LAN connectivity with the SecureTrack Central server, forming a central group with it.

Setting up a Distributed Deployment

For a distributed deployment, the SecureTrack Central server must first be installed, with the Setup wizard completed, before you add distributed components (Distribution servers and Remote Collectors) to the deployment. The SecureTrack Central server is set up as a regular, non-distributed SecureTrack.

An existing (non-distributed) SecureTrack can be used as a SecureTrack Central server. To use an existing SecureTrack server as a Distribution server or Remote Collector, please contact Tufin support.

Distributed Architecture is currently supported only on TufinOS appliances or TufinOS VMware virtual machines.

Every component, including the Central server, Distribution Servers, and Remote Collectors, must run the same operating system, the same version of Tufin Orchestration Suite, the same version of TLS, and have the same time zone configuration.

Use the screen command to ensure that the da_remote_configuration.sh command runs to completion.

Prerequisites

- The Central Server and all Distribution Servers must be on the same network. NAT is not supported between the Central Server and Distribution Servers.
- The database time zone of each component must match the Central Server time zone. See Changing the Database Time Zone for more information.
- If the IP address that you are using for the new distributed component was used previously for a distributed component, make sure you remove the old distributed component from the SecureTrack Central server. To do this, from the command line of the old distributed

component run:

```
/usr/local/st/da_remote_configuration.sh uninstall
```

Procedure

To add a new distributed component to the deployment, on the SecureTrack server that you want to be the distributed component:

1. Install SecureTrack.
2. Login to SecureTrack and run the Setup wizard on it.
3. From the command line, run:

   ```
   /usr/local/st/da_remote_configuration.sh install
   ```

   At the prompts, do the following:

   a. Select whether this is to be a Distribution server or a Remote Collector.

   b. Type the SecureTrack Central server's IP address.

   c. Type the password of the admin user of the SecureTrack Central server.

   d. Accept the fingerprint and confirm establishing the connection.

      Record the fingerprint so that you can compare it with the fingerprint on the other servers.

   e. Type a unique identifying name for the distributed component in the context of the deployment. Once set, this name cannot be changed.

   f. Type the IP address of this host.

      If the IP address was used previously for a distributed component, make sure you remove the old distributed component from the SecureTrack Central server. To do this, from the command line of the old distributed component run: `/usr/local/st/da_remote_configuration.sh uninstall`

   g. Confirm the settings.

   The distributed component is added to the deployment.
4. After adding the distributed component, the operating system on the server needs to maintain an accurate date and time. Use chrony to automatically configure the server to self-synchronize with an NTP server.

To see the certificate fingerprint of a server when you are configuring HA, you can either:

- Login to the server with a web browser and view the server's certificate
- Open a terminal session to the server, login as root, and run: `/usr/local/st/web_srv_fingerprint.sh`

Removing a Component from a Distributed Deployment

Use the screen command to ensure that the da_remote_configuration.sh command runs to completion.

To remove a SecureTrack distributed component (Distribution Server or Remote Collector) from a distributed deployment:

1. Migrate all devices from the distributed component to another distributed component.
   1. Login to the Central server.
   2. Go to: **Settings** > **Monitoring**
   3. Select a device monitored by the distributed component.
   4. Click **Migrate (ST servers)** and select a different distributed component from the menu.
   5. Repeat this for all devices that are monitored by the distributed component.
2. On the distributed component, run:

   /usr/local/st/da_remote_configuration.sh uninstall
3. At the prompt, confirm removing the component from the deployment.

Changing IP Addresses in a Distributed Deployment

Changing IP addresses in a distributed deployment requires re-establishing trust between components. Change the IP for each of the components.

Use the screen command to ensure that the da_remote_configuration.sh command runs to completion.

Distribution Servers

After changing the IP address of a SecureTrack Distribution server, re-establish trust by running the following two commands on the Distribution server:

```
/usr/local/st/stunnel_sslcert.sh /usr/local/st/conf/stunnel.cnf > /dev/null 2>&1
```

```
/usr/local/st/da_remote_configuration.sh update
```

At the prompts, type the relevant information as when adding a distributed component.

Remote Collectors

After changing the IP address of a SecureTrack Remote Collector, re-establish trust by running the following command on the Remote Collector:

```
/usr/local/st/da_remote_configuration.sh update
```

At the prompts, type the relevant information as when adding a distributed component.

Central Management Server

After changing the IP address of the SecureTrack Central management server, re-establish trust as follows:

1. On the Central management server, if there are Distribution servers (not just Remote Collectors) in the deployment, run:

   /usr/local/st/stunnel_sslcert.sh /usr/local/st/conf/stunnel.cnf > /dev/null 2>&1
2. On each Distribution server, run the following two commands:

   /usr/local/st/stunnel_sslcert.sh /usr/local/st/conf/stunnel.cnf > /dev/null 2>&1

   /usr/local/st/da_remote_configuration.sh update

   At the prompts, type the relevant information as when adding a distributed component.
3. On each Remote Collector, run the following command:

   /usr/local/st/da_remote_configuration.sh update

   At the prompts, type the relevant information as when adding a distributed component.

Multi-Domain Management

- Overview
- What Can I Do Here?
- How Do I Get Here?

Overview

TOS Classic initially shows and manages all network devices under a single organizational entity. However, some organizations need to manage their devices under different entities. Examples are:

- Managed security service providers (MSSPs) who use a single instance of TOS Classic to manage devices belonging to different customers and therefore need complete separation between organizations.
- Large segmented organizations that want the ability to manage different groups of devices by different criteria, with regards policy and violations, or give users and administrators access to some groups and not others.

This separation of devices and their management is achieved by configuring your system for multi-domain management - creating new organizational entities called domains and placing devices into the appropriate domain. Until you configure your system for multi-domain management, the term domain doesn't appear anywhere in the product.

There are no restrictions as to which devices can be assigned to which domain, except where noted under "Managing Monitored Devices" on page 48. For example, management devices such as Checkpoint MDS and managed devices e.g. CMAs can belong to different domains and a parent device can be in one domain, with its virtual devices being assigned to others.

⚠ Once a second domain is added, multi-domain management is implemented automatically and there is no going back!

When switching from single to multi-domain, a number of changes occur in your system:

- All existing devices become allocated to an entity called The Default Domain, from which they can be moved or 'migrated' to any one of the new domains created.
- The two user types - Administrator and User - are replaced with four new user types - Super Administrator, Multi-Domain Administrator, Multi-Domain User and Domain User - see "Managing TOS Classic Users" on page 501.
- Existing Administrators automatically become Super Administrators, which gives them access to all domains, and existing Users automatically become Multi-domain Users but do not have access to any domain until access is granted by a super administrator.

- For the new super administrators, a new domain selector field will appear at the bottom of every screen, from which they can switch domains by selecting the desired domain from the list displayed. The Default Domain is always excluded from this list, but there is an additional option - Global - which when selected gives the super administrator access to all domains together with The Default Domain. This access is called the Global Context and is described in more detail in "Contexts in Multi-Domain Management" below
- Access to specific domains and to the Global Context can subsequently be granted to multi-domain administrators and multi-domain users.
- Existing zones that you have created and the predefined Users Networks zone will appear only in the Global Context and will apply to The Default Domain only.
    - Existing USPs and USP exceptions will be set to apply to the Global Context meaning all the domains defined in the system, including The Default Domain.

Contexts in Multi-Domain Management

Once your system is configured for multi-domain management, a user will always be in one of two 'contexts'.

- A domain context - the user sees and manages a single domain but it cannot be The Default Domain.
- The Global Context - the user sees and manages The Default Domain together with all other domains to which he is permitted.

There are functions available in the domain context that are not available in the Global Context and vice versa. Reports (configured and generated), queries, and audits are created in the currently selected context (Global Context or domain-specific), and are not available in any other context. Similarly, Network Zones are created in the currently selected context, and are then available only for the queries and reports of that context.

Any access or permissions given to multi-domain administrators or multi-domain users while the administrator is in a domain context are limited to that domain.

Domain Context

A user of any kind is in a domain context when a specific domain is selected from the domain selector or the user only has access to a single domain. The Default Domain is not available for selection as a domain context.

Only devices in the selected domain can be viewed and policy revisions, queries, audits and reports can be configured only for these devices.

Multi-domain users working in a domain context have the same access as domain users.

Multi-domain administrators and super administrators working in a domain context can configure for the currently selected domain only. This includes managing domain users, devices, and network zones. System-level configuration, including configuring super administrators, are not available.

The Global Context

A user is in the Global Context when Global is selected from the domain selector. It is available to all super administrators, and to multi-domain administrators and multi-domain users who have been granted access to the Global Context (see "Managing TOS Classic Users" on page 501).

Multi-domain users working in the Global Context can:

- View devices and policy revisions from all domains to which they have access including The Default Domain
- Run aggregated queries, audits and reports, and alerts that have been defined by a super administrator with the Global Context, which will include only the devices and domains to which they have access
- View Global Context entities that have been defined by a super administrator, such as USPs, and USP exceptions.
- View and select Network Zones that were defined in the Global Context

A multi-domain administrator working in the Global Context can do everything the multi-domain user can do and additionally configure Global Context entities that have been defined by a super administrator, such as USPs, and USP exceptions, queries, audits and reports and change topology.

A multi-domain administrator working in the Global Context cannot do any domain-specific administration tasks such as managing Domain Users, devices, and network zones.

A super administrator working in the Global Context can do everything the multi-domain administrator can do and additionally:

- Perform system-level configuration - define entities for the Global Context, such as USPs, USP exceptions, queries, audits and reports.
- Define Network Zones for the Global Context

Recommended Best Practice for Multi-Domain Management

1. Create one or more new domains as required.
2. Migrate all existing devices to the new domains. See "Managing Monitored Devices" on page 48.
3. Give users and administrators access to domains. See Users.

For SecureChange users:

In SecureChange, you can assign SecureChange domains to users and groups. When selecting devices for tickets, such as in access requests, users and groups assigned to domains can only select devices in those domains. This segregation of data can help in scenarios such as when you have multiple groups of administrators responsible for separate areas of the network. You can assign the groups to separate domains and each group can only see the devices for its domain.

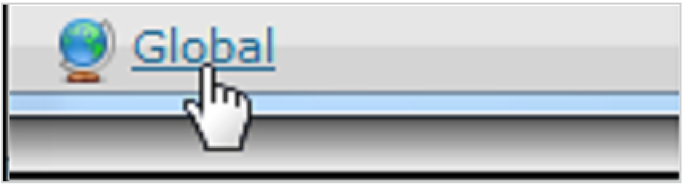
See "Enabling Multi-Domain in SecureChange" on the next page.

In SecureApp, you can import the list of domains as customers. You can then define applications according to the customers that use the applications to allow for:

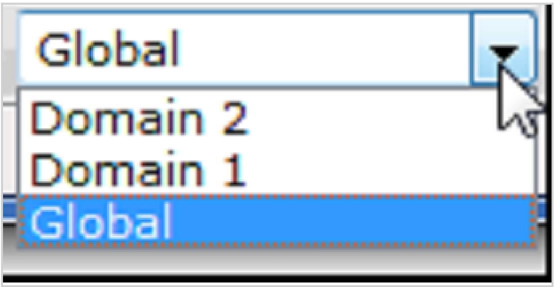
- Data segregation - Connections can only contain resources that belong to related customers.
- IP address segmentation - If different customers use the same IP address scheme in their networks (also known as IP overlapping), SecureApp analyzes traffic correctly for each customer separately.

Switching Contexts

When the logged-in user has access to more than one domain, the current context appears in the domain selector which is displayed on most screens. Clicking on the context name, displays a list of all contexts to which the user has access, including Global if the user also has access to the Global Context. When a different domain is selected, the user is returned to the dashboard.



Clicking on the context name, displays a list of all contexts to which the user has access, including Global if the user also has access to the Global Context. When a different domain is selected, the user is returned to the dashboard.

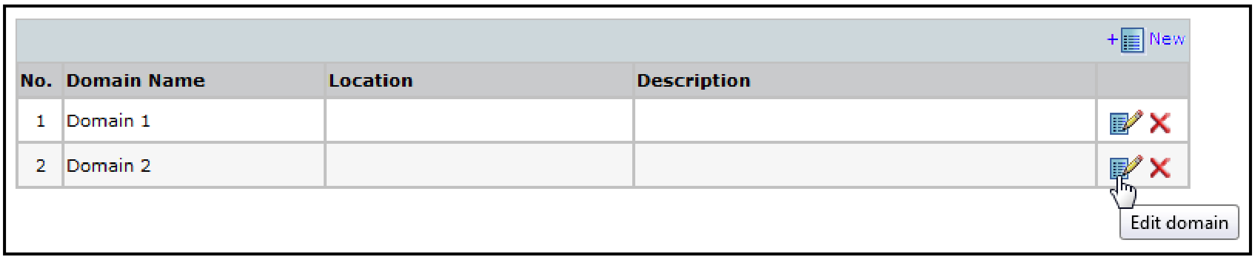


What Can I Do Here?

- Create a domain
- Delete a domain - click ✕ on the desired domain
- Edit a domain - click ✎ on the desired domain, change details then save by clicking ✓

Create a Domain

1. Click + New
2. enter details. **Location** and **Description** are optional for your information only.
3. save by clicking ✓.



No.	Domain Name	Location	Description	
1	Domain 1			✎ ✕
2	Domain 2			✎ ✕

How Do I Get Here?

SecureTrack > **Settings** > **Configuration** > **Domains**:

Enabling Multi-Domain in SecureChange

Overview

MSSPs and large enterprises commonly must control the provisioning process for many network domains, such as customers, business partners, or departments. In some organizations the domains are interconnected with communication between the domains, and in other organizations communication between domains is prohibited.

When you enable multi-domain, you must choose either:

- **Segregated domains**: Customers are separated from each other and each connection can only include resources from one customer.
  - Assign users to domains so that each user can only see devices and objects in their domains
  - Restrict a ticket to handlers that are in the domain that the requester created the ticket in
  - Restrict handlers so that they can only select targets and objects from that domain
  - Restrict Target Suggestion, Designer, and Verifier to analyze access requests only within domain of the ticket
- **Interconnected domains**: Customers are all in one environment and each connection can include resources from multiple customers.
  - Define access requests from resources in one domain to resources in another domain
  - Use the Target Suggestion, Designer, and Verifier to analyze access requests across domains

> The Clone Server Policy workflow supports only single domain mode and Segregated Domains mode.

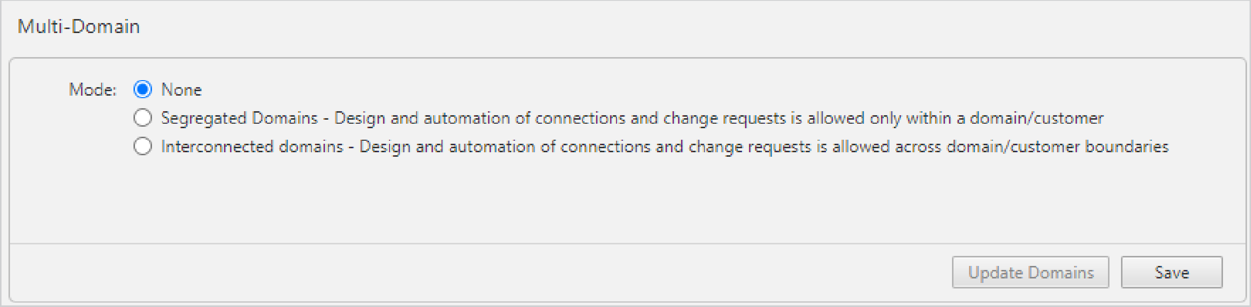
> ⚠
> 1. SecureApp supports interconnected domains only
> 2. SecureApp connection discovery is available in single domain mode only

What Can I Do Here?

Enabling Multi-Domain Modes

1. Check with the SecureTrack administrator to make sure that there are domains configured in SecureTrack.
2. In SecureChange go to **Settings** > **Multi-Domain**, and then select one of the following options:
   - **Segregated domains** - Design and automation of connections and change requests is allowed only within a domain/customer
   - **Interconnected domains** - Design and automation of connections and change requests is allowed across domain/customer boundaries

     Multi-domain mode applies to both SecureChange and SecureApp, and the selection cannot be undone.



Multi-Domain

Mode: ● None
○ Segregated Domains - Design and automation of connections and change requests is allowed only within a domain/customer
○ Interconnected domains - Design and automation of connections and change requests is allowed across domain/customer boundaries

3. Click one of the following:
   - **Update Domains** (Recommended) - Retrieve the domain list from SecureTrack now.
   - **Save** - Save this configuration.

The list of domains is updated once a day at midnight.

After you enable multi-domain in SecureChange, you can:

- Assign users to domains
- Search for tickets by domain

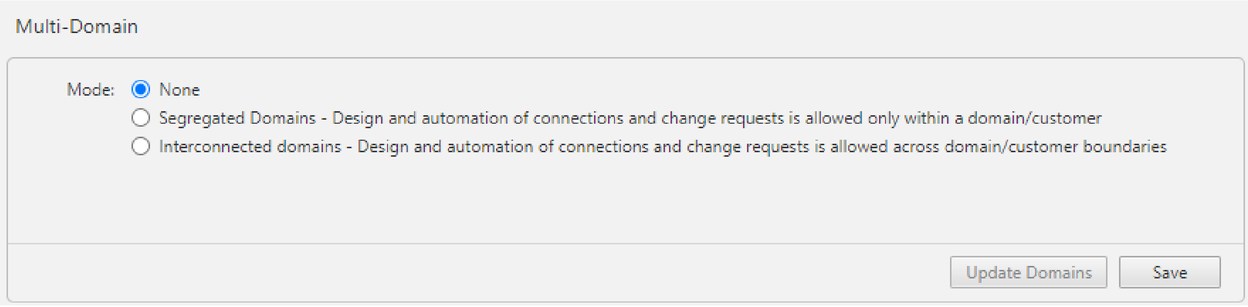
Enabling Multi-Domain in SecureApp

When you enable multi-domain mode, you can:

- Manage applications for each customer separately
- Allow or prohibit connections between customers

Multi-Domain for SecureApp must be set up in SecureChange . Select interconnected domains as segregated domains are not supported in SecureApp.

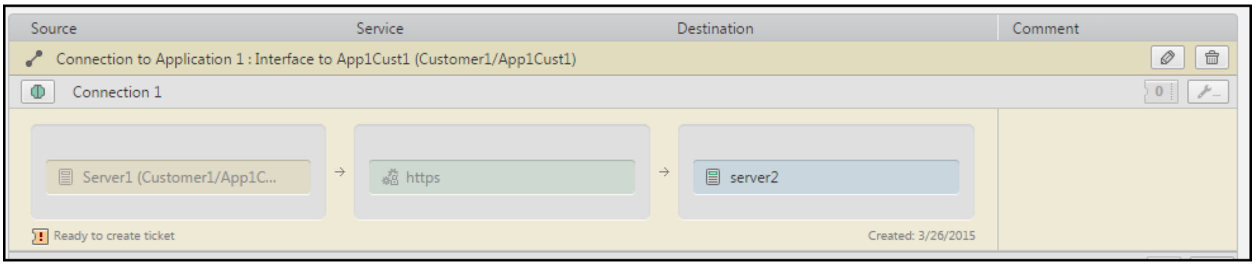
1. SecureApp supports interconnected domains only
2. Connection discovery is available in single domain mode only (see multi-domain management for more information on single and multiple domains).



Multi-Domain

Mode:
● None
○ Segregated Domains - Design and automation of connections and change requests is allowed only within a domain/customer
○ Interconnected domains - Design and automation of connections and change requests is allowed across domain/customer boundaries

With **Interconnected domains**, customers are all in one environment and each connection can include resources from multiple customers. This is helpful if multiple customers use the same IP addressing scheme. For example, Customer 1 assigns an IP address to a server and Customer 2 assigns the same IP address for one of its clients. Using multi-customer mode in SecureApp, you can distinguish between customers and manage each one accordingly. When multi-customer mode is set to interconnected, the business owner can also create applications packs.



Source | Service | Destination | Comment

Connection to Application 1 : Interface to App1Cust1 (Customer1/App1Cust1)

Connection 1

Server1 (Customer1/App1C... → https → server2

Ready to create ticket

Created: 3/26/2015

After you enable multi-domain mode and the list of domains is updated, you can go to **Customers** to:

- Import customers into SecureApp
- Create applications and connections for each customer

Monitoring and Maintenance

TOS maintenance tasks include backup, restore, upgrade and uninstallation. TOS monitoring lets you receive email notification or SNMP traps when there is a problem with the hardware or software resources on your server.

SNMP Monitoring

As with all of your business critical servers, you must have real-time knowledge of the hardware and software health of your systems. Suite Administration lets you monitor resource usage and important services running on your TOS server. Enable Suite Administration to send notifications, and then configure your desired notification method - email or SNMP traps.

If you use a network monitoring system that collects SNMP information, it is important that all of your systems report into the system so you can prevent downtime that results from failed servers. You can monitor the health of your TOS servers using the same tools you use to monitor any other resource in your environment. Review the Tufin SNMP MIBs and the traps used for monitoring the OS.

You can also monitor policy changes discovered by SecureTrack using SNMP. This lets you use your existing centralized SNMP monitor system to see changes made to devices.

The following table summarizes the various SNMP monitoring options available:

	Standard SNMP	Extended SNMP	Heartbeat and Policy Change
Standalone TOS server	✓	✓	✓
Primary HA server	✓	✓	✓
Secondary HA server	✓		
Central Server (in Distributed Architecture)	✓	✓	✓
Remote collector (in Distributed Architecture)	✓		
Distribution Server (in Distributed Architecture)	✓		

What can I do?

- Monitor policy changes - Enable or disable SNMP heartbeat and policy change monitoring of SecureTrack.
- Monitor TOS servers - Enable or disable SNMP monitoring of a standalone TOS server, a primary HA server, or a Central Server in a Distributed Architecture deployment.
- Monitor other TOS servers - Enable or disable standard SNMP monitoring for any device, including a remote collector, distribution server, or a secondary HA server.
- Tufin MIBs - Review the Tufin MIBS.

Enable Standard SNMP on TufinOS

You can enable standard SNMP support in TufinOS on any device, including standalone devices, HA servers, a central server, remote collectors, and distribution servers.

Extended SNMP monitoring is available for certain servers. See SNMP Monitoring for details regarding which servers support extended SNMP monitoring.

To enable SNMP on TufinOS for SNMP v1 or v2c

1. Start the snmpd daemon, and configure it to start when the server boots.

```
# systemctl start snmpd
# chkconfig snmpd on
```

2. Verify that snmpd will run for boot levels 2, 3, 4, and 5, and that SNMP is listening on the correct port rather than the loopback adapter.

```
[root@RC1 ~]# systemctl list-unit-files|grep snmpd
snmpd.service enabled
# netstat -an | grep 161
udp 0 0 0.0.0.0:161 0.0.0.0:*
```

   If you receive the following, then SNMP is incorrectly listening on the loopback port.

```
# netstat -an | grep 161
udp 0 127.0.0.1:161 0.0.0.0:*
```

3. Edit `/etc/snmp/snmpd.conf` and modify it to suit your requirements. The edits suggested below provide basic SNMP access and configuration only.
   - Find and change the community string (the password for SNMP access) from `public` to a password of your choosing.

```
# sec.name source community
com2sec notConfigUser default public
```

   becomes

```
# sec.name source community
com2sec notConfigUser default <NEWPASSWORD>
```

- Find and change the system location (`syslocation`) and system contact (`syscontact`) strings.

```
syslocation Unknown (edit /etc/snmp/snmpd.conf)
syscontact Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
```

becomes

```
syslocation '<Device Location details>'
syscontact 'Contact Name <someone@yourdomain.com>'
```

- Expand the collection of MIBs being utilized, for example:

```
# name incl/excl subtree mask(optional)
view systemview included .1.3.6.1.2.1.1
```

becomes

```
# name incl/excl subtree mask(optional)
view systemview included .1
```

To enable SNMP on TufinOS for SNMP v3

1. Stop to snmpd daemon.

```
# systemctl stop snmpd
```

2. Set the SNMP v3 username and password.

```
# net-snmp-create-v3-user -ro -A <mypassword> -a SHA -X <mypassword> -x AES <myuser>
```

3. Start the snmpd:

```
# systemctl start snmpd
```

4. Test that you can read the MIBs using the `snmpwalk` command.

```
# snmpwalk -v 3 -u myuser -l authPriv -A mypassword -a SHA -X mypassword -x AES localhost
```

TOS Suite Administration

As with all of your business critical servers, you must have real-time knowledge of the hardware and software health of your systems. Suite Administration lets you monitor resource usage and important services running on your TOS server. Enable Suite Administration to send notifications, and then configure your desired notification method - email or SNMP traps.

If you use a network monitoring system that collects SNMP information, it is important that all of your systems report into the system so you can prevent downtime that results from failed servers. When you enable SNMP trap notification, you can monitor the health of your TOS server using the same tools you use to monitor any other resource in your environment. Review the Tufin SNMP MIBs in the Tufin Knowledge Center or in your TOS server at: `/usr/local/st/mibs/TUFIN-MIB.txt`, and the traps used for monitoring the OS.

You can enable Suite Administration for a standalone TOS server, a primary High Availability (HA) server, the Central Server in a Distributed Architecture (DA) deployment.

The following hardware resources are monitored:

- CPU (default threshold - 10%)
- Memory (default threshold - 70%)
- Disk (default threshold - 70%)

The following software resources are monitored:

- Tomcat application server
- Apache web server
- PostgresSQL database
- Cron
- Syslog
- JMS Tunnel (Disabled by default; Enable for HA and DA deployments only)
- Stunnel (Disabled by default; Enable for HA and DA deployments only)

You can use one of these methods to monitor system health:

- Email notifications - Configure email addresses to which TOS sends notifications to through a specified SMTP server
- SNMP traps - Configure the SNMP server to which TOS sends SNMP traps on port 162
- SNMP get - Configure an SNMP server to connect to the SNMP agent on the TOS server on port 10161 to retrieve resource status

  SNMP get is available as soon as Suite Administration is enabled, and no additional configuration is required.

What can I do?

- Enable Suite Administration - Enable or disable Suite Administration.
- Configure Thresholds and Services - Configure the usage thresholds and which services are monitored.
- Configure SNMP Settings - Configure the settings required to send SNMP traps.
- View SNMP Suite Administration messages - View the SNMP messages for Suite Administration.
- Configure Email Notification - Enable and configure email:
  1. Configure SMTP - Configure the SMTP settings
  2. Configure recipient list - Manage the recipient list for the email notifications
- Extend SNMP - Customize SNMP to use additional standard MIBS or to use non-default ports.

Enable/Disable Suite Administration

Prerequisites

These ports must be open in your firewall to allow SNMP traffic:

From	To	Port	Description
SNMP Management Server	Tufin server	10161	Port used for SNMP queries
SNMP Management Server	Tufin server	161	Port used by built-in linux SNMP agent
Tufin server	SNMP Management Server	162	Default SNMP trap port (configurable)

To enable or disable Suite Administration:

(Click here to view a complete CLI sample.)

1. From the command line of your TOS server, enter: `tos conf`

   ```
   # tos conf
   Tufin Orchestration Suite control panel
   =======================================
   Component Setting
   ----------------------- --------
   (1) SecureTrack Enabled
   (2) SecureChange Enabled
   (3) Suite Administration Disabled

   To change a product setting enter its number (1-3)
   To apply changes and continue enter c
   >
   ```

2. Enter **3** to change the Suite Administration state.
3. Enter **c** to save any changes you have made. If a change has been made, this prompt is shown:

   ```
   Tomcat will restart and current users will be disconnected.
   Are you sure you want to continue? (yes/no):
   ```

4. Enter **yes**.

   This step restarts tomcat, which disconnects any users currently connected to SecureTrack or SecureChange. The step takes up to 5 minutes to complete.

Enable/Disable Suite Administration - Sample Code

```
# tos conf
Tufin Orchestration Suite control panel
=======================================
Component Setting
----------------------- --------
(1) SecureTrack Enabled
(2) SecureChange Enabled
(3) Suite Administration Disabled

To change a product setting enter its number (1-3)
To apply changes and continue enter c
> 3
Tufin Orchestration Suite control panel
=======================================

Component Setting
----------------------- --------
(1) SecureTrack Enabled
(2) SecureChange Enabled
(3) Suite Administration Enabled

To change a product setting enter its number (1-3)
To apply changes and continue enter c
> c
Tomcat will restart and current users will be disconnected.
```

```
Are you sure you want to continue? (yes/no): yes

Enabling Suite Administration...

Stopping Tomcat service... done

Starting Tomcat service, please wait (this may take up to 5 minutes)... done

#
```

Enable/Disable SecureTrack or SecureChange

To meet your specific deployment configuration requirements, run the `tos conf` command to enable or disable SecureTrack or SecureChange on a server. The command output displays the current status of each TOS component with one of the following status settings:

Status Setting	Description
`Enabled`	TOS component is enabled and running on this server
`Disabled`	TOS component is disabled and is not running on this server
`Not Available`	TOS component cannot be enabled on this server. For example, SecureChange and Suite Administration cannot run on a Remote Collector or Distribution Server and is therefore disabled.
`Enabled (Locked - DA cluster)`	TOS component is enabled and running, but cannot be disabled. For example, SecureTrack must be enabled on a Remote Collector or Distribution Server and is therefore enabled and locked.

Follow the command instructions to make any desired changes. If the setting change is not allowed, a message will display explained the reason the chnage was disallowed.

To enable/disable SecureChange or SecureTrack:

1. From the command line of your server, enter `tos conf`

   ```
   # tos conf

   Tufin Orchestration Suite control panel

   =======================================

   Component Setting

   ----------------------- --------

   (1) SecureTrack Enabled

   (2) SecureChange Enabled

   (3) Suite Administration Disabled


   To change a product setting enter its number (1-3)

   To apply changes and continue enter c

   >
   ```

2. Enter **1** to enable/disable SecureTrack, or **2** to enable/disable SecureChange. The new setting is displayed.

   ```
   # tos conf

   Tufin Orchestration Suite control panel

   =======================================

   Component Setting

   ----------------------- --------

   (1) SecureTrack Enabled

   (2) SecureChange Disabled

   (3) Suite Administration Disabled


   To change a product setting enter its number (1-3)

   To apply changes and continue enter c
   ```

```
>
```

3. Enter **c** to save and implement any changes you have made. If a change has been made, this prompt is shown:

   ```
   Tomcat will restart and current users will be disconnected.

   Are you sure you want to continue? (yes/no):
   ```

4. Enter **yes**.

   This step restarts tomcat, which disconnects any users currently connected to SecureTrack or SecureChange. The step takes up to 5 minutes to complete.

Configure SNMP Settings

To configure SNMP settings:

(Click here to view a complete CLI sample.)

1. From the command line of your TOS server, enter: `configure_os_monitoring`
2. Enter `3` to select `SNMP Settings`. The SNMP Settings menu appears.

   ```
   / --> [ SNMP Settings ]

   =======================

   (1) Manager IPv4 Address Not Defined

   (2) Manager Port 162

   (3) Community Name public

   (4) Trap Sending Interval 60 minutes

   To change the settings, enter the item number to change.

   To quit, enter q. To return to the previous menu enter r:
   ```

3. Enter the item number of the element you want to set, and follow the instructions displayed in the menu.

   Repeat this step until all the settings are configured as desired.

Configure SNMP Settings - Sample Code

```
# configure_os_monitoring

[ OS Monitoring Control Panel ]

==============================

(1) Recipient Settings

(2) SMTP Settings

(3) SNMP Settings

(4) Threshold Settings

To change the settings, enter the item number to change.

To quit, enter q: 3

/ --> [ SNMP Settings ]

=======================

(1) Manager IPv4 Address Not Defined

(2) Manager Port 162

(3) Community Name public

(4) Trap Sending Interval 60 minutes

To change the settings, enter the item number to change.

To quit, enter q. To return to the previous menu enter r: 1

To change SNMP manager IPv4 address, enter the IPv4 address.
```

```
To quit, enter q. To return to the previous menu, enter r.
To delete SNMP manager IPv4 address, press ENTER.
Manager IPv4 Address > 122.33.3.3

/ --> [ SNMP Settings ]
======================

(1) Manager IPv4 Address 122.33.3.3
(2) Manager Port 162
(3) Community Name public
(4) Trap Sending Interval 60 minutes

To change the settings, enter the item number to change.
To quit, enter q. To return to the previous menu enter r: 3

To change SNMP community name, enter the community name.
To quit, enter q. To return to the previous menu, enter r.
To delete SNMP community name, press ENTER.
Community Name > OurPrivateName

/ --> [ SNMP Settings ]
======================

(1) Manager IPv4 Address 122.33.3.3
(2) Manager Port 162
(3) Community Name OurPrivateName
(4) Trap Sending Interval 60 minutes

To change the settings, enter the item number to change.
To quit, enter q. To return to the previous menu enter r: 4

To change sending interval, enter the number of minutes.
To quit, enter q. To return to the previous menu, enter r.
Note: The minimum allowed interval is 2 minutes.
To delete SNMP sending interval, press ENTER.
Trap Sending Interval > 15

/ --> [ SNMP Settings ]
======================

(1) Manager IPv4 Address 122.33.3.3
(2) Manager Port 162
(3) Community Name OurPrivateName
(4) Trap Sending Interval 15 minutes

To change the settings, enter the item number to change.
To quit, enter q. To return to the previous menu enter r: q
#
```

Tufin SNMP Suite Administration Messages

The following table summarizes the different elements contained in the CPU Usage notification SNMP messages, their meaning and possible values:

SNMP trap element	Meaning	Possible values
TUFIN-MIB::cpuUsageDescription.0	The CPU usage description	String (0-256 characters)
TUFIN-MIB::cpuUsageValue.0	The percentage of CPU time spent processing system-level code, calculated over the last minute	Integer
TUFIN-MIB::cpuUsageThreshold.0	The CPU usage threshold	Integer
TUFIN-MIB::cpuUsageSeverity.0	The CPU usage severity	String (0-256 characters)

The following table summarizes the different elements contained in Disk Usage notification SNMP messages, their meaning and possible values:

SNMP trap element	Meaning	Possible values
TUFIN-MIB::diskUsageDescription.0	The disk usage description	String (0-256 characters)
TUFIN-MIB::diskUsageValue.0	Used space on the disk. For large heavily-used disks (>2Tb), this value will latch at INT32_MAX (2147483647)	String (0-256 characters)
TUFIN-MIB::diskUsageThreshold.0	The disk usage threshold	Integer
TUFIN-MIB::diskUsageSeverity.0	The disk usage severity	String (0-256 characters)

The following table summarizes the different elements contained in general notification SNMP messages, their meaning and possible values:

SNMP trap element	Meaning	Possible values
TUFIN-MIB::stEvent.0	Policy change type	Install, Save, Automatic
TUFIN-MIB::stManagementName.0	Check Point management friendly name	String (0-256 characters)
TUFIN-MIB:: stManagementIP.0	Check Point management IP address	String (0-256 characters)
TUFIN-MIB:: stManagementPeriodicStatus.0	Periodic status message	String (0-1024 characters)

Configure Thresholds and Services

To configure the usage thresholds and monitored services:

(Click here to view a complete CLI sample.)

If the server is used in an HA deployment or is the Central Server in a DA deployment, enable JMS Tunnel and Stunnel.

1. From the command line of your TOS server, enter: `configure_os_monitoring`
2. Enter 4 to select `Threshold Settings`. The Threshold Settings menu appears.

   ```
   / --> [ Threshold Settings ]
   ==============================

   (1) CPU Usage 10%
   (2) Memory Usage 70%
   (3) Disk Usage 70%
   (4) Services Settings

   To change the settings, enter the item number to change.
   To quit, enter q. To return to the previous menu enter r:
   ```

3. Enter the item number of the element you want to set, and follow the instructions displayed in the menu.

   Repeat this step until all the settings are configured as desired.

   The services settings (option 4 of the menu) lets you select which specific services to monitor.

   If the server is used in an HA deployment or is the Central Server in a DA deployment, enable JMS Tunnel and Stunnel.

Configure Thresholds and Services - Sample Code

```
# configure_os_monitoring

[ OS Monitoring Control Panel ]

===============================

(1) Recipient Settings

(2) SMTP Settings

(3) SNMP Settings

(4) Threshold Settings

To change the settings, enter the item number to change.

To quit, enter q: 4

/ --> [ Threshold Settings ]

=============================

(1) CPU Usage 10%

(2) Memory Usage 70%

(3) Disk Usage 70%

(4) Services Settings

To change the settings, enter the item number to change.

To quit, enter q. To return to the previous menu enter r: 4

/ --> Thresholds Settings --> [ Services Settings ]

===================================================

(1) Application Server Enabled

(2) Cron Enabled

(3) Database Enabled

(4) JMS Tunnel Disabled

(5) Stunnel Disabled

(6) Syslog Enabled

(7) Web Server Enabled

To change the service monitoring status, enter the item number to change.

To quit, enter q. To return to the previous menu enter r.

Change Service > 6

/ --> Thresholds Settings --> [ Services Settings ]

===================================================

(1) Application Server Enabled

(2) Cron Enabled

(3) Database Enabled

(4) JMS Tunnel Disabled

(5) Stunnel Disabled

(6) Syslog Disabled

(7) Web Server Enabled

To change the service monitoring status, enter the item number to change.
To quit, enter q. To return to the previous menu enter r.

Change Service > r

/ --> [ Threshold Settings ]

==============================

(1) CPU Usage 10%

(2) Memory Usage 70%

(3) Disk Usage 70%

(4) Services Settings

To change the settings, enter the item number to change.

To quit, enter q. To return to the previous menu enter r: 1

To change threshold, enter the threshold in percentage 0-99.

To quit, enter q. To return to the previous menu, enter r.

To disable monitoring on the resource, press ENTER.

CPU Usage > 30

/ --> [ Threshold Settings ]

==============================

(1) CPU Usage 30%

(2) Memory Usage 70%

(3) Disk Usage 70%

(4) Services Settings

To change the settings, enter the item number to change.

To quit, enter q. To return to the previous menu enter r: 2

To change threshold, enter the threshold in percentage 0-99.

To quit, enter q. To return to the previous menu, enter r.

To disable monitoring on the resource, press ENTER.

Memory Usage > <Enter>

/ --> [ Threshold Settings ]

==============================

(1) CPU Usage 30%

(2) Memory Usage Disabled

(3) Disk Usage 70%

(4) Services Settings

To change the settings, enter the item number to change.

To quit, enter q. To return to the previous menu enter r: q

[root@TufinOS ~]#
```

Manage Recipient List for Notifications

To configure the recipient list for notifications:

(Click here to view a complete CLI sample.)

1. From the command line of your TOS server, enter: `configure_os_monitoring`
2. Enter 1 to select `Show defined recipients`. The Recipient Settings menu appears.

   ```
   / --> [ Recipient Settings ]
   =============================

   (1) Show defined recipients
   (2) Add recipient
   (3) Delete recipient
   (4) Modify recipient

   To change the settings, enter the item number to change.
   To quit, enter q. To return to the previous menu enter r:
   ```
3. Enter the item number of the element you want to set, and follow the instructions displayed in the menu.

   Repeat this step until all the settings are configured as desired.

Manage Recipient List for Notifications - Sample Code

```
# configure_os_monitoring

[ OS Monitoring Control Panel ]
===============================

(1) Recipient Settings
(2) SMTP Settings
(3) SNMP Settings
(4) Threshold Settings

To change the settings, enter the item number to change.
To quit, enter q: 1

/ --> [ Recipient Settings ]
=============================

(1) Show defined recipients
(2) Add recipient
(3) Delete recipient
(4) Modify recipient

To change the settings, enter the item number to change.
To quit, enter q. To return to the previous menu enter r: 2

To add a recipient, enter a valid mail address.
To quit, enter q. To return to the previous menu, enter r.
Add recipient > joe@yourdomain.com

Recipient 'joe@yourdomain.com' added.
Press ENTER to continue <Enter>

/ --> [ Recipient Settings ]
=============================

(1) Show defined recipients
(2) Add recipient
(3) Delete recipient
```

```
(4) Modify recipient

To change the settings, enter the item number to change.
To quit, enter q. To return to the previous menu enter r: 2

To add a recipient, enter a valid mail address.
To quit, enter q. To return to the previous menu, enter r.
Add recipient > nancy@yourdomain.com

Recipient 'nancy@yourdomain.com' added.
Press ENTER to continue <Enter>

/ --> [ Recipient Settings ]
==============================

(1) Show defined recipients
(2) Add recipient
(3) Delete recipient
(4) Modify recipient

To change the settings, enter the item number to change.
To quit, enter q. To return to the previous menu enter r: 1

/ --> Recipients Settings --> [ Defined Recipients List ]
===========================================================

(1) joe@yourdomain.com
(2) nancy@yourdomain.com

To quit, enter q. To return to the previous menu, enter r. q
[root@TufinOS ~]#
```

Configure SMTP Settings

To configure the SMTP settings:

(Click here to view a complete CLI sample.)

1. From the command line of your TOS server, enter: `configure_os_monitoring`
2. Enter `3` to select `SMTP Settings`. The SMTP Settings menu appears.

   ```
   / --> [ SMTP Settings ]
   ========================

   (1) Server Name Not Defined
   (2) Server Port 25
   (3) User Name Not Defined
   (4) User Password Not Defined
   (5) Sender Email tufin-monitor@tufin.com
   (6) Mail Sending Interval 60 minutes

   To change the settings, enter the item number to change.
   To quit, enter q. To return to the previous menu enter r:
   ```
3. Enter the item number of the element you want to set, and follow the instructions displayed in the menu.

   Repeat this step until all the settings are configured as desired.

Configure SMTP Settings- Sample Code

```
# configure_os_monitoring

[ OS Monitoring Control Panel ]
================================

(1) Recipient Settings
(2) SMTP Settings
(3) SNMP Settings
(4) Threshold Settings

To change the settings, enter the item number to change.
To quit, enter q: 2

/ --> [ SMTP Settings ]
========================

(1) Server Name Not Defined
(2) Server Port 25
(3) User Name Not Defined
(4) User Password Not Defined
(5) Sender Email tufin-monitor@tufin.com
(6) Mail Sending Interval 60 minutes

To change the settings, enter the item number to change.
To quit, enter q. To return to the previous menu enter r: 1

To change SMTP server, enter the server name.
To quit, enter q. To return to the previous menu, enter r.
To delete SMTP server name, press ENTER.
Server Name > smtp.yourdomain.com

/ --> [ SMTP Settings ]
========================

(1) Server Name smtp.yourdomain.com
(2) Server Port 25
(3) User Name Not Defined
(4) User Password Not Defined
(5) Sender Email tufin-monitor@tufin.com
(6) Mail Sending Interval 60 minutes

To change the settings, enter the item number to change.
To quit, enter q. To return to the previous menu enter r: 3

To change SMTP server user, enter the user name.
To quit, enter q. To return to the previous menu, enter r.
To delete SMTP server user, press ENTER.
User Name > smtp_notifications@yourdomain.com

/ --> [ SMTP Settings ]
========================
(1) Server Name smtp.yourdomain.com

(2) Server Port 25

(3) User Name smtp_notifications@yourdomain.com

(4) User Password Not Defined

(5) Sender Email tufin-monitor@tufin.com

(6) Mail Sending Interval 60 minutes

To change the settings, enter the item number to change.

To quit, enter q. To return to the previous menu enter r: 5

To change sender email, enter the email address.

To quit, enter q. To return to the previous menu, enter r.

To delete SMTP sender email, press ENTER.

Sender Email > smtp_notifications@yourdomain.com

/ --> [ SMTP Settings ]

======================

(1) Server Name smtp.yourdomain.com

(2) Server Port 25

(3) User Name snmtp_notifications@yourdomain.com

(4) User Password Not Defined

(5) Sender Email smtp_notifications@yourdomain.com

(6) Mail Sending Interval 60 minutes

To change the settings, enter the item number to change.

To quit, enter q. To return to the previous menu enter r: q

#
```

Extend SNMP in Suite Administration

You can extend SNMP on your server to support additional SNMP MIBs, and customize the behavior of SNMP.

Support additional MIBs:

1. Edit: `/etc/snmp/snmpd.conf`
2. Extend the exposed view, as desired. For example, to expose the MIB-2 OIDs, add the following line:

   ```
   view systemview included .1.3.6.1.2.1
   ```

3. Restart the SNMPD daemon:

   ```
   # service snmpd restart
   ```

   If the restart process fails, run the following:

   ```
   # killall snmpd
   ```

   ```
   # service snmpd start
   ```

Change the default port:

To use port 10161 instead of the default SNMPd port to query the server:

1. Edit: `/etc/snmp/snmpd.conf`
2. Find the "Access control" section. Go to third step, and add the line:

   ```
   view systemview included .1.3.6.1.4.1.21834
   ```

3. At the end of the file (just before the "Further Information" section), add the lines:

   proxy [-Cn CONTEXTNAME] [SNMPCMD_ARGS] HOST OID [REMOTEOID] proxy -v 2c -c public localhost:10161 .1.3.6.1.4.1.21834

4. Restart the SNMPD daemon:

   ```
   # service snmpd restart
   ```

   If the restart process fails, run the following:

   ```
   # killall snmpd
   ```

   ```
   # service snmpd start
   ```

Generating Graphical Display of Monitored Data

Log files extracted for usage thresholds and monitored services can be viewed in a graphical format. Allowing you to review complex information in a manageable format. The gathered data is saved as a .csv file which can be imported into Microsoft Excel, allowing you to analyze the data using various Microsoft Excel features.

Generating data in a graphical format lets you evaluate the performance of hardware behavior of the production environment, instantly highlighting problematic periods where irregularities occurred. For example, the results may highlight when a server is down and the resulting behavior of this incident.

Generating Graphical Data

Data relating to usage thresholds and monitored services are saved every five minutes and the output of the results can be displayed per day of the week, specific blocks of days (up to seven days) or for a whole week.

All the commands files are located at:

```
/opt/tufin/securitysuite/scripts/res_mon_statistics
```

Below is a list of the which can be used in a command:

- CPU usage : Tomcat, Tufin-Jobs
- Memory usage: Postgres
- General usage: Load average
- Server hardware usage:
  - Swap: swapped from disk (/s), swapped to disk (/s)
  - IO: blocks (read/s), blocks (wrtn/s)
  - System:
    - interrupts (/s), context switches (/s)
    - CPU-User [%], CPU-System [%]

The following format is used for the command script:

```
./<script name> <path to resource monitor file(s)>
```

Sample Code

Load Average for specific day:

```
./load-average.sh /var/log/tufin/resource_monitor/res_mon-Sun.log
```

- Load Average for two days:

  ```
  ./load-average.sh /var/log/tufin/resource_monitor/res_mon-Wed.log
  ```

- Load Average for a week: ()

  ```
  ./TufinJobs_CPU.sh /var/log/tufin/resource_monitor/res*
  ```

The outputs of these scripts can be found at:

```
. . . /var/log/tufin/resource_monitor/statistics_results
```

Open these .csv files with Microsoft Excel and create an applicable graph.

Backup and Restore

The TOS backup command can backup all or specific parts of the TOS database, including Marketplace app data. You can restore the backup to the same host, or to another host with the same TOS version. You can also use the restore command to migrate the database to a host with a higher operating system version.

In SecureTrack Distributed Architecture, make sure you backup all distribution servers and remote collectors. These backups include only the TOS local configuration. You can only restore these backups as the same component type.

A procedure for automating backup to a remote location is described in a Tufin Technical Note.

The backup and topology synchronization processes should not run at the same time. To prevent these processes from running at the same time:

a. Before backing up your database, check that the topology synchronization is not also running.

b. Schedule the Backup and Topology Synchronization to run at different times in which there will be no overlap between the two processes.

Configuration-only vs. Full Backup

When you backup SecureTrack, you can do either:

- Configuration-only Backup - backup only the SecureTrack configuration information
- Full Backup - backup the entire SecureTrack database, including configuration, policy revisions and historical reports

The configuration-only backup lets you run a fast backup. The backup file is small so that you can transfer it easily. When you restore from a configuration-only backup, you have everything you need to start collecting revisions, analyzing rules and running reports.

	Configuration-only Backup	Full Backup
All Settings, including: • Users • Domains • Zones • Licenses • TOP plugins	✓	✓
Policy Analysis Queries	✓	✓
Report and Audit Definitions*	✓	✓
Performance Alerts	✓	✓
Topology	✓	✓
Policy Revisions		✓
Revision Comments		✓
Automatic Policy Generator Data		✓
Policy Browser		✓
Rule and Object Usage Data		✓
Firewall OS Monitoring Data		✓
Published Reports		✓
Plug-n-Play License Information		✓

* When you restore from a configuration-only backup, you need to redefine:

- Rule Change Reports
- Security Risk report exceptions
- SecureChange Access Requests

Backing up TOS Classic

The backup command creates a backup of the Tufin Orchestration Suite Classic current configuration and databases for restore and disaster recovery purposes. The backup includes all files necessary to restore a TOS Classic server, but does not include files that are part of the operating system, such as `postgresql.conf`.

When the database takes up most of the hard drive's disk space, this command may fail if the backup is made to a local (non-NFS) file.

For SecureTrack, you can backup only the SecureTrack configuration (conf-only) or backup the configuration with all of the reports and collected policy revisions.

Use the screen command to ensure that the backup command runs to completion.

To backup Tufin Orchestration Suite (TOS) Classic, run:

```
tos backup [--st] [--conf-only] [--stop-all] [--scw ] [--sa] <backup file>
```

If you do not include `--st` or `--scw`, the backup includes both SecureChange and SecureTrack.

`--st` - Makes a backup of the SecureTrack database and configuration only

`--conf-only` - Makes a backup that includes only SecureTrack configuration information. When you use `--conf-only`, you must also use `--st`.

`--stop-all` - Stops all SecureTrack and SecureChange processes before performing the backup. Use this option only if you need to make sure that revisions from after the time the backup is run are not included in the backup.

When `--stop-all` is used, some traffic usage information may be lost.

`--scw` - Makes a backup the SecureChange and SecureApp database and configuration only

`--sa` - Include Suite Administration backup data

`<backup_file>` - the name of the backup file. The file is compressed in TGZ format.

We recommend that you always verify the integrity of a backup file after you copy it to another location. See Verifying TOS Backups.

> The backup and topology synchronization processes should not run at the same time. To prevent these processes from running at the same time:
>
> a. Before backing up your database, check that the topology synchronization is not also running.
>
> b. Schedule the Backup and Topology Synchronization to run at different times in which there will be no overlap between the two processes.

Restoring TOS from a Backup

Use the screen command to make sure that the restore command runs to completion.

We recommend that you always verify the integrity of a backup file after you copy it to another location. See Verifying TOS Backups.

To restore a Tufin Orchestration Suite database from a backup file, on a TOS host run:

```
tos restore [--st] [--scw] [--sa] <path\file>
```

`--st` - Restores the SecureTrack database and configuration

`--scw` - Restores the SecureChange and SecureApp database and configuration

`--sa` - Restores the Suite Administration backup data

The restore completely replaces the existing configuration and database of the TOS products specified by `--st`, `--scw`, `--sa` or any combination of them.

The target restore server must have the same TOS version and at least the same amount of installed RAM as the source backup server.

Verifying TOS Backups

You should always verify the integrity of a backup file after it is copied to new location. The procedure below describes how to verify the integrity of the file copy using `sha1sum` on a Unix-based operating system. There are equivalent `sha1sum` utilities available for Windows.

Verify File Integrity Using sha1sum

1. Determine the checksum of the exported backup file on the source server:

   ```
   [source]# sha1sum <filename>
   ```

   ```
   <checksum_1> <filename>
   ```

   Save the `<checksum_1>` value.

2. Copy the file to the desired destination server, and rerun the sha1sum command.

   ```
   [destination]# sha1sum <filename>
   ```

   ```
   <checksum_2> <filename>
   ```

3. Verify that `<checksum_1>` = `<checksum_2>`.

Verify File Integrity Using sha256sum

1. Determine the checksum of the exported backup file on the source server:

   ```
   [source]# sha256sum <filename>
   ```

   ```
   <checksum_1> <filename>
   ```

   Save the `<checksum_1>` value.

2. Copy the file to the desired destination server, and rerun the sha1sum command.

   ```
   [destination]# sha256sum <filename>
   ```

   ```
   <checksum_2> <filename>
   ```

3. Verify that `<checksum_1>` = `<checksum_2>`.

Create a New SecureTrack Administrator Username

The original SecureTrack administrator username and password created when the initial setup wizard was run is required for certain configuration settings. If you do not know the username or password, you can create a new administrator username.

To create a new administrator username

1. Connect to the remote server via SSH.

2. Run the `st_add_user` command and follow the instructions in the wizard.

   ```
   [root@TufinOS ~]# st_add_user
   Username: <username>
   Password: <pwd>
   Confirm Password: <pwd>
   Admin user <username> is added.
   ```

Ensuring TOS Management Commands Run To Completion

Some TOS management commands (such as `backup`, `restore`, `upgrade`, `archive`, `hactl`, and `da_remote_configurartion.sh`) take time to complete. If the network session to the server terminates before the management command has successfully completed, the command will stop running and the system may become unstable. We recommend that you use the `screen` command to create a named session and run the management command in that session. This ensures that the management command will run to completion even if the network session terminates unexpectedly.

- **To create a named screen session**:

  ```
  # screen -S <session_name>
  # <TOS_management_command>
  ```

  where <session_name> is the name for the screen session (for example `TufinCommands`) and <TOS_management_command> is the specific TOS command (for example `backup` or `restore`).

  The session will be listed as `<pid>.<session_name>` in the list of screen sessions. Execute the management command from within the new screen session. Exit the screen session when the management command has completed.

- **To list all screen sessions**:

```
# screen -ls
There is a screen on:
6350.TufinCommands (Attached)
1 Socket in /var/run/screen/S-root.
```

- **To detach from the screen session**:

  Type `Ctrl-A` and then '`d`'.

- **To attach to a named screen session**: You can reconnect to a named screen session from another network connection on the server.

  ```
  # screen -d -r 6350.TufinCommands
  ```

  Note: `-d` detaches the named screen session if it is attached elsewhere, and `-r` attaches you to the specified screen session.

- **To terminate a screen session**: You must be attached to the screen session to terminate it.

  Do not terminate the screen session while the TOS management command is still running.

  1. Type `exit` at the prompt, or
  2. Type `Ctrl-A`, then type "`:quit<enter>`".

View TOS Database Size

Run the command:

```
# sudo du -sh /opt/tufin/data/volumes/
```

Example Output:

```
# 13G     /opt/tufin/data/volumes/
```

Advanced Intrusion Detection Environment (AIDE)

Overview

Advanced Intrusion Detection Environment (AIDE) is a file and directory integrity checker, which creates a database from the regular expression rules that it finds in the config files. Once this database is initialized it can be used to verify the integrity of the config files. AIDE has several message digest algorithms which it uses to check the integrity of the config files, and it can also check file attributes for inconsistencies.

Running AIDE will have a performance impact. Therefore you may want to disable AIDE checks, or schedule them to run at specific times. Mounted network and external file systems in `/mnt` are automatically excluded from the AIDE scans.

AIDE is supported for TufinOS 3.30 and later.

Discover The Status of AIDE Scans

- Run the following command on the cron.d file:

  ```
  cat /etc/cron.d/aide-check
  ```

  The command returns the following output:

  Enabled AIDE

  ```
  0 5 * * * /usr/sbin/aide --check &> /dev/null
  ```

  Disabled AIDE

  ```
  #0 5 * * * /usr/sbin/aide --check &> /dev/null
  ```

Enable AIDE Scans

Remove the # to enable AIDE checks. For example:

```
0 5 * * * /usr/sbin/aide --check &> /dev/null
```

Disable AIDE Scans

Add the # to disable AIDE checks. For example:

```
#0 5 * * * /usr/sbin/aide --check &> /dev/null
```

Customize The AIDE Schedule

The schedule is a standard `cron` operation. Customize it according to your needs.

Exclude Network and External File Systems

Mounted network and external file systems in /mnt are automatically excluded from AIDE scans.

If you have mounted external network and/or file system in a different location, at the end of the /etc/aide.conf file add a row for each mount path you want to exclude in the following format:

```
!<path to file or directory>/mnt
```

Linux Management

Automating a Remote Backup

You can automate a periodical backup of SecureTrack. The target location can be one of the following:

- A Windows shared folder
- A central storage device, such as NAS/SAN
- Locally on the host

The following solution covers the first option: automating backup to a remote Windows shared folder. The solution includes preparing the targets, configuring the backup script file, and creating a crontab job for automatic scheduling.

The solution leaves temporary data in `/tmp` , which should be cleaned out after confirming successful backup.

The script works on Tufin appliances (TufinOS 1.3 build 60 and higher). For other installations, make sure samba is installed.

To automate a remote backup:

1. Prepare the target Windows host as follows:
    a. Create a shared directory on the target Windows host.
    b. On the Windows host, configure a user account with read and write permissions.
2. Create target directories on SecureTrack, if they do not yet exist, as follows:
    a. Under directory `var`, create a directory called `backup`:

    ```
    mkdir /var/backup
    ```

    b. Under `mnt` create `backup`:

    ```
    mkdir /mnt/backup
    ```

3. Create a new backup script file with this content:

```
#!/bin/sh
export PATH="${PATH}:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin"
DATE=`/bin/date +%F`
VER=`st ver | grep SecureTrack |awk '{print $3$4$5$6}'`
RESULT=`tos backup --st /tmp/tufin-$VER`
echo $RESULT | grep -i "Backup finished successfully" >/dev/null
if [ $? -ne 0 ]; then
echo "backup failed. reason: " $RESULT
exit 1;
fi
mount -t cifs //<IP_of_target_host>/<target_directory_name> -o username=<username>@<domain>,password=<password> /mnt/backup
if [ $? -ne 0 ]; then
echo "Mount failed"
exit 1;
fi
cp /tmp/tufin-$VER"_"$DATE.zip /mnt/backup/tufin-$VER"_"$DATE.zip
if [ $? -ne 0 ]; then
echo "Copy failed"
exit 1;
fi
umount //<IP_of_target_host>/<target_directory_name>
echo "Backup finished successfully"
```

4. Edit the file, and replace the following variables with the appropriate values for your environment:

   - `<IP_of_target_host>`: The IP address or resolvable name of the target Windows host.

     This variable appears twice in the backup script file.

   - `<target_directory_name>`: The path to the target directory on the target Windows host.

   - `<username>`: The user name for the user account with read/write permissions for the target directory.

- `<domain>`: The domain of the user account.
- `<password>`: The password for this user account.

Save and close the file.

5. Place the file on SecureTrack, under `/usr/local/bin`.
6. Give the file executable permissions, by running:

```
cd /usr/local/bin
chmod +x backup.sh
```

7. Edit Crontab to enable periodic scheduling of the backup process, as follows:
   a. Enter Crontab file edit mode:

   ```
   crontab -e
   ```

   b. Add a line to run the backup script file according to a desired schedule. For example, the following will initiate the script every Monday at midnight:

   ```
   0 0 * * 1 /usr/local/bin/backup.sh
   ```

   For full instructions on using crontab, see the crontab page.

Configuring Web HTTP Session Durations

Configuring the Web HTTP Session Timeout

By default, a SecureTrack and SecureChange user is automatically logged out after 30 minutes of inactivity. The web HTTP session timeout for SecureChange and SecureTrack is configured in `httpd.conf` file, and can be changed to meet your security requirements. In a Distributed Architecture deployment, only edit the settings for the Central Server.

To change the web HTTP session timeout

1. On the relevant server, open the file: `/etc/httpd/conf/httpd.conf`
2. Change the `OIDCSessionInactivityTimeout` setting to the desired value.

   The session timeout value is in seconds, and must be in the range of 600 - 86400 s.
3. If the `OIDCSessionInactivityTimeout` parameter does not exist, add it to the file.
4. Run:

```
systemctl restart httpd
systemctl restart tomcat
```

For example, to change the timeout to 15 minutes, set the value to 900 and restart the httpd and tomcat services:

```
OIDCSessionInactivityTimeout 900
```

Configuring the Maximum Duration for a Web HTTP Session

By default, the Web HTTP Session in SecureTrack and SecureChange is automatically terminated for both the UI and for APIs approximately12 hours after a user logs in.

You can change this time period to meet your security requirements. In a Distributed Architecture deployment, only edit the settings for the Central Server.

To change the maximum web HTTP session duration

1. On the relevant server, open the file: `/etc/httpd/conf/httpd.conf`
2. Change the `OIDCSessionMaxDuration` setting to the desired value.

   The maximum session duration value is in seconds. The default setting is 43000 s.
3. If the `OIDCSessionMaxDuration` parameter does not exist, add it to the file.
4. Run:

   ```
   systemctl restart httpd
   systemctl restart tomcat
   ```

For example, to change the timeout to 8 hours, set the value to 28800 and restart the httpd and tomcat services:

```
OIDCSessionMaxDuration 28800
```

> ℹ To continue working after the maximum Web HTTP session duration is exceeded, refresh your browser and log in again.

> ℹ The `OIDCSessionMaxDuration` value is not retained when you upgrade Tufin Orchestration Suite.

Configuring NTP Using Chrony

Overview

Chrony is used to maintain synchronization automatically with an NTP (Network time protocol) server.

- If you are running RHEL/CentOS, you need to install and enable chrony.
- If you are running TufinOS, chrony is installed by default. Continue with Configure the Chrony Service.

Chrony does not synchronize the time zone. To configure the time zone manually, see Setting the Time Zone.

Installing and Enabling Chrony

If you are running TufinOS, chrony is installed by default, continue with "Configure the Chrony Service" on the next page.

If you are running RHEL/CentOS, chrony must be installed and enabled first as follows:

1. Log in to the CLI as user **tufin-admin**.
2. Log in as root user:

   ```
   sudo su -
   ```

   Or

   ```
   sudo -i
   ```
3. Install chrony:

   ```
   yum install chrony
   ```
4. Enable the service:

   ```
   systemctl enable chronyd.service
   ```

Configure the Chrony Service

1. Log in to the CLI as user **tufin-admin**.
2. Log in as root user:

   ```
   sudo su -
   ```

   Or

   ```
   sudo -i
   ```

3. Stop chrony synchronization:

   ```
   systemctl stop chronyd.service
   ```

4. In the chrony configuration file `/etc/chrony.conf`, replace the default servers (`centos.pool.ntp.org`) with the NTP server.
5. Restart the chronyd service:

   ```
   systemctl restart chronyd.service
   ```

6. Check time synchronization:

   ```
   chronyc sources -v
   chronyc sourcestats -v
   chronyc tracking
   ```

Changing the Time and Date

SecureTrack and SecureChange must maintain accurate date and time. If the host is not configured to automatically self-synchronize with an NTP server, you should periodically make sure that the date and time are correct. If the host does self-synchronize with an NTP server, the time zone still needs to be manually configured.

To change the time zone, see Changing the Time Zone.

To check the current date and time settings:

1. Log into the host as the root user.
2. Run:

   ```
   date
   ```

   The resulting output includes the date, time, time zone, and year. For example:

   ```
   Wed Feb 24 13:20:04 CET 2021 ST
   ```

   This means: Wednesday, February 24th 2021, 1:20PM, Central European Time zone.

3. If anything needs to be changed, follow the relevant instructions below.

To change the date or time:

1. Run:

   ```
   date --set "YYYY-MM-DD HH:MM:SS"
   ```

For example, to set to: February 24th, 2021, 14:00, run:

```
date --set "2021-02-24 14:00:00"
```

2. Set the hardware clock according to the software clock, by running:

```
/sbin/hwclock --systohc
```

Setting the Time Zone

Overview

Set the time zone on the hosts server using the `timedatectl set-timezone` command. If the host self-synchronizes with an NTP server, the time zone still needs to be manually configured.

> Creating a symbolic link from the time zone file to `/etc/localtime` is no longer supported.

To change the date or time, see Changing the Time and Date.

To change the time zone

1. Log in as root user:

```
sudo su -
```

2. Use the `tzselect` command to find a specific time zone:

```
tzselect
```

Or use the following command to list all available time zones:

```
timedatectl list-timezones
```

3. Identify the correct time zone and run the following:

```
timedatectl set-timezone <Timezone>
```

For example:

```
timedatectl set-timezone America/New_York
```

4. Run the following command to verify the changes:

```
timedatectl status
```

Changing the Database Time Zone

Overview

To configure the database time zone to match your operating system time zone, stop the relevant services to ensure that all the components synchronize correctly, edit the `log_timezone` and `timezone` fields, and restart the services.

To change the database time zone:

1. Stop the services in the following order:

   ```
   # systemctl stop crond
   # systemctl stop tufin-jobs
   # systemctl stop jms
   # systemctl stop postgresql-11
   ```

2. Edit the database configuration file `/var/lib/pgsql/11/data/postgresql.conf` with the desired values for the `log_timezone` and `timezone` fields:

   ```
   # vim /var/lib/pgsql/11/data/postgresql.conf
   log_timezone = '<timezone value>'
   timezone = '<timezone value>'
   ```

3. Start the services in the following order:

   ```
   # systemctl start postgresql-11
   # systemctl start jms
   # systemctl start tufin-jobs
   # systemctl start crond
   ```

Adding a Persistent Static Routes

You can add static routes in the OS in one of two ways:

Method 1: Route Command

The following command will add static routes to /etc/rc.local :

```
route add -net <Destination Network> netmask <netmask> gw <gatewayIP>
```

For example:

```
route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.1.1
```

This method will survive a reboot, but will not survive a restart of the network service or an interface going down (for example, by running: service network restart).

Method 2: Configuration File

The preferred method is to create a configuration file for each interface, to define routing information for traffic going out of that interface. The file should be named:

```
/etc/sysconfig/network-scripts/route-<interface>
```

For example:

```
/etc/sysconfig/network-scripts/route-eth0
/etc/sysconfig/network-scripts/route-eth1
```

Once you have created the file, you can configure a static route, for example:

```
192.168.2.0/24 via 192.168.1.1 dev eth0
```

Discovering the Name of the First Network Interface

Tufin Orchestration Suite is managed on the first network interface, which is automatically assigned by the operating system based on the PCI ID. Any changes made to the network and DNS settings need to be made on this interface. If you do not know the name of the first network interface, you are going to need to discover it first.

For TufinOS 3.50 or above you can modify the first network interface using the tools provided by TOS. See details in Configuring Network and DNS Settings.

To discover the name of the first network interface

For **CentOS 7/RHEL 7** you will need to download the script. Download the script from the Tufin Portal, and unpack it to your machine

1. Download the script **network_interface_by_pci_order.sh**
1. Run the script.
2. Enter the command:

   ```
   /opt/tufin/scripts/os/network_interface_by_pci_order.sh | grep "NET_IFS\[0\]"
   ```

   The name of the first network interface is displayed (index number is 0), which in the example below is `ens161`

   ```
   NET_IFS[0]='ens161'
   ```

Configuring Network and DNS Settings

You can configure network information such as the IP address and hostname of the server. The procedures described below modify the TOS management interface.

For TufinOS 3.50 or higher see Configuring on TufinOS 3.50 or higher.

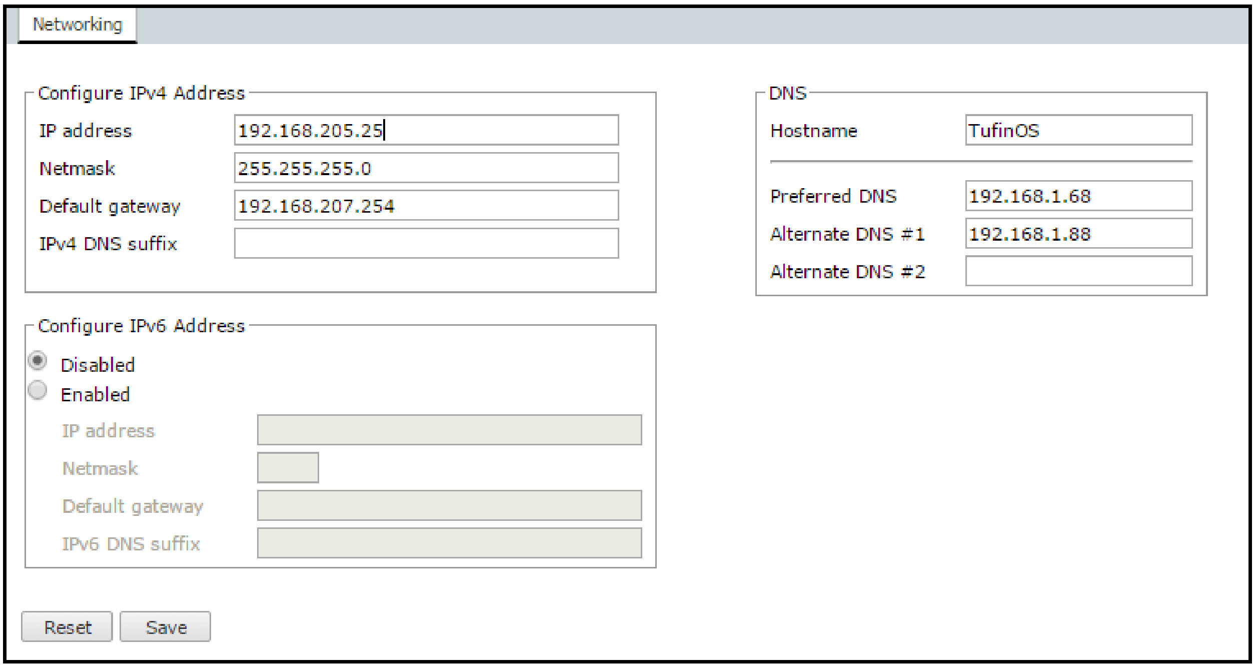
For RHEL/CentOS 7 see Configuring on RHEL/CentOS 7.

Configuring on TufinOS 3.50 or higher

You can access SecureTrack from a browser

If you can access SecureTrack then you can configure the setting from the networking settings page.

1. Log in to **SecureTrack:** as an Administrator.
2. Navigate to **Configure** > **System** > **Networking**.



Configure IPv4 Address

IP address	192.168.205.25
Netmask	255.255.255.0
Default gateway	192.168.207.254
IPv4 DNS suffix	

DNS

Hostname	TufinOS
Preferred DNS	192.168.1.68
Alternate DNS #1	192.168.1.88
Alternate DNS #2	

Configure IPv6 Address

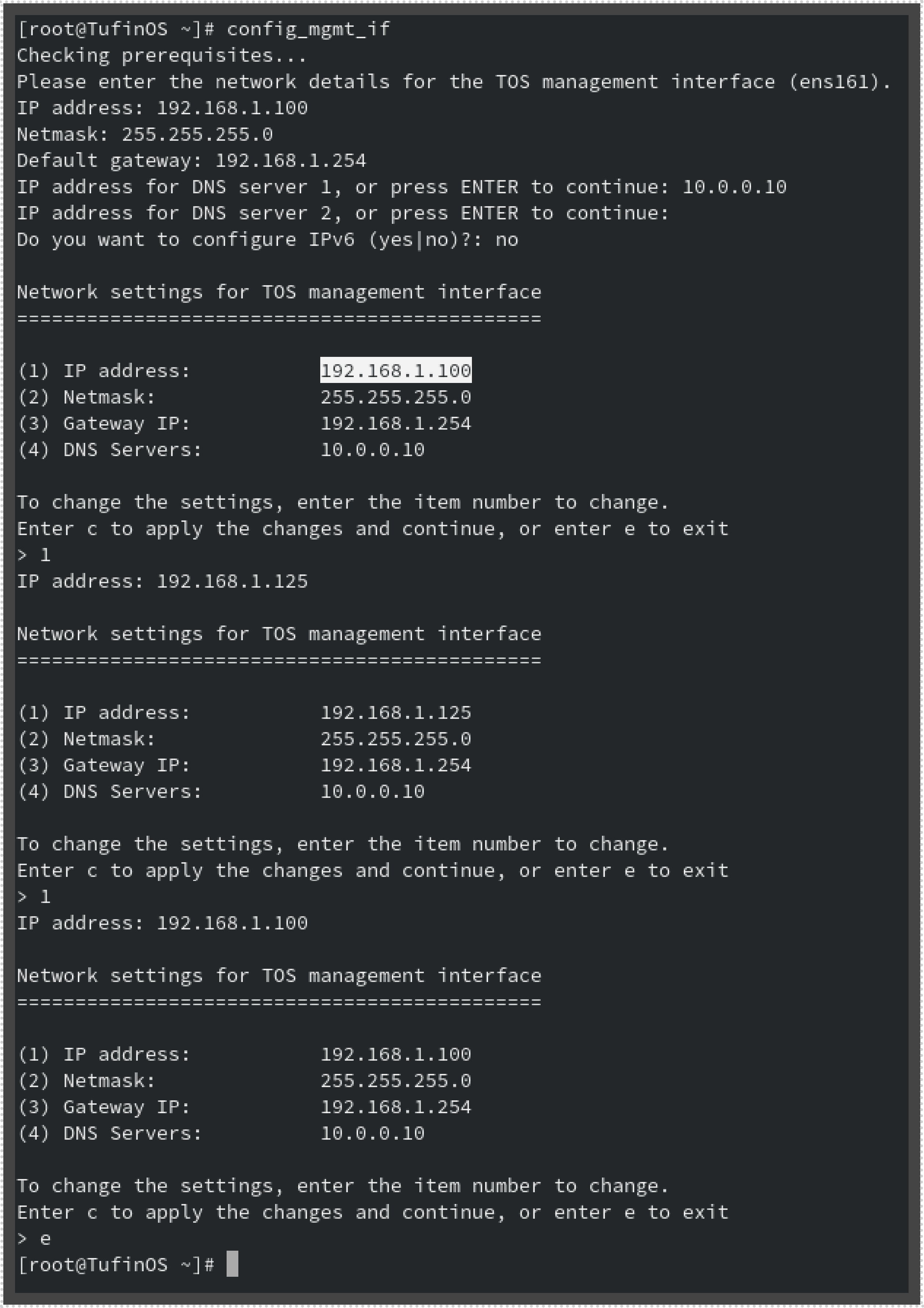
● Disabled
○ Enabled

IP address	
Netmask	
Default gateway	
IPv6 DNS suffix	

3. Configure the desired networking settings.

You cannot access SecureTrack from a browser

If you cannot access SecureTrack from a browser (for example after a clean install of TufinOS) then you can configure the network settings using the CLI command `config_mgmt_if`. The command will prompt you for the configurable network settings. The CLI menu lets you view current settings, modify specific settings, and save your changes only when you have the desired settings.



```
[root@TufinOS ~]# config_mgmt_if
Checking prerequisites...
Please enter the network details for the TOS management interface (ens161).
IP address: 192.168.1.100
Netmask: 255.255.255.0
Default gateway: 192.168.1.254
IP address for DNS server 1, or press ENTER to continue: 10.0.0.10
IP address for DNS server 2, or press ENTER to continue:
Do you want to configure IPv6 (yes|no)?: no

Network settings for TOS management interface
=============================================

(1) IP address:          192.168.1.100
(2) Netmask:             255.255.255.0
(3) Gateway IP:          192.168.1.254
(4) DNS Servers:         10.0.0.10

To change the settings, enter the item number to change.
Enter c to apply the changes and continue, or enter e to exit
> 1
IP address: 192.168.1.125

Network settings for TOS management interface
=============================================

(1) IP address:          192.168.1.125
(2) Netmask:             255.255.255.0
(3) Gateway IP:          192.168.1.254
(4) DNS Servers:         10.0.0.10

To change the settings, enter the item number to change.
Enter c to apply the changes and continue, or enter e to exit
> 1
IP address: 192.168.1.100

Network settings for TOS management interface
=============================================

(1) IP address:          192.168.1.100
(2) Netmask:             255.255.255.0
(3) Gateway IP:          192.168.1.254
(4) DNS Servers:         10.0.0.10

To change the settings, enter the item number to change.
Enter c to apply the changes and continue, or enter e to exit
> e
[root@TufinOS ~]#
```

If you do not have direct SSH access to the server, you can connect to the server via the console.

1. Run the following:

   ```
   sudo su -
   config_mgmt_if
   ```

2. Follow the prompts and instructions displayed.

Configuring on RHEL/CentOS 7

To configure the network settings on RHEL/CentOS 7 you must have root privileges.

Configure the interface IP, DNS, Gateway

To configure the interface IP of SecureTrack you must edit the configuration file of the first network interface. If you do not know the name of the first network interface, see Discovering the name of the First Network Interface.

1. Edit the file `/etc/sysconfig/network-scripts/ifcfg-<first interface name>`.
2. Modify the desired network settings and save your changes.
3. Run the following to make your changes take effect:

   ```
   systemctl restart network
   systemctl restart NetworkManager
   ```

The format of the configuration file for IPv4:

```
TYPE=<network interface device type>
BOOTPROTO=<boot-time protocol>
NAME=<network interface name>
DEVICE=<network interface device name>
UUID=<generated automatically>
ONBOOT=yes
IPADDR=<IP address>
PREFIX=<network prefix>
GATEWAY=<Default_gateway>
DOMAIN=<interface domain>
DNS1=<DNS1 address>
DNS2=<DNS2 address>
DNS3=<DNS3 address>
```

For example, to set interface ens161 to address 192.168.1.100 with a class A netmask in an IPv4 file, edit `/etc/sysconfig/network-scripts/ifcfg-ens161` with these details:

```
TYPE=Ethernet
BOOTPROTO=none
NAME=ens161
DEVICE=ens161
ONBOOT=yes
IPADDR=192.168.1.100
PREFIX=24
GATEWAY=192.168.1.254
DOMAIN=yourdomain.com
DNS1=10.0.0.1
DNS2=10.0.0.2
DNS3=10.0.0.3
```

With IPv6 files you also have the following two fields:

```
IVPV6INIT=yes
IPV6ADDR=<IPv6 address>
```

For example:

```
IVPV6INIT=yes
IPV6ADDR=2001:db8::2/48
```

Associate a hostname with an IP address

To associate a hostname with a specific IP address, you must edit the file `/etc/hosts`.

1. Edit the file `/etc/hosts`.
2. Edit the file, as desired.

   After the third line (beginning with `127.0.0.1`), add a line in this format:

   ```
   <IP> <hostname> <hostname.domain>
   ```

   The IP Address for the hostname configuration must belong to the First Network Interface

   For example:

   ```
   10.0.0.1 yourdomain yourdomain.com
   ```

3. Run the `hostnamectl` command:

   ```
   hostnamectl set-hostname <hostname>
   ```

   For example:

   ```
   hostnamectl set-hostname yourdomain
   ```

4. Reboot the machine to start all services with the new hostname.

   Verify the hostname with the `hostnamectl` command:

   ```
   [root@tufinos ~]# hostnamectl status
     Static hostname: yourdomain
     Pretty hostname: yourdomain
           Icon name: computer-vm
             Chassis: vm
          Machine ID: edea429cc120475383c451380a028b13
             Boot ID: 18e063b724bd4e598e0bc94cdd45a7d0
      Virtualization: vmware
    Operating System: CentOS Linux 7 (Core)
         CPE OS Name: cpe:/o:centos:centos:7
              Kernel: Linux 3.10.0-1160.11.1.el7.x86_64
        Architecture: x86-64
   [root@tufinos ~]#
   ```

   Confirm that `Static hostname` is the new hostname

Configuring a Network Interface on a Virtual Machine

After a network interface has been added to a virtual machine you need to manually create a network interface configuration file (`ifcfg`) for the new interface and then reconfigure the first network interface to make the new interface recognized as the first interface.

To configure a network interface on a virtual machine

1. Run the following command to find network interfaces which do not have an interface configuration file (`ifcfg`):

   ```
   # for i in $(ls -1 /sys/class/net/ | grep -v "lo") ; do [ ! -e /etc/sysconfig/network-
   scripts/ifcfg-${i} ] && echo "$i" ; done
   ```

2. Use either the `nmcli` or the `nmtui` tool to create an `ifcfg` file:

   - **`nmcli` tool (recommended):**

     a. Run the following command to create an `ifcfg` file for each of the interfaces identified in the previous step:

     ```
     nmcli connection add type ethernet ifname [Interface] con-name [Interface]
     ```

     Where **`[Interface]`** corresponds to an interface name. For example:

     ```
     nmcli connection add type ethernet ifname ens193 con-name ens193
     Connection 'ens193' (620eaccd-ac71-42c1-bbb1-77bd97a1c2a3) successfully added.
     ```

   - **`nmtui` tool:**

     a. Run the command `nmtui`

     b. Select **Edit a connection**.

     c. In the list of connections, select an interface without an `ifcfg` file. The interface typically has a name starting with `Wired connection`.

     d. Click **Edit** and change the profile name to match the name of a network interface identified in the first step.

     For example, Before:

     ```
         Profile name   Wired Connection 2
               Device   00:50:56:B2:8C;C6 (ens225)
     ```

     After:

     ```
         Profile name   ens225
               Device   00:50:56:B2:8C;C6 (ens225)
     ```

     e. Modify any other configuration settings needed for the inferface.

3. Repeat step 2 for each interface that does not have an `ifcfg` file.

4. Tufin Orchestration Suite is managed on the first network interface. Discover and configure the first network interface using the following procedures:

   a. Discovering The Name of The First Network Interface

   b. Configuring Network and DNS Settings

Changing the OS Password

To change the operating system password for any user, including root or tufin-admin:

1. Log in.

2. Run:

   ```
   passwd
   ```

3. Type a new password.

Adding Missing Linux Packages

If your **supported Linux OS** is missing required packages, add them in one of the following ways:

- If the Linux host (Red Hat Enterprise Linux or CentOS) has internet access, run the following command:

  `yum install <packages>`

  where `<packages>` is the list of missing packages, separated by spaces. For example:

  `yum install php net-snmp-utils`

- If the Linux host does not have internet access:

  Package file names are the package names, appended with version numbers, host types, and the .rpm extension.

  a. Obtain the .rpm files for the missing packages, in one of the following ways:

     - (For CentOS:) Go to the CentOS website, and click **HTTP** (for any mirror). Click your Linux version number; click **os/** , and then your host type (**x86_64/**). The package files are then under **CentOS/** (you can search the page for the desired packages).
     - Locate the package files on your installation CDs, DVD or ISOs.

  b. Copy the package files to the Linux host, and then run:

     `rpm -Uvh --replacepkgs <package_files>`

     where `<package_files>` is the list of missing package files, separated by spaces. For example:

     `yum install php-4.3.9-3.22.9.i386.rpm net-snmp-utils-5.1.2-13.el4.i386.rpm`

     The packages **net-snmp** and **net-snmp-libs** are interdependent. If one of these packages is installed and the other is missing, first remove the existing one, as follows:

     `rpm -e --nodeps <existing_package_file>`

     `rpm -Uvh --replacepkgs net-snmp net-snmp-libs`

Redirect HTTP traffic to HTTPS

You can access the TOS products over HTTPS protocol using port 443. When you enter the address of the TOS server in a web browser without the https:// prefix, the connection fails because the TOS processes are not listening for the HTTP protocol on port 80.

To avoid this common error, you can configure your TOS server to redirect requests received on port 80 to port 443. This lets users connect to the TOS server even when they mistakenly enter the address of the server without the https:// prefix.

This configuration assumes some knowledge of Linux.

To redirect port 80 requests to port 443:

1. Login to the command line interface of the TOS server.
2. To create a new `custom.conf` file and edit it with vi, enter:

   ```
   vi /etc/httpd/conf.d/custom.conf
   ```

3. Enter these lines in the file:

   ```
   Listen <server_ip_address>:80
   RewriteEngine On
   RewriteCond %{HTTPS} off
   RewriteCond %{REMOTE_HOST} !^127\.0\.0\.1.*$
   RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
   ```

   Change the <server_ip_address> in the `Listen` statement to the host IP or VIP (for example, if HA is configured for automatic failover) address.

4. Save the file.
5. To restart the httpd service, enter:

   ```
   systemctl restart httpd
   ```

Configuring the TufinOS Rsyslog Server to Send Logs to a Remote Rsyslog Server

Overview

You can configure the TufinOS rsyslog server to send logs to a remote rsyslog server. By sending the logs to a remote server, you can maintain a large archive of system logs without worrying about how much storage the logs are consuming on the TufinOS server. The remote server can also be used as a backup in cases where hard drive failure causes information to be lost, and it protects the integrity of log data in cases of attacks on the local system.

How Do I Configure the TufinOS Rsyslog Server to Send Logs to an Rsyslog Server

1. In the TufinOS Rsyslog server, edit `/etc/rsyslog.conf` file. Edit the remote host forwarding rule as follows (second line in example below):

   - Uncomment the line
   - Replace **`remote-host`** with the IP address or domain name of the remote rsyslog server
   - For UDP servers, add one '@' before the IP or Domain name. For TCP servers, leave the two '@@' before the IP or Domain name as is
   - If the default port of the remote syslog server is not 514, enter the correct port number

   Before:

   ```
   # remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
   #*.* @@remote-host:514
   ### end of the forwarding rule ###
   ```

   After:

   ```
   #remote host: name/ip:port, e.g. 192.168.0.1:514, port optional
   *.*@@<IP or Domain of remote rsyslog server>:514
   ### end of the forwarding rule ###
   ```

2. Restart the rsyslog service:

   ```
   systemctl restart rsyslog.service
   ```

Resetting The Password of the Root User

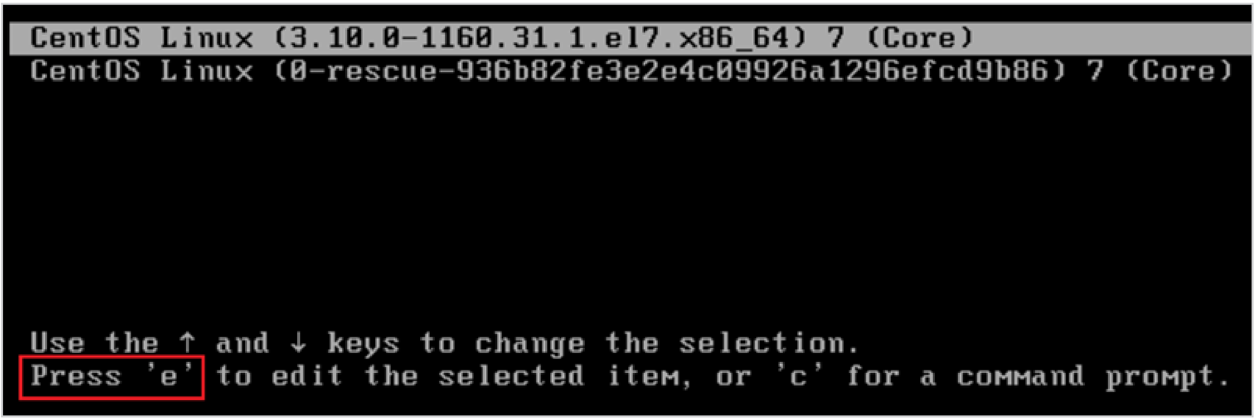
In TufinOS administration privileges are handled through the tufin-admin user. However, there are rare cases where the root user is also required, such as when you need to recovering the password for the tufin-admin user.

If faced with such a situation, and you don't have the password of the root user, you are going to need to enter `rd.break` mode and reset it.

This procedure is also relevant for non-TufinOS Linux systems.

Reset The Password of The Root User

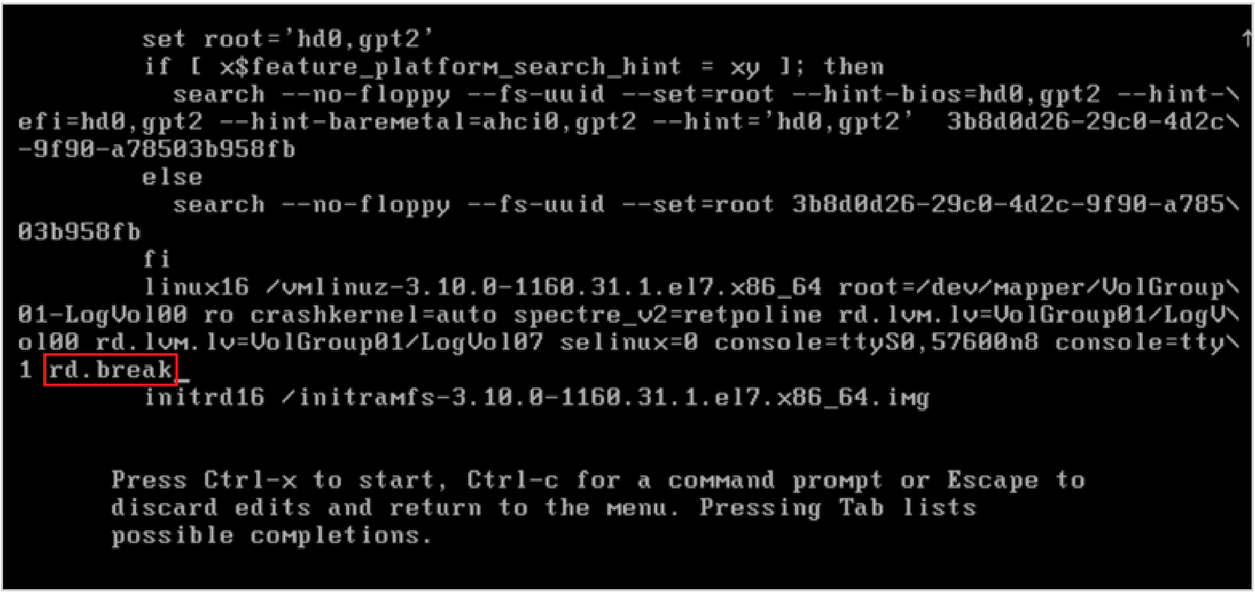
1. Reboot your operating system.
2. While rebooting, press `e` to edit the first boot entry - the kernel name autogenerated by the operating system.



```
CentOS Linux (3.10.0-1160.31.1.el7.x86_64) 7 (Core)
CentOS Linux (0-rescue-936b82fe3e2e4c09926a1296efcd9b86) 7 (Core)




Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

If you upgrade to TufinOS 3.100 from an older version, the grub menu displays three boot entries. Edit the first entry.

3. From the grub options, find the line that starts with `linux16.`. Enter `rd.break` without quotes at the end of this line.



```
        set root='hd0,gpt2'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,gpt2 --hint-\
efi=hd0,gpt2 --hint-baremetal=ahci0,gpt2 --hint='hd0,gpt2'  3b8d0d26-29c0-4d2c\
-9f90-a78503b958fb
        else
          search --no-floppy --fs-uuid --set=root 3b8d0d26-29c0-4d2c-9f90-a785\
03b958fb
        fi
        linux16 /vmlinuz-3.10.0-1160.31.1.el7.x86_64 root=/dev/mapper/VolGroup\
01-LogVol00 ro crashkernel=auto spectre_v2=retpoline rd.lvm.lv=VolGroup01/LogV\
ol00 rd.lvm.lv=VolGroup01/LogVol07 selinux=0 console=ttyS0,57600n8 console=tty\
1 rd.break_
        initrd16 /initramfs-3.10.0-1160.31.1.el7.x86_64.img


      Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
      discard edits and return to the menu. Pressing Tab lists
      possible completions.
```

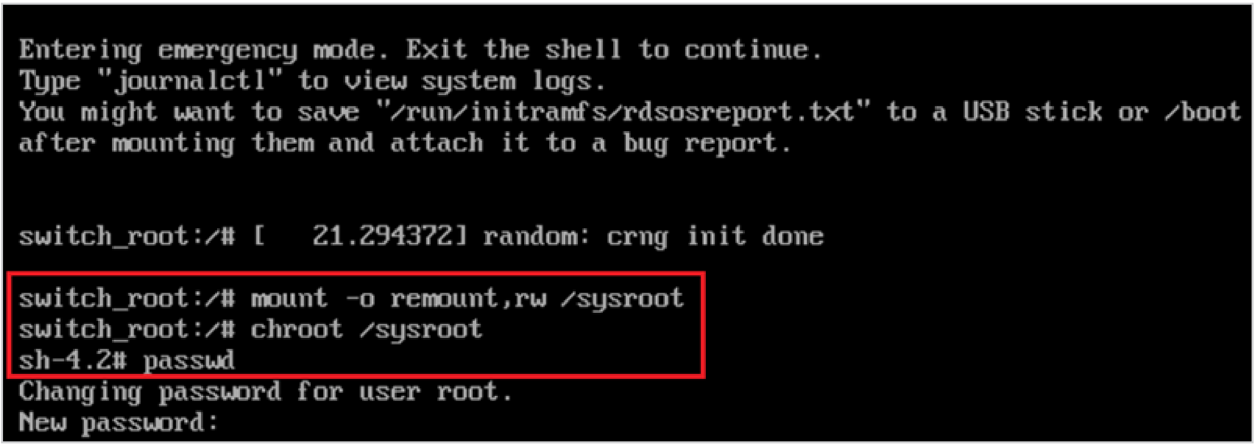
4. Press **Ctrl+X** to reboot.

   The root file system is mounted in read only mode to `/sysroot` and must be remounted with read/write (rw) permissions.

5. Enter `mount -o remount,rw /sysroot`.

   After remounting, you are going to need to switch to chroot jail so that that `/sysroot` is used as the root of the file system. This is required so that any further commands you run will be in regards to `/sysroot`.

6. Enter `chroot/sysroot`.



```
Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.


switch_root:/# [   21.294372] random: crng init done

switch_root:/# mount -o remount,rw /sysroot
switch_root:/# chroot /sysroot
sh-4.2# passwd
Changing password for user root.
New password:
```

7. To reset the password of the root user, enter `passwd`.

8. Enter the new password and then retype it.

   You have updated the password of the root user.

9. To exit the chroot jail environment and reboot the system, enter `Exit` twice.

   Once the system reboots, you will be able to access the root user account with the password you created.

Patents and Trademarks

Patents

For a listing of Tufin patents see www.tufin.com/patents.

Trademarks

Tufin, SecureChange, SecureTrack, Automatic Policy Generator, and the Tufin logo are trademarks of Tufin Software Technologies Ltd.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Some TOP plugins include software developed by Terrapin Communications, Inc. and its contributors for RANCID.

Document Version Information

This document is relevant for all R21-3 releases up to HF6.

Published on Sunday, 4 December, 2022 3:22 PM.