

Juniper Connected Security Use Case: Automated Threat Remediation Using Forescout CounterACT

Published
2021-12-21

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Connected Security Use Case: Automated Threat Remediation Using Forescout CounterACT
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

1

Introduction

About This Guide | 7

2

What is Juniper Connected Security?

Juniper Connected Security Building Blocks | 9

Why Develop Juniper Connected Security ? | 9

Benefits of Juniper Connected Security | 11

Components of Juniper Connected Security | 13

Centralized Policy | 13

Sophisticated Threat Detection and Analytics | 15

Enforcement Everywhere | 17

Juniper Networks' Devices | 18

Private and Public Cloud Hosting Platforms | 19

Third-Party Devices | 19

Automated Threat Remediation for the Enterprise | 20

Protecting the Campus and Branch | 20

Threat Detection | 21

Enforcement | 22

3

Use Case

Use Case Overview: Threat Remediation of Infected Hosts with Forescout CounterACT | 25

Customer Benefits | 26

Use Case Building Blocks | 27

Security Fabric Building Block | 28

ATP Cloud Realm (Management) Building Block | 28

Threat Intelligence Feed Building Block | 28

Enforcement Building Block | 29

Workflow for Endpoint Visibility and Access Control | 29

Device Detection and Profiling | 31

Agentless Endpoint Compliance | 31

Guest Access and BYOD | 32

Use Case Implementation: Juniper Connected Security Automated Threat Remediation with ForeScout CounterACT and Juniper Networks Devices | 32

Requirements | 33

Use Case Topology | 34

Install and Configure Junos Space, Security Director, and Log Collector | 35

Install Junos Space, Security Director, and Log Collector | 36

Configure Basic Junos Space Networking | 36

Install the required DMI Schemas on Security Director | 36

Install and Configure SRX Series, EX Series, and QFX Series Devices | 37

Install and Configure Microsoft Windows Server and Active Directory | 38

Download, Deploy, and Configure Policy Enforcer Virtual Machine | 38

Identify and Connect Policy Enforcer to Security Director | 39

Obtain an ATP Cloud license and Create an ATP Cloud Web Portal Account | 39

Install Root CA on the ATP Cloud Supported SRX Series Devices | 39

Generate Root CA Certificate using Junos OS CLI or OpenSSL on a UNIX Device | 40

Configure a Certificate Authority Profile Group | 41

Export and Import Root CA Certificate into a Web Browser | 42

Download, Deploy, and Configure the ForeScout CounterACT Virtual Machine | 43

Prerequisite Tasks | 44

Install and Configure CounterACT Software | 45

Install and Configure CounterACT Plugins | 59

Configure User Directory Plugin | 61

Configure Switch Plugin | 63

Configure 802.1X Plugin | 67

Configure Windows 7 Supplicant | 71

Test and Troubleshoot 802.1X Authentication | 77

Configure Data Exchange Plugin | 80

Configure Web API Plugin | 84

Verify Plugins | 86

Configure Automated Threat Remediation Policies | 86

Configure the Policy Enforcer Connector for Third-Party Switches | 96

Configure ATP Cloud with Threat Prevention Policies | 97

Use Case Verification | 110

Verify the Enrollment of Devices in ATP Cloud on an SRX Series Device | 110

Verify the Enrollment of Policy Enforcer and SRX Series Devices in ATP Cloud | 111

Verify the Enrollment of Devices with ATP Cloud in Security Director | 111

Verify ForeScout CounterACT Functionality to Block Infected Endpoint (with 802.1X Authentication) | 112

Verify ForeScout CounterACT Functionality to Quarantine Infected Endpoint (with 802.1X Authentication) | 116

Verify ForeScout CounterACT Functionality to Block Infected Endpoint (with NETCONF) | 122

Verify ForeScout CounterACT Functionality to Quarantine Infected Endpoint (with NETCONF) | 129

Appendix A: Device Configurations | 136

CLI Configuration for SRX Series Device | 136

CLI Configuration for EX4300 Switch | 141

CLI Configuration for QFX Switch | 142

Appendix B: Troubleshooting Adding Third-Party Connector | 144

Troubleshooting Policy Enforcer | 144

Troubleshooting ForeScout CounterACT | 145

1

CHAPTER

Introduction

[About This Guide | 7](#)

About This Guide

The purpose of this guide is to provide networking professionals with the concepts and tools needed to build a solution that includes Juniper Networks equipment integrated with a ForeScout CounterACT security appliance. The ForeScout CounterACT security appliance provides threat remediation within the solution.

This document is intended for system engineers, network architects, network security administrators, professional services personnel, Juniper Networks' partners, and anybody else that is installing or wants to learn more about Juniper Connected Security that utilize Juniper Networks equipment or ForeScout CounterACT security appliances.

2

CHAPTER

What is Juniper Connected Security?

Juniper Connected Security Building Blocks | 9

Benefits of Juniper Connected Security | 11

Components of Juniper Connected Security | 13

Automated Threat Remediation for the Enterprise | 20

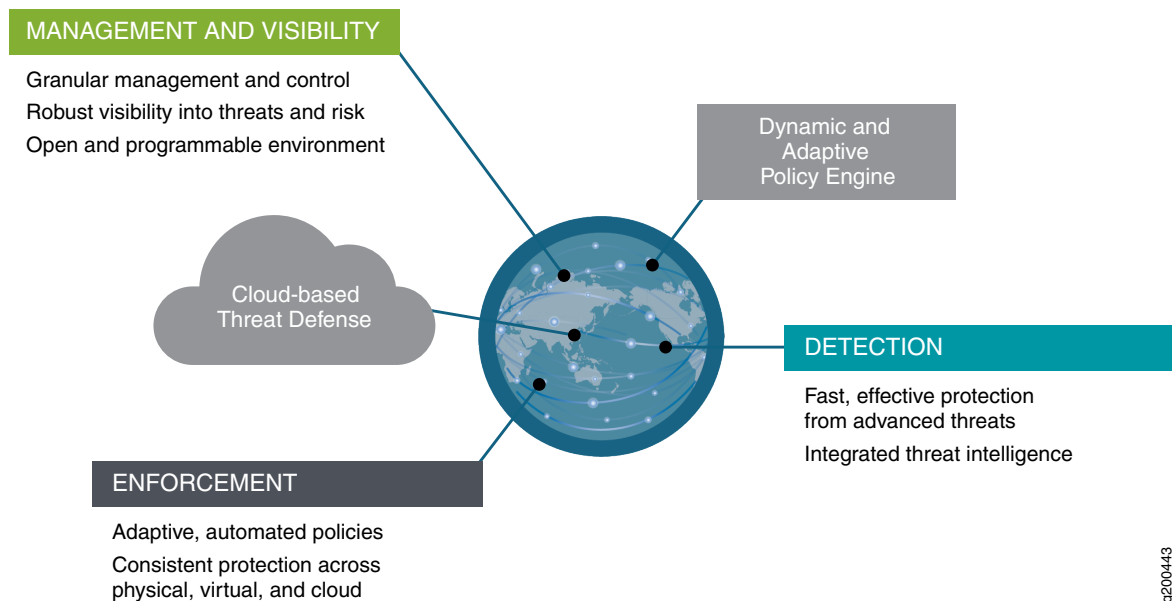
Juniper Connected Security Building Blocks

Juniper Connected Security is Juniper's open and extensible cyber security platform that leverages cloud economics to integrate, centralize, and automate defense from today's sophisticated threat landscape. Juniper Connected Security automatically and dynamically detects and responds to threats as a whole ecosystem rather than as an individual entity. Because a network is only as secure as its weakest link, every physical and virtual element in a Juniper Connected Security platform becomes an active participant (policy enforcement point) in detecting or containing threats across any environment.

The building blocks of Juniper Connected Security are:

- Detection
- Enforcement
- Management and visibility

Figure 1: Building Blocks of Juniper Connected Security

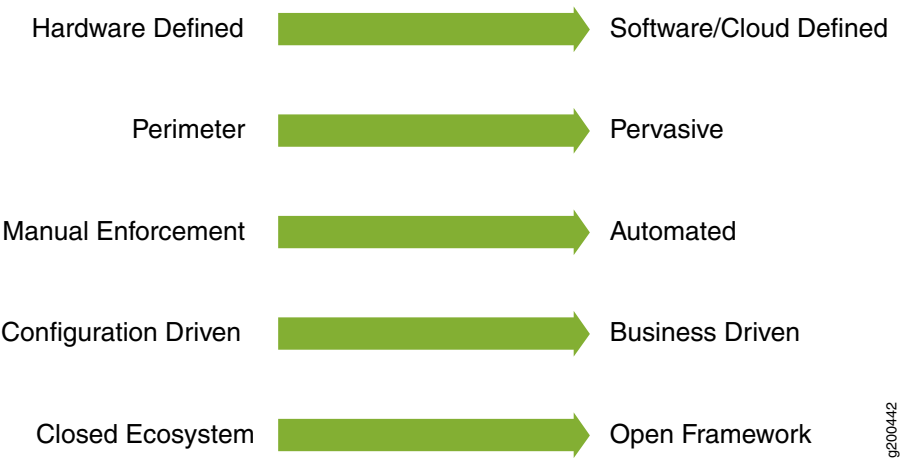


Why Develop Juniper Connected Security ?

Current network practices and architectural models were becoming less effective and more difficult to operate. In particular, the security continuum was moving from firewalls to next-generation firewalls

(NGFW). However, the future of securing the network required a new approach and change in mindset to shift from NGFW to Juniper Connected Security.

Figure 2: Change in Mindset



Architecture, technology, and market transitions aligned and provided the timely environment used to reinvent secure networking and develop Juniper Connected Security.

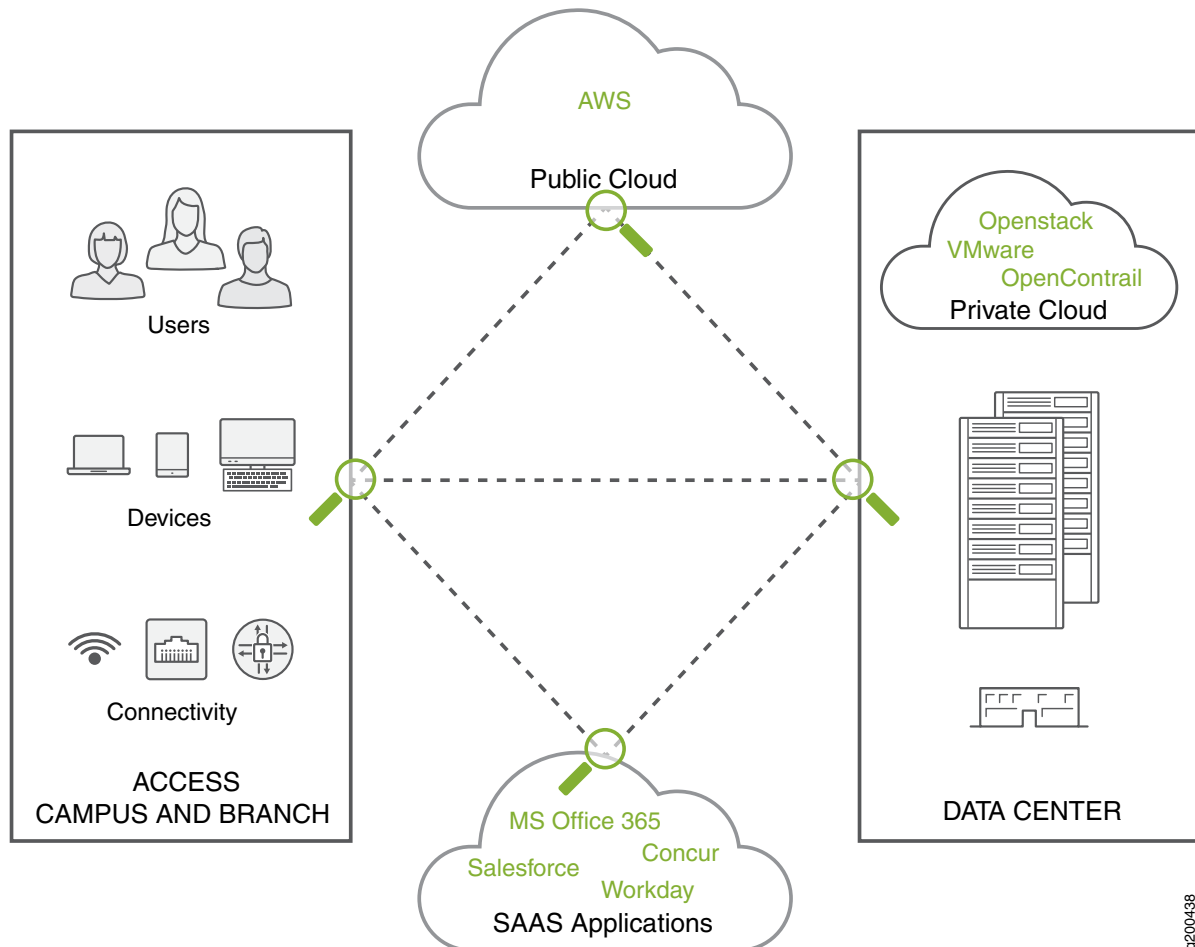
RELATED DOCUMENTATION

Benefits of Juniper Connected Security 11
Components of Juniper Connected Security 13

Benefits of Juniper Connected Security

Based on an inside-out security model, the Juniper Connected Security platform delivers pervasive security and automated threat remediation without complexity. It is a user intent-based policy model that provides consistent policy enforcement across multiple enforcement domains, and robust visibility and management. User intent-based policies are created according to logical business structures such as: users/groups, geographical locations, applications, or threat risks. This enables network devices (switches, routers, firewalls and other security devices) to share information, resources, and when threats are detected, dynamically adapt to take remediation actions within the network. Automation is prevalent throughout Juniper Connected Security.

Figure 3: Inside-out Security Model



The elements in the Juniper Connected Security provide the following benefits:

- **Centralized management and visibility.** You gain visibility of North–South traffic and the ability to block (and view certain traffic when using the ATP Appliance) East–West traffic when a threat is detected originating from an internal source. The entire network infrastructure is operationalized and managed as a single enforcement domain. As each device in Juniper Connected Security meets the security requirement, it is configured with the same policy as other devices, thereby reducing administrative overhead and simplifying the operation of the whole network.
- **Comprehensive security.** Firewalls are right-sized for their application in the network, and their capabilities are consistent across different deployment models ranging from on-premises physical deployment or private clouds in a data center, to public clouds, to software as a service (SaaS) applications. The Juniper Connected Security extends security on both public and private cloud environments by integrating with native cloud mechanisms to isolate infected hosts within the public cloud (such as AWS) and private cloud (such as Contrail and VMWare NSX) environments. This enables administrators to provide a uniform security policy and threat protection on application resources irrespective of whether they reside on campus, in a local data center, or in a public or private cloud.
- **Protection from advanced malware.** Elements of the Juniper Connected Security (ATP Cloud integrated with SRX/vSRX, and Advanced Threat Prevention Appliance) automatically detect known and unknown threats. The Juniper Connected Security platform gathers and transforms the threat intelligence information into actionable items for the various enforcement points, such as blocking or quarantining those threats at the network layer to prevent further propagation.
- **Multi-vendor integration.** Juniper Connected Security adopts an open, multivendor ecosystem to detect and enforce security across Juniper products and solutions, as well as on third-party devices through Juniper's ecosystem partners. A portfolio of APIs provides integration with ecosystem partners and vendors in public and private clouds, as well as with SaaS applications. This fosters a collaborative and comprehensive approach to network security.
- **Access and application mobility.** Elements of the Juniper Connected Security secure and consolidate threats from different sources to protect network access for all users, devices (laptops, mobile devices, and so on) and connectivity methods (wireless and wired).

RELATED DOCUMENTATION

[Components of Juniper Connected Security | 13](#)

[Juniper Connected Security Building Blocks | 9](#)

Components of Juniper Connected Security

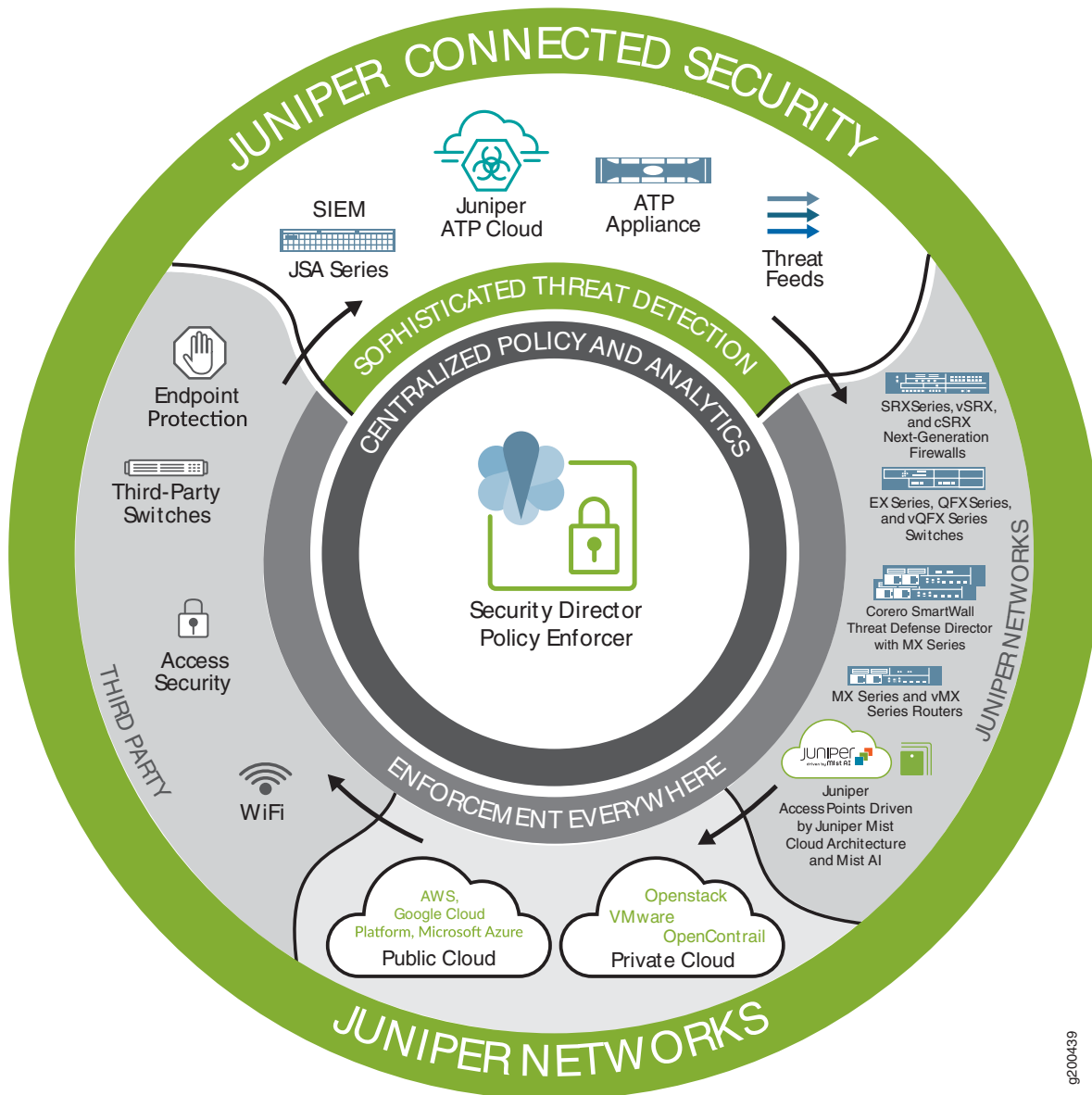
Juniper Connected Security uniquely protects your business, unifying all your network elements into a threat-aware network. It dynamically enforces security policy with software-defined containment designed to reduce the overall attack surface.

Because Juniper Networks security solutions are open and extensible, our partnerships with network and security vendors extend the Juniper Connected Security vision by providing customers with a choice of products to deploy a best of breed solution.

Centralized Policy

At the core of the Juniper Connected Security, Junos Space Security Director provides centralized policy and management. Security Director is a management application designed to quickly create, maintain, and apply accurate and consistent network security policies. It also manages the firewalls.

Figure 4: Juniper Connected Security



g200439

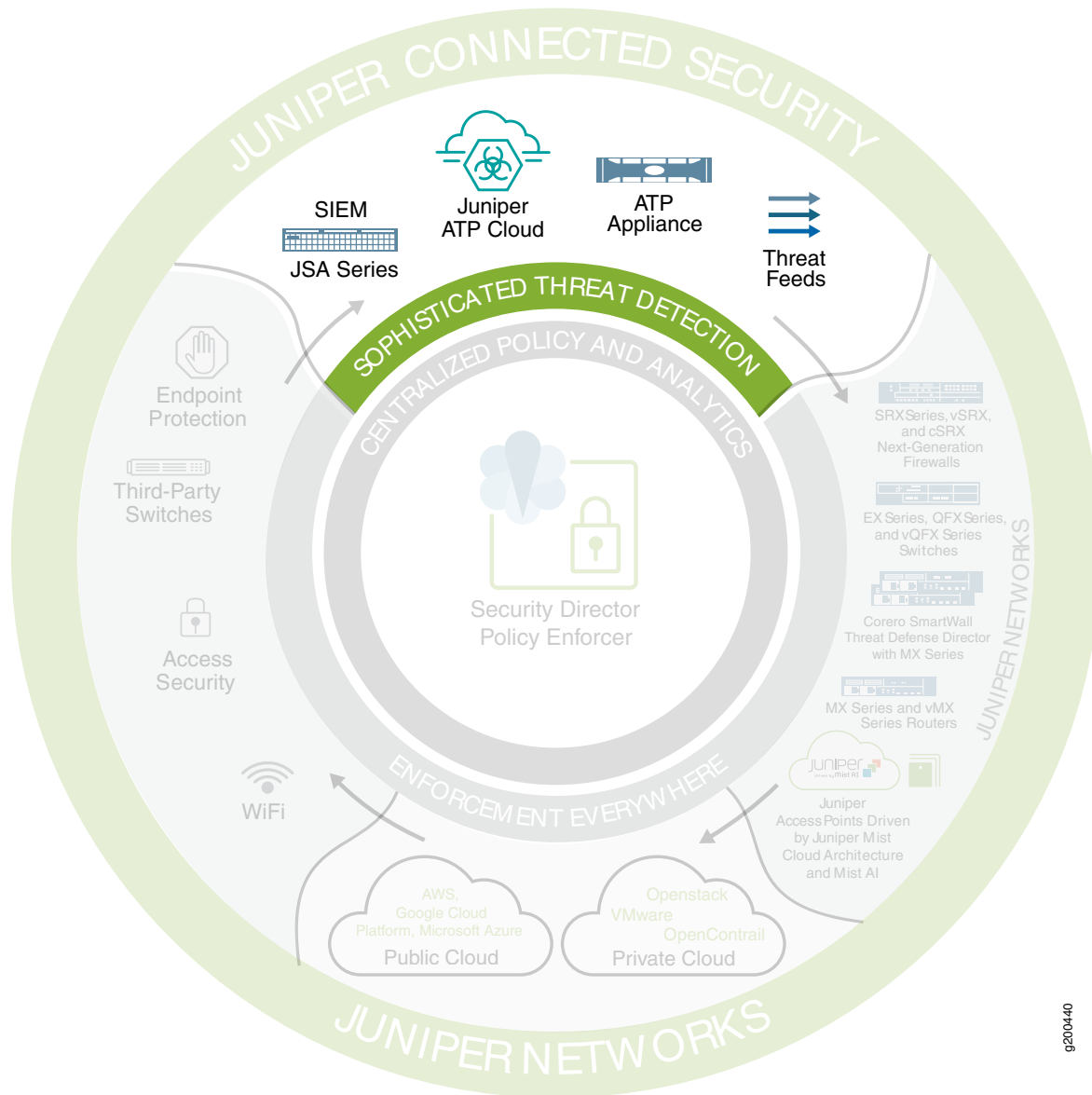
Policy Enforcer provides the management interface that communicates with Juniper devices and third-party devices (through Juniper's ecosystem partners) across the network, globally enforcing threat prevention policies and consolidating threat intelligence from different sources. It enables you to act on that intelligence from a single management interface where you can view, analyze, and apply your threat prevention policies.

Sophisticated Threat Detection and Analytics

Sophisticated threats to your network can come from both known sources (in-house logging, cloud feeds) and unknown sources (cybercrime, Internet-of-Things (IoT) botnets, machine learning, hacktivism). Additionally, each threat can pose various degrees of network disruption ranging from low/moderate impact (where damage from these attacks have the potential to disrupt core business functions and access some sensitive data) to severe/catastrophic impact (where business functions are severely impacted, outages of critical services occur, sensitive data is compromised, and systems and infrastructure are destroyed).

Starting at the top of the diagram, the Juniper Connected Security includes products that can detect and combat these threats by leveraging the entire network and ecosystem.

Figure 5: Sophisticated Threat Detection



g200440

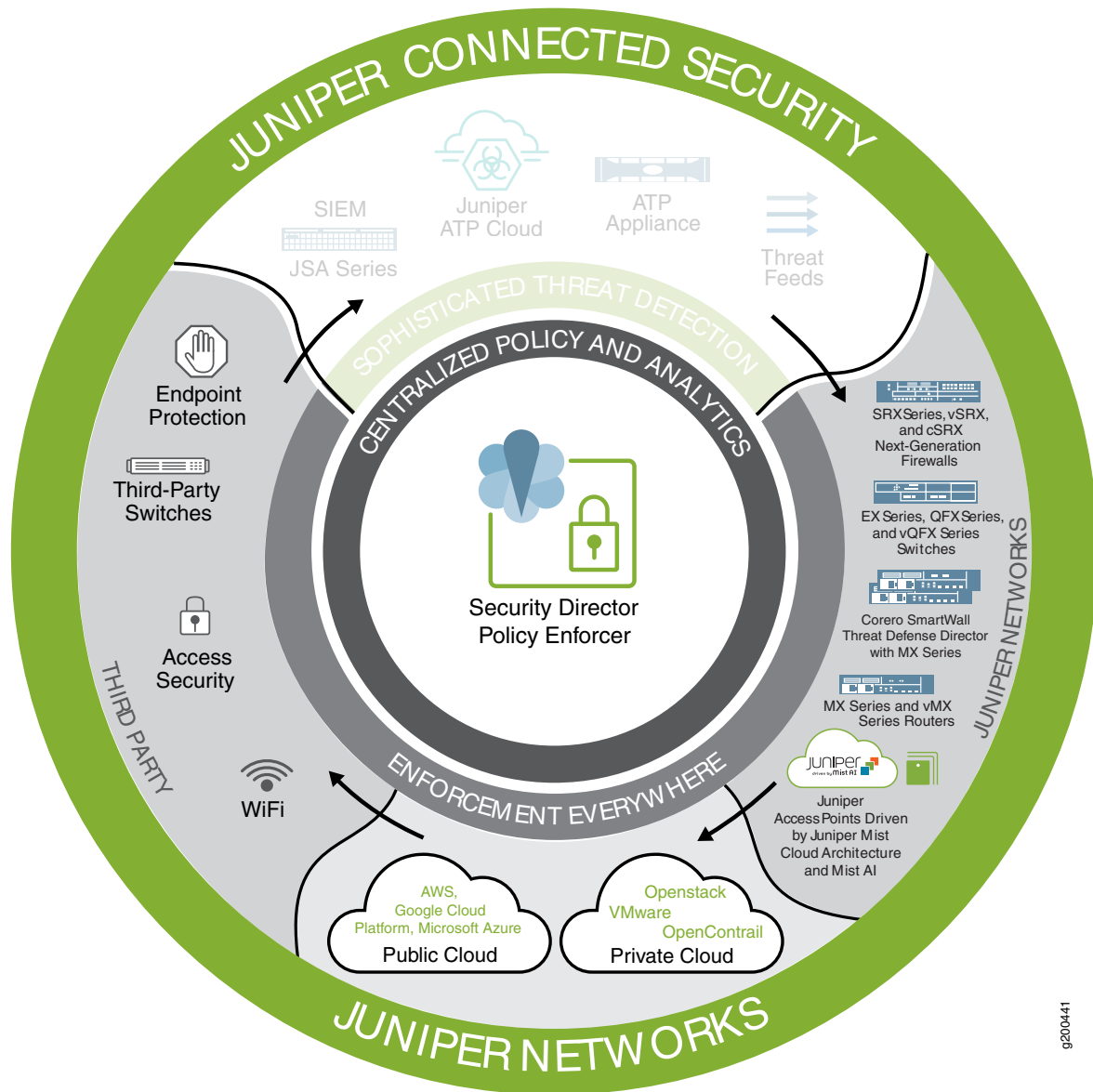
- JSA Series Secure Analytics Appliance (physical and virtual) is an industry-leading security information and event management (SIEM) system optimized for virtualized environments, and suited for cloud-based deployments.
- ATP Cloud (Advanced Threat Prevention Cloud) is a cloud-based solution that integrates with Policy Enforcer to secure sensitive data and detect malware in a cloud shared environment. The SRX device sends the threat information to the ATP Cloud. ATP Cloud then gathers information about the threats (inside and outside the network perimeter) and reports it to Policy Enforcer. Policy Enforcer learns about these threats, and based on the configured policy, the enforcement points then respond to and take action to block and quarantine those threats.

- Advanced Threat Prevention (ATP) Appliance (physical and virtual) leverages advanced machine learning and behavioral analysis technologies to identify existing and unknown advanced threats in near real time through continuous, multistage detection and analysis of Web, email, and lateral spread traffic.
- Threat intelligence (TI) and Command & Control (C&C) feeds are ongoing internal and external streams of data related to potential or current threats to your company's security. Possible sources of threat intelligence data include free and paid feeds, bulletins, internal intelligence gathering and strategic partnerships. Policy Enforcer can also gather third-party feeds, and based on the configured policy, the enforcement points can then respond to and take action to block and quarantine those threats.

Enforcement Everywhere

Continuing clock-wise from the top of the Juniper Connected Security diagram, any physical or virtual point of the network can be used as enforcement point including: switches, firewalls, and routers, public cloud and private cloud platforms, and third-party devices.

Figure 6: Enforcement Points



g200441

Juniper Networks' Devices

Policy Enforcer integrates with Juniper's physical and virtual devices: switches, firewalls, and routers. With information learned from threat detection, Policy Enforcer automatically updates security policies with dynamic address entries and deploys new enforcement to firewalls and switches, blocking, quarantining and tracking infected hosts in the network.

- EX Series and QFX Series switches. EX Series switches deliver switching services in branch, campus, and data center networks, while QFX Series switches are high-performance, high-density edge devices optimized for data center environments. These switches provide access security, control, and connection to servers and clients. EX Series and QFX Series devices act as access and aggregation switches, and connect clients/endpoints with endpoint protection software.
- SRX Series next-generation physical, virtual (vSRX), and container (cSRX) firewalls provide high-performance network security with advanced integrated threat intelligence delivered on a scalable and resilient platform. You can modernize and upgrade your perimeter to make it adaptable, while simplifying your network and removing niche appliances. SRX Series firewalls connect EX Series and QFX Series switches securely. You can use Security Director to manage the SRX Series firewalls to provide security enforcement and deep inspection across all network layers and applications. Juniper Secure Connect on SRX Series devices allows you to securely connect and access protected resources on your network from devices anywhere across the globe.
- MX Series and vMX (virtual MX) Series routers support a universal set of edge applications, enabling you to rapidly respond to evolving business and technical requirements, simplify operations, and gain flexibility. With the Juniper Trio chipset, you can scale MX Series routers for bandwidth, subscribers, and services, and support new features without upgrading hardware. MX Series routers with Corero SmartWall Threat Defense Director deliver real-time DDoS protection on networks.
- Juniper Wireless Access Points work in conjunction with the Juniper Mist Cloud Architecture and Mist AI to collect and analyze metadata in near real-time from all wireless clients.

Private and Public Cloud Hosting Platforms

Juniper Connected Security taps into the power of cloud computing by adopting an open, multivendor ecosystem to detect and enforce security across Juniper solutions, private and public clouds, and third-party ecosystems.

- Private cloud (also known as internal, corporate, or enterprise cloud) –A cloud type implemented in a proprietary network or data center that uses cloud computing technologies to create a virtualized infrastructure dedicated to the needs and goals of a single organization, whether managed internally or externally. Private cloud examples are: VMware NSX, Juniper Contrail.
- Public cloud–A cloud type in which a hosting service provider makes resources such as applications, storage, and CPU usage available to the public. Public clouds must be based on a standard cloud computing model. Public cloud examples are Amazon AWS, Google Cloud Platform (GCP), and Microsoft Azure.

Third-Party Devices

The Juniper Connected Security enforces threat prevention policies for the following third-party devices:

- Access security points. Supports any network element (physical devices, virtual machines, software applications, third-party switches, wi-fi devices, and mobile devices) that is part of a network access controller (NAC) solution, such as: Cisco Identity Services Engine (ISE), Aruba ClearPass, ForeScout CounterACT, or Cisco's Wireless LAN Controller (WLC).

RELATED DOCUMENTATION

[Juniper Connected Security Building Blocks | 9](#)

[Benefits of Juniper Connected Security | 11](#)

Automated Threat Remediation for the Enterprise

IN THIS SECTION

- [Protecting the Campus and Branch | 20](#)
- [Threat Detection | 21](#)
- [Enforcement | 22](#)

This use case deploys Juniper Connected Security for an enterprise and illustrates how to secure your network.

Protecting the Campus and Branch

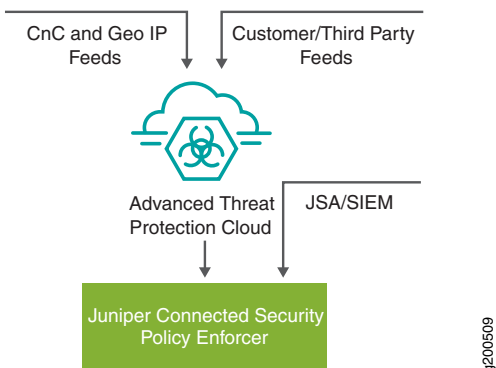
Maintaining reliable and secure campus and branch networks is vital to organizations. With the proliferation of mobile devices and cloud services, securing them has become a fundamental strategic part of enterprise cybersecurity.

Threat remediation is comprised of 2 parts:

- Threat detection
- Enforcement

Threat Detection

Figure 7: Advanced Threat Prevention Cloud Overview



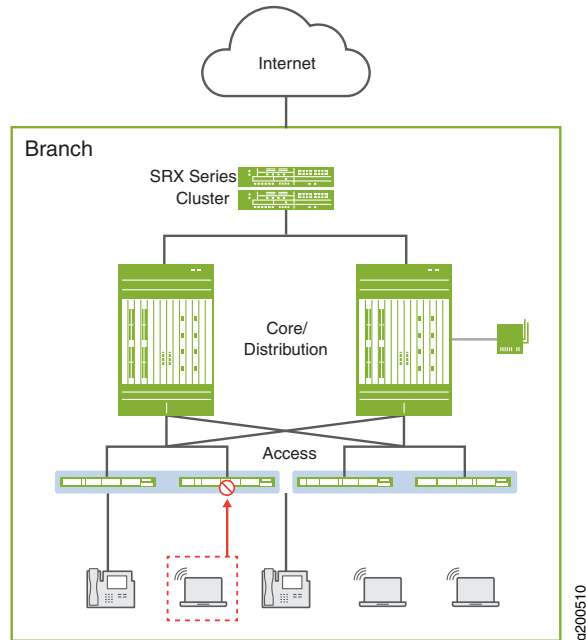
Advanced Threat Prevention Cloud (ATP Cloud) receives threat intelligence and detects threats from these sources:

- ATP Cloud feeds, where zero-day and known malware can be detected.
- Custom and third-party feeds, where custom blacklists, whitelists, infected hosts, dynamic addresses, and DDoS threats can be detected.
- Command & Control (C&C) and Geo IP feeds, where botnet traffic and geo-specific security controls can be detected.

The Juniper Connected Security Policy Controller (comprised of Security Director and Policy Enforcer) controls and enforces threat remediation policies across the network framework (firewalls, routers, and switches). The JSA Series Secure Analytics Appliance (physical and virtual) feeds into the Juniper Connected Security Policy Controller.

Enforcement

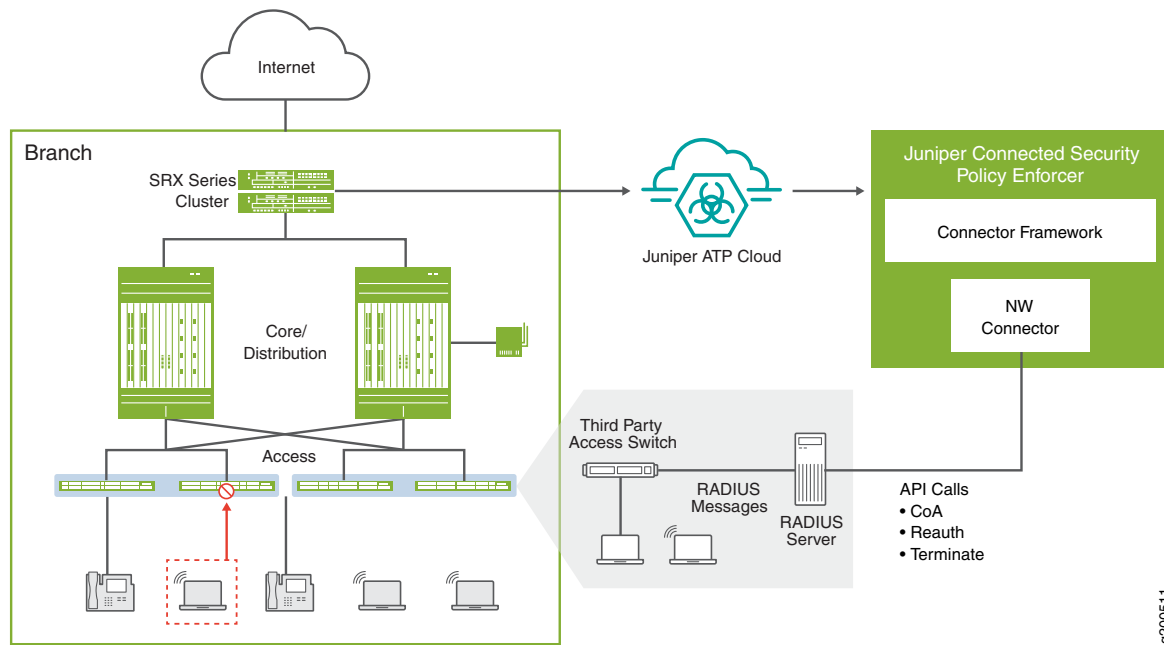
Figure 8: Juniper Connected Security Enforcement in a Branch Network Overview



With information learned from threat detection, Policy Enforcer automatically updates security policies in the campus and branch with dynamic address entries and deploys new enforcement to the following network levels:

- Security and firewall level: Juniper Networks SRX Series devices
- Core and distribution level: Juniper Networks MX/vMX Series routers
- Access level containing the following switches:
 - Juniper Networks EX Series and QFX Series switches
 - Access switches configured with third-party connectors, such as ForeScout CounterACT

Figure 9: Threat Remediation = Threat Detection + Enforcement



Juniper Connected Security protects the campus and branch physical network by performing real-time remediation of infected hosts and prevents infected end points from moving across different parts of the network. By reducing the time to remediate threats, the amount of time that the network is exposed to attacks is reduced.

RELATED DOCUMENTATION

[Juniper Connected Security Building Blocks | 9](#)

[Use Case Implementation: Juniper Connected Security Automated Threat Remediation with ForeScout CounterACT and Juniper Networks Devices | 32](#)

3

CHAPTER

Use Case

Use Case Overview: Threat Remediation of Infected Hosts with Forescout CounterACT | **25**

Use Case Implementation: Juniper Connected Security Automated Threat Remediation with ForeScout CounterACT and Juniper Networks Devices | **32**

Use Case Overview: Threat Remediation of Infected Hosts with ForeScout CounterACT

IN THIS SECTION

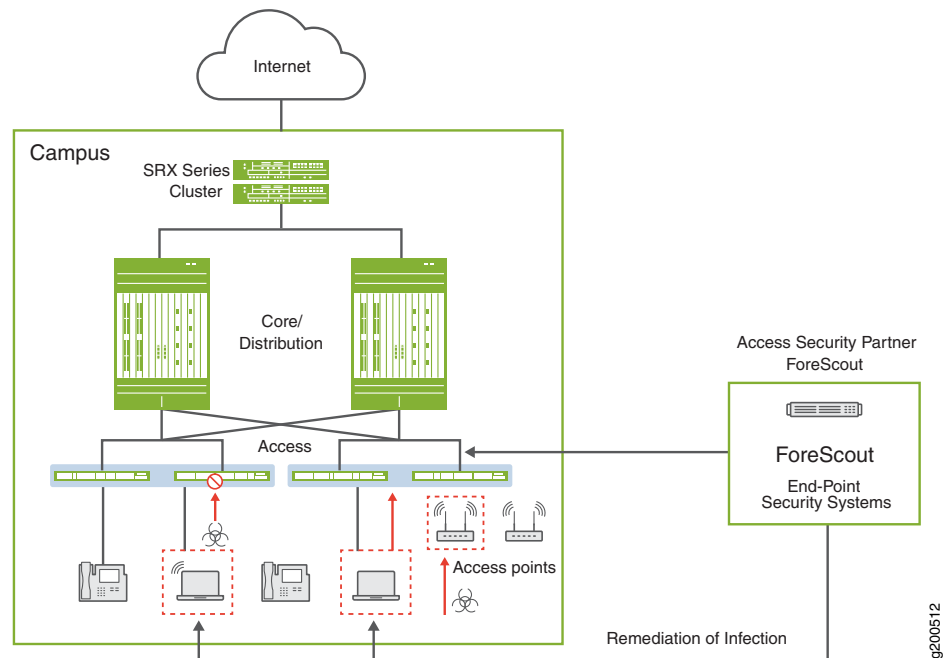
- [Customer Benefits | 26](#)
- [Use Case Building Blocks | 27](#)
- [Workflow for Endpoint Visibility and Access Control | 29](#)
- [Device Detection and Profiling | 31](#)
- [Agentless Endpoint Compliance | 31](#)
- [Guest Access and BYOD | 32](#)

This use case provides a step-by-step Juniper Connected Security for enterprises to remediate threats of infected hosts using a third-party device, ForeScout CounterACT. ForeScout CounterACT is an agentless security appliance that dynamically identifies and evaluates network endpoints and applications the instant they connect to your network. CounterACT applies an agentless approach and integrates with Juniper Connected Security to block or quarantine infected hosts on Juniper Networks' devices, third-party switches, and wireless access controllers with or without 802.1X protocol integration.

Without requiring management agents or previous device awareness, CounterACT uses active and passive techniques to discover and classify endpoints as they connect to the network, including:

- BYOD (bring your own device), such as smartphones, laptops, tablets, and guest devices
- Non-traditional devices, such as IoT devices, handhelds, and sensors
- Unknown and rogue endpoints; such as unauthorized endpoints, switches, routers, and wireless access points

Figure 10: Threat Remediation with ForeScout CounterACT



Using agentless visibility, CounterACT checks for device posture and compliance according to the security policies defined by the organization. Then, based on device classification and posture, CounterACT coordinates an automated host- or network-based response.

Customer Benefits

The elements in this use case provide the following benefits:

- *Multilayer Security*

You gain layered security, policy enforcement, and control at the access, aggregation, core, and perimeter while greatly increasing your network security profile and reducing noncompliance risks and unauthorized access.

- *Agentless*

No endpoint agents are required for device profiling, compliance, remediation, and access control. CounterACT detects and controls managed, unmanaged, and IoT devices which greatly simplifies deployment.

- *Open Interoperability*

Elements in this use case are based on industry-standard protocols, enabling interoperability with other third-party solutions. CounterACT integrates with various switches, routers, VPNs, firewalls, and endpoint operating systems without requiring infrastructure changes or upgrades.

- *802.1X and Non-802.1X authentication*

You can deploy CounterACT with Juniper Networks switches using 802.1X authentication or a robust non-802.1X approach. This use case provides a hybrid deployment approach, allowing you to select to authenticate traditional devices using 802.1X, or connect non-traditional devices using a non-802.1X approach.

- *Comprehensive Endpoint Visibility and Assessment*

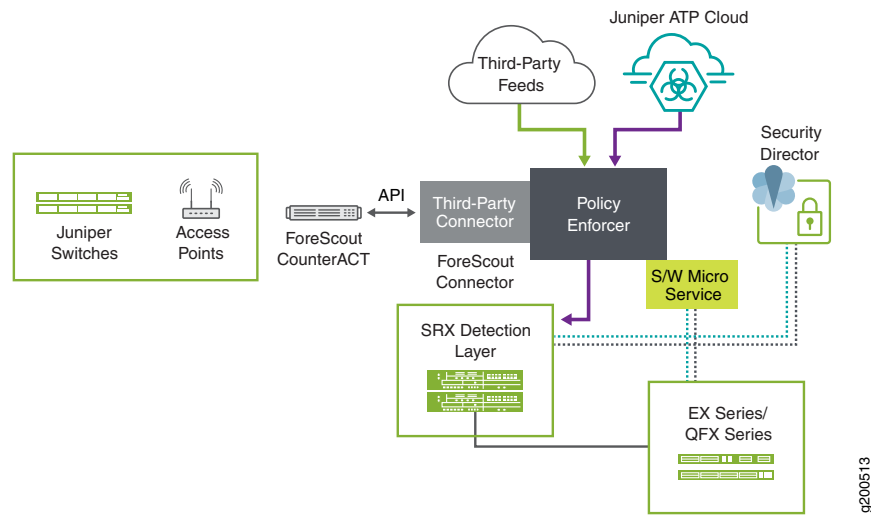
With great detail and speed, CounterACT detects the network to identify, evaluate, and monitor network endpoints and applications, as well as determine the device's operating system, configuration, software, services, patch state, and presence of security agents. CounterACT automatically classifies a growing number of IoT endpoints as it quickly clarifies and assesses the status and security posture of devices on the network.

Use Case Building Blocks

IN THIS SECTION

- [Security Fabric Building Block | 28](#)
- [ATP Cloud Realm \(Management\) Building Block | 28](#)
- [Threat Intelligence Feed Building Block | 28](#)
- [Enforcement Building Block | 29](#)

Figure 11: Use Case Building Blocks



There are four building blocks for this use case.

Security Fabric Building Block

Juniper Networks SRX Series firewalls provide security enforcement and deep inspection across all network layers and applications. In this particular Juniper Connected Security use case, a vSRX Series device is deployed as a perimeter firewall connected to ATP Cloud for anti-malware services.

ATP Cloud Realm (Management) Building Block

Juniper Networks ATP Cloud (integrated with SRX Series firewalls and registered with Policy Enforcer) identifies varying levels of risk, and provides a higher degree of accuracy in threat protection. Policy Enforcer orchestrates threat remediation workflows based on threats detected by Juniper's ATP Cloud solution or custom threat feeds, and enforces these policies on firewalls, in particular SRX Series devices, and EX Series and QFX Series switches.

Threat Intelligence Feed Building Block

- ATP Cloud feeds gather threat intelligence from multiple sources (including third-party feeds) and reports the gathered intelligence to Policy Enforcer. Then, Policy Enforcer uses the information gathered and reported by ATP Cloud to learn about the threats and rapidly respond to new threat conditions.
- Policy Enforcer gathers third-party feeds, and based on the configured policy, the enforcement points can then respond to and take action to block and quarantine those threats.

Enforcement Building Block

On the SRX Series firewall using Security Director:

- ATP policy is pushed to the SRX Series firewall from Security Director.
- SRX Series firewall pulls the infected host feed from Policy Enforcer. Policy Enforcer automatically orchestrates threat remediation workflows based on threats detected by Juniper’s ATP Cloud solution or custom threat feeds, and enforces these policies on the SRX Series firewall and EX Series/QFX Series switch. Infected hosts are tracked and stop the progress of threats.

On the EX Series and QFX Series switches:

EX Series and QFX Series switches deliver layered policy enforcement and control at the access, aggregation, core, and perimeter. In the Juniper Connected Security, clients and endpoints are connected to EX Series and QFX Series switches with endpoint protection software. This multilayer approach mitigates risk and noncompliance at multiple levels while increasing the security profile of the network.

- Policy Enforcer identifies an infected host by its IP and MAC address, allowing tracking and continued blocking of the host even if it moves to another switch or access point on the network.
- Commits a MAC F/W filter on the switch for enforcement.
- ForeScout CounterACT is an agentless security appliance that dynamically identifies (discovers) and evaluates network endpoints and applications the instant they connect to your network. In the Juniper Connected Security, using standard protocols such as SNMP, CLI, and IETF Network Configuration (NETCONF) protocol, CounterACT classifies and assesses device compliance posture, then applies automated policy actions at the EX Series and QFX Series switches. CounterACT also provides continuous device monitoring of HTTP and DHCP requests. Additionally, CounterACT leverages RADIUS CoA to enforce automated actions on an 802.1X environment.

Workflow for Endpoint Visibility and Access Control

When CounterACT detects a device that is either unknown, rogue, or noncompliant, it coordinates an instant response through its integration with EX Series switches and wireless controllers.

Table 1 on page 29 summarizes these responses.

Table 1: CounterACT Response Actions

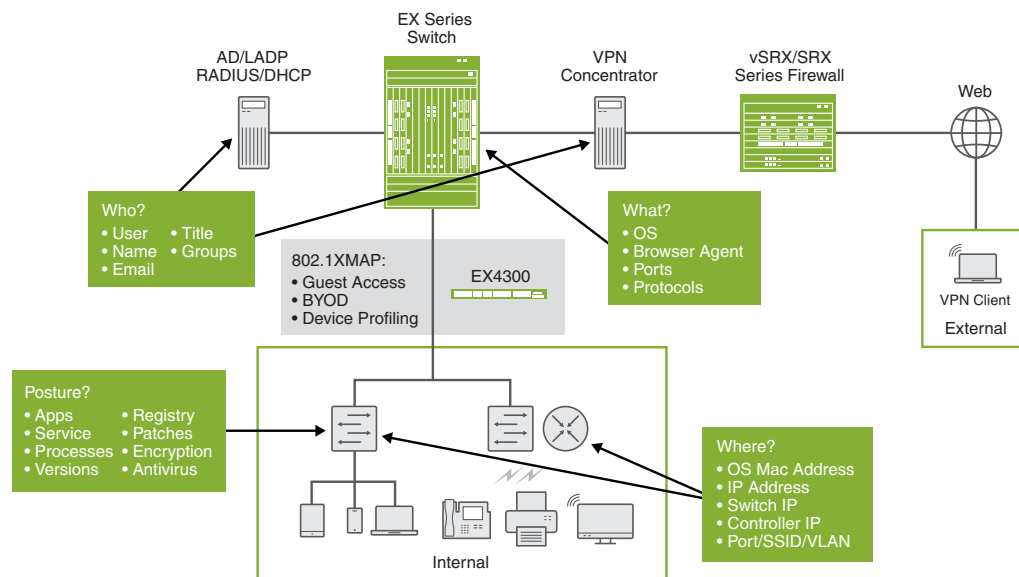
Connection Type	Connection State	Juniper Connected Security Message	Counter ACT Action
-----------------	------------------	------------------------------------	--------------------

Table 1: CounterACT Response Actions (continued)

Wired	Non-Dot1x	Block	Apply VACL
		Quarantine	Quarantine VLAN
	Dot1x	Block	802.1x Authorize—Deny
		Quarantine	802.1x Authorize—Specify VLAN
Wireless	Non-Dot1x	Block	WLAN Block
		Quarantine	WLAN Role
	Dot1x	Block	802.1x Authorize—Deny
		Quarantine	802.1x Authorize—Attribute Value

CounterACT responds to these threats by pushing NETCONF files to Juniper Networks EX and QFX switches. [Figure 12 on page 30](#) shows the flow chart of the response process.

Figure 12: CounterACT NETCONF Configuration File Push Flow Chart



g200514

Based on endpoint classification, ownership, and posture, CounterACT pushes NETCONF configuration files to the switch to take one of the following actions:

1. Block the switch port and deny all network access.
2. Assign the device to a quarantine VLAN with restricted source access.
3. Apply an ACL to the interface to restrict access.
4. Downgrade infected host privileges through RADIUS CoA.

Device Detection and Profiling

The Juniper Networks and ForeScout CounterACT joint solution performs the following for device detection and profiling:

- Identifies the type of connected device, such as printer, IP phone, tablet, Windows, iOS device, and so on.
- Assigns network access based on the user identity or role, device type, location, ownership, and security compliance status.
- Eliminates the need for enterprises to manually maintain a list of known device MAC IP addresses and device-type mappings.
- Enables dynamic provisioning of ports based on the connected device type.

Agentless Endpoint Compliance

The Juniper Networks and ForeScout CounterACT joint solution delivers the following for agentless endpoint compliance:

- Performs granular compliance checks on items such as antivirus software, OS patches, personal firewall, Peer-to-Peer Instant Messaging (P2P-IM), disk encryption, and so on, with the option to remediate any non-compliant issues.
- Enforces compliance on corporate Windows, MAC, and Linux endpoints without installing agents.
- Applies host and network actions, such as notifying users and administrators, moving to a remediation VLAN, pushing a restrictive ACL, and so on.

Guest Access and BYOD

Juniper Networks and ForeScout CounterACT joint solution provides the following for guest access and BYOD:

- Delivers consistent wired and wireless experience to all personally owned devices.
- Redirects users to a webpage through a captive portal to provide instructions on how to authenticate or register.
- Presents users with an acceptable user policy (AUP) that they must agree to in order to obtain restricted guest access.
- Enables guest users to log in using pre-allocated guest access credentials or can easily self-enroll.
- Enables employees with non-corporate devices to be required to authenticate and auto-configure their endpoints. Once their devices have been auto-configured, these employee-owned devices are continuously monitored on the corporate network to ensure security policy compliance.

RELATED DOCUMENTATION

[Use Case Implementation: Juniper Connected Security Automated Threat Remediation with ForeScout CounterACT and Juniper Networks Devices | 32](#)

[Benefits of Juniper Connected Security | 11](#)

Use Case Implementation: Juniper Connected Security Automated Threat Remediation with ForeScout CounterACT and Juniper Networks Devices

IN THIS SECTION

- [Requirements | 33](#)
- [Use Case Topology | 34](#)
- [Install and Configure Junos Space, Security Director, and Log Collector | 35](#)
- [Install and Configure SRX Series, EX Series, and QFX Series Devices | 37](#)
- [Install and Configure Microsoft Windows Server and Active Directory | 38](#)

- Download, Deploy, and Configure Policy Enforcer Virtual Machine | 38
- Identify and Connect Policy Enforcer to Security Director | 39
- Obtain an ATP Cloud license and Create an ATP Cloud Web Portal Account | 39
- Install Root CA on the ATP Cloud Supported SRX Series Devices | 39
- Download, Deploy, and Configure the ForeScout CounterACT Virtual Machine | 43
- Configure the Policy Enforcer Connector for Third-Party Switches | 96
- Configure ATP Cloud with Threat Prevention Policies | 97
- Use Case Verification | 110
- Appendix A: Device Configurations | 136
- Appendix B: Troubleshooting Adding Third-Party Connector | 144

This use case shows how to integrate and configure a ForeScout CounterACT security appliance, a Windows 7 supplicant, a Juniper Networks vSRX virtual firewall, a Juniper Networks EX4300 switch, and a Juniper Networks QFX series switch into a Juniper Connected Security.

To implement this use case for threat remediation (block or quarantine) of infected hosts with ForeScout CounterACT, perform the following required set of installation, configuration, and verification steps:

Requirements

This use case uses the following hardware and software components:

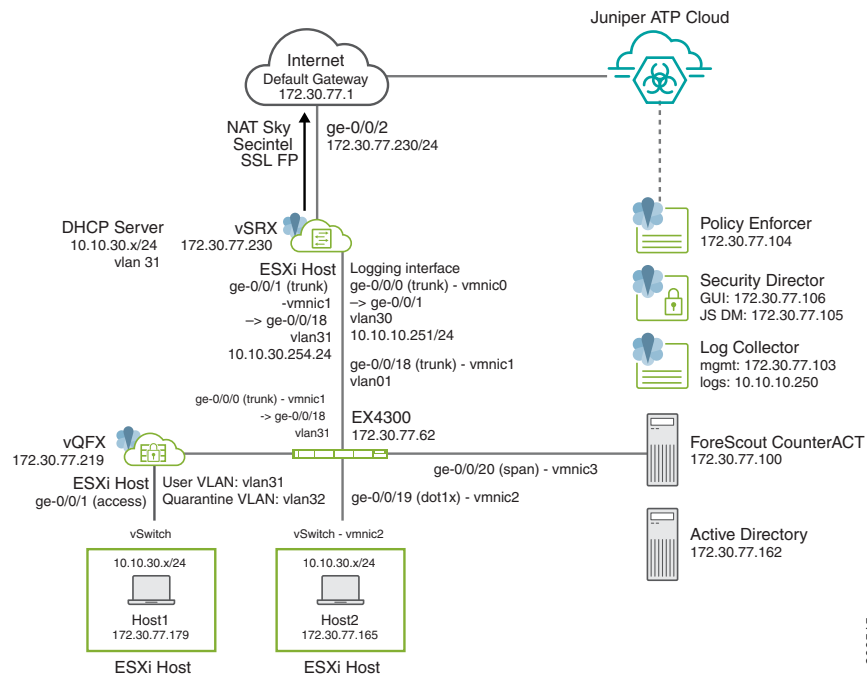
- vSRX virtual firewall running Junos OS Release 15.1X49-D110.4 or later
- a QFX series switch running Junos OS Release 15.1X53-D60.4 or later
- an EX4300 switch running Junos OS Release 15.1R5.5 or later
- Advanced Threat Prevention Cloud (ATP Cloud)
- Junos Space Network Management Platform, Release 17.2R1 or later
- Junos Space Security Director, Release 17.2R2 or later
- Log Collector, Release 17.2R2 or later
- Policy Enforcer, Release 17.2R2 or later
- ForeScout CounterACT version 7.0.0-513-2.3.0-1605
- A virtual machine (VM) running Windows 7 with 2x dual NIC hosts

For a list of supported devices, please refer to the [Policy Enforcer Release Notes](#).

Use Case Topology

The use case topology is illustrated in [Figure 13 on page 34](#)

Figure 13: Juniper Connected Security Automated Threat Remediation with ForeScout CounterACT and Juniper Networks Devices Use Case Topology



The ForeScout CounterACT security appliance applies an agentless approach to network security and integrates with Juniper Connected Security to block or quarantine infected hosts on Juniper Networks' devices, third-party switches, and wireless access controllers that support and do not support 802.1X protocol integration.

In this use case, the infected end user is quarantined into the user vlan VLAN31 on the EX4300 switch. The EX4300 switch has enabled ForeScout CounterACT and has 802.1X authentication enabled on ge-0/0/19. The end user authenticates to the network using 802.1X.

The following events occur in this use case:

1. The infected endpoint is detected by ATP Cloud.
2. Policy Enforcer downloads the infected host feed, and then enforces the infected host policy through CounterACT.
3. CounterACT queries the server for endpoint details for the infected host's IP address.
4. CounterACT sends a message to the EX4300 switch, telling it to terminate the session by blocking or quarantining vlan31.
5. Enforcement occurs on the EX4300 switch on which the endpoint is authenticated.
6. CounterACT inventories the applications, services, and processes running on the device, checks the OS version and registry settings, and verifies the presence of security agents. As a result, a complete profile of the device and its security status is obtained.

Install and Configure Junos Space, Security Director, and Log Collector

IN THIS SECTION

- [Install Junos Space, Security Director, and Log Collector | 36](#)
- [Configure Basic Junos Space Networking | 36](#)
- [Install the required DMI Schemas on Security Director | 36](#)

This section shows how to install and configure Junos Space, Security Directory, and Log Collector for this use cases. These applications are used in this use case to provide the centralized policy and management application for consistent network security policies.

This section covers the following procedures:

Install Junos Space, Security Director, and Log Collector

1. Download the Junos Space Network Management Platform image from <https://www.juniper.net/support/downloads/?p=space#sw>.
2. Install Junos Space using the instructions at https://www.juniper.net/documentation/en_US/junos-space172/information-products/pathway-pages/junos-space-virtual-appliance-pw.html.
3. Install Junos Security Director using the instructions at https://www.juniper.net/documentation/en_US/junos-space172/topics/task/multi-task/junos-space-sd-log-collector-installing.html.
4. Install Log Collector using the instructions at https://www.juniper.net/documentation/en_US/junos-space172/topics/task/multi-task/junos-space-sd-log-collector-installing.html.

Configure Basic Junos Space Networking

To configure basic Junos Space Networking in this use case:

1. Configure relevant routes, netmask, gateway, DNS, and NTP so that all components except Log Collector can connect to the Internet.
2. Ensure all components are in same time zone.
3. Ensure that SSH is enabled.
4. Ensure that Security Director can connect to the ATP Cloud server, Policy Enforcer, and all devices.

For additional information on configuring Junos Space, see [Junos Space Network Management Platform Documentation](#).

Install the required DMI Schemas on Security Director

Download and install the correct matching Junos OS schemas to manage the Juniper Networks' devices:

1. Add the DMI schemas for the Juniper Networks' devices using the instructions at https://www.juniper.net/documentation/en_US/junos-space172/platform/topics/task/operational/dmi-schemas-adding-updating.html.
2. Ensure that device software version and schema version match for all managed devices (SRX Series and EX Series devices).

Install and Configure SRX Series, EX Series, and QFX Series Devices

To install and configure vSRX virtual firewalls, EX Series switches, and QFX Series switches for this use case:

1. Configure the vSRX device as the enforcement point per your requirements. Click “[CLI Configuration for SRX Series Device](#)” on [page 136](#) to review the detailed Junos OS CLI code for this use case.
2. Configure the EX4300 switch per your requirements. Click “[CLI Configuration for EX4300 Switch](#)” on [page 141](#) to review the detailed Junos OS CLI code for this use case. You configure the EX4300 as an 802.1X authenticator and forward the Windows 7 Supplciant’s credentials to ForeScout CounterACT through the RADIUS protocol. The EX4300 switch also mirrors traffic entering from the port where the Windows 7 Supplciant is connected to a destination port that is connected to the “Monitor” interface of the ForeScout CounterACT virtual appliance.

NOTE: For detailed instructions on how to deploy both the EX4300 switch and the QFX switch , click the follow

- https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/ex
- https://www.juniper.net/documentation/en_US/junos/topics/example/802-1x-pnac-ex-series-connecting-se
- <https://github.com/juniper/vqfx10k-vagrant>

3. Configure the QFX switch per your requirements. Click “[CLI Configuration for QFX Switch](#)” on [page 142](#) to review the detailed Junos OS CLI code for this use case. You configure the QFX switch as standard access switch. The QFX switch’s uplink port on the EX4300 switch also mirrors traffic to a destination port that is connected to the *Monitor* interface of the ForeScout CounterACT virtual appliance.
4. Configure basic networking on Junos devices:
 - a. On all Junos devices, configure the necessary routing and DNS settings to enable Internet access, as well as connectivity to Junos Space, Policy Enforcer, and the ATP Cloud server.
 - b. For the SRX device, ensure that Internet access is enabled both in-band and out-of-band.
5. Add devices to the Junos Space Network Management platform:
 - a. In Junos Space, discover and import the SRX device in your environment.
 - b. In Security Director, assign, publish, and update any existing firewall policies to ensure Security Director and the SRX device are in sync.

Install and Configure Microsoft Windows Server and Active Directory

Because ForeScout CounterACT does not have a local user database to use for 802.1X authentication, you must install and configure a Windows Server 2008R2 with Active Directory.

1. To set up and configure Windows Server 2008R2, click <https://docs.microsoft.com/en-us/iis/install/installing-iis-7/install-windows-server-2008-and-windows-server-2008-r2>.
2. To set up and configure Active Directory, click <https://www.petri.com/installing-active-directory-windows-server-2008>.
3. Create a user domain account to use later during 802.1X authentication.

Download, Deploy, and Configure Policy Enforcer Virtual Machine

To download, deploy, and configure the Policy Enforcer Virtual Machine:

1. Download the Policy Enforcer virtual machine image from <http://www.juniper.net/support/downloads/?p=sdpe> to the management station where the vSphere client is installed.
2. On the vSphere client, select *File > Deploy OVF Template* from the menu bar.
3. Click *Browse* to locate the OVA file that was downloaded.
4. Click *Next* and follow the instructions in the installation wizard.
5. Once the installation is complete, log in to the virtual machine using **root** and **abc123** as the username and password, respectively.
6. Configure the network settings, NTP information, and customer information, and complete the wizard.

For more detailed instructions, see

https://www.juniper.net/documentation/en_US/release-independent/policy-enforcer/topics/task/installation/policy-enforcer-vm-config.html.

Identify and Connect Policy Enforcer to Security Director

To identify and connect Policy Enforcer to Security Director:

1. In Security Director, identify the Policy Enforcer virtual machine.
2. Log in to Security Director and select *Administration > PE Settings*.
3. Enter the IP address of the Policy Enforcer virtual machine and the root password, and click OK.
4. Select Threat Prevention Type as *Sky ATP with PE*.

NOTE: At this point, do *not* run the wizard/guided setup.

Obtain an ATP Cloud license and Create an ATP Cloud Web Portal Account

To obtain an ATP Cloud license and create an ATP Cloud Web Portal account:

1. ATP Cloud has three service levels: free, basic, and premium. The free license provides limited functionality and is included with the base software. To obtain and install an ATP Cloud basic or premium license, click [Managing the Advanced Threat Prevention Cloud License](#).

For more details on ATP Cloud service levels and license types, click [Advanced Threat Prevention Cloud License Types](#).

2. Create an ATP Cloud Web portal account by clicking <https://sky.junipersecurity.net> and filling in the required information.

Install Root CA on the ATP Cloud Supported SRX Series Devices

IN THIS SECTION

- [Generate Root CA Certificate using Junos OS CLI or OpenSSL on a UNIX Device | 40](#)
- [Configure a Certificate Authority Profile Group | 41](#)
- [Export and Import Root CA Certificate into a Web Browser | 42](#)

NOTE: This section is required only if you are enabling HTTPS inspection as part of a malware profile or threat prevention policy.

This section covers the following topics:

Generate Root CA Certificate using Junos OS CLI or OpenSSL on a UNIX Device

NOTE: Use only one of these options.

To generate a root CA certificate using the Junos OS CLI on the SRX device:

1. Generate a PKI public key or private key pair for a local digital certificate.

```
user@host> request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type rsa
```

2. Using the key pair, define a self-signed certificate by providing FQDN and other details.

```
user@host> request security pki local-certificate generate-self-signed certificate-id ssl-inspect-ca  
domain-name domain-name subject subject email email-id add-ca-constraint
```

Or

To generate a root CA certificate using OpenSSL on a UNIX device:

1. Generate a PKI public key or private key pair for a local digital certificate.

```
% openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout ssl-inspect-ca.key -out  
ssl-inspect-ca.crt
```

2. Copy the key pair onto the SRX device or devices.
3. On the SRX device(s), import the key pair.

```
user@host> request security pki local-certificate load key ssl-inspect-ca.key filename ssl-inspect-ca.crt
certificate-id ssl-inspect-ca
```

4. Apply the loaded certificate as root-ca in the SSL proxy profile.

```
user@host> set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-ca
```

Configure a Certificate Authority Profile Group

To configure a Certificate Authority (CA) profile group.

1. Create the CA profile.

```
user@host# set security pki ca-profile ssl-inspect-ca ca-identity ssl-inspect-ca
user@host# commit
```

2. Junos OS provides a default list of trusted CA certificates that you can load on your system using the default command option.

```
user@host> request security pki ca-certificate ca-profile-group load ca-group-name ssl-inspect-ca filename
default
Do you want to load this CA certificate ? [yes,no] (no) yes

Loading 155 certificates for group 'ssl-inspect-ca'.
ssl-inspect-ca_1: Loading done.
ssl-inspect-ca_2: Loading done.
ssl-inspect-ca_3: Loading done.
ssl-inspect-ca_4: Loading done.
ssl-inspect-ca_5: Loading done.
...
```

3. Verify that the *ssl-inspect-ca* certificates are loaded.

```
user@host> show security pki local-certificate
...
Certificate identifier: ssl-inspect-ca
...
```

Export and Import Root CA Certificate into a Web Browser

To export and import the Root CA Certificate into a web browser:

1. On the SRX device, first export the root CA certificate to a .pem file.

```
user@host> request security pki local-certificate export certificate-id  
ssl-inspect-ca type pem filename /var/tmp/ssl-inspect-ca.pem
```

2. Transfer the .pem file to your Windows client.

NOTE: If you are using the UNIX device with OpenSSL, the certificate is already on the device and no action is required.

3. Import the certificate into a browser.

If you are using a Windows client, instruct the browser to trust the CA root certificate.

- Internet Explorer (version 8.0):
 - a. From the *Tools* menu, select *Internet Options*.
 - b. On the *Content* tab, click *Certificates*.
 - c. Select the *Trusted Root Certification Authorities* tab and click *Import*.
 - d. In the *Certificate Import Wizard*, navigate to the required root CA certificate and select it.
- Firefox (version 39.0):
 - a. From the *Tools* menu, select *Options*.
 - b. From the *Advanced* menu, select the *Certificates* tab and click *View Certificate*.
 - c. In the *Certificate Manager* window, select the *Authorities* tab and click *Import*.
 - d. Navigate to the required root CA certificate and select it.
- Google Chrome (version 45.0):
 - a. From the *Settings* menu, select *Show Advanced Settings*.
 - b. From the *Advanced* menu, select the *Certificates* tab and click *View Certificate*.
 - c. Under HTTPS/SSL, click *Manage Certificates*.
 - d. In the *Certificate* window, select *Trusted Root Certification Authorities* and click *Import*.
 - e. In the *Certificate Import Wizard*, navigate to the required root CA certificate and select it.

For more details, click:

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/ssl-proxy-workflow-configuring.html

Or

If you are using a UNIX device, import the certificate into the browser:

```
% sudo cp ssl-inspect-ca.crt /usr/local/share/ca-certificates/ ssl-inspect-ca.crt
% sudo update-ca-certificates
```

Download, Deploy, and Configure the ForeScout CounterACT Virtual Machine

IN THIS SECTION

- Prerequisite Tasks | 44
- Install and Configure CounterACT Software | 45
- Install and Configure CounterACT Plugins | 59
- Configure User Directory Plugin | 61
- Configure Switch Plugin | 63
- Configure 802.1X Plugin | 67
- Configure Windows 7 Supplicant | 71
- Test and Troubleshoot 802.1X Authentication | 77
- Configure Data Exchange Plugin | 80
- Configure Web API Plugin | 84
- Verify Plugins | 86
- Configure Automated Threat Remediation Policies | 86

This section covers the following topics:

Prerequisite Tasks

Before you begin this procedure, complete the following tasks:

1. Obtain an evaluation copy of CounterACT (version: 7.0.0-513-2.3.0-1605) to use with Policy Enforcer.
2. Obtain a license key and the following plugin packages from the ForeScout representative:
 - ForeScout-dot1x-4.2.0.1010-42001010.fpi
 - ForeScout-eds-3.2.0-32000032.fpi
 - ForeScout-webapi-1.2.2-12020005.fpi
3. Download and deploy the CounterACT (CA) OVF or the ISO file on an ESXi host.
 - If you download and deploy the ISO file, then:
 - a. Create a new virtual machine (VM) and select *other 2.6.x Linux (32bit)* as the Guest OS.
 - b. Upload your ISO file to *Datastore*.
 - c. Configure your CD or DVD drive to boot from *Datastore ISO file*.

NOTE: Before you power on the VM, you must enable the *Connected at power on* option.

For vSwitch and Network Adaptor configuration settings on the VM required for the Management, Monitor, and Response interfaces, click:

- <https://www.forescout.com/company/resources/counteract-7-0-quick-install-guide/>
- and
- <http://manualzz.com/doc/7208632/forescout-counteract-forescout-counteract>

For this use case, standard deployment mode was used with separate *Management*, *Monitor*, and *Response* interfaces. To gain greater network visibility, the EX4300 switch was configured to mirror traffic from ports where the Windows and Linux hosts were connected, to a destination port that was connected to the Monitor interface of the ForeScout CounterACT virtual appliance. This is also required for IP Address/MAC-ID binding in non-802.1X access switch deployments when no Layer 3 gateway (switch) exists to collect IP information.

Only the Management interface is used for Auto Threat Remediation actions.

4. Edit your VM settings based on your performance requirements.

For more details, click <https://www.forescout.com/products/specifications/>.

Install and Configure CounterACT Software

To install and configure ForeScout CounterACT software:

1. Power on the VM and follow the instructions on the console:
 - a. Select *Install CounterACT* to begin the installation. Once the installation completes, the VM reboots.
 - b. From the console, select *Configure CounterACT* to configure the network and system settings.
 - c. Select *CounterACT Appliance* as the installation type.
2. Ensure that the CounterACT Management interface can connect to the Internet to access your switches.
3. Use a browser and enter <https://pact.ly/S1Int3> to access and install Juniper CounterACT product trial software. Enter your credentials to confirm and install the product trial software.

Figure 14: Juniper CounterACT Trial Software Page



Download and install either Windows or Linux for your operating system.

4. From the *Start* menu, select *ForeScout CounterACT > CounterACT Console*. The CounterACT Login page appears:

Figure 15: CounterACT Login Page

The image shows a Windows-style application window titled "CounterACT Login". The window has a blue header bar with the "CounterACT" logo on the left and the "ForeScout" logo on the right. The main area is light blue. It contains several input fields: "IP/Name:" with the text "CA_MGT_IP", "Login Method:" with a dropdown menu showing "Password", "User Name:" with the text "admin", and "Password:" with a masked field of dots. Below these is a checkbox labeled "Save address and user name" which is checked. At the bottom right are two buttons: "Login" and "Cancel".

CounterACT Login

CounterACT

ForeScout

IP/Name: CA_MGT_IP

Login Method: Password

User Name: admin

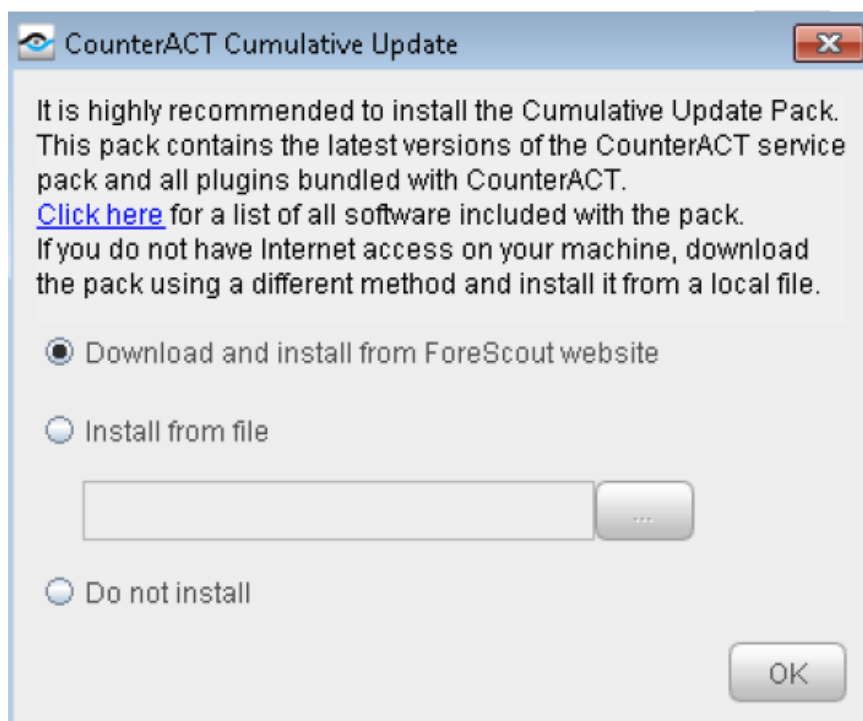
Password:

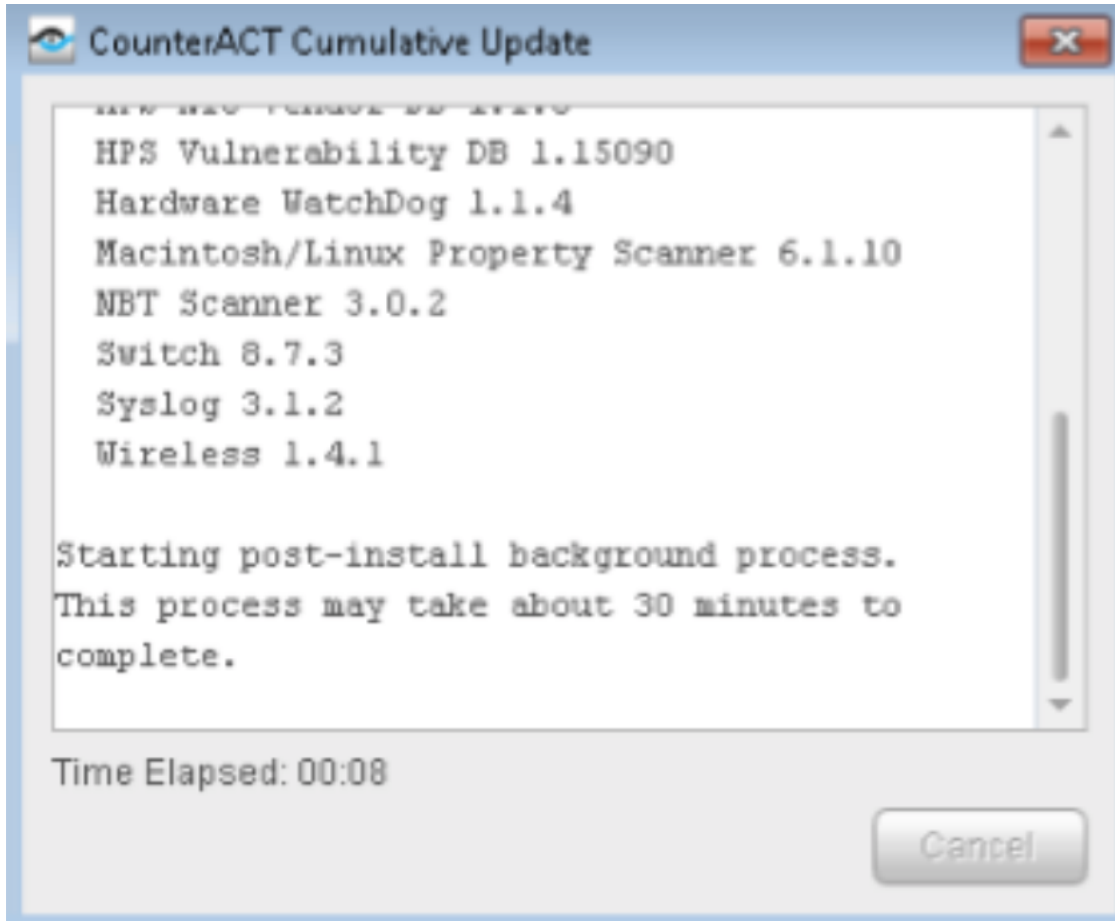
☒ Save address and user name

Login Cancel

- a. In the *IP/Name* field, enter the CounterACT device IP name.
 - b. From the *Login Method* list, select *Password* to perform a standard user authentication.
 - c. In the *User Name* and *Password* fields, enter your ForeScout username and password.
 - d. Click *Login*.
5. Download and install the CounterACT cumulative update.

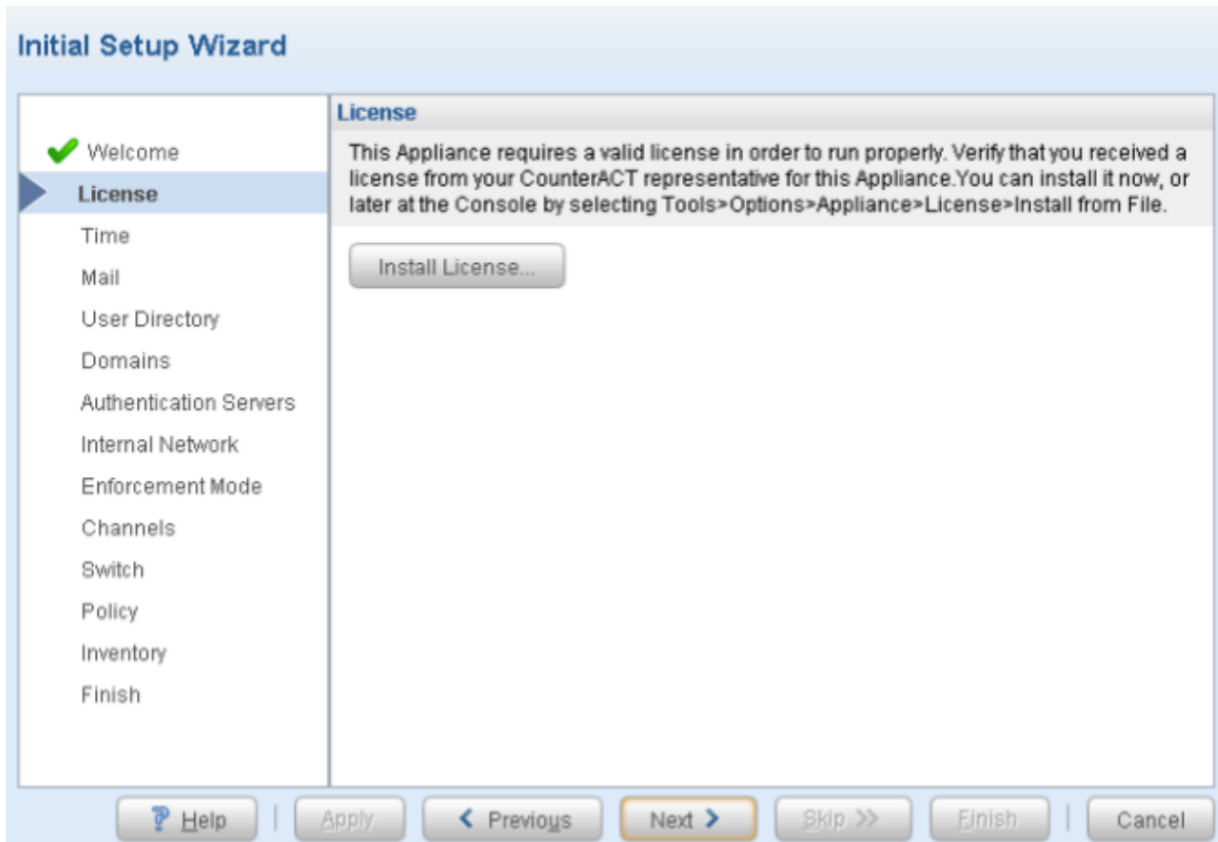
Figure 16: CounterACT Cumulative Update





6. Log in to the console again and follow the initial setup wizard. The *Welcome* page displays the CounterACT component to which you logged in, and information you previously defined during the data center installation.
7. From the *License* page, click *Install License* to install the CounterACT virtual system license.
Click *Next*.

Figure 17: License Installation Page



8. From the *Time* page, define the time settings for your appliance.

Figure 18: Time Settings Page

Initial Setup Wizard

✓ Welcome
✓ License
Time
Mail
User Directory
Domains
Authentication Servers
Internal Network
Enforcement Mode
Channels
Switch
Policy
Inventory
Finish

Time
Use this option to set the CounterACT Appliance time zone. Set a time zone according to geographic location or by GMT offset.

Local time Fri Mar 2 13:50:19 2018
GMT time Fri Mar 2 18:50:19 2018
Time Zone America/New_York
NTP Server ntp.forescout.net Test

Help | Apply | < Previous | Next > | Skip >> | Finish | Cancel

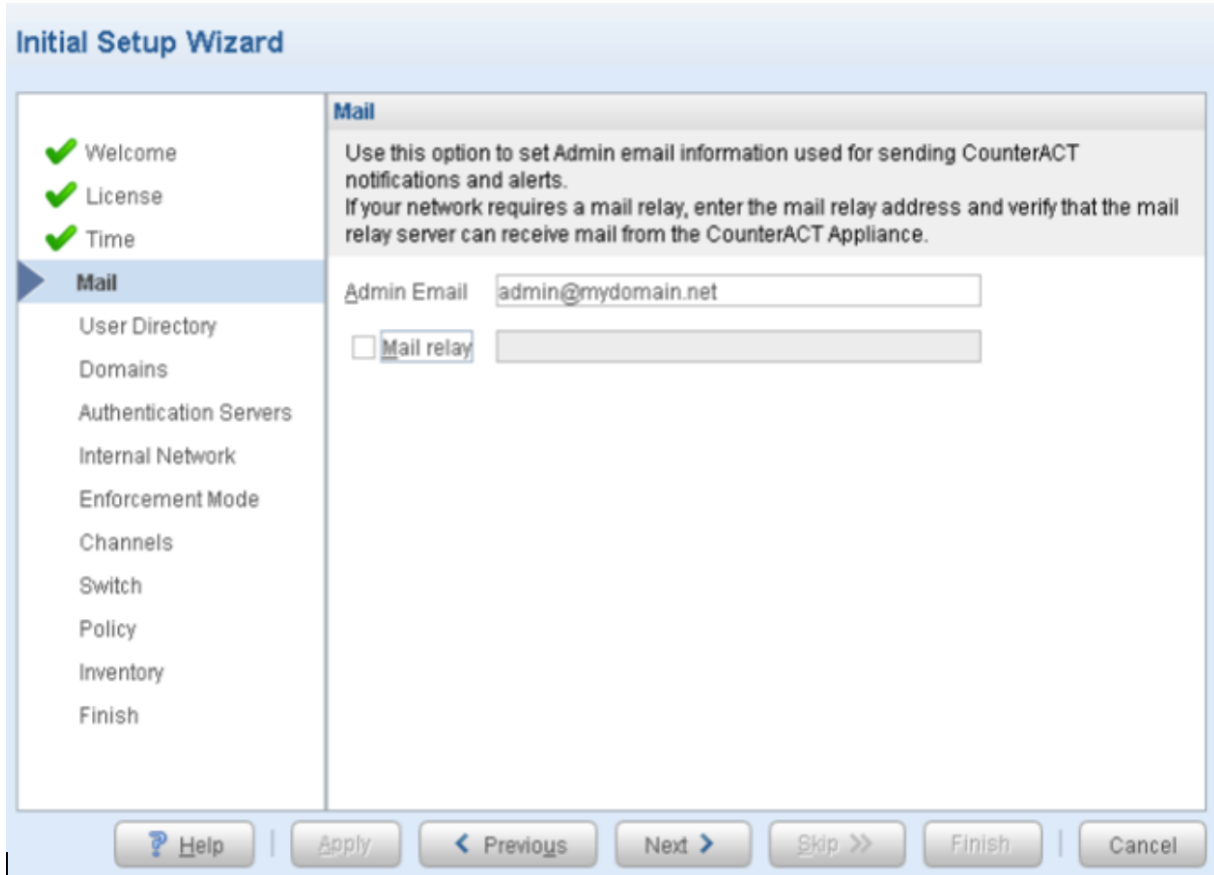
CounterACT devices require NTP connectivity (port 123 UDP) to an NTP server. Enter an NTP server for your organization's connection, or use the default ForeScout NTP server (ntp.foreScout.net). Click Test to verify that NTP Server returns a successful connection.

Click *Next*.

- CounterACT generates e-mail messages regarding policy and threat protection alert, scheduled reports, critical system operation alerts, and license alerts from the *Mail* page.

NOTE: For this use case, do not use the Email Notifications and Alerts option. However, you cannot skip this step, and must enter a dummy e-mail address. Click *Next*.

Figure 19: Mail Settings Page



The image shows the 'Initial Setup Wizard' window, specifically the 'Mail' configuration page. On the left is a sidebar with a list of steps: Welcome, License, Time, Mail (highlighted with a blue arrow), User Directory, Domains, Authentication Servers, Internal Network, Enforcement Mode, Channels, Switch, Policy, Inventory, and Finish. The main content area is titled 'Mail' and contains the following text: 'Use this option to set Admin email information used for sending CounterACT notifications and alerts. If your network requires a mail relay, enter the mail relay address and verify that the mail relay server can receive mail from the CounterACT Appliance.' Below this text, there is a text input field for 'Admin Email' containing 'admin@mydomain.net'. Below that is a checkbox labeled 'Mail relay' which is currently unchecked, followed by an empty text input field. At the bottom of the window is a row of buttons: 'Help' (with a question mark icon), 'Apply', '< Previous', 'Next >', 'Skip >>', 'Finish', and 'Cancel'.

10. To continue the Initial Setup Wizard, skip setting up the User Directory, Domains, and Authentication Servers plug-ins for now. You will define them later in the procedure. Click *Skip >>* from the wizard until the *Internal Network* page appears.
11. From the *Internal Network* page, add the IP address range (10.10.10.0 to 10.10.30.255) for the internal network that you want CounterACT to manage. Click *Next*.

Figure 20: Internal Network Settings

Initial Setup Wizard

- ✓ Welcome
- ✓ License
- ✓ Time
- ✓ Mail
- ✓ User Directory
- ✓ Domains
- ✓ Authentication Servers
- Internal Network**
- Enforcement Mode
- Channels
- Switch
- Policy
- Inventory
- Finish

Internal Network

The Internal Network is the range of IP addresses in your organization that you want CounterACT to manage. It is recommended that you include your entire organizational network in this definition, including unused IP ranges. IPs outside this range will not be handled by the Appliance. Hosts in the Internal Network must be visible to CounterACT Appliances.

Assign a segment name to the Internal Network for easy identification.

Segment name

Ranges

From	To
10.10.30.0	10.10.30.255

1 items (1 selected)

| | | | | |

12. From the *Enforcement Mode* page, enable *NAT Detection*, and accept the other default enforcement mode settings and click *Next*.

Figure 21: Enforcement Mode Settings

The screenshot shows the 'Initial Setup Wizard' window. On the left is a sidebar with a list of steps: Welcome, License, Time, Mail, User Directory, Domains, Authentication Servers, Internal Network, **Enforcement Mode** (highlighted), Channels, Switch, Policy, Inventory, and Finish. The main area is titled 'Enforcement Mode' and contains the following text: 'Use this option to define Appliance enforcement mode. The Full Enforcement mode allows complete functionality. The Partial Enforcement mode lets you monitor network traffic but limits your ability to respond to it. The Partial enforcement mode is recommended for evaluation purposes only.'

There are two radio button options:

- ☒ Full Enforcement
- ☐ Partial Enforcement (with a green key icon next to it)

Below the radio buttons, under the heading 'The following are disabled', there are three disabled options:

- Threat Protection
- HTTP Actions
- Virtual Firewall

At the bottom of the main area, there is a checked checkbox for 'Auto Discovery'.

The bottom of the window features a navigation bar with buttons: Help, Apply, Previous, Next (highlighted), Skip >>, Finish, and Cancel.

13. From the *Channels* page:

- Define a new channel by selecting *Add* from the *Channels* list. This channel is used to match the appliance interface connections that detect and respond to traffic on the network interfaces.
- From the *Monitor* list, select *eth1* as an interface.
- From the *Response* list, select *eth2* as an interface.
- Assign both interfaces at the Data Center.
- Enable the *All VLANs* option and verify that the *Monitor* interface receives the mirrored traffic from the configured EX4300 switch.

Figure 22: Channels Settings

Initial Setup Wizard

- ✓ Welcome
- ✓ Time
- ✓ Mail
- ✓ User Directory
- ✓ Domains
- ✓ Authentication Servers
- ✓ Internal Network
- ✓ Enforcement Mode
- Channels**
- Switch
- Policy
- Inventory
- Finish

Channels

A channel is a pair of monitor and response interfaces used by the CounterACT Appliance to interact with the network.
A **monitor interface** examines traffic going through the network and a **response interface** generates traffic back to the network.
Make sure the physical connections made at the Data Center match the logical channel setting below and that your network traffic is seen.
VLAN discovery after channel configuration might take a few moments.

Channel ▼ VLAN ▼ Traffic... ☒ Use DHCP by Default

Channels List

✓	Monit	Traffi	Mirro	Symr	# Hc	Respt	Traffi	Res	IP Addre
✓	eth1 -> eth2	1 K...	0 %	✓	0	→	eth1	N/A	✓ None (...)

1 items (0 selected)

|
 |
 |
 |
 |
 |

14. To continue the Initial Setup Wizard, skip setting up the Switch plug-in for now. You will define them later in the procedure. Click *Skip >>* from the wizard until the *Policy* page appears.

15. From the *Policy* page, accept the default setting for *Classify hosts* (enabled) for Asset Classification. Click *Next*.

Figure 23: Policy Settings

Initial Setup Wizard

- ✓ Welcome
- ✓ Time
- ✓ Mail
- ✓ User Directory
- ✓ Domains
- ✓ Authentication Servers
- ✓ Internal Network
- ✓ Enforcement Mode
- ✓ Channels
- ✓ Switch
- Policy**
- Inventory
- Finish

Policy

Use the Asset Classification Template to organize your network hosts into easily manageable groups, for example Windows, Printers, Linux, Macintosh. With automatic ongoing asset classification, you quickly get a picture of your network devices, and can easily filter detection results by groups, as well as optimize policy implementation by filtering to specific groups.

Use the Guest Template to automatically detect and classify hosts into Guest and Corporate groups and quickly gain an understanding of compliance levels at your network.

Note: It is recommended to use both templates.

Asset Classification

☒ Classify hosts

☒ Classify hosts in all Internal Network

☐ Classify hosts in range:

Guest Detection

☐ Detect guests

☒ Detect guest hosts in all Internal Network

☐ Detect guest hosts in range:

Help

Apply

Previous

Next

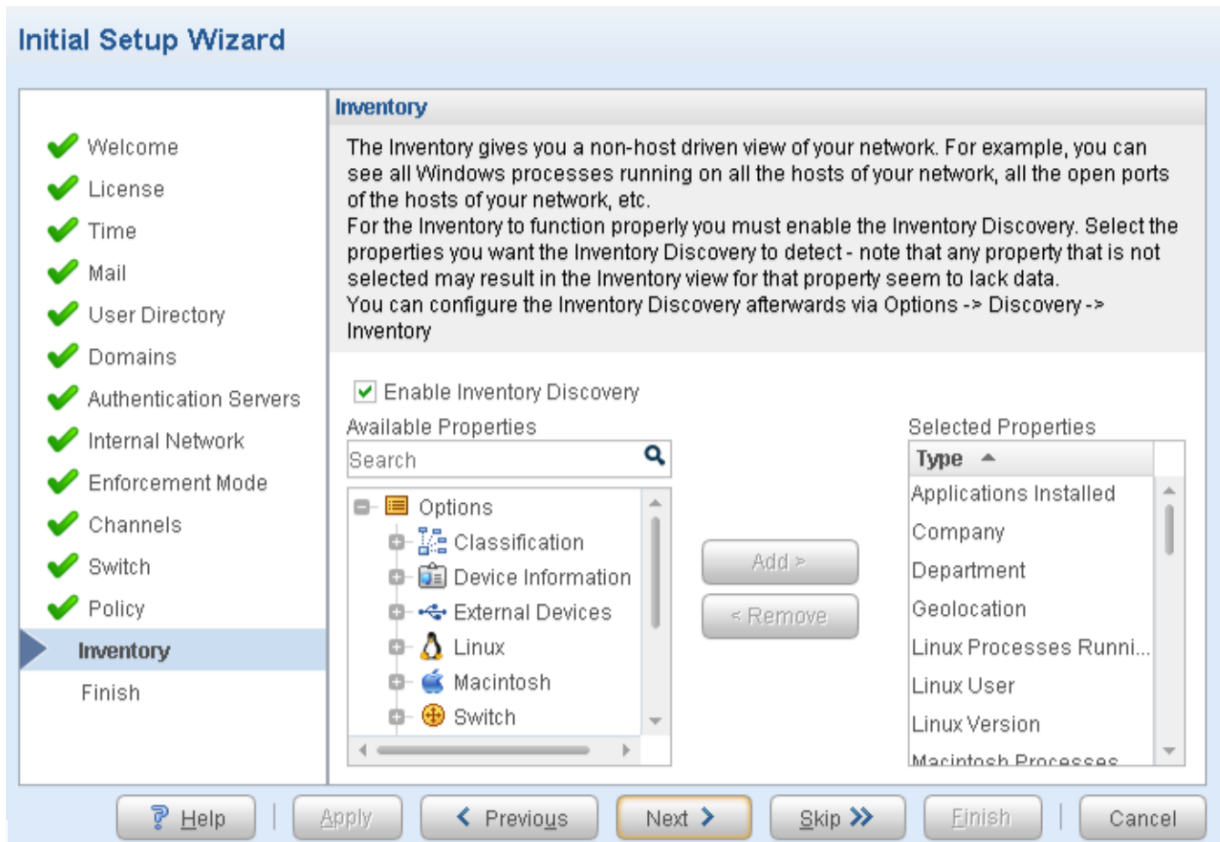
Skip >>

Finish

Cancel

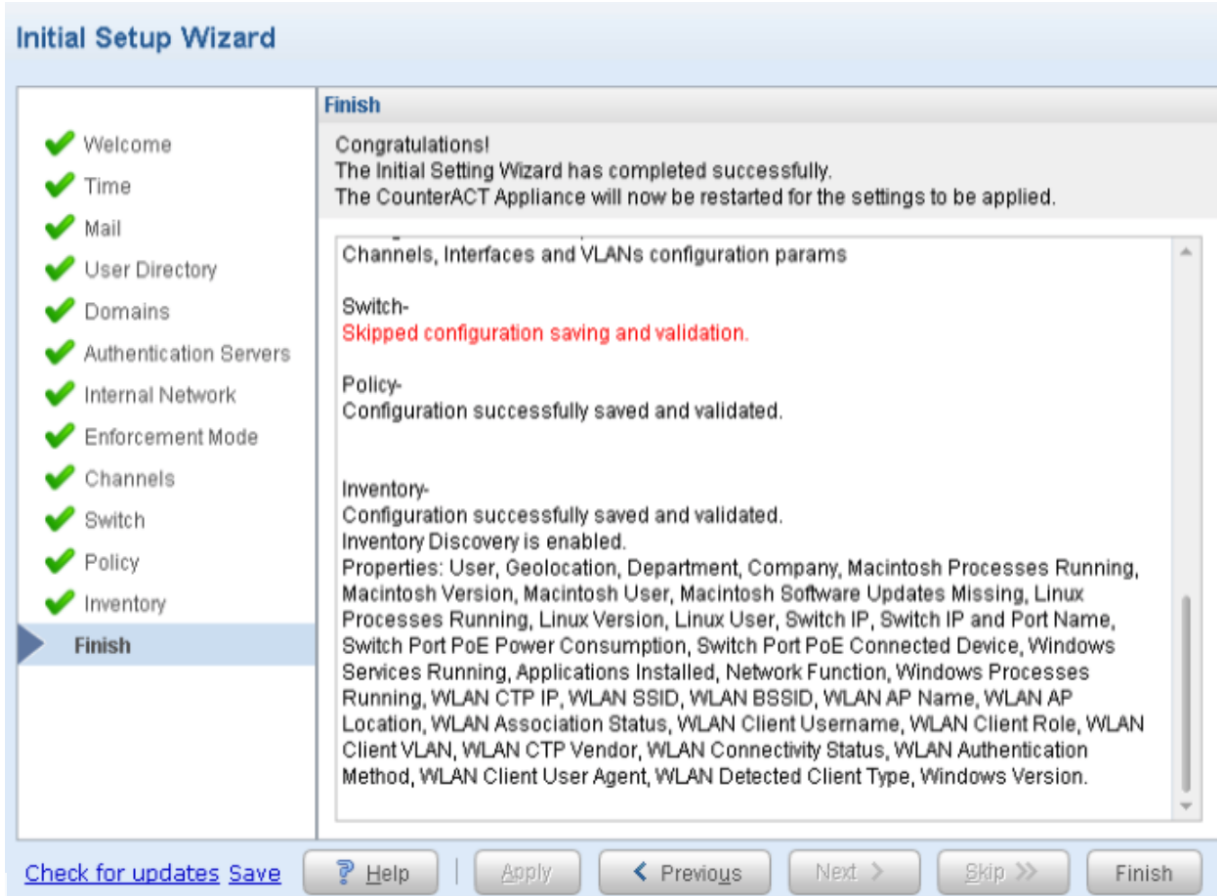
16. From the *Inventory* page, accept the default setting for *Enable Inventory Discovery* (enabled). Click *Next*.

Figure 24: Inventory Settings



17. From the *Finish* page, review the wizard configuration summary. Click *Finish* to complete the initial setup. Click *Save* to save the configuration file to the external file.

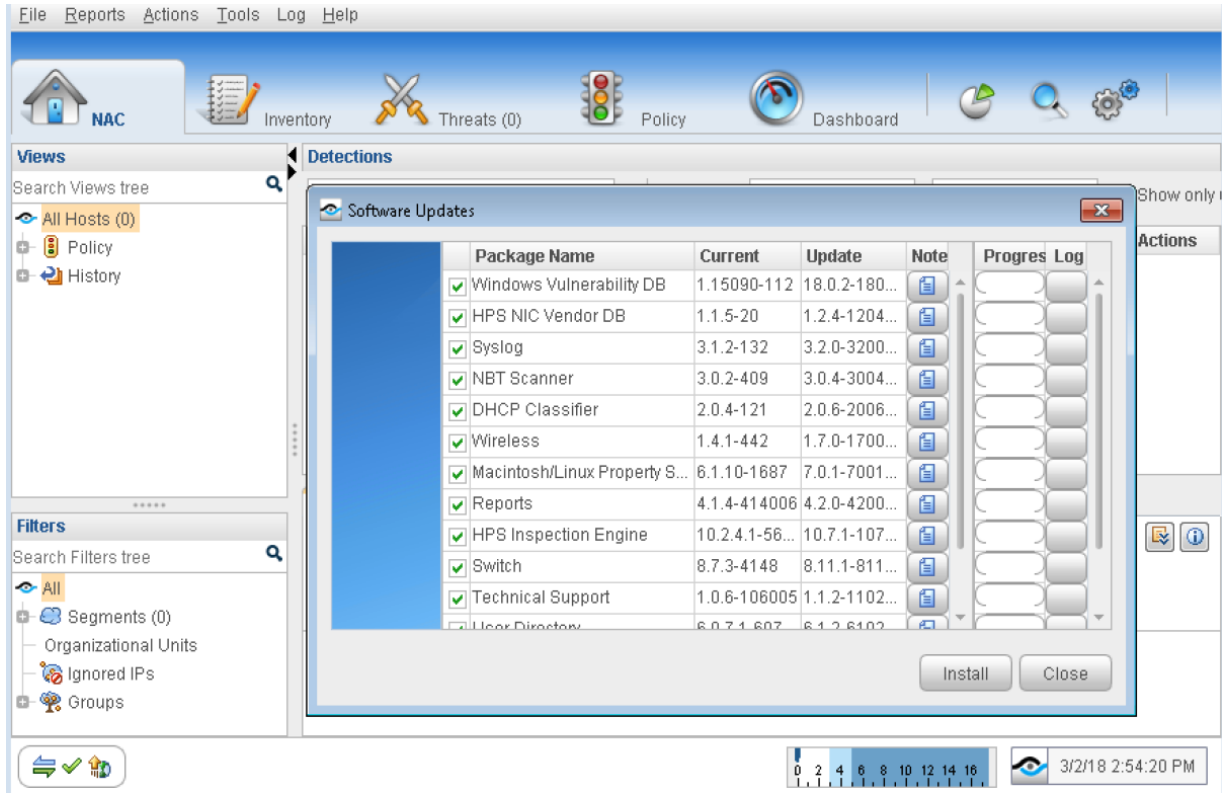
Figure 25: Finish Initial Setup Page



NOTE: (Optional) To disable the map functionality, select *Tools > Options > Map*.

18. To download and install the updated packages, click *Check for updates* (or select *Tools > Check for Updates*).

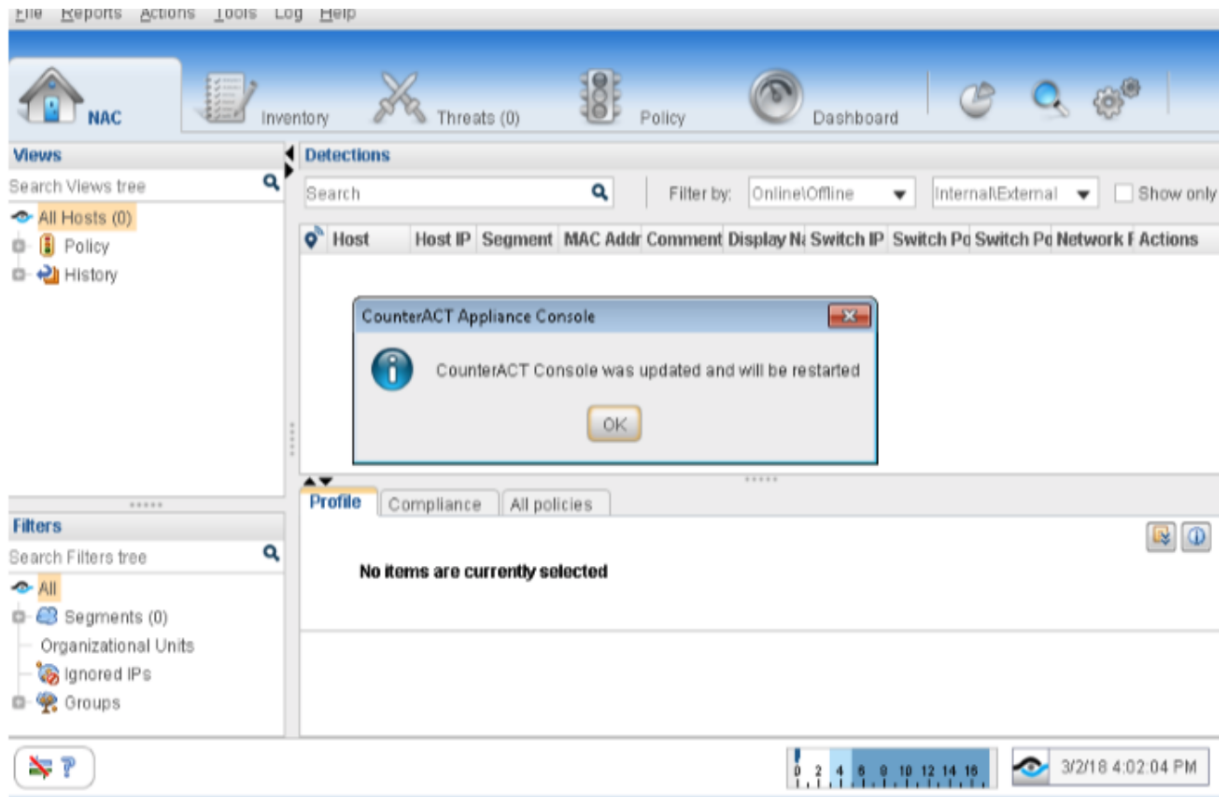
Figure 26: Check for Updates Screen



19. From the *Software Updates* page:

- a. Install the Infrastructure Update Pack.
- b. Install the second Service Pack. After the service package installation is complete, CounterACT will automatically restart. Click OK to restart the console.

Figure 27: Service Package Installation Complete Screen



- c. Log in with your credentials.
- d. Click *Check for updates* (or select *Tools > Check for Updates*) and install the other remaining software update packages.

NOTE: For this use case, de-select both HPS Inspection Engine and Macintosh/Linux Property Scanner packages. These are not required for this use case example.

Install and Configure CounterACT Plugins

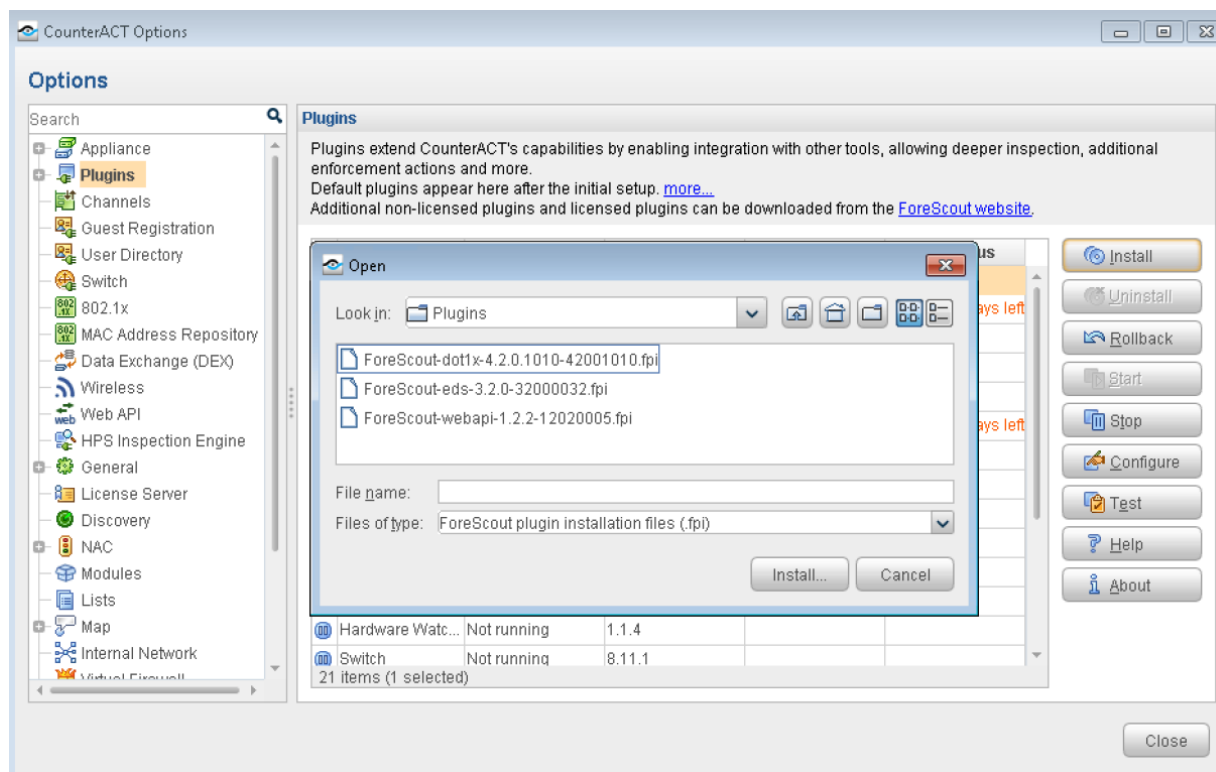
CounterACT is delivered with several bundled plugins:

- ForeScout-dot1x-4.2.0.1010-42001010.fpi
- ForeScout-eds-3.2.0-32000032.fpi
- ForeScout-webapi-1.2.2-12020005.fpi

These plugins link CounterACT to the network infrastructure (switches, domain servers, and user directories), and provide core endpoint detection and management functionality, including a comprehensive set of host properties and actions.

1. Log in to the CounterACT console and select *Tools > Options > Plugins* to install the packages.

Figure 28: CounterACT Plugins Screen



2. Select each plugin and click *Install*. After the installation completes, click *Close*.
3. Select *Tools > Options > Plugins* to verify that the following services are running:
 - User Directory
 - Switch
 - 802.1X
 - Data Exchange (DEX)
 - WebAPI

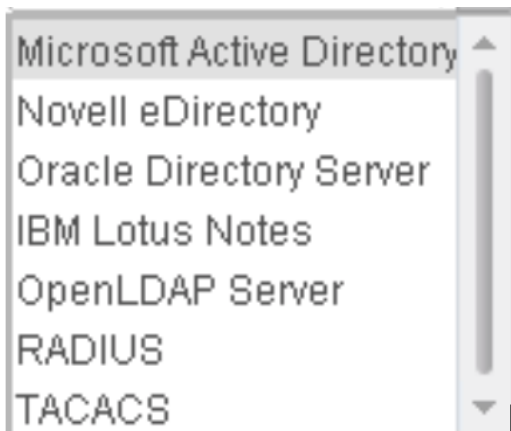
Configure User Directory Plugin

The User Directory Plugin resolves endpoint user details and performs endpoint authentication through authentication and directory servers.

To configure the User Directory servers:

1. Select *Tools > Options > User Directory*. From the User Directory page, click *Add*.
2. From the *Edit Server* page, on the *General* pane, define basic server parameters and functionality:
 - a. Enter the hostname of the server in the *Name* field.
 - b. From the *Type* list, select the server type. The server type can be any one of the following:

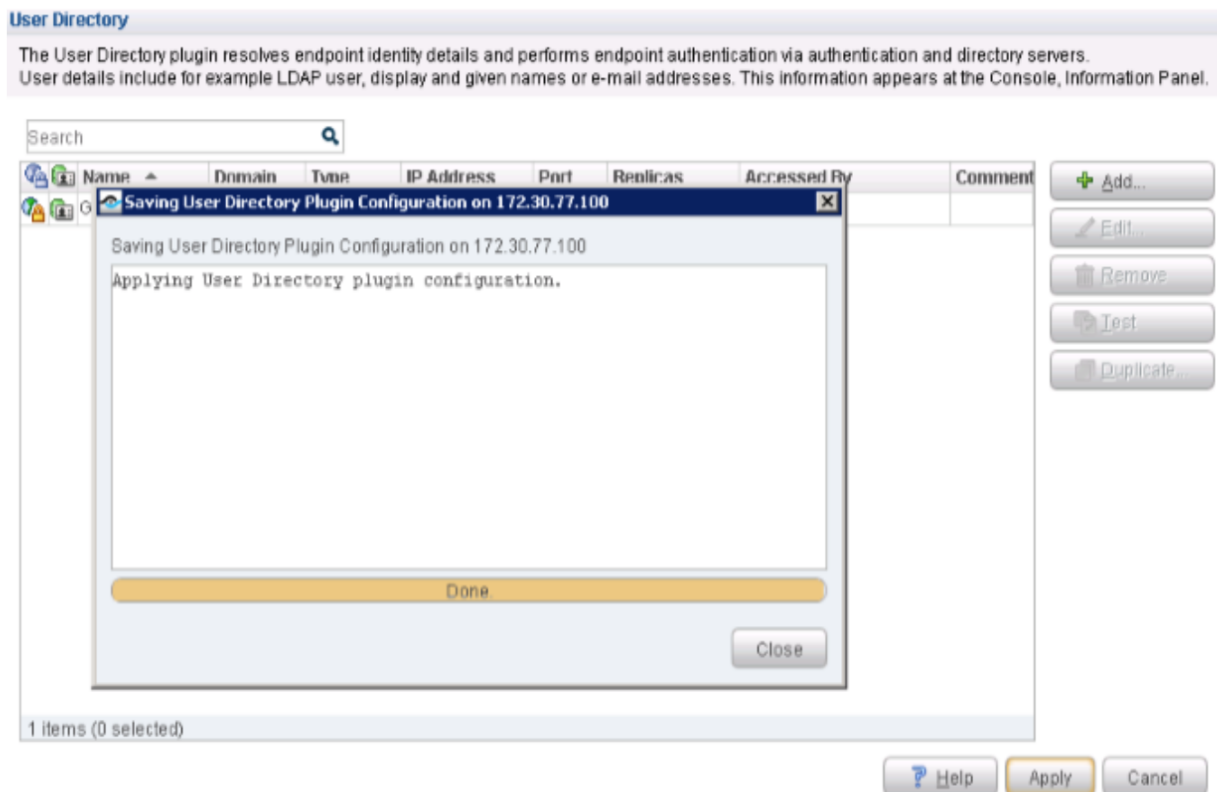
Figure 29: Server Type Options



- c. Enable these configuration parameters for the server: *Use as directory*, *Use for authentication*, and *Use for Console Login*.
 - d. Enter a comment about the server configuration in the *Comment* field.
 - e. Click the *Settings* tab.
3. From the *Settings* pane, define Microsoft Active Directory server parameters:
 - a. In the Communication section, enter the IP address of the server in the *Address* field.
 - b. Enter the port number in the *Port* field.
 - c. Enable *All* for the *Accessed By* field. This ensures that all of the CounterACT devices can communicate and have access to the configured server.
 - d. In the Directory section, enter the domain name in the *Domain* field.
 - e. Enter the credentials to authenticate the directory for querying other user details in the *Administrator* field.
 - f. Enter and verify the Administrator's password in the *Password* fields.

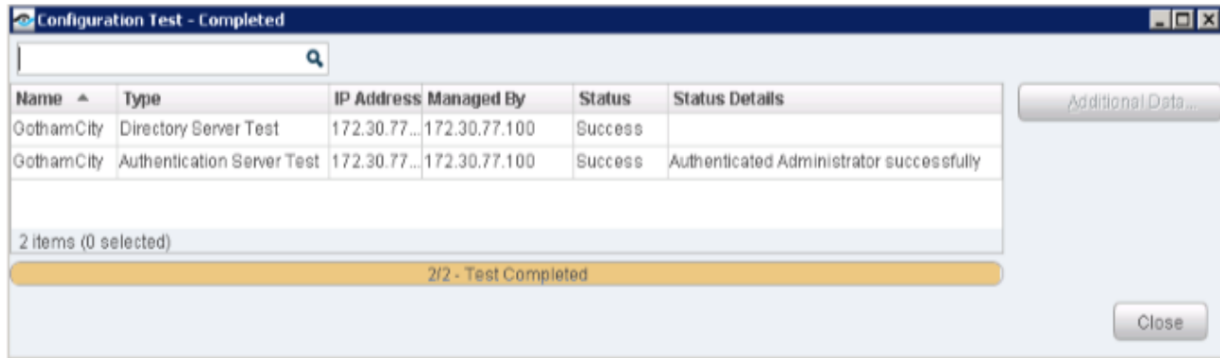
- g. Select *None* for the *Additional Domain Aliases* field. The system looks up a user in this directory only if its domain name matches the configured directory domain.
 - h. Click the *Test* tab.
4. From the *Test* pane, define parameters for testing the connection between the server and the User Directory Plugin.
- a. In the *Directory* section, enter the user name to query in the *User* field.
 - b. In the *Authentication* section, enter *Administrator* in the *User* field and enter and verify the administrator's password in the *Password* fields.
 - c. Click *OK*, then click *Apply* to save and apply the configuration settings.

Figure 30: User Directory Plugin Parameters



- 5. Click *Test* to test your configuration.

Figure 31: Configuration Test Screen



Configure Switch Plugin

The Switch Plugin queries each switch for:

- Switch port attributes and information about connected endpoints.
- ARP table to discover new endpoints connected to the switch.

The information can be obtained via CLI and/or SNMP.

To configure the Switch Plugin for the EX4300 switch:

1. Select *Tools > Options > Switch*. From the Switch page, click *Add*.
2. From the *Edit Switch* page, on the *General* pane, define basic switch parameters and functionality.
 - a. Enter the IP address or FQDN of the switch in the *Address* field. The Console uses the value you enter to identify the switch entry.
 - b. From the *Connecting Appliance* list, specify the CounterACT device that will manage this switch.
 - c. From the *Vendor* list, specify the vendor of the network device you want the plugin to manage. Since each Vendor CLI and SNMP are different, it is important to pick the right vendor. CounterACT will associate the right format for the switch then.
 - d. Enter a comment about the switch configuration in the *Comment* field.
 - e. Click the *CLI* tab.
3. From the *CLI* pane, configure the use of CLI for communication from the Switch Plugin to the switch.

- a. Enable the *Use CLI* option to activate CLI access.

NOTE: *SSH* is the permanently selected connection type for Juniper Networks switches.

- b. Enter a user name and password in the *User* and *Password* fields. The Switch Plugin uses these credentials to log in to the switch.

NOTE: For plugin management of Juniper's switches, the user that you configure must have superuser permission on Juniper's switches.

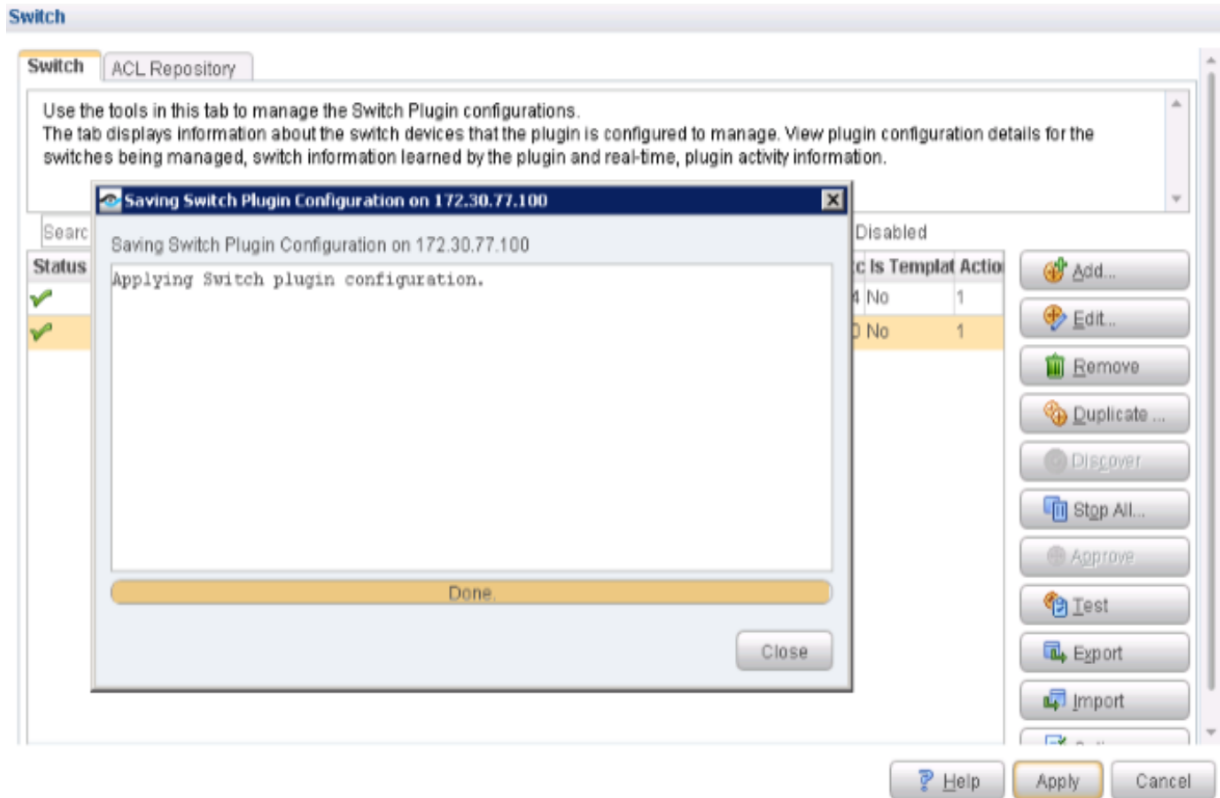
Do not use the root login for CLI access to EX Series switches.

- c. In the Privileged Access Parameters section, enable the *Enable privileged access* option to provide the plugin write privileges on the switch.
 - d. Select the *No password* option to indicate that the switch set up does not require a password.
 - e. Click the *Permissions* tab.
4. From the *Permissions* pane, define read, write, and advanced permission settings for the switch.
 - a. In the MAC Permissions section, enable the *Read: MACs connected to switch port and port properties (MAC address table)* option. Enabling MAC read permission allows CounterACT to read a switch's MAC address table and discover connected endpoints and their network interface.
 - b. Enable the *Write: Enable Actions (Switch block, Assign to VLAN, ACL)* option to enable the Switch Plugin permission to apply the Assign to VLAN action, the Switch Block action, and ACL actions on endpoints detected on the managed switch.

NOTE: ACL configuration is not required for this use case configuration.

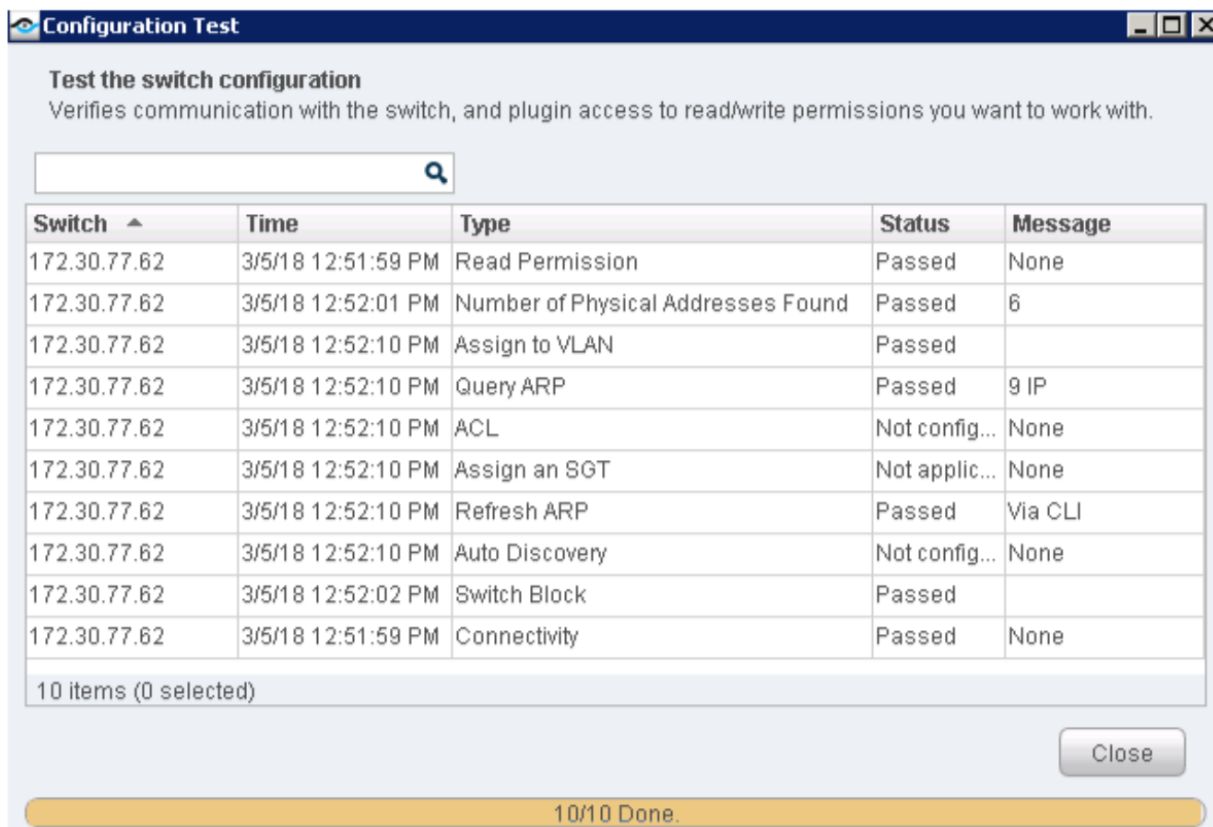
- c. Click the *802.1X* tab. (This pane shows up only if the 802.1X plugin is installed)
5. From the *802.1X* pane, configure RADIUS-based authentication and authorization for detected endpoints when attempting to connect to a Juniper Networks' network through an EX4300 Series switch.
 - a. In the *RADIUS Secret as configured in switches* fields, enter the necessary RADIUS secret to allow communication between the CounterACT RADIUS server and the managed switch.
 - b. Click *OK*, then click *Apply* to save and apply the configuration settings.

Figure 32: 802.1X RADIUS-based Authentication Secret Confirmation



6. Click *Test* to test your configuration.

Figure 33: Switch Configuration Test Screen



NOTE: To configure the QFX switch, repeat the same configuration steps as for the EX4300 switch. However, you must configure ACL functionality for the QFX switch because QFX is deployed as a standard access switch (without 802.1X), and auto-threat remediation is performed by applying ACLs.

From the User Directory page, enable and/or select the following fields from the ACL pane:

- Enable ACL
- Add ACL firewall filter to physical ports
- Add CounterACT authentication servers permit rules
- Use system-defined name (forescout_acl)

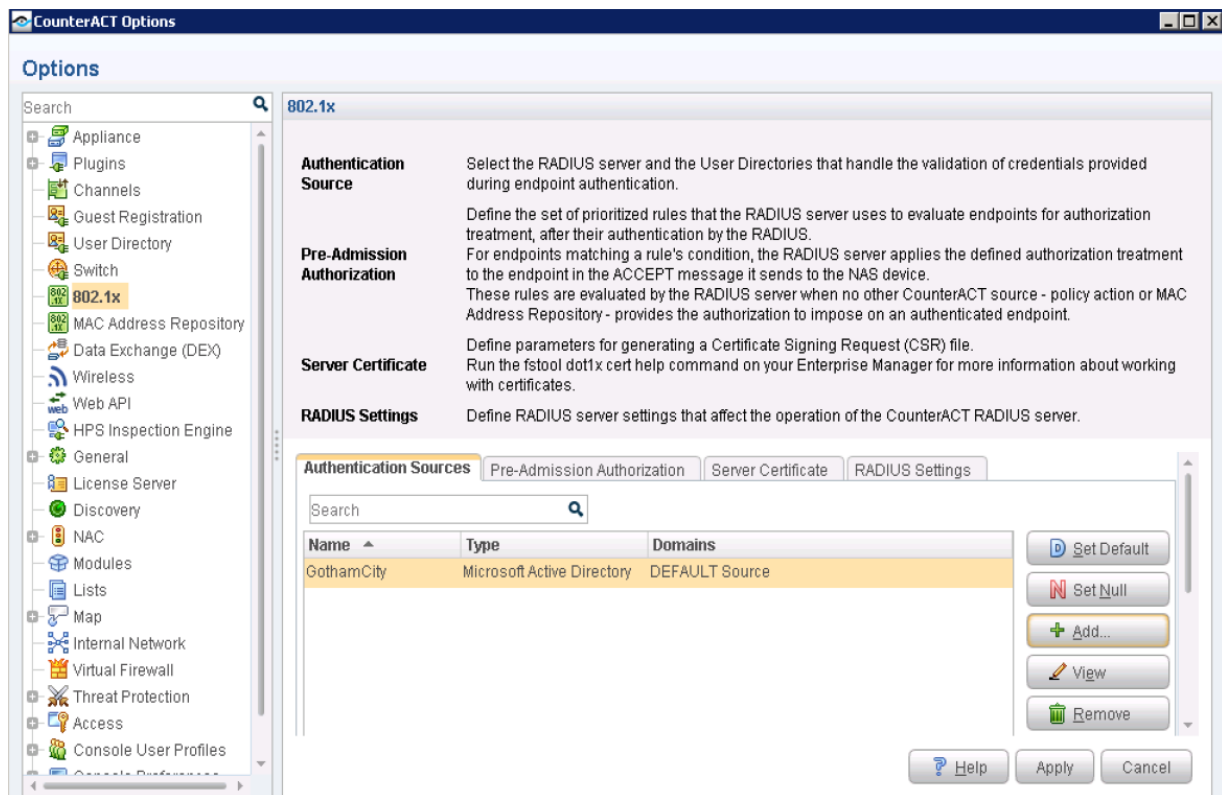
Configure 802.1X Plugin

The 802.1X Plugin enables CounterACT to authenticate 802.1X switch or wireless connections to the network. The plugin is compatible with the IEEE 802.1X specification and the RADIUS authentication protocol.

To configure the 802.1X Plugin:

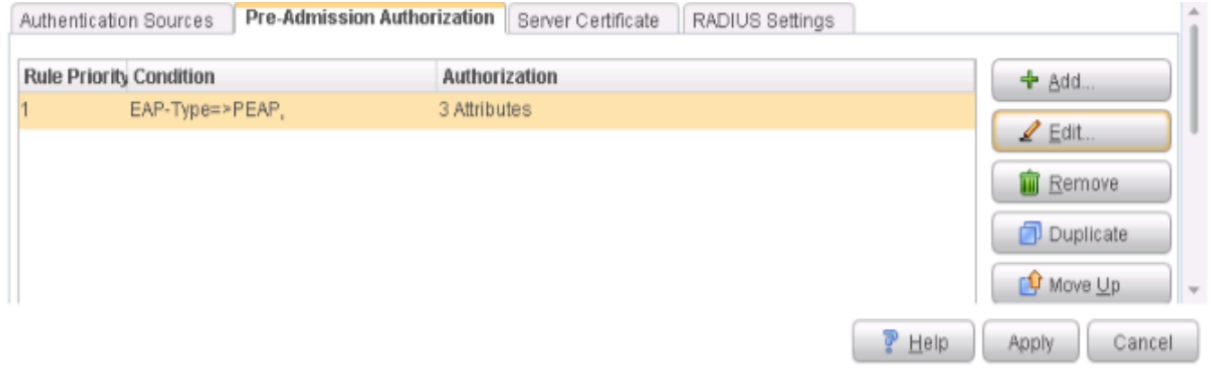
1. Select *Tools > Options > 802.1x*.

Figure 34: 802.1X Options



2. From the 802.1X page, on the *Authentication Sources* pane, select the user directory that validates the credentials provided during the endpoint authentication. You configure all of the authentication sources in the User Directory Plugin.
3. Click the *Pre-Admission Authorization* tab and define a set of prioritized rules. The CounterACT RADIUS server uses these rules to evaluate the endpoints for authorization after they have been authenticated by the applicable RADIUS server (an Authentication Source selection).

Figure 35: Pre-Admission Authorization Tab



- Click *Add* to add multiple conditions for the rule.

Figure 36: Pre-Admission Authorization Conditions



- Add your Authorization Attributes. Enter *VLAN* as the Tunnel-Type, and *31* as the Tunnel-Private-Group. Click *OK*.

Figure 37: Adding Authorization Attributes

Authorization

☐ Deny Access

VLAN

Attribute Name	Attribute Value
Tunnel-Medium-Type	IEEE-802
Tunnel-Type	VLAN
Tunnel-Private-Grou...	31

+ Add...

Edit...

Remove

3 items (0 selected)

OK Cancel

6. Click the *Server Certificate* tab. Enable the *Use self-signed certificate* option.

Figure 38: Server Certificate Options

Authentication Sources Pre-Admission Authorization **Server Certificate** RADIUS Settings

☒ Use self-signed certificate

☐ Use local server certificate

Private Key Password

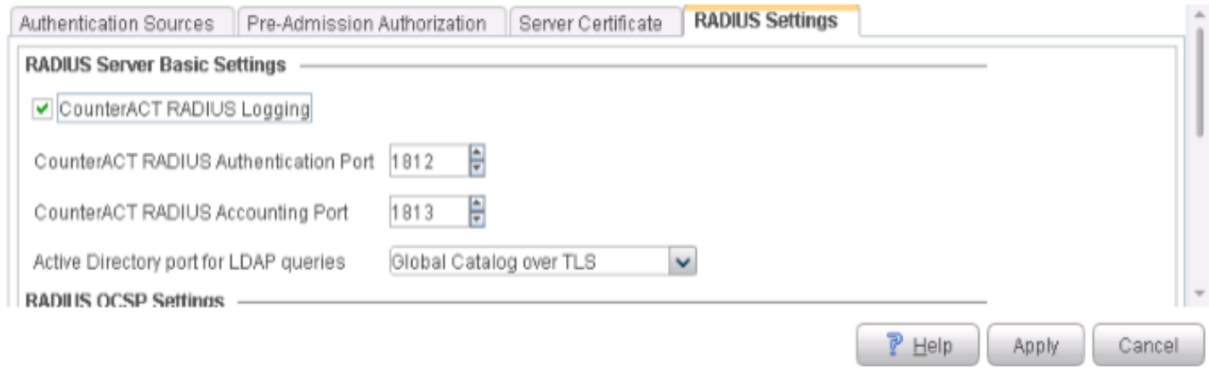
Retype Private Key Password

CA Host OS Windows-Based

Help Apply Cancel

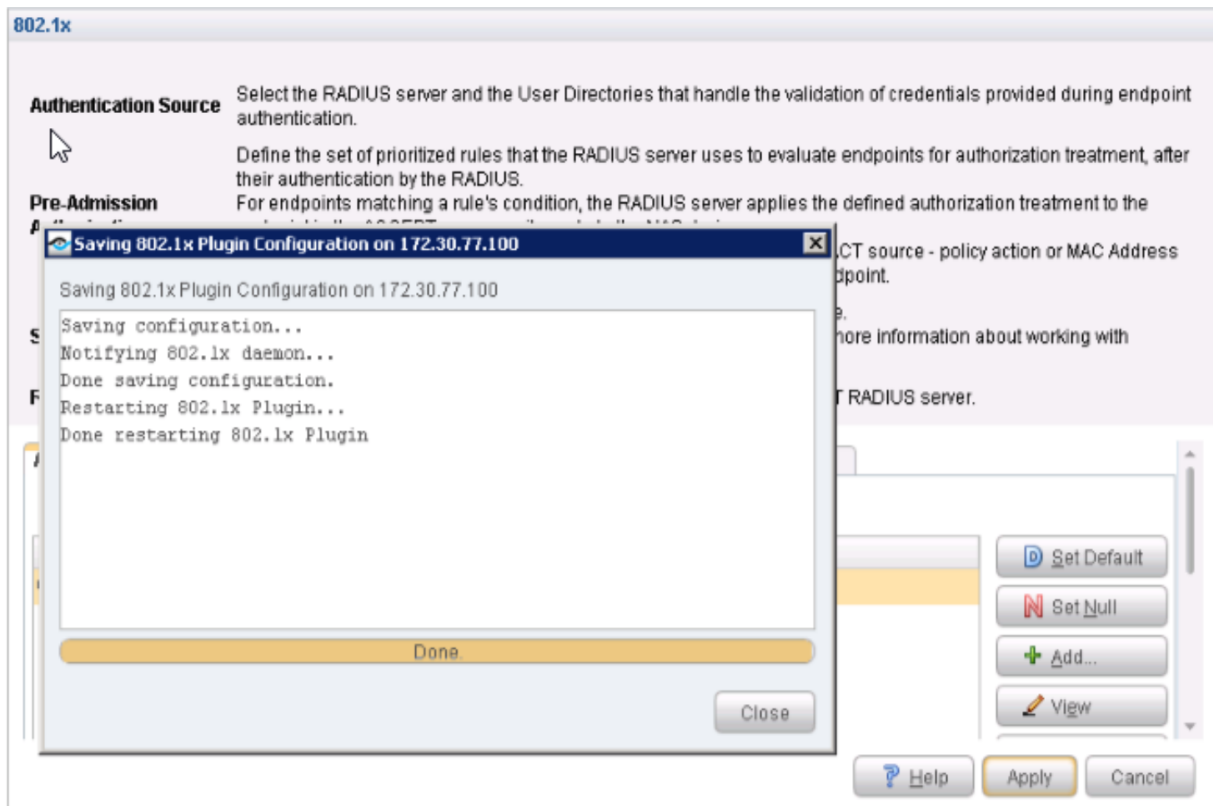
- Click the *RADIUS Settings* tab. Enable the *CounterACT RADIUS Logging* option, and accept all of the other default settings.

Figure 39: RADIUS Settings



- Click *Apply* to save and apply the configuration settings.

Figure 40: Applying 802.1X Configuration Settings



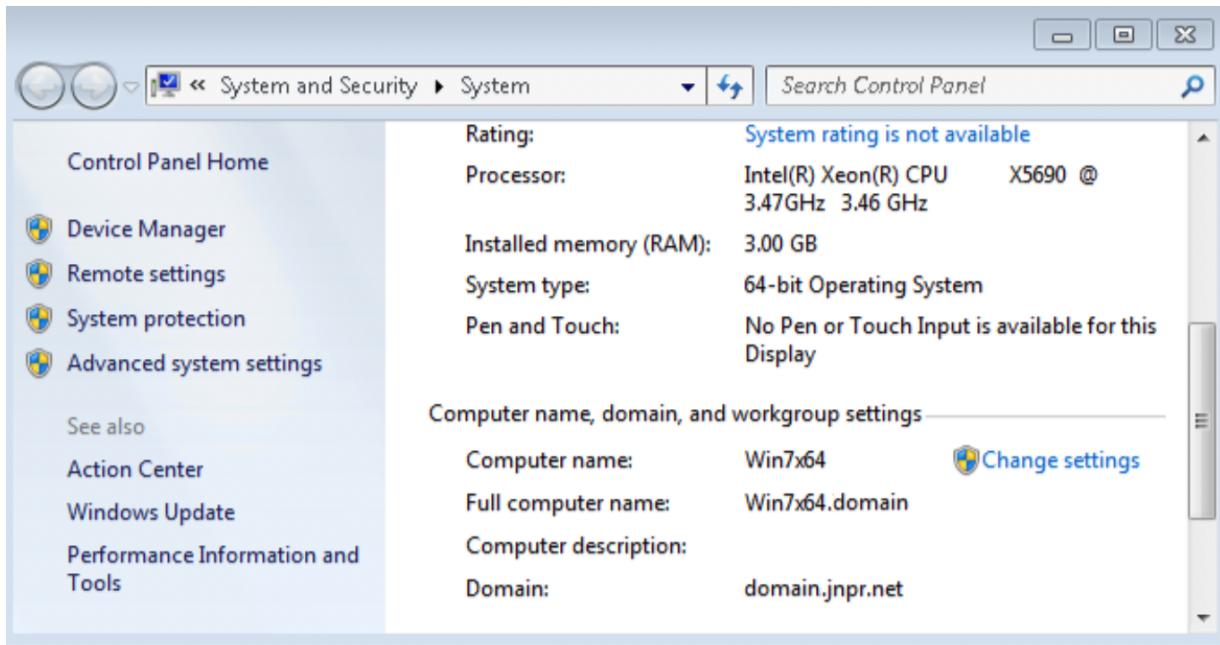
Configure Windows 7 Supplciant

You should have already installed the Microsoft Windows Server and Active Directory. Click [“Install and Configure Microsoft Windows Server and Active Directory”](#) on [page 38](#) to review the instructions.

To configure the Windows 7 Supplciant:

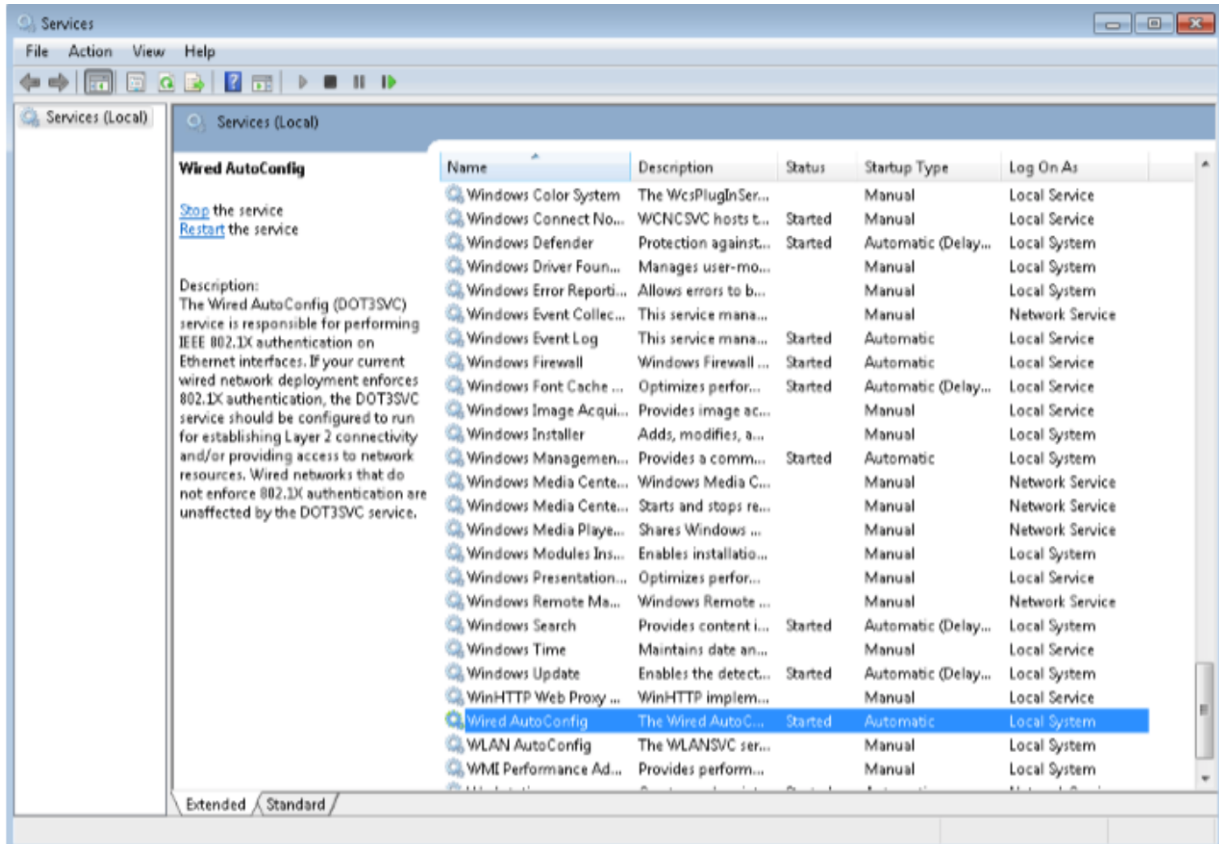
1. Ensure that the Windows 7 Supplciant is configured with the Active Directory domain that you previously created.

Figure 41: Windows Supplciant Configuration Verification



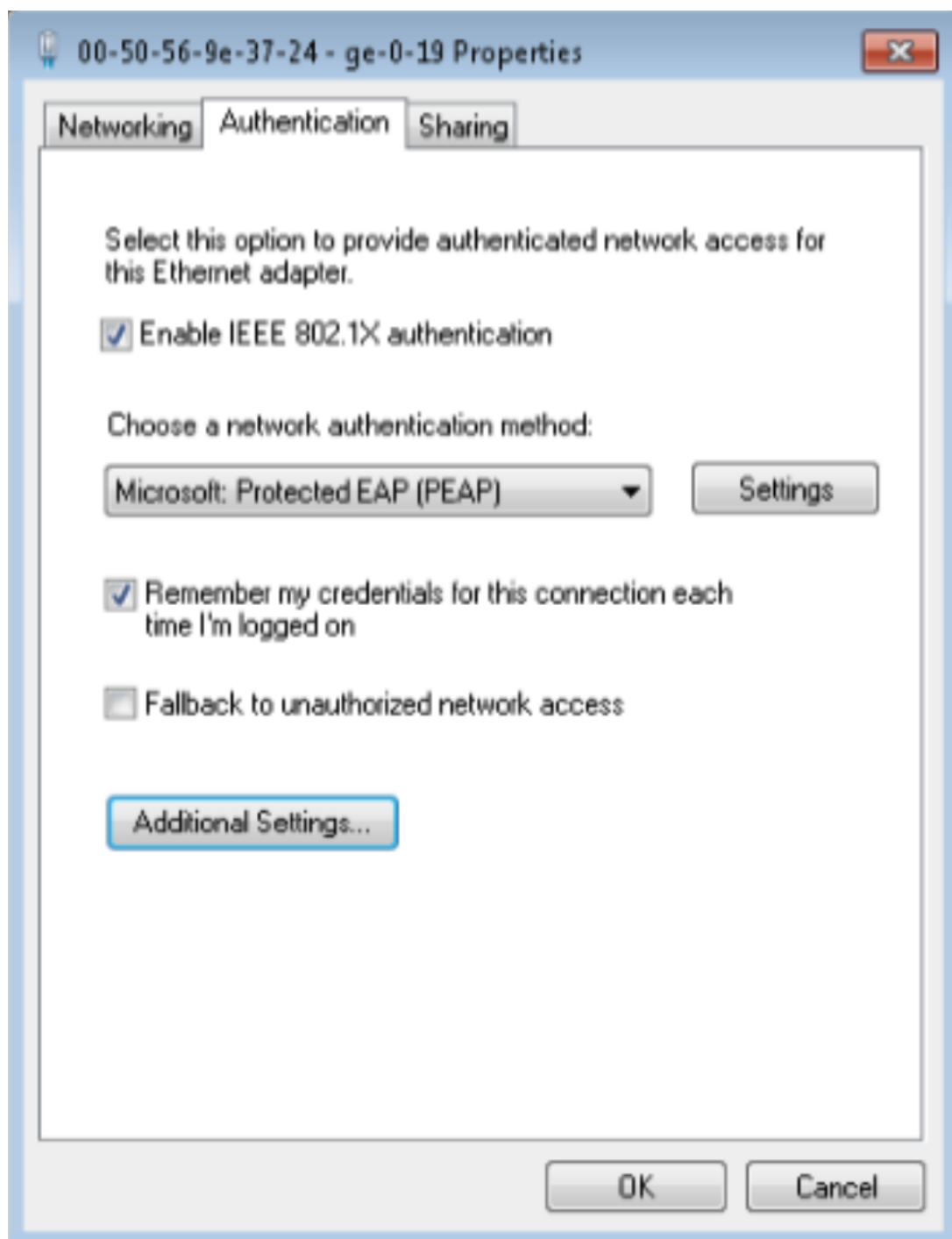
2. Ensure that the Wired AutoConfig service is running.

Figure 42: Wired AutoConfig Service Configuration Confirmation



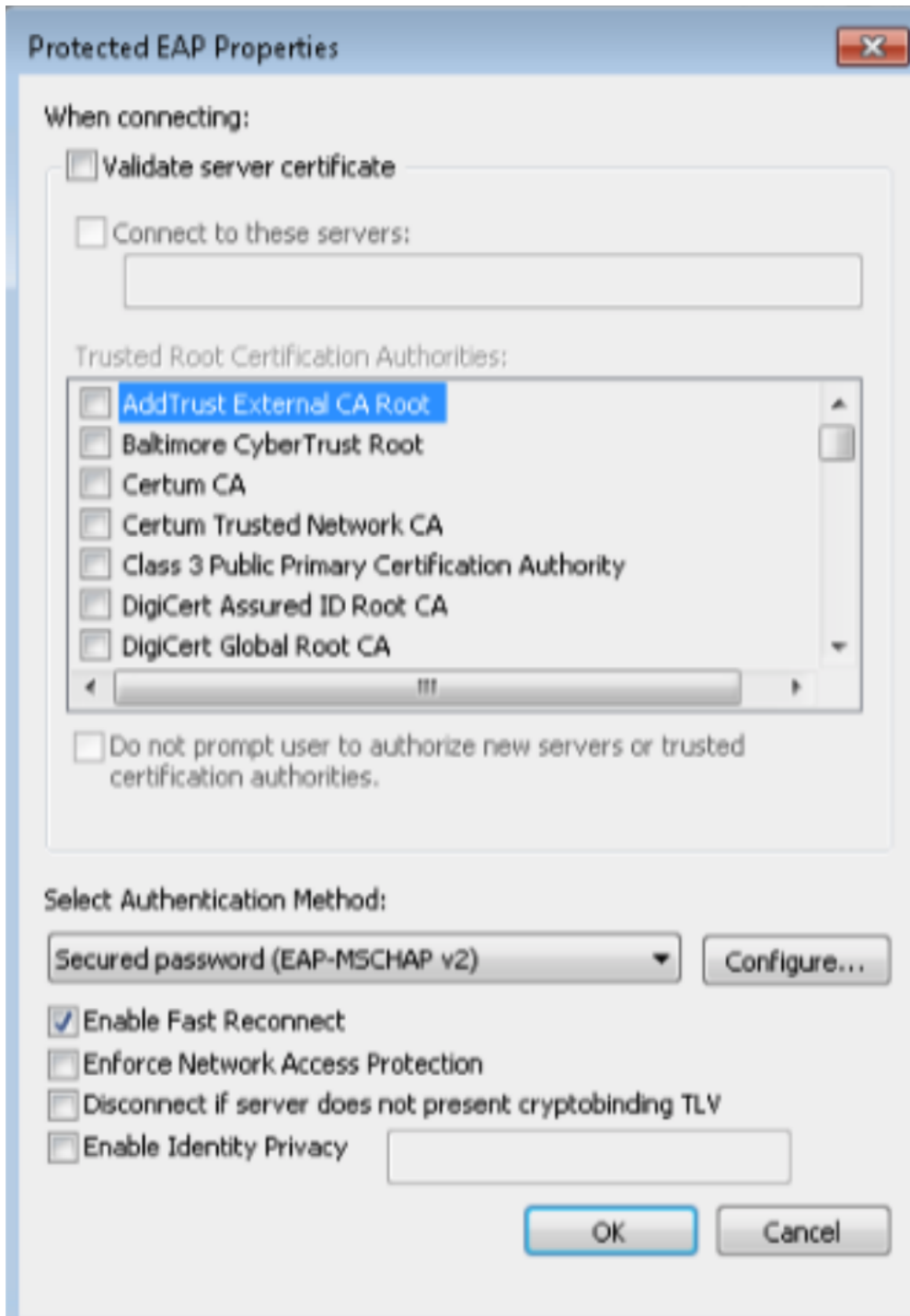
3. Enable 802.1X PEAP authentication for the Local Area Connection.

Figure 43: 802.1X PEAP Authentication Confirmation



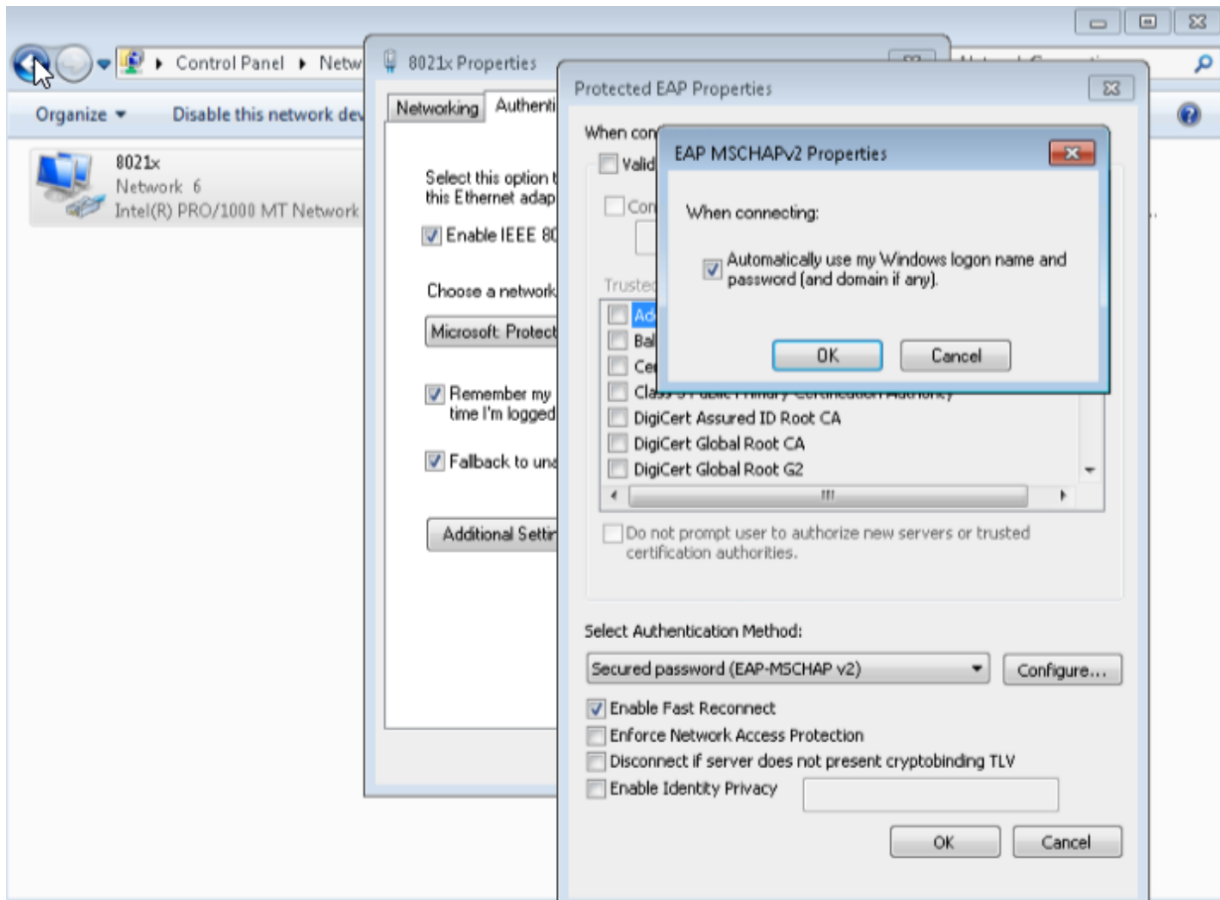
4. Click *Settings* and ensure that the *Validate server certificate* option is not selected.

Figure 44: Protected EAP Properties



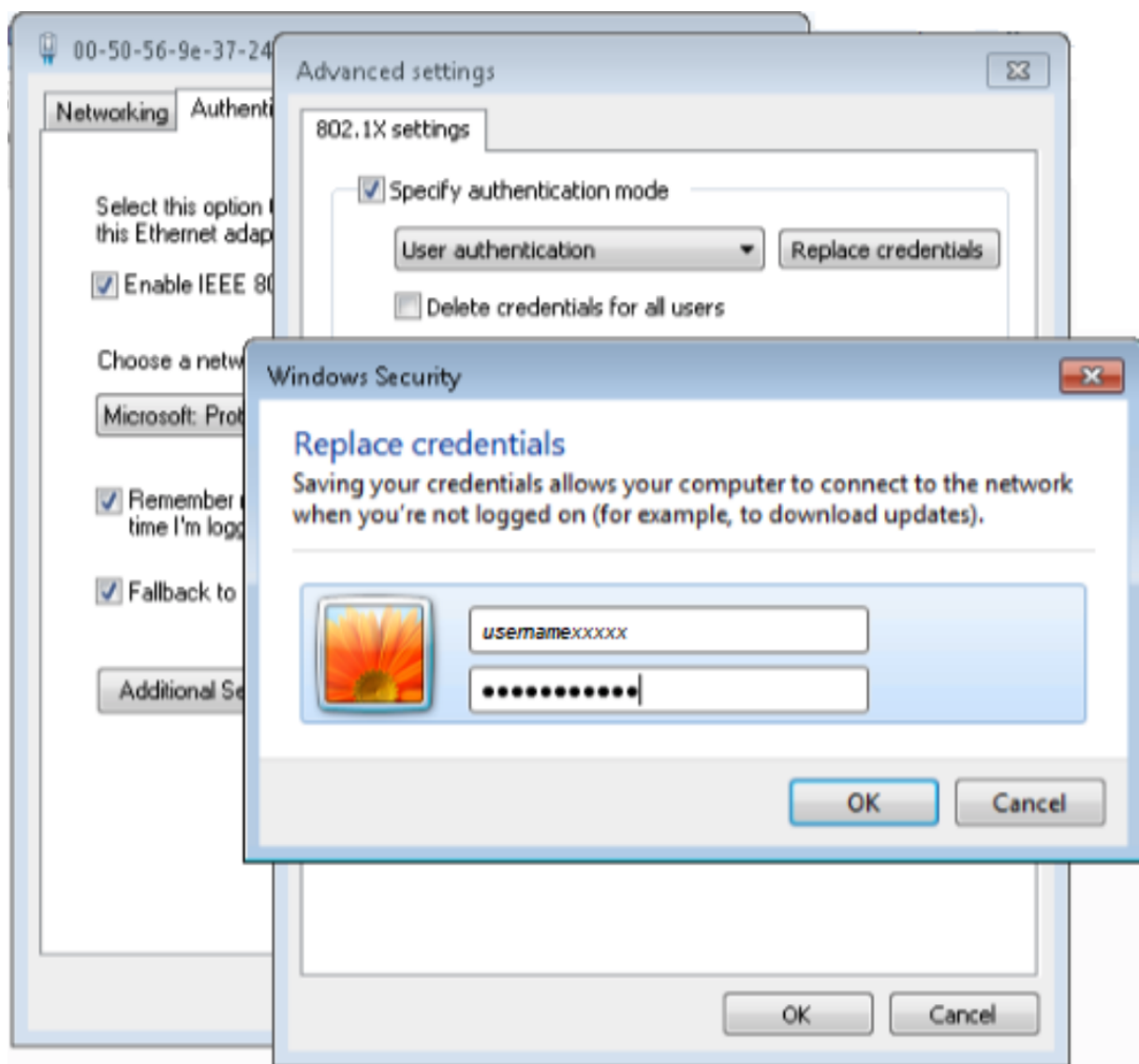
5. Configure the user credential settings. Select the *Automatically use my Windows login name and password* option to use the user credentials you previously configured in Active Directory.

Figure 45: Windows Login and Password Confirmation



6. Click *Authentication > Additional Settings > Replace credentials* and enter the credentials of the user you created in Active Directory.

Figure 46: Replacing Credentials



7. To confirm that the 802.1X authentication works on Windows 7 Supplicant and verify that the user is placed correctly in the User VLAN (vlan31), enter the **show dot1x interface** and **show vlans vlan31** commands.

Figure 47: show dot1X interface and show vlans Output

```

root@ xxxx> show dot1x interface
802.1x Information:
Interface      Role           State           MAC address      User
ge-0/0/19.0    Authenticator  Authenticated   00:50:56:9E:37:24 JTAC-EMEA\ xxxxxxxx

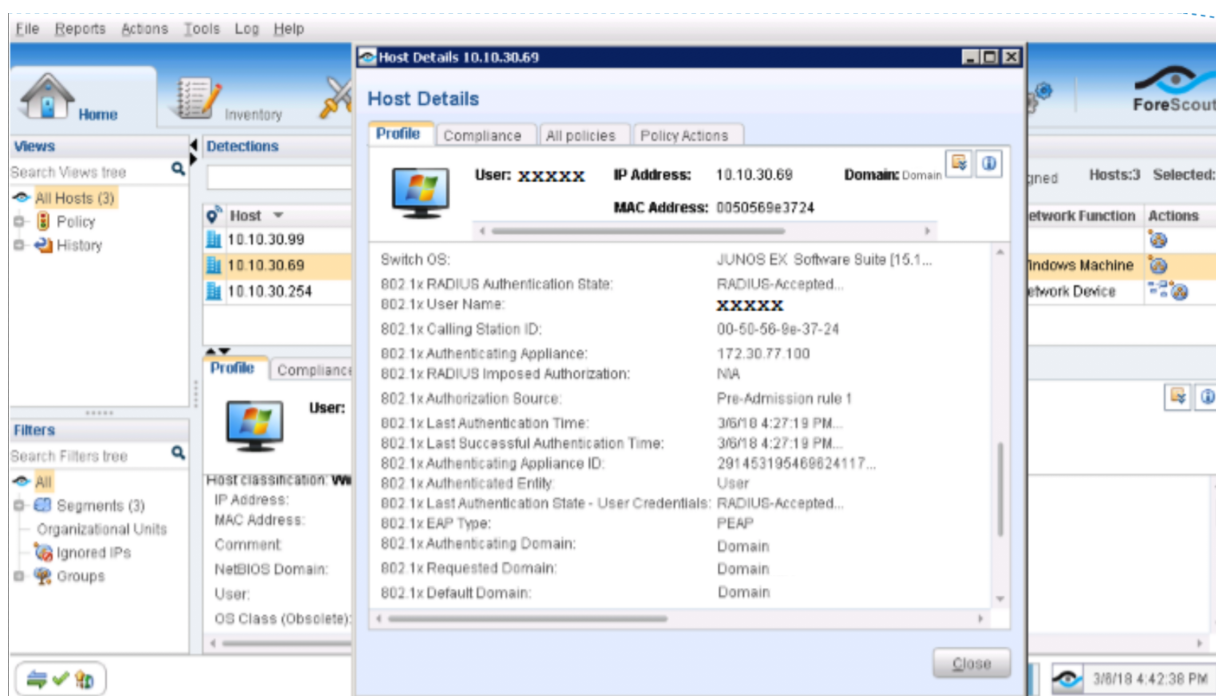
{master:0}
root@ xxxx> show vlans vlan31
Name           Tag           Interfaces
vlan31         31           ge-0/0/18.0*, ge-0/0/19.0*

{master:0}
root@ xxxx> █

```

8. To review the session information (username, IP address, and MAC-ID) on the CounterACT Console, right-click on your host, and select *Information > Details*.

Figure 48: Session Information Verification



Test and Troubleshoot 802.1X Authentication

To test the 802.1X authentication against ForeScout CounterACT:

1. Log in using the credentials of the domain account (user) you created in the User Directory.

Figure 49: Troubleshoot Rejected Authentications



2. Ensure that the EX4300 switch is configured properly for 802.1X authentication. Click [“CLI Configuration for EX4300 Switch”](#) on page 141 to review the configuration file.

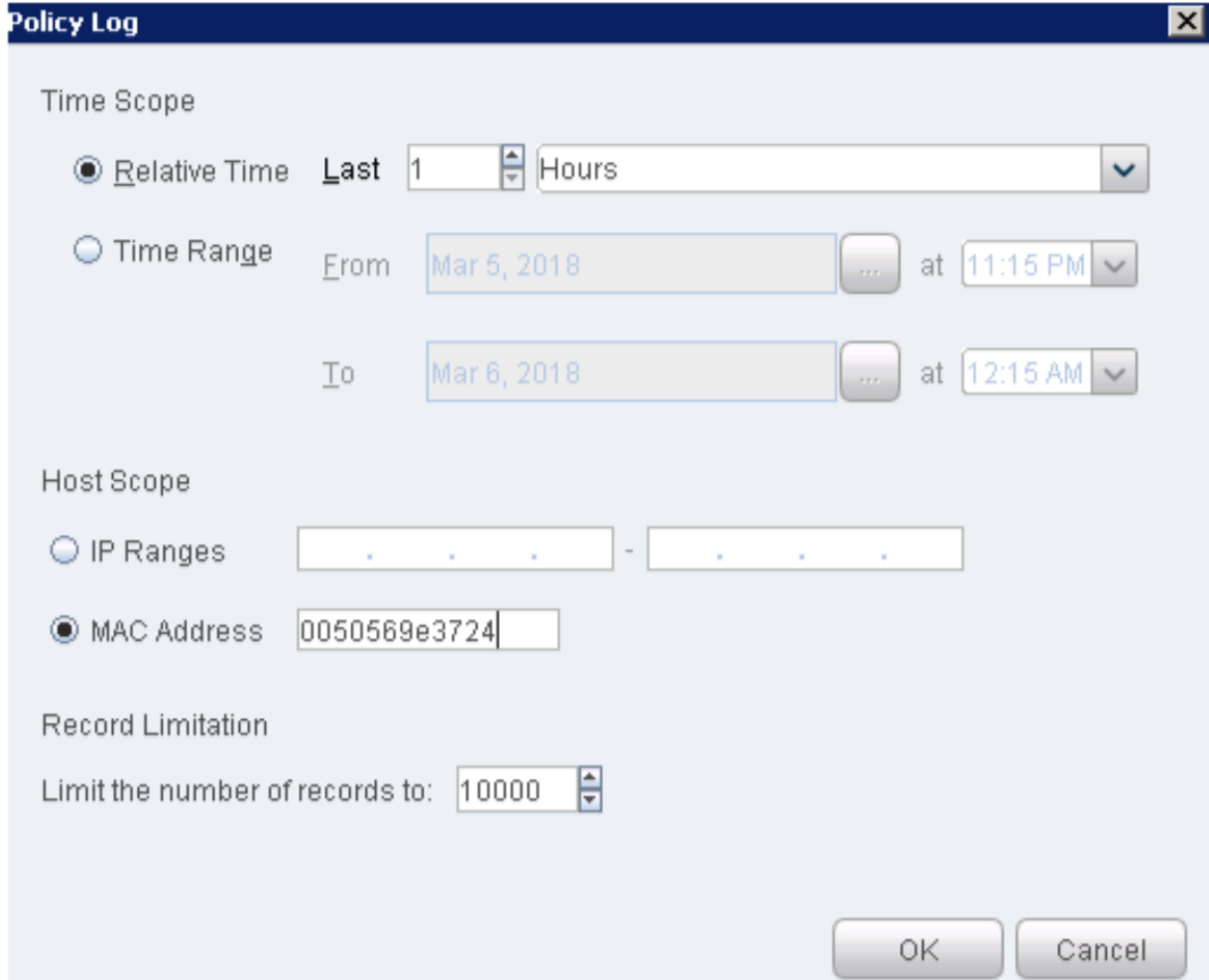
To troubleshoot 802.1X authentication issues:

1. From the ForeScout CounterACT Console, click the Policy tab and create a policy using the *Troubleshoot Rejected Authentications* template (listed under 802.1X Enforcement).
2. Start your policy to troubleshoot the issue.

To view logs from the ForeScout CounterACT Console:

1. Select *Log > Policy Log*. From the Policy Log page, enter your Windows 7 supplicant's MAC or IP address.

Figure 50: Policy Log Settings



Policy Log

Time Scope

☒ Relative Time Last 1 Hours

☐ Time Range From Mar 5, 2018 at 11:15 PM

To Mar 6, 2018 at 12:15 AM

Host Scope

☐ IP Ranges . . . - . . .

☒ MAC Address 0050569e3724

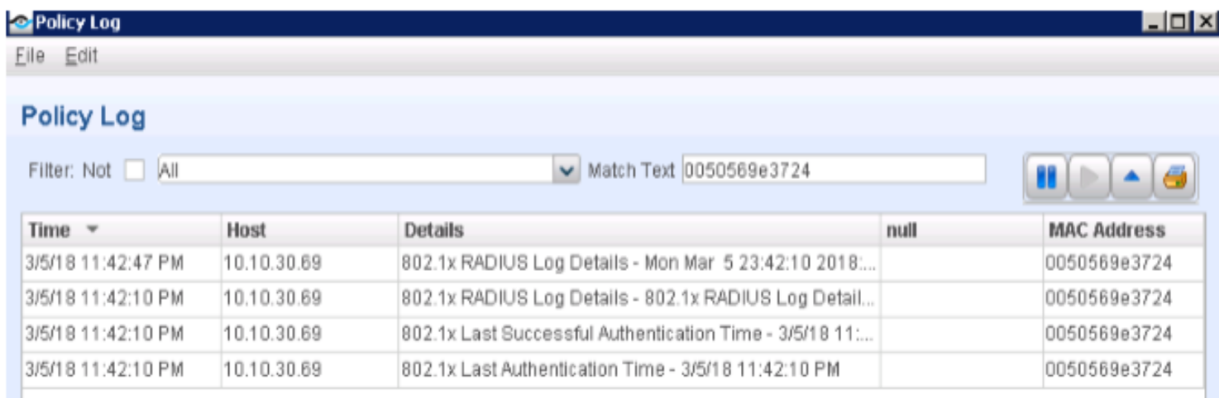
Record Limitation

Limit the number of records to: 10000

OK Cancel

2. Click OK. The policy log files appear.

Figure 51: Policy Log Files



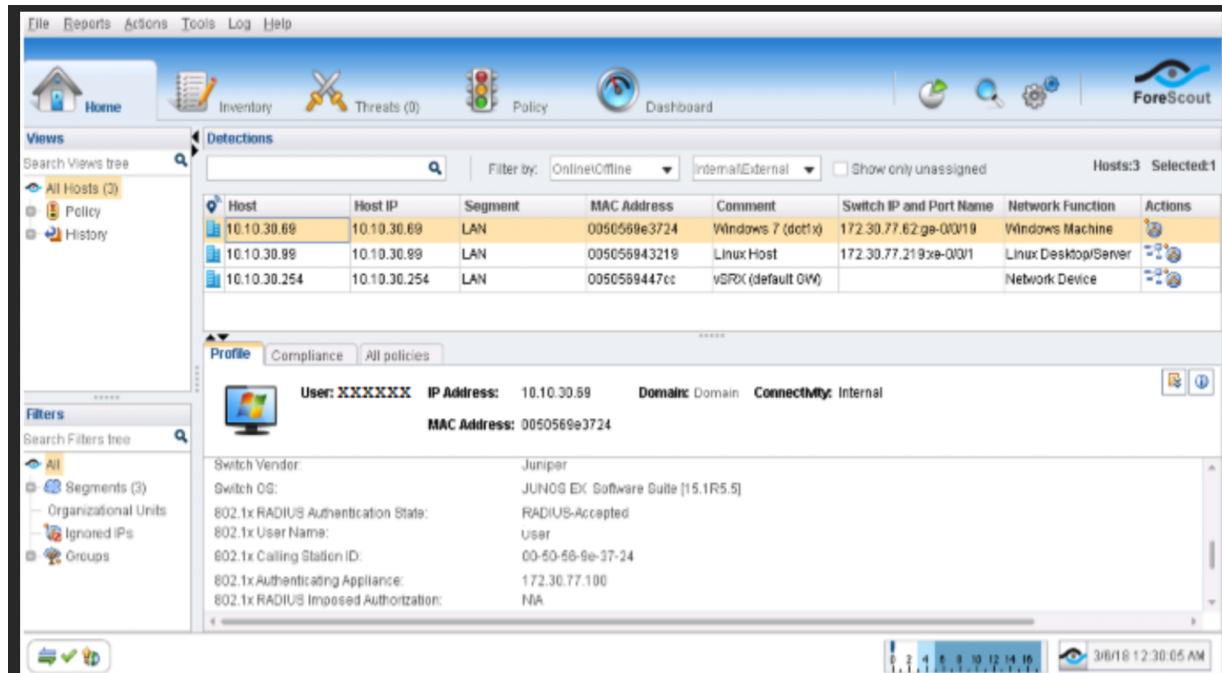
Policy Log

Filter: Not All Match Text 0050569e3724

Time	Host	Details	null	MAC Address
3/5/18 11:42:47 PM	10.10.30.69	802.1x RADIUS Log Details - Mon Mar 5 23:42:10 2018:...		0050569e3724
3/5/18 11:42:10 PM	10.10.30.69	802.1x RADIUS Log Details - 802.1x RADIUS Log Detail...		0050569e3724
3/5/18 11:42:10 PM	10.10.30.69	802.1x Last Successful Authentication Time - 3/5/18 11:...		0050569e3724
3/5/18 11:42:10 PM	10.10.30.69	802.1x Last Authentication Time - 3/5/18 11:42:10 PM		0050569e3724

3. If 802.1X authentication works and your Windows 7 supplicant obtains an IP address from the DHCP server running on SRX, you can then generate some traffic to verify that your Windows 7 supplicant (for example, 10.10.30.69) appears on the Host list under the Home tab.

Figure 52: Policy Log 802.1X Authentication Confirmation



NOTE: Additionally, if you already configured the other host (Windows or Linux system) that is connected to the QFX switch and obtained an IP address from the DHCP server running on SRX, you can then generate some traffic for it, and the host address (for example, 10.10.30.99) will also appear on the Host list.

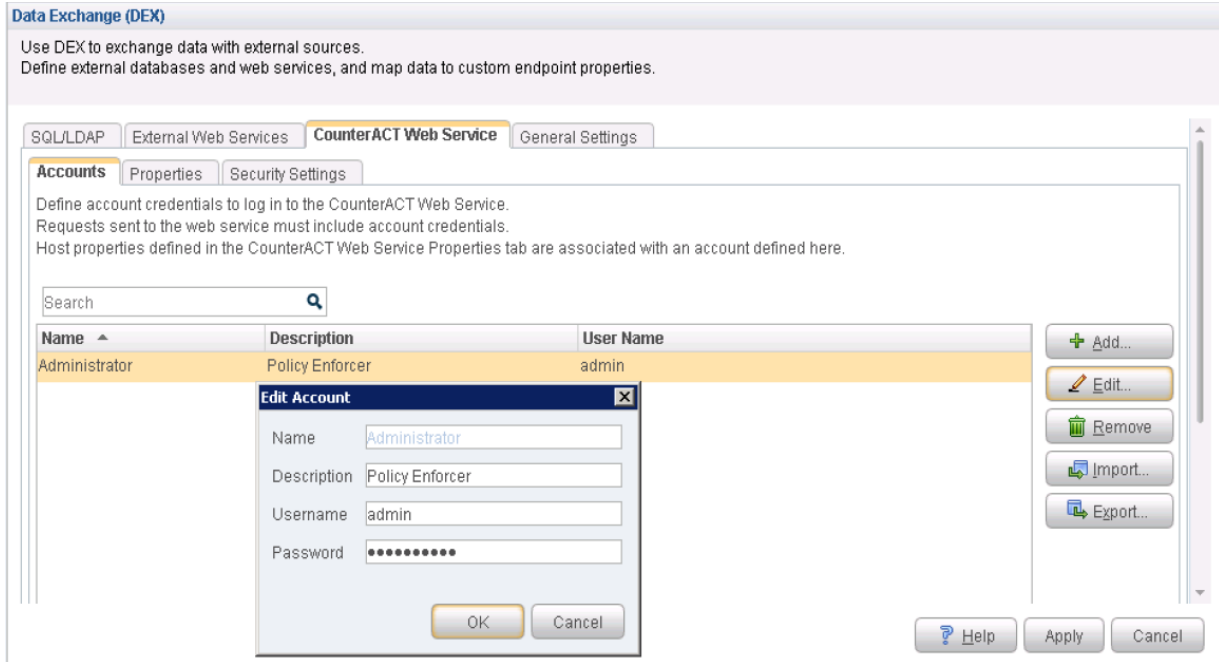
Configure Data Exchange Plugin

The Data Exchange (DEX) Plugin enables CounterACT to use web services to communicate with external entities. CounterACT queries external services and receives updates through the CounterACT web service hosted by the plugin. In this case DEX in conjunction with the ForeScout Connector will monitor PE for any communication.

To configure the Data Exchange (DEX) Plugin:

1. Select *Tools > Options > Data Exchange (DEX)*.
2. From the Data Exchange (DEX) page, select *CounterACT Web Service > Accounts* tab.

Figure 53: Data Exchange Accounts



3. Click *Add* and enter the following information:
 - a. In the *Name* field, enter the name of the CounterACT web service account.
 - b. In the *Description* field, enter a brief description of the purpose of the web service account.
 - c. In the *Username* field, enter the username used to authorize CounterACT to access the web service account.
 - d. In the *Password* field, enter the password used to authorize CounterACT to access the web service account.
 - e. Click *OK* and the account appears in the Account tab.
4. Click the *Properties* tab. From the Properties page, click *Add* to add the following properties:
 - block
 - quarantine
 - Test

NOTE: You must include the Test property; otherwise, you cannot add CounterACT as a third-party connector to Policy Enforcer successfully.

Figure 54: Data Exchange Properties

Data Exchange (DEX)

Use DEX to exchange data with external sources.
Define external databases and web services, and map data to custom endpoint properties.

SQLLDAP External Web Services **CounterACT Web Service** General Settings

Accounts **Properties** Security Settings

Define host properties that are set by the CounterACT Web Service.
Each host property defined in this tab is associated with one of the accounts in the CounterACT Web Service Accounts tab.
To set a property, a client must send a request that uses the account credentials of the associated account for authentication.

Search

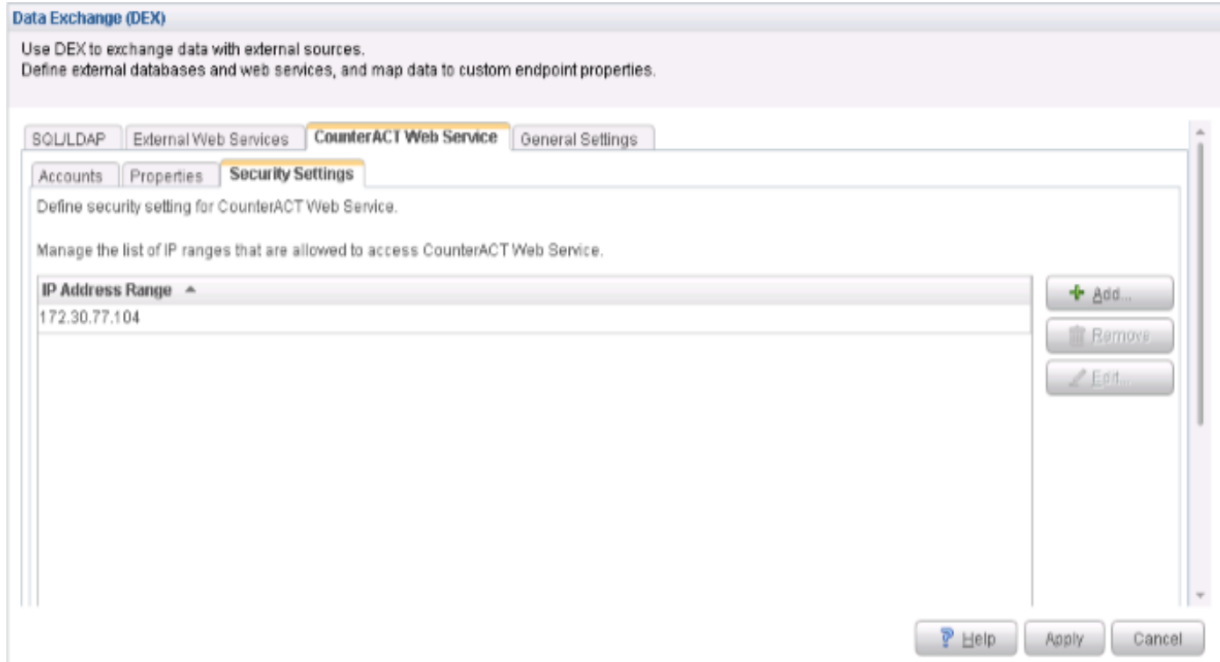
Name	Description	Type ^	Account
block	Policy Enforcer Block Action	Boolean	Administrator
quarantine	Policy Enforcer Quarantine Action	Boolean	Administrator
Test		Boolean	Administrator

+ Add...
Edit...
Remove
Import...
Export...

? Help Apply Cancel

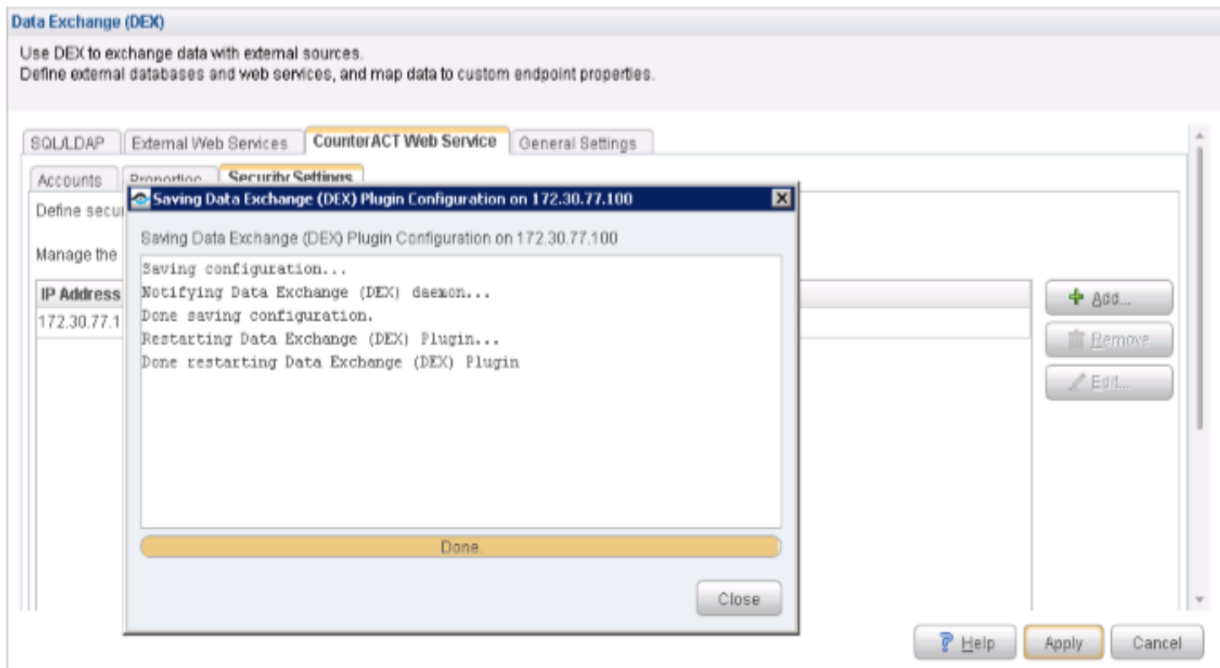
- Click the *Security Settings* tab. A white list of IP addresses is used to permit access to the CounterACT web service. From the Security Settings page, click *Add* and add the IP address range for the Policy Enforcer. Click *OK*. The IP address appears in the IP Address Range list.

Figure 55: Data Exchange Security Settings



6. From the Data Exchange (DEX) page, click *Apply* to save and apply the configuration settings.

Figure 56: Data Exchange Applying Configuration Settings



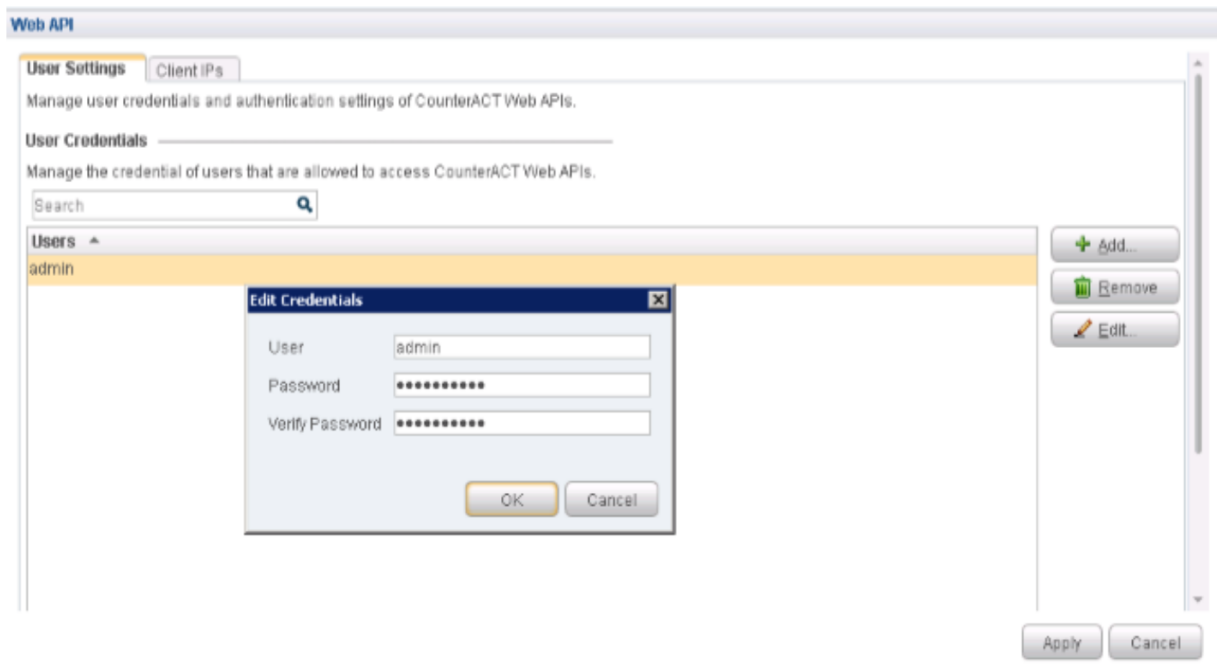
Configure Web API Plugin

The Web API Plugin enables external entities to communicate with CounterACT using simple, yet powerful web service requests based on HTTP interaction. Configure the Web API Plugin to create an account for Policy Enforcer integration.

To configure the Web API Plugin:

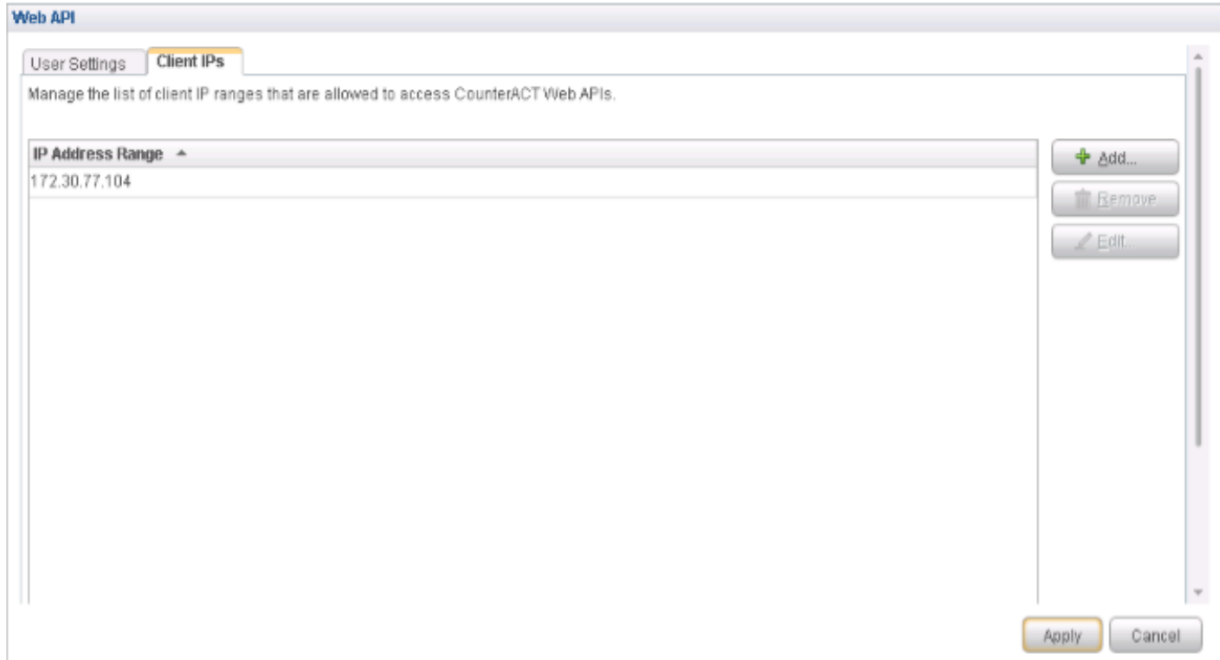
1. Select *Tools > Options > Web API*.
2. From the Web API page, in the User Credentials section, click *Add*.

Figure 57: Web API User Credentials



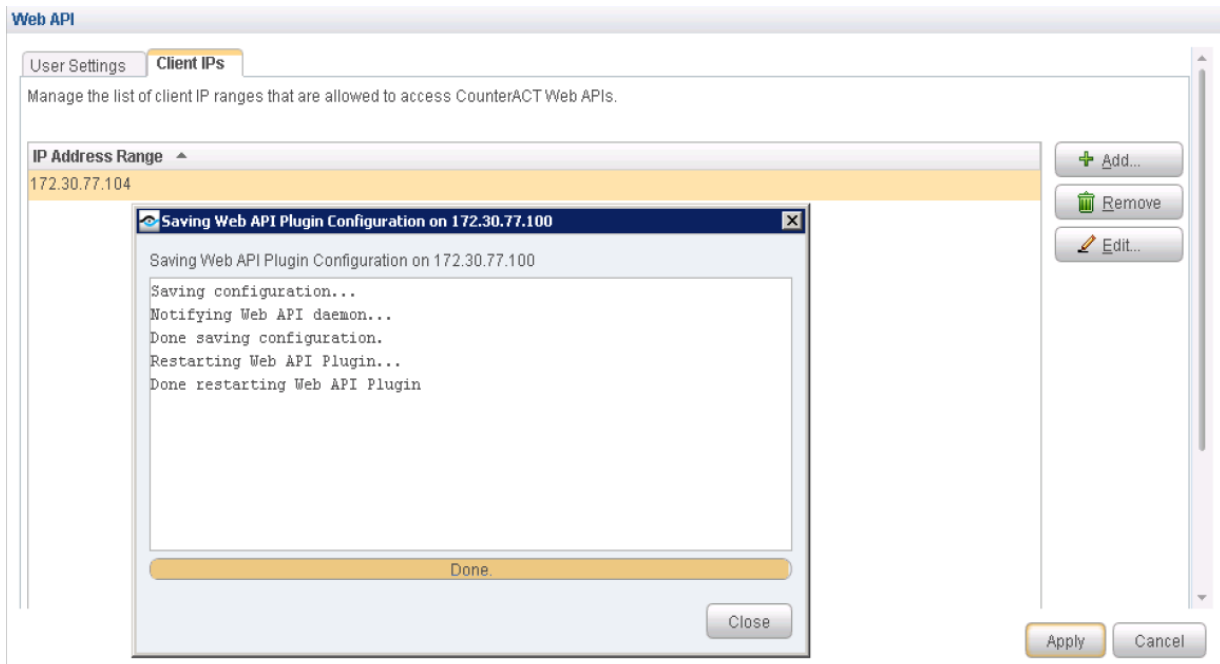
3. Enter the same username and password that you previously created for the Data Exchange (DEX) configuration and click *OK*.
4. Click the *Client IPs* tab and click *Add*. Add the Policy Enforcer IP address into the access list. Click *OK*.

Figure 58: Web API Client IP Tab



5. From the Web API page, click *Apply* to save and apply the configuration settings.

Figure 59: Web API Applying Configuration Settings



Verify Plugins

To verify that all of the required plugins are running, select *Tools > Options > Plugins*. The Plugins page appears showing the status of each plugin.

Figure 60: Verifying Plugins

Plugins

Plugins extend CounterACT's capabilities by enabling integration with other tools, allowing deeper inspection, additional enforcement actions and more. Default plugins appear here after the initial setup. [more...](#)
Additional non-licensed plugins and licensed plugins can be downloaded from the [ForeScout website](#).

Plugin	Status	Version	Module	Module Status
HPS Inspection Engine	Running	10.4.1.1		
Web API	Running	1.2.2	Open Integration Module	Demo - 78 days left
Macintosh/Linux Propert...	Running	7.0.1		
DNS Client	Running	2.11080		
DHCP Classifier	Running	2.0.6		
Data Exchange (DEX)	Running	3.2.0	Open Integration Module	Demo - 78 days left
DNS Query Extension	Running	1.1.1		
802.1x	Running	4.2.0.1010		
Switch	Running	8.11.1		
NBT Scanner	Running	3.0.4		
User Directory	Running	6.1.2		
Wireless	Not running	1.7.0		
Syslog	Not running	3.2.0		
Hardware WatchDog	Not running	1.1.4		
CounterACT Infrastructur...	N/A	2.0.8		
Technical Support	N/A	1.1.2		

21 items (1 selected)

Install

Uninstall

Rollback

Start

Stop

Configure

Test

Help

About

Configure Automated Threat Remediation Policies

Using Policy Manager, create these automated threat remediation policies:

- NETCONF policies—used to connect hosts to the QFX switch.
- 802.1X policies—used to connect hosts to the EX4300 switch and used for 802.1X authentication.

To create an automated threat remediation NETCONF policy or 802.1X policy:

1. Select *Policy > Policy Manager*.
2. From the Policy Manager page, click *Add*.

Figure 61: Policy Manager Page

Policy Manager

Search ☒ Show subfolder policies

Name	Category	Status	User Scope	Segments	Conditions	Actions
Asset Classification	Classificati...		Complete	LAN	No Conditions	
SDSN BLOCK - dot1x	None		Complete	LAN	block: Event previously detected	
SDSN BLOCK - netconf	None		Complete	LAN	block: Event previously detected	
SDSN QUARANTINE - dot1x	None		Complete	LAN	quarantine: Event previously detected	
SDSN QUARANTINE - netconf	None		Complete	LAN	quarantine: Event previously detected	

5 items (1 selected)

Add...
 Edit...
 Categorize...
 Remove
 Duplicate...
 Move to...
 Export...
 Start
 Stop
 Custom...
Apply

3. Click *Custom* and click *Next*.

- a. Based on your requirements, create the following sets of SDSN block and quarantine policies to secure host-to-switch and switch-to-802.1X server traffic. In the *Name* field, enter these policy names:
- SDSN BLOCK—dot1x
 - SDSN QUARANTINE—dot1x
 - SDSN BLOCK—NETCONF
 - SDSN QUARANTINE—NETCONF

Figure 62: Block and Quarantine Policies

Policy: 'SDSN BLOCK - dot1x' -

Name

Name: SDSN BLOCK - dot1x Edit...

Description: Deny Access -> Default VLAN

Scope

IP Ranges: LAN Edit...

Filter by Group: None.

Exceptions: None.

Main Rule

Conditions	Actions	Re-check
block: Event previously d...		Every 8 hours, All admiss...

Edit...

Sub-Rules

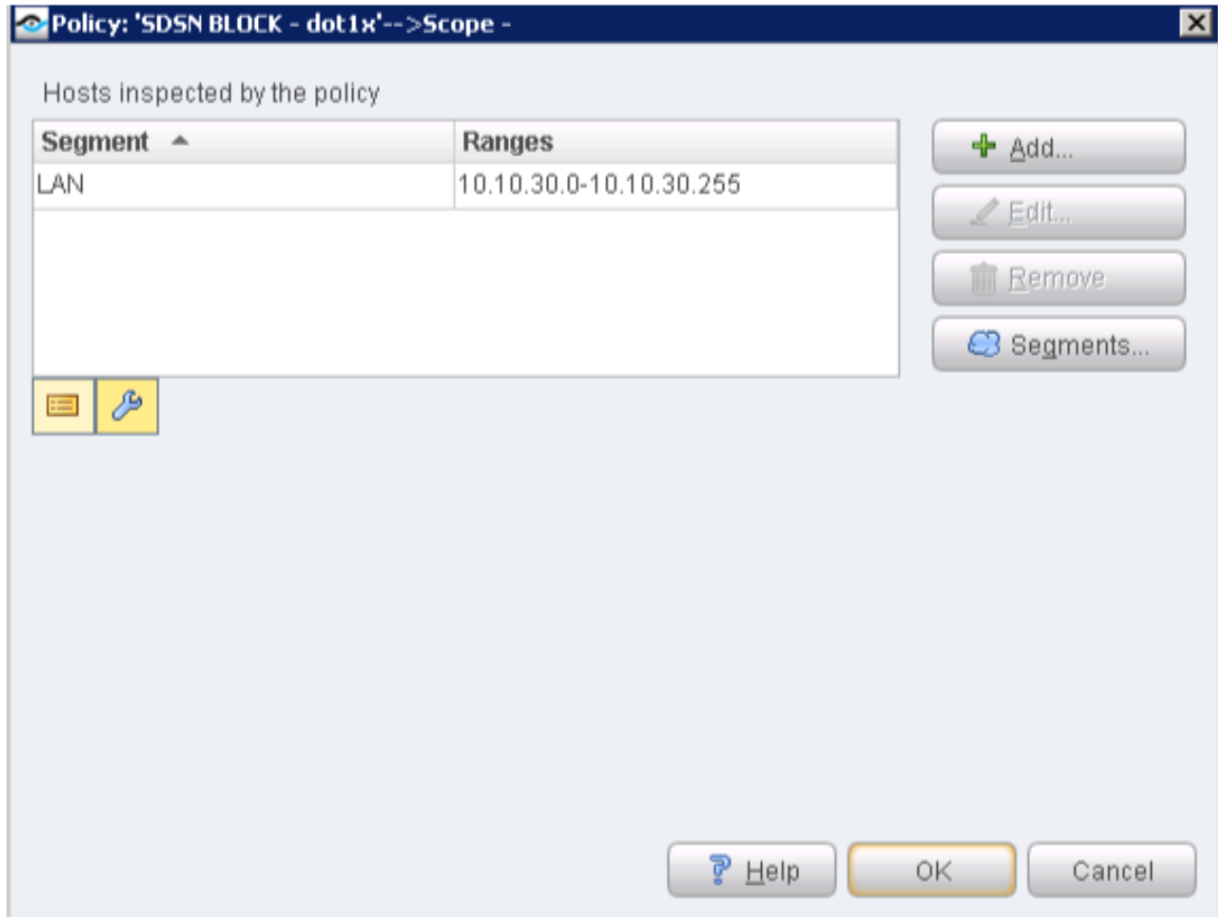
Name	Conditions	Actions	Exceptions
No items to display			

+ Add...
Edit...
Remove
Duplicate
Up
Down

? Help OK Cancel

- b. In the *Description* field, enter a description for each policy. Click *Next*.
4. From the *Scope* page, select the *IP Range* option. Enter the IP address range for the LAN segment as endpoints to be inspected for this policy. Click *OK*.

Figure 63: IP Address Range in Block and Quarantine Policies





5. Click *Next* to skip the Advanced section and open the *Main Rule* page. A rule contains a set of conditions and actions:
 - A condition is a set of properties that is queried when evaluating endpoints.
 - An action is the measure that CounterACT takes at endpoints.
6. From the *Main Rule* page, click *Add* from the Condition section of the page to add a condition.

Figure 64: Adding Conditions to Block and Quarantine Policies




Policy: 'SDSN BLOCK - dot1x'-->Main Rule -

Condition

A host matches this rule if it meets the following condition:


All criteria are True  




Criteria
block - Event previously detected

 Add...
 Edit...
 Remove

Actions


Actions are applied to hosts matching the above condition.


Enable	Action	Details
<input checked="" type="checkbox"/>	 802.1x Authorize	802.1x Autho...

 Add...
 Edit...
 Remove

Advanced

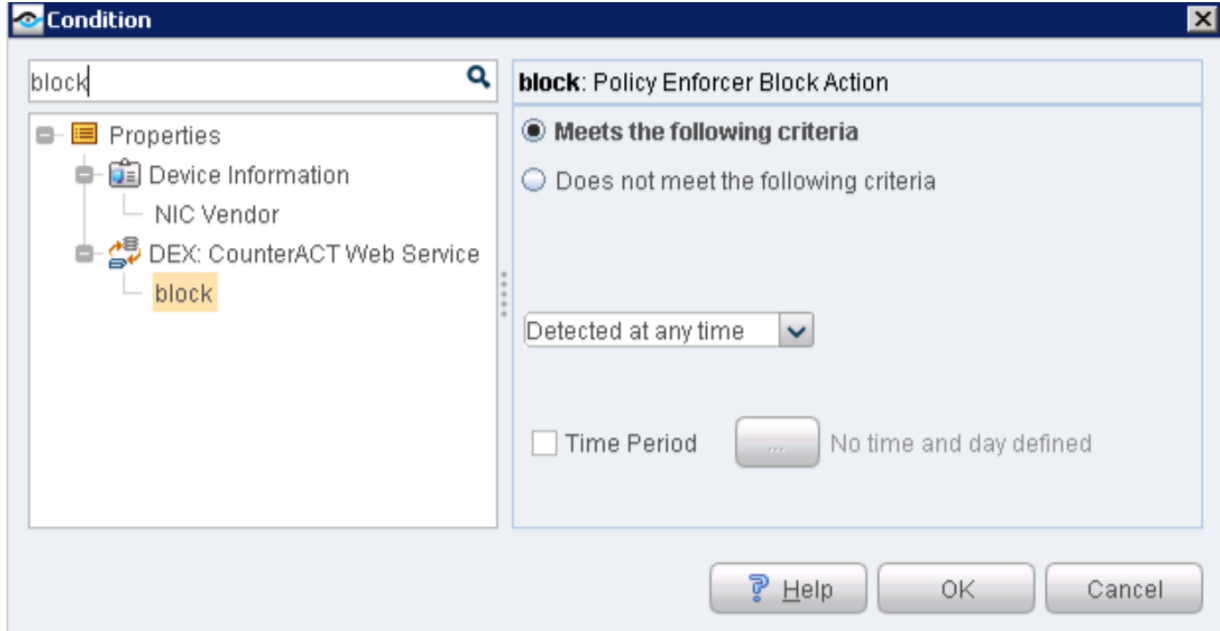
Recheck unmatched Every 8 hours
 Recheck match Every 8 hours, All admissions

 Edit...

 Help OK Cancel

7. Define the condition for block or quarantine.

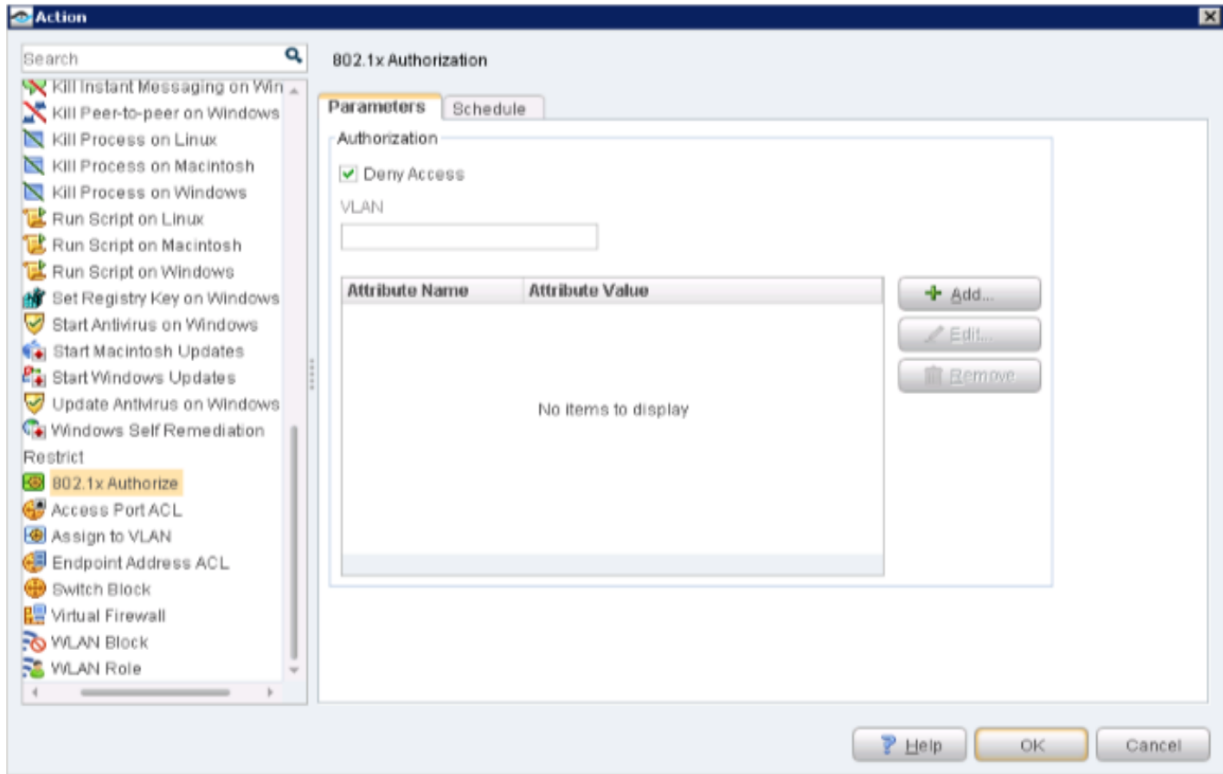
Figure 65: Defining Conditions for Block and Quarantine Policies



8. From the *Main Rule* page, click *Add* from the Actions section of the page. From the *Action* page, define these actions:

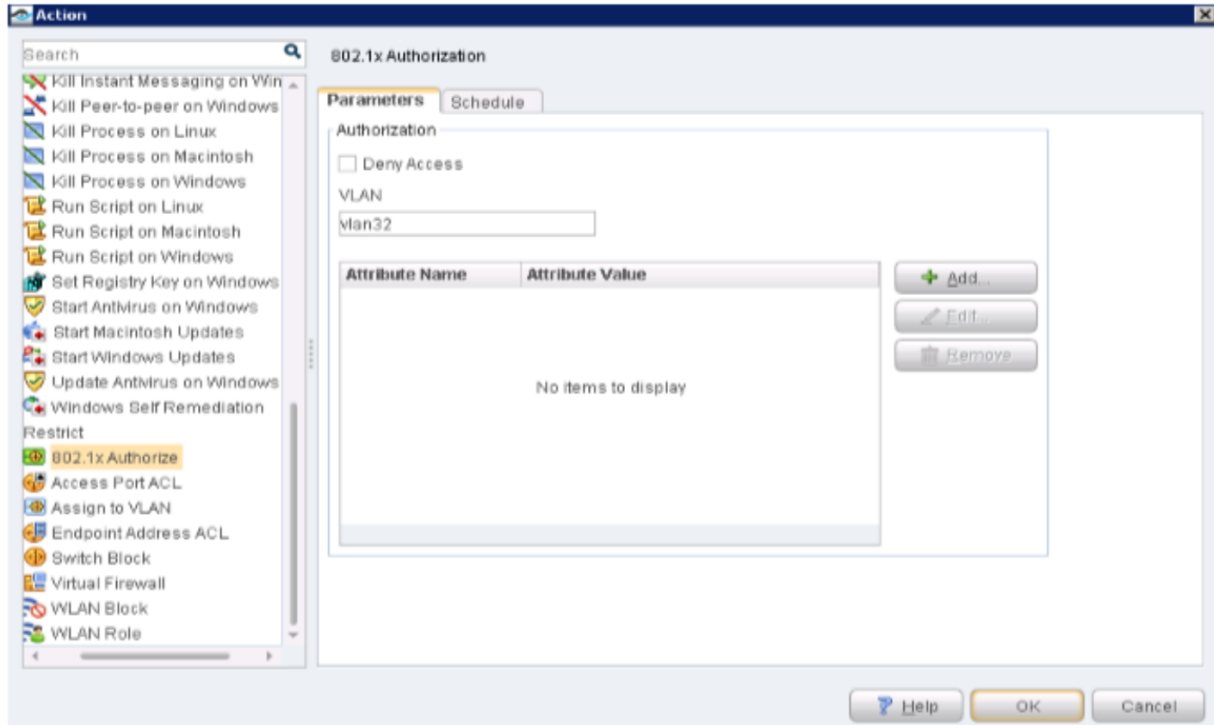
- a. *SDSN BLOCK - dot1x*—select 802.1x Authorize in the left pane and enable the *Deny Access* option as an action.

Figure 66: 802.1X Blocking Access



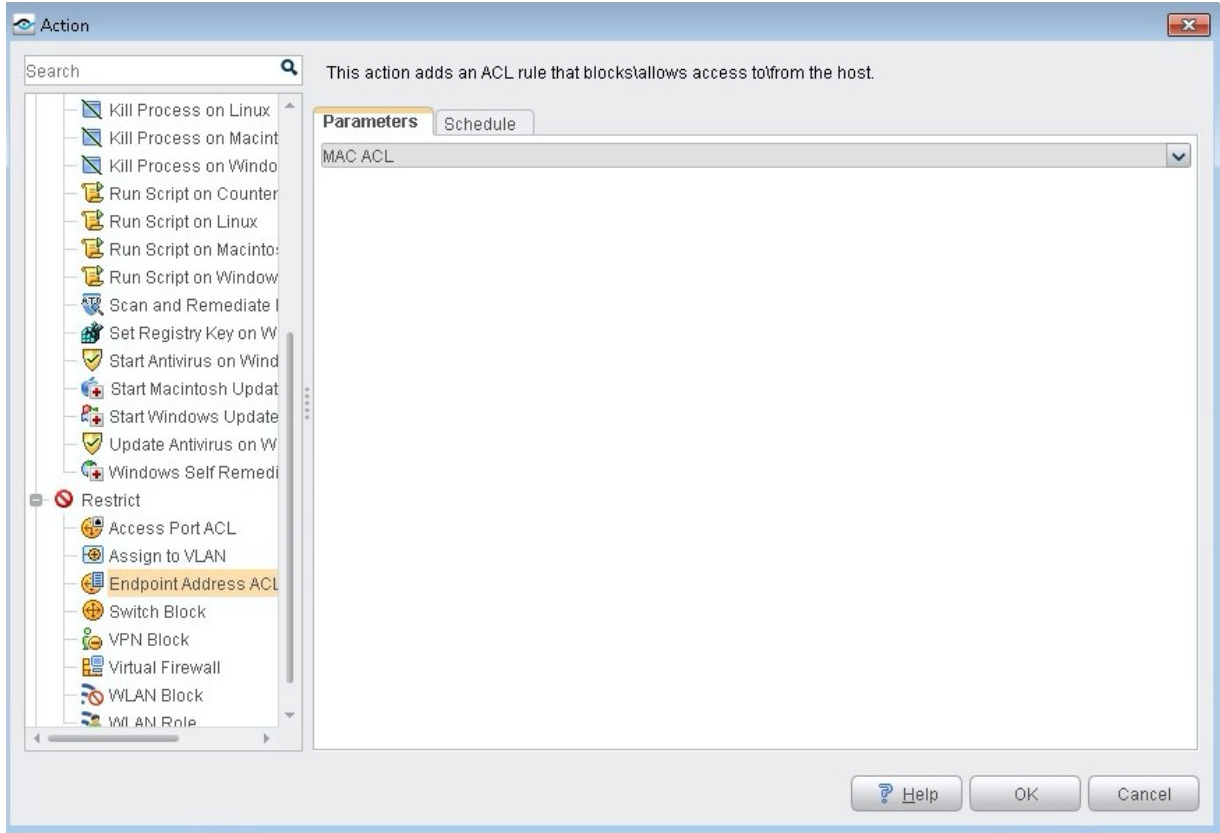
- b. *SDSN QUARANTINE - dot1x*—select 802.1x Authorize in the left pane and enter vlan32 in the VLAN field as an action.

Figure 67: 802.1X Quarantine Traffic to a VLAN



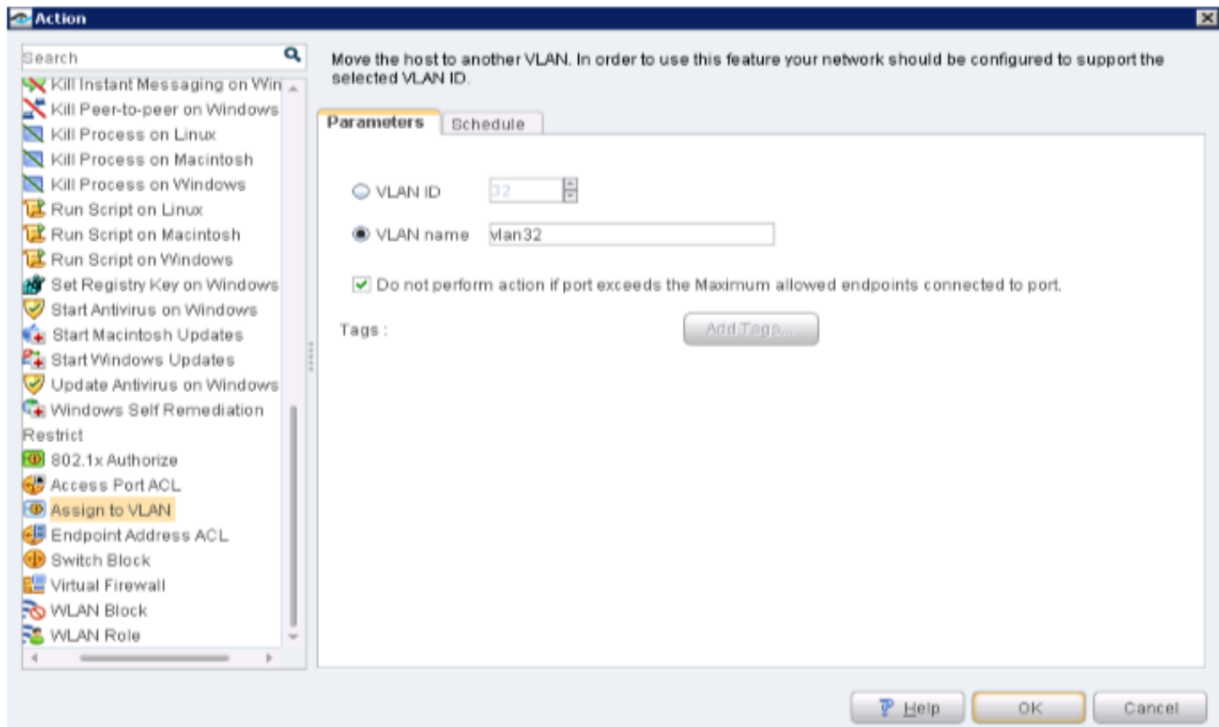
- c. *SDSN BLOCK - NETCONF*—select *Endpoint Address ACL* in the left pane and enter an ACL as an action in the *Parameters* tab.

Figure 68: Endpoint Access ACL



- d. *SDSN QUARANTINE - NETCONF*—select *Assign to VLAN* in the left pane and enter *vlan32* in the *VLAN name* field under the *Parameters* tab to add as an action.

Figure 69: SDSN Quarantine Assign to VLAN

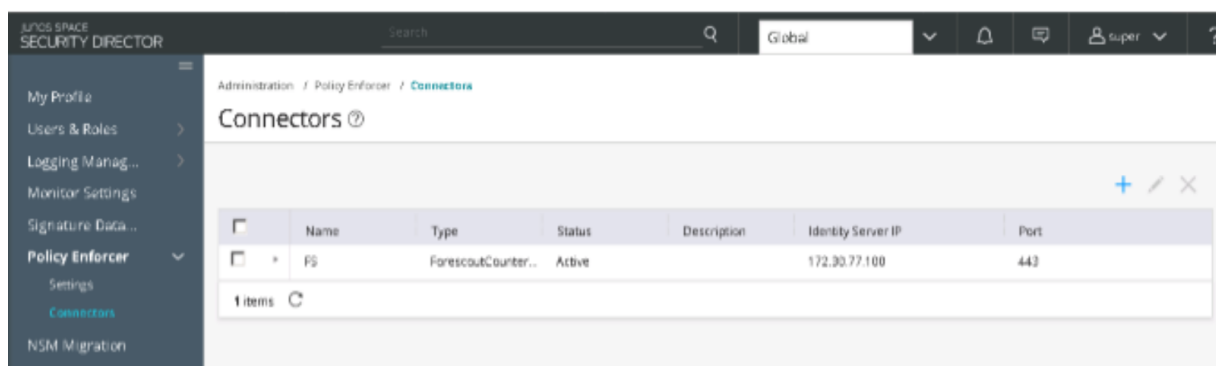


9. Click OK and then click Next. Skip configuring sub-rules on the *Sub-Rules* page.
10. From the Policy Manager page, click *Apply* to save and apply the configuration settings. Review the *Status* of your policy and verify that it is active indicated with an arrow and green box:

Configure the Policy Enforcer Connector for Third-Party Switches

1. Log in to Security Director and navigate to *Administration > Policy Enforcer > Connectors* and create a new connector. A blue loading/wait circle indicates that creation of the connector is in progress.

Figure 70: Connectors



2. Enter the following General page details:
 - *Name*—Enter a unique string.
 - *Description*—Enter a description.
 - *ConnectorType*—Select the required third-party network of devices to connect to your secure fabric and create policies for this network. Select *ForeScout CounterACT*. Click *Next*.
3. Enter the following General page details:
 - *IP Address*—Enter the IP (IPv4 or IPv6) address of the product management server.
 - *Port*—Select the port to use from the list. If you leave this blank, port 443 is the default.
 - *Username*—Enter the username of the server for the selected ForeScout CounterACT connector type. For example, Admin.
 - *Password*—Enter the password of the server for the selected ForeScout CounterACT connector type.
 - *DEX User Role*—Enter the password of the server for the selected ForeScout CounterACT connector type. For example, Administrator. This has to match the Name field configured on page 58 under the DEX plugin. Click *Next*.
4. On the Network Details page, add subnet information to the connector configuration so you can include those subnets in groups and then apply policies to those groups. Click *Next*.
5. On the Configuration page, enter the values for the Web API username and password. Click *Finish*.

Configure ATP Cloud with Threat Prevention Policies

To configure ATP Cloud and set up threat prevention policies:

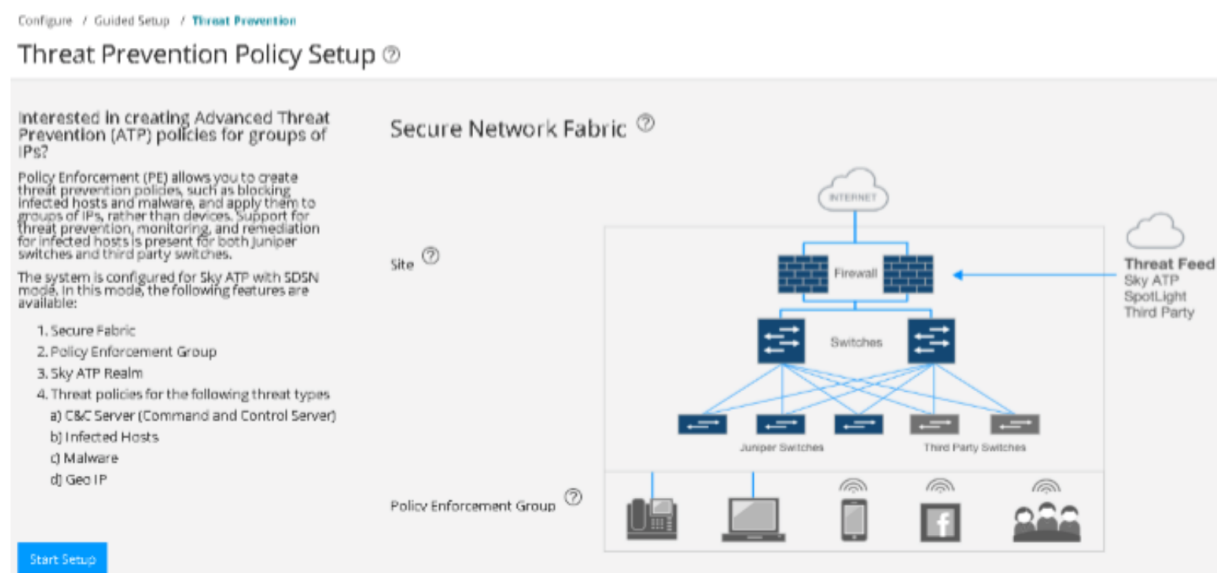
- Configure a secure fabric. A secure fabric is a collection of sites which contain network devices (switches, routers, firewalls, and other security devices) used in policy enforcement groups.
- Define a site and add endpoints to it (switches and firewalls).
- Configure policy enforcement groups. A policy enforcement group is a grouping of endpoints to which threat prevention policies are applied.
- Create a threat prevention policy.
- Apply threat prevention policies to policy enforcement groups

NOTE: If you are using Policy Enforcer for threat prevention with ATP Cloud, Guided Setup is the most efficient way to complete the initial configuration.

To perform the configuration using Guided Setup:

1. In Security Director, navigate to *Configure > Guided Setup > Threat Prevention*.

Figure 71: Threat Prevention Policy Setup



2. Click *Start Setup* and follow the wizard.

Figure 72: Sky ATP with SDSN Setup

Sky ATP with SDSN Setup ?

1 2 3 4

Secure Fabric Policy Enforcement Groups Sky ATP Realm Policies

Secure Fabric ?

Sites

	Site	Enforcement Points	IP	Model	Description
<input type="checkbox"/>					

3. Create a secure fabric site that includes enforcement points for only the SRX Series device and the ForeScout CounterACT connector. Click Next.

Figure 73: Secure Fabric Threat Prevention Policy Setup

Threat Prevention Policy Setup ?

1 2 3 4 5

Secure Fabric Policy Enforcement Groups Sky ATP Realm Policies Geo IP

Secure Fabric ?

Sites

	Site	Enforcement Points	IP	Model	Description
<input type="checkbox"/>	BETA	vSRX_L3_QFX PS	172.30.77.230 172.30.77.100	VSRX Connector	

1 items

Cancel Next

4. Create a policy enforcement group and select the site. As per your requirements, determine the type of endpoints you are including in your policy enforcement group: IP address, subnet, or location. Endpoints cannot belong to multiple policy enforcement groups. Click Next.

Figure 74: Policy Enforcement Groups

Threat Prevention Policy Setup ⓘ

1 Secure Fabric 2 **Policy Enforcement Groups** 3 Sky ATP Realm 4 Policies 5 Geo IP

+

✎

✕

<input type="checkbox"/>	Name	Type	Items	Description
<input type="checkbox"/>	IPSUBNET	IP Address	10.10.30.0/24	

1 items ↻

Cancel Back Next

5. Add the ATP Cloud realm by providing the relevant details from your ATP Cloud account.

Before you configure the ATP Cloud realm, ensure that you:

- Have an ATP Cloud account with an associated license.
- Understand which type of ATP Cloud license you have: free, basic, or premium. The license controls which ATP Cloud features are available. Click [“Obtain an ATP Cloud license and Create an ATP Cloud Web Portal Account”](#) on page 39 for more details.
- Know which region is covered by the realm you are creating. You must select a region when you configure a realm.

Figure 75: Sky ATP Realm

Sky ATP Realm ?

Sky ATP realm credentials
Provide your Sky ATP realm credentials

Location * North America ▼

Username

Password

Realm ?

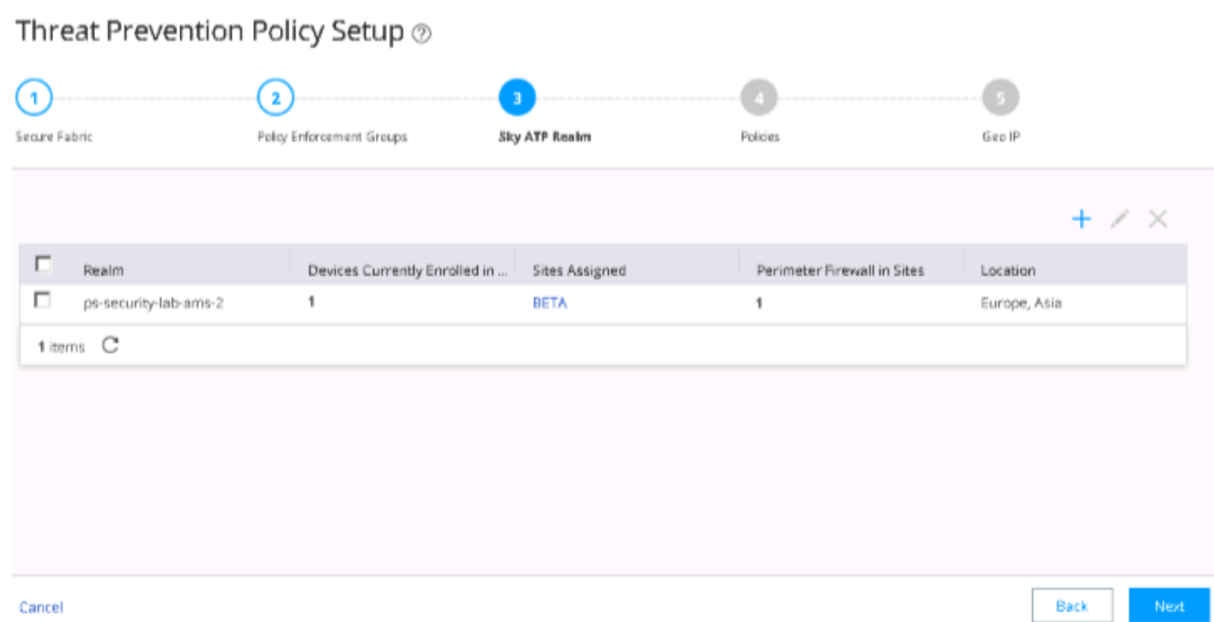
No Sky ATP account? Select your region using the Location in the menu above, then [click here](#) to create an account. You will be redirected to the Sky ATP account page.

Cancel OK

Enter *Location*, *Username* (Your username for ATP Cloud is your e-mail address), *Password*, and a name for the *Realm*. Click OK.

6. Verify that the ATP Cloud realm has been added.

Figure 76: ATP Cloud Realm Creation Verification



The value 1 should appear in the *Perimeter Firewall in Sites* column, indicating that ATP Cloud has detected the SRX Series device.

NOTE: If the realm addition is not successful, it indicates that there is a network issue and Security Director or Policy Enforcer cannot connect to the Internet. Ensure all devices/components can connect to the Internet and each other.

7. Create a threat prevention policy, as per your requirements. Threat prevention policies provide protection and monitoring for selected threat profiles, including command & control (C&C) servers, infected hosts, and malware.
- Determine the type of profile to use for this policy: C&C server, infected hosts, or malware. You can select one or more threat profiles in a policy.
 - Determine which action to take if a threat is found.
 - Know which policy enforcement group to add to this policy.

Figure 77: Create Threat Prevention Policy

Create Threat Prevention Policy ?

Name * ?

POLICY

Description

Profiles

☒ Include C&C profile in policy

Select the threat score ranges to apply when users try to access a C&C Server.

Threat Score

5

8

1

2

3

4

5

6

7

8

9

10

Permit 1 - 4

Monitor 5 - 7

Block 8 - 10

Actions

Drop connection silently {recommended} ▾

Cancel

OK

Click OK.

8. Threat Prevention Policy needs a profile for HTTP downloads; this profile indicates what type of files need to be scanned for threats. To add a profile for HTTP file downloads, in the *Device Profile* area, expand the *Realm* and select the required profile. Click OK.

Figure 78: Threat Prevention Device Profile

Device Profile

<input type="checkbox"/>	Realm	Name	File Categories
<input type="checkbox"/>	ps-security-lab-ams-2		
<input checked="" type="checkbox"/>		default_profile	Document (32 MB) Executable (32 MB) Library (32 MB) PDF (32 MB)

1 items

Actions

Drop connection silently

SMTP Attachments

☐

IMAP Attachments

☐

Threat Score

12345678910

8

Permit 1 - 7Block 8 - 10

☐ Include DDoS profile in policy

Log Setting

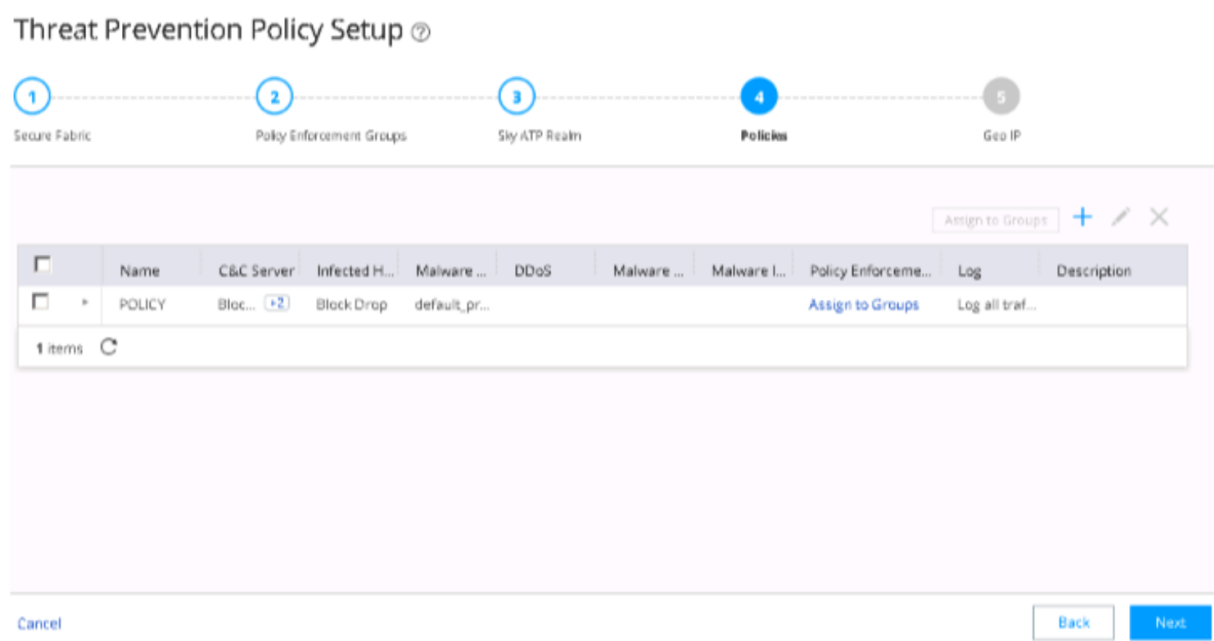
Log all traffic

Cancel

OK

9. Assign the threat prevention policy to the desired policy enforcement group by clicking *Assign to Groups*.

Figure 79: Assigning a Threat Prevention Policy to a Policy Enforcement Group



10. Select the policy enforcement group and click OK.

Figure 80: Policy Enforcement Group Selection

Assign to Policy Enforcement Groups ?

Select one or more set of policy enforcement groups to include in policy

Policy Enforcement Groups

Available0 Items

☐ Groups

>

<

Selected1 Items

☐ Groups

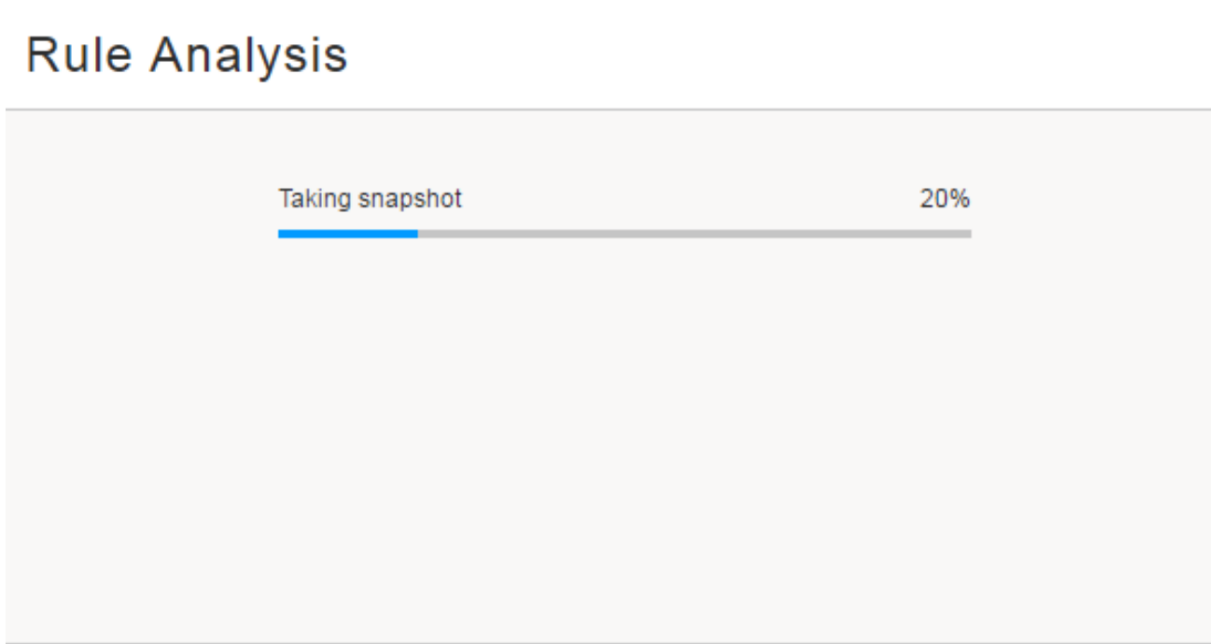
☐ IPSUBNET

Cancel

OK

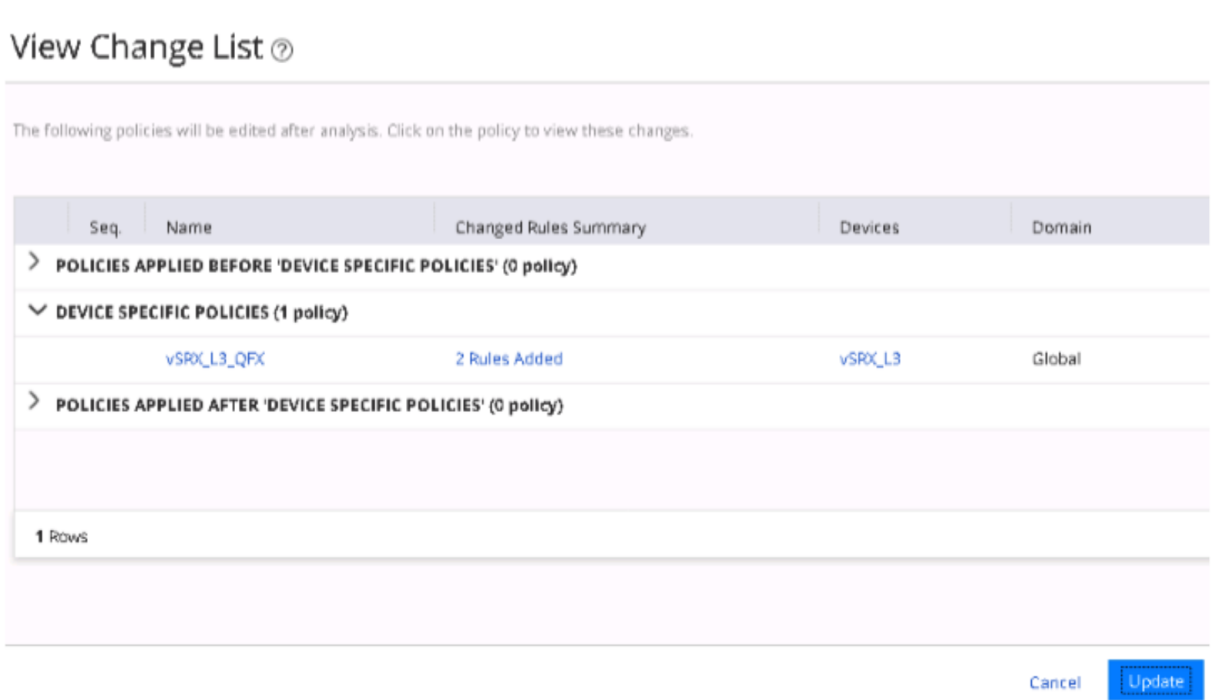
- 11. The system performs a rule analysis, and prepares device configurations that include the threat prevention policies.

Figure 81: Rule Analysis



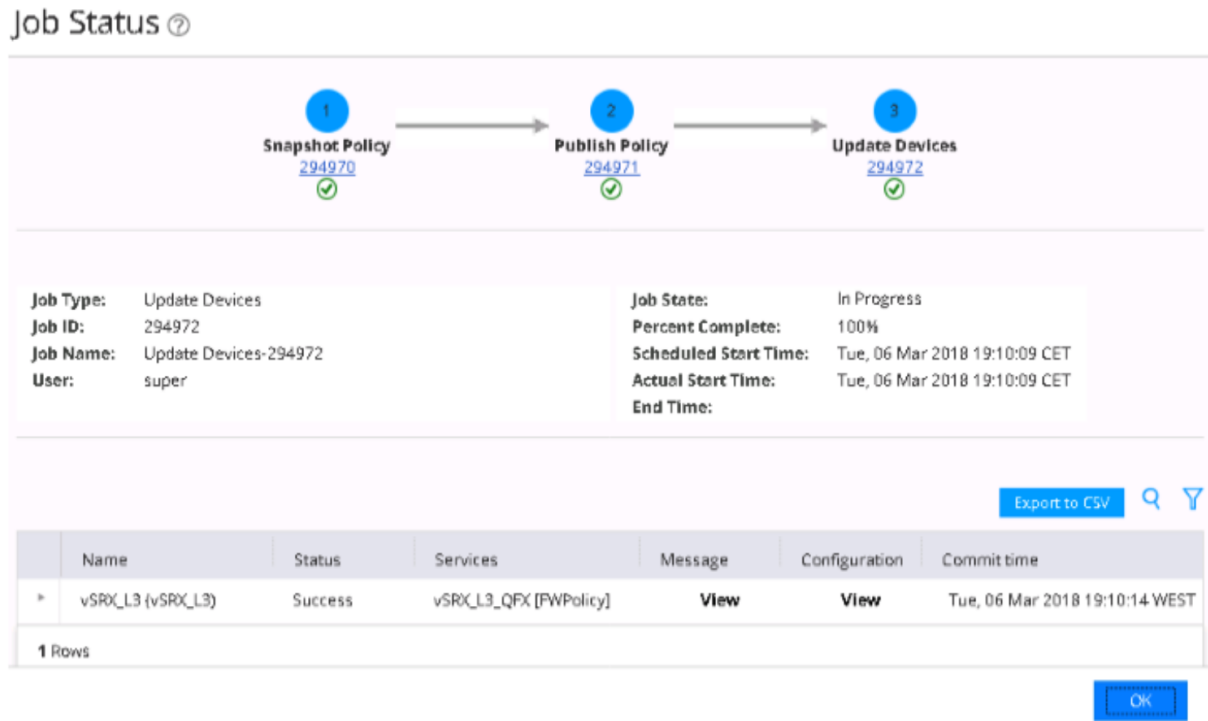
12. Once the analysis is complete, instruct the system to push the updated policy and configuration changes to the SRX Series device by clicking *Update*.

Figure 82: Updating Policy and Configuration Changes



13. When the push is complete, the system returns to the *Policies* page. Click OK.

Figure 83: Policy Update Confirmation



NOTE: If the update fails, complete the Threat Prevention Policy Guided Setup. Navigate to *Devices > Security Devices* and resynchronize your SRX with the network. Then, navigate to *Configure > Threat Prevention -> Policies*, click *Update Required* and push the update once again. If additional troubleshooting is required, you can view the configuration changes pushed onto an SRX Series device by selecting *Monitor > Job Management*.

Configuration changes pushed to the SRX device:

Figure 84: SRX Configuration

View configuration for vSRX_L3 (vSRX_L3) ?

CLI

XML

Added

Deleted

Modified

Comments

```

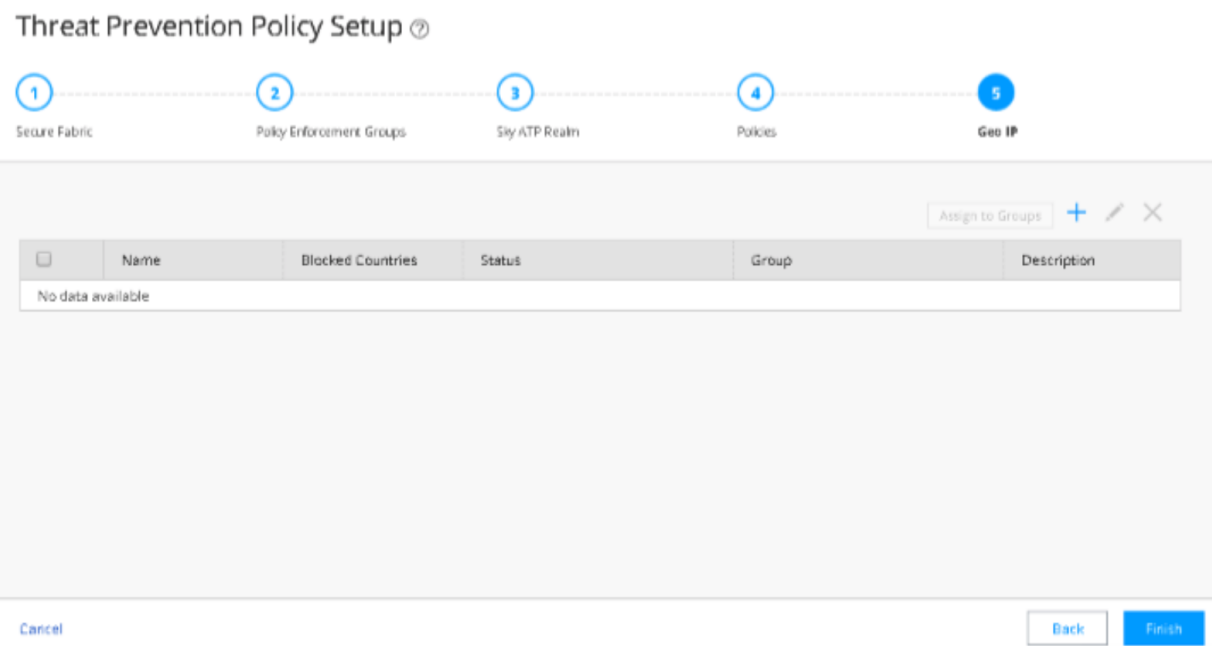
##Global address book configurations##
set security address-book global address IPSUBNET_10.10.30.0/24 10.10.30.0/24
##Security Firewall Policy : trust - untrust##
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match application any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 match source-address IPSUBNET_10.10.30.0/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit application-services advanced-anti-malware-policy POLICY
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1 then permit application-services security-intelligence-policy POLICY
##Security Firewall Policy : trust - untrust##
Insert security policies from-zone trust to-zone untrust policy default-permit after policy PolicyEnforcer-Rule1-1
##Security Firewall Policy : global ##
set security policies global policy PolicyEnforcer-Rule1-1 match application any
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address any
set security policies global policy PolicyEnforcer-Rule1-1 match source-address IPSUBNET_10.10.30.0/24
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services advanced-anti-malware-policy POLICY
set security policies global policy PolicyEnforcer-Rule1-1 then permit application-services security-intelligence-policy POLICY
##Security Intelligence Policy Configurations##
set services security-intelligence policy POLICY CC POLICY_CC
set services security-intelligence policy POLICY Infected-Hosts POLICY_Infected-Hosts
##Security Intelligence Profile Configurations##
set services security-intelligence profile POLICY_CC category CC
set services security-intelligence profile POLICY_CC rule Rule-1 match threat-level 1
set services security-intelligence profile POLICY_CC rule Rule-1 match threat-level 2
set services security-intelligence profile POLICY_CC rule Rule-1 match threat-level 3
set services security-intelligence profile POLICY_CC rule Rule-1 match threat-level 4
set services security-intelligence profile POLICY_CC rule Rule-1 then action permit
set services security-intelligence profile POLICY_CC rule Rule-1 then log
set services security-intelligence profile POLICY_CC rule Rule-2 match threat-level 5
set services security-intelligence profile POLICY_CC rule Rule-2 match threat-level 6
set services security-intelligence profile POLICY_CC rule Rule-2 match threat-level 7
set services security-intelligence profile POLICY_CC rule Rule-2 then action permit
set services security-intelligence profile POLICY_CC rule Rule-2 then log
set services security-intelligence profile POLICY_CC rule Rule-3 match threat-level 8
set services security-intelligence profile POLICY_CC rule Rule-3 match threat-level 9
set services security-intelligence profile POLICY_CC rule Rule-3 match threat-level 10
set services security-intelligence profile POLICY_CC rule Rule-3 then action block drop
set services security-intelligence profile POLICY_CC rule Rule-3 then log
set services security-intelligence profile POLICY_Infected-Hosts category Infected-Hosts
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match threat-level 1
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match threat-level 2
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match threat-level 3
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match threat-level 4
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match threat-level 5
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match threat-level 6
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 then action permit
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 then log
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 match threat-level 7
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 match threat-level 8
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 match threat-level 9
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 match threat-level 10
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 then action block drop
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 then log
##Advanced AntiMalware Policy Configurations##
set services advanced-anti-malware policy POLICY blacklist-notification log
set services advanced-anti-malware policy POLICY default-notification log
set services advanced-anti-malware policy POLICY fallback-options action permit
set services advanced-anti-malware policy POLICY fallback-options notification log
set services advanced-anti-malware policy POLICY http action block
set services advanced-anti-malware policy POLICY http inspection-profile default_profile
set services advanced-anti-malware policy POLICY http notification log
set services advanced-anti-malware policy POLICY verdict-threshold 8
set services advanced-anti-malware policy POLICY whitelist-notification log

```

OK

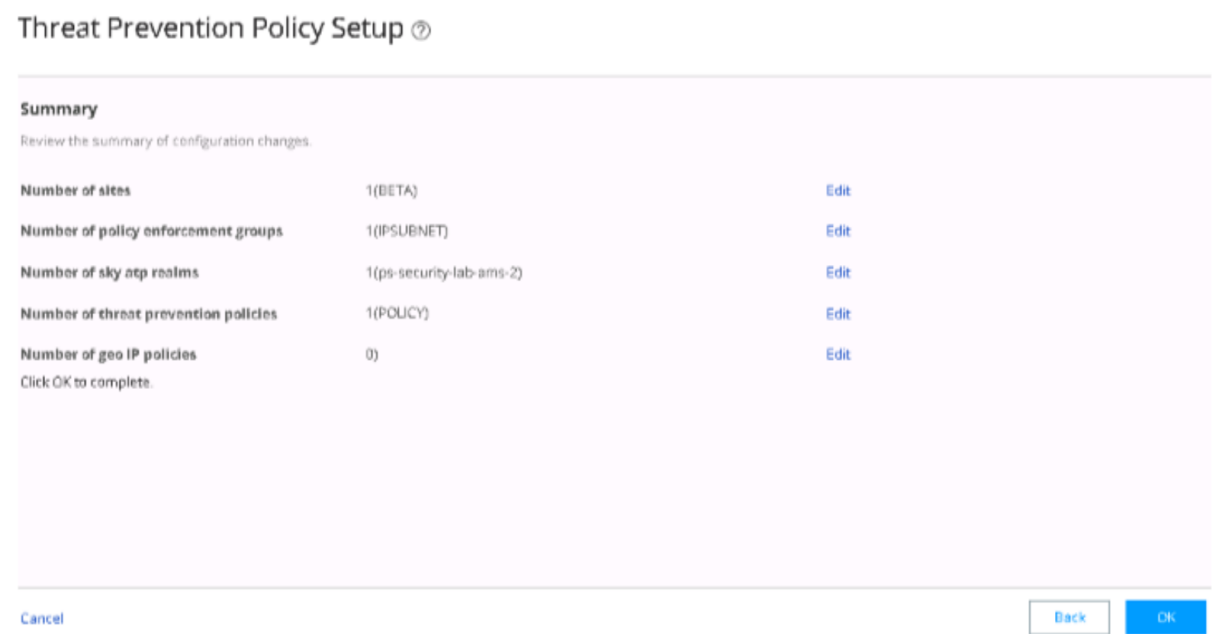
14. Click *Finish* to finalize the Threat Prevention Policy Guided Setup.

Figure 85: Threat Prevent Policy Setup



The system displays the summary of the configuration. Click OK.

Figure 86: Threat Prevention Policy Configuration Summary



Use Case Verification

IN THIS SECTION

- [Verify the Enrollment of Devices in ATP Cloud on an SRX Series Device | 110](#)
- [Verify the Enrollment of Policy Enforcer and SRX Series Devices in ATP Cloud | 111](#)
- [Verify the Enrollment of Devices with ATP Cloud in Security Director | 111](#)
- [Verify ForeScout CounterACT Functionality to Block Infected Endpoint \(with 802.1X Authentication\) | 112](#)
- [Verify ForeScout CounterACT Functionality to Quarantine Infected Endpoint \(with 802.1X Authentication\) | 116](#)
- [Verify ForeScout CounterACT Functionality to Block Infected Endpoint \(with NETCONF\) | 122](#)
- [Verify ForeScout CounterACT Functionality to Quarantine Infected Endpoint \(with NETCONF\) | 129](#)

To verify the use case configuration, perform the following actions:

Verify the Enrollment of Devices in ATP Cloud on an SRX Series Device

Purpose

Verify that the SRX Series device is connected to the ATP Cloud server.

Action

On the SRX device, use the **show services advanced-anti-malware status** CLI command.

```
user@host> show services advanced-anti-malware status
Server connection status:
  Server hostname: srxapi.eu-west-1.sky.junipersecurity.net
  Server port: 443
  Control Plane:
    Connection time: 2018-02-25 13:37:09 CET
    Connection status: Connected
  Service Plane:
    fpc0
      Connection active number: 1
      Connection retry statistics: 280
```

Meaning

The CLI output displays the **Connection status** as **Connected**. The **Server hostname** field displays the ATP Cloud server hostname.

Verify the Enrollment of Policy Enforcer and SRX Series Devices in ATP Cloud

Purpose

Verify that Policy Enforcer and the SRX Series device are enrolled with ATP Cloud.

Action

In ATP Cloud, navigate to the *Enrolled Devices* page and review the connection information for enrolled devices, including the serial number, model number, tier level (free, basic, premium) enrollment status in ATP Cloud, last telemetry activity, and last activity seen.

Figure 87: Verifying Enrolled Devices in ATP Cloud

Devices / All Devices

Enrolled Devices ?

Enroll

Disenroll

Device Lookup

Remove

<input type="checkbox"/>	Serial Number	Host	Model Num...	Tier	Submission State	Last Telemetry Activity	Last Activity	License Expires
<input checked="" type="checkbox"/>	UN7302CE3...	ps-vm34.jtac...	PolicyEnforcer	premium	allowed		24 Feb 2018 18:56	Unlimited
<input type="checkbox"/>	ED08A7FF4...	vSRX_L3_QFX	VSRX	premium	allowed		25 Feb 2018 12:39	10 Nov 2026 06:06

Meaning

The *Host* field displays details for the enrolled firewall (vSRX_L3_QFX) and for the Policy Enforcer device. You can click the serial numbers for more details.

Verify the Enrollment of Devices with ATP Cloud in Security Director

Purpose

Verify that the SRX Series device enrolled with ATP Cloud in Security Director.

Action




In Security Directory, navigate to *Devices > Secure Fabric*.


Figure 88: Verifying Device Enrollment in Security Director

Devices / Secure Fabric

Secure Fabric ?

Sites Add Enforcement Points + ✎ ✕

	Site	Enforcement Points	IP	Model	SKYATP Enroll ...	Last Updated	Descripti...
<input type="checkbox"/>	BETA	vSRX_L3_QFX 	172.30.77.230	VSRX		March 06, 2018	
		FS 	172.30.77.100	Connector			

1 items 

Meaning

A green dot with checkmark displays in the *SkyATP Enroll Status* field and confirms the enrollment of the SRX Series device with the ATP Cloud realm.

Verify ForeScout CounterACT Functionality to Block Infected Endpoint (with 802.1X Authentication)

Purpose

Test the ForeScout CounterACT integration and functionality when an endpoint is infected. In this example, you verify when the enforcement policy is configured to block the infected host with 802.1X authentication.

Action

NOTE: A client VM or physical PC is required to trigger an attack.

Before the attack, confirm the following:

- Confirm that Windows Supplciant is authenticated and in User VLAN (vlan31).

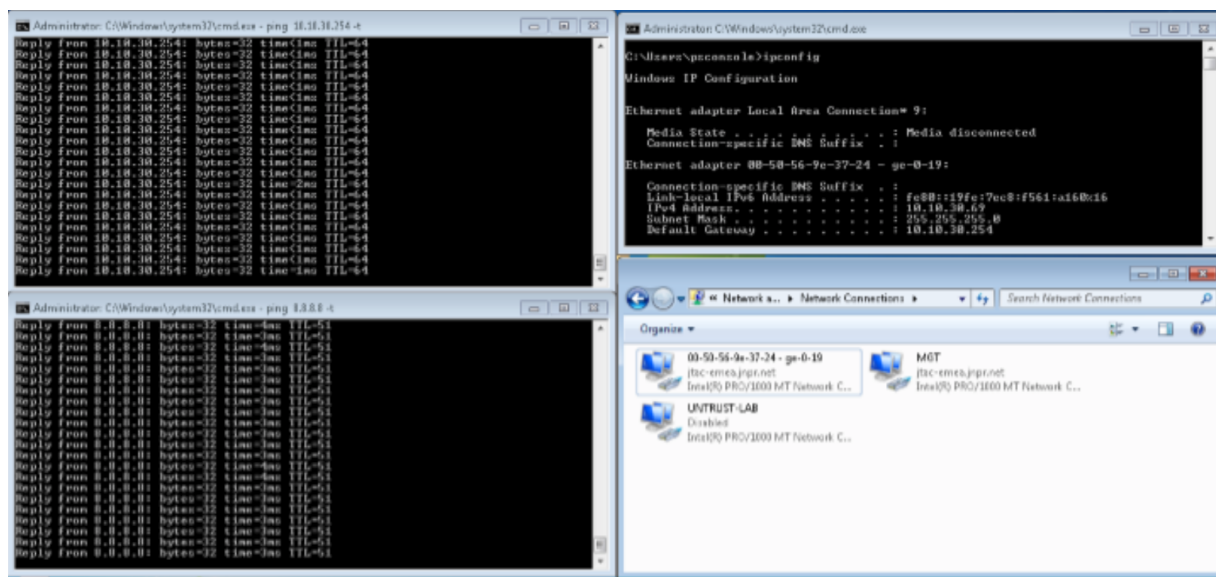
```
user@host> show vlans 31
Name Tag Interfaces
vlan31 31 ge-0/0/0/18.0*, ge-0/0/0/19.0*

user@host>
```

- Confirm that the endpoint 10.10.30.69 can ping to Internet (IP address 8.8.8.8) and Layer 2 connected default gateway (10.10.30.254). Before the attack, the endpoint starts continuous pings to other endpoints on the LAN and Internet.

The endpoint pings the C&C server on the Internet from Windows Supplciant (in this example from the IP address 184.75.221.43).

Figure 89: Confirming Ping from Windows Supplicant

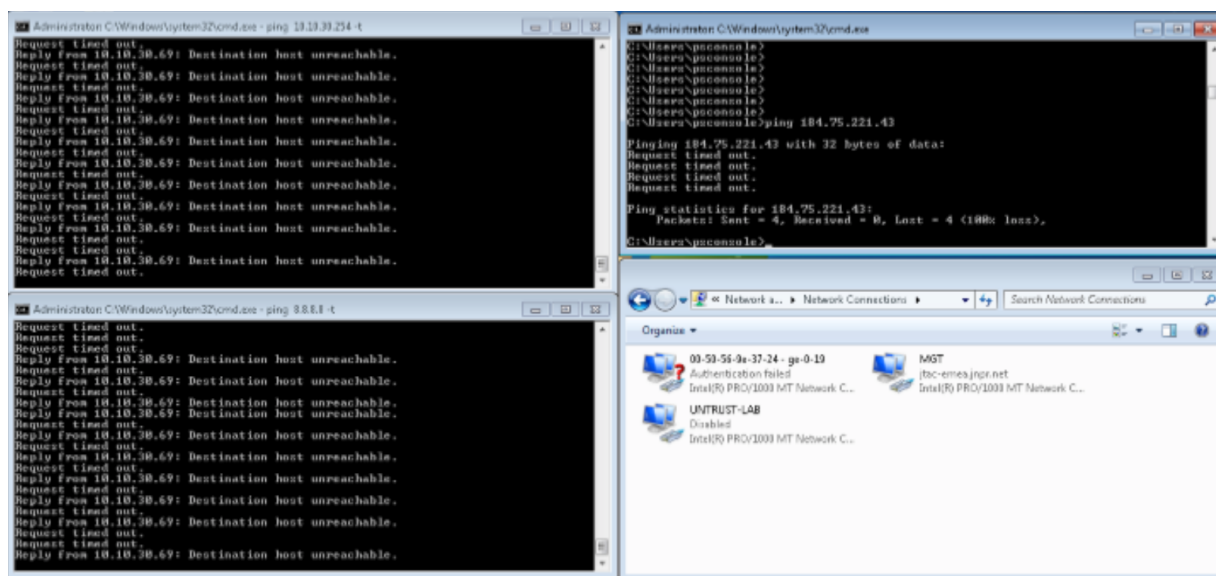


After the attack, the 802.1X session is terminated with RADIUS CoA on the EX4300 switch initiated by ForeScout CounterACT.

Confirm the following:

- Confirm that Windows Supplicant cannot connect to the Internet or the LAN anymore.

Figure 90: Confirming Ping from Windows Supplicant is Blocked After the Attack



- After the RADIUS CoA disconnect message, confirm that the Windows Supplicant is not in User VLAN (vlan31) anymore but in the default VLAN.

- Confirm that further authentication requests are rejected by ForeScout CounterACT.

```
user@host> show vlans default
```

```
Name Tag Interfaces
```

```
default ge-0/0/0/19.0*
```

```
user@host>
```

```
user@host> show vlans 31
```

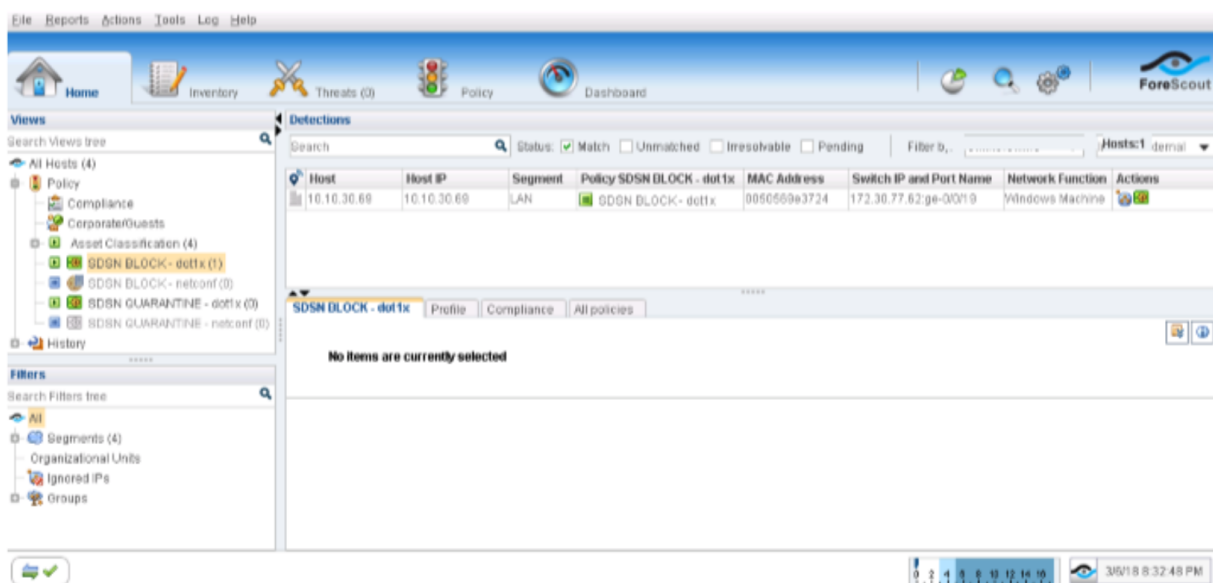
```
Name Tag Interfaces
```

```
vlan31 31 ge-0/0/0/18.0*
```

```
user@host>
```

- Confirm the SDSN BLOCK (dot1x) policy match and automated threat remediation action details by navigating to *ForeScout CounterACT* > *Home*.

Figure 91: 802.1X SDSN Block Policy Match Verification



- Navigate to *Log* > *Host Log*. Review the details for the SDSN BLOCK (dot1x) policy.

Figure 92: 802.1X Host Log

Host Log 10.10.30.69

File Edit

Host Log

Filter: Not ☐ All ☐ Match Text

Time	Host	Details	MAC Address
3/6/18 8:23:42 PM	10.10.30.69	802.1x Last Rejected Authentication Time - 3/6/18 8:23:42 PM	0050569e3724
3/6/18 8:23:42 PM	10.10.30.69	802.1x RADIUS Authentication State - RADIUS-Rejected	0050569e3724
3/6/18 8:23:42 PM	10.10.30.69	802.1x RADIUS Log Details - 802.1x RADIUS Log Details no longer includes T...	0050569e3724
3/6/18 8:23:42 PM	10.10.30.69	802.1x Authorization Source - Policy Action	0050569e3724
3/6/18 8:23:42 PM	10.10.30.69	802.1x RADIUS Imposed Authorization - reject	0050569e3724
3/6/18 8:23:42 PM	10.10.30.69	802.1x Last Successful Authentication Time - 3/6/18 8:23:42 PM	0050569e3724
3/6/18 8:23:42 PM	10.10.30.69	802.1x Last Authentication Time - 3/6/18 8:23:42 PM	0050569e3724
3/6/18 8:23:42 PM	10.10.30.69	802.1x Accounting session ID - 802.1x81e915ce0009d900	0050569e3724
3/6/18 8:23:41 PM	10.10.30.69	802.1x Authorize Action Summary - Authorization action complete; [1:reauth res...	0050569e3724
3/6/18 8:23:41 PM	10.10.30.69	Policy"SDSN BLOCK - dot1x" - Action completed reauth response: reauth succ...	0050569e3724
3/6/18 8:23:40 PM	10.10.30.69	802.1x Requested Authorize Action - reject	0050569e3724
3/6/18 8:23:40 PM	10.10.30.69	Policy"SDSN BLOCK - dot1x" - Executing action - 802.1x Authorize. Details: 80...	0050569e3724
3/6/18 8:23:40 PM	10.10.30.69	block - Yes	0050569e3724
3/6/18 8:23:40 PM	10.10.30.69	Policy"SDSN BLOCK - dot1x" - Host evaluation changed from "SDSN BLOCK -...	0050569e3724
3/6/18 7:56:09 PM	10.10.30.69	802.1x RADIUS Log Details - Tue Mar 6 19:56:06 2018: Acct-Authentic = RADIU...	0050569e3724

34 items (0 selected)

Done

Close

- Confirm that the Windows Supplicant's IP address was also added to the Infected-Hosts Feed on the SRX Series device to block Internet access.

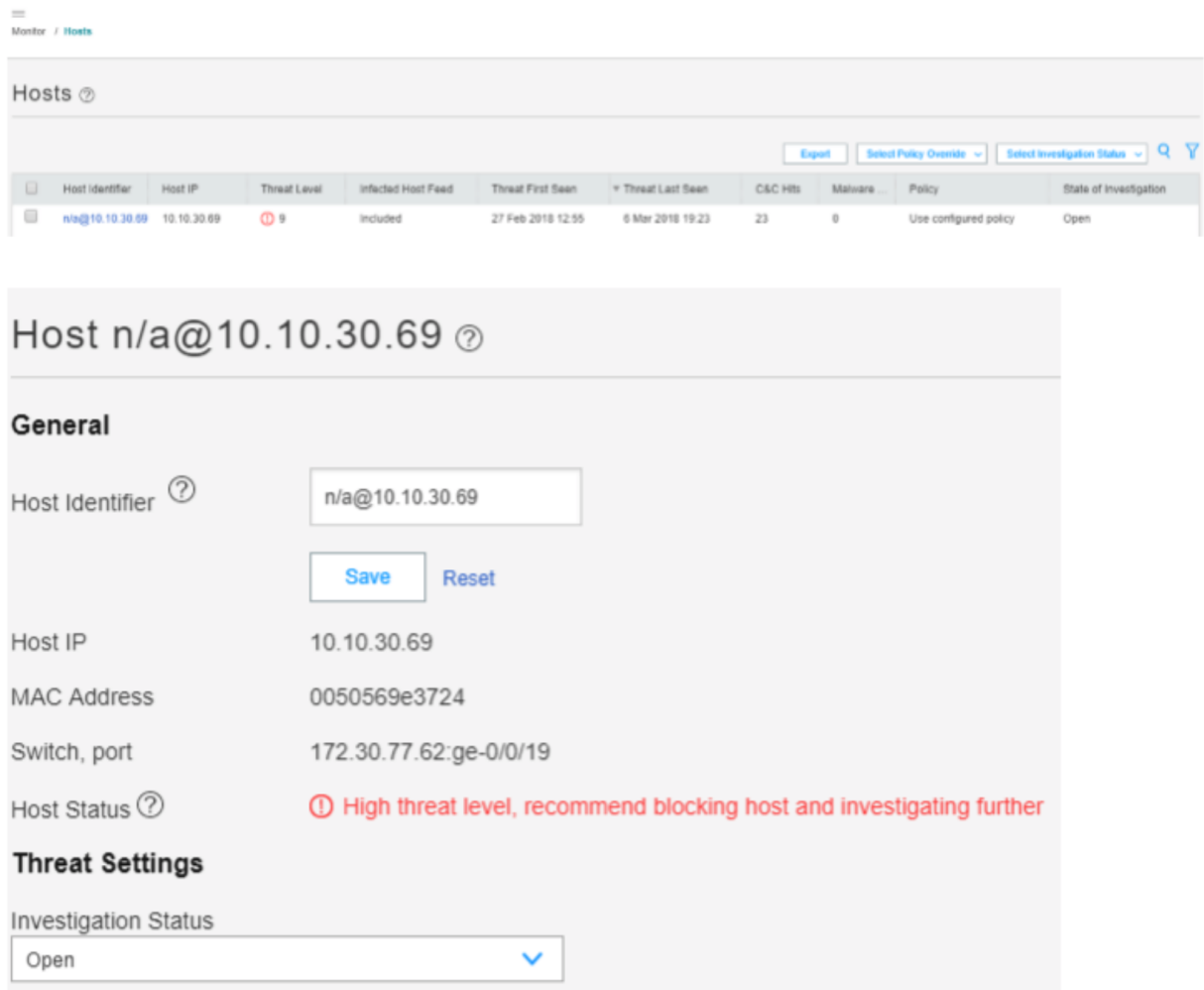
```

user@vSRX_L3> show security dynamic-address category-name Infected-Hosts
No.  IP-start  IP-end  Feed      Address
1   10.10.30.69 10.10.30.69 Infected-Hosts/1 ID-2150001a
Total number of matching entries: 1
user@vSRX_L3>

```

- In the ATP Cloud portal, navigate to *Monitor > Hosts*. Confirm the host IP address (10.10.30.69), MAC-ID, and switch port of the Windows Supplicant.

Figure 93: ATP Cloud Host Monitoring



Meaning

All ping sessions show that the traffic is blocked after the threat was detected, confirming that the automated threat remediation use case is working properly.

The *Hosts* page lists compromised hosts and their associated threat levels. The output confirms that ATP Cloud and Security Director have detected the infected host. You can monitor and mitigate malware detections on a per host basis.

Verify ForeScout CounterACT Functionality to Quarantine Infected Endpoint (with 802.1X Authentication)

Purpose

Test the ForeScout CounterACT integration and functionality when an endpoint is infected. In this example, you verify when the enforcement policy is configured to quarantine the infected host with 802.1X authentication.

Action

NOTE: A client VM or physical PC is required to trigger an attack.

Before the attack, confirm the following:

- Release the infected host on the ATP Cloud portal or in Security Director (*Monitor > Threat Prevention > Hosts*).
- Ensure that Internet or LAN access is restored for the Windows Supplicant.
- On the *Policy Enforcer > Threat Prevention Policy* page, change infected host profile actions to *Quarantine* and add the VLAN ID as *vlan32*. Click *OK*.

Figure 94: Threat Prevention Policy Pre-Attack Configuration

Modify Threat Prevention Policy ⓘ

Actions: Drop connection silently (recommended) ▼

☒ Include infected host profile in policy

Select an action to apply to infected hosts:

Actions: Quarantine ▼

vlan32

☒ Include malware profile in policy

HTTP File Download ⓘ ☒

Select a file scanning device profile and threat score ranges to apply to HTTP and HTTPS traffic.

Cancel OK

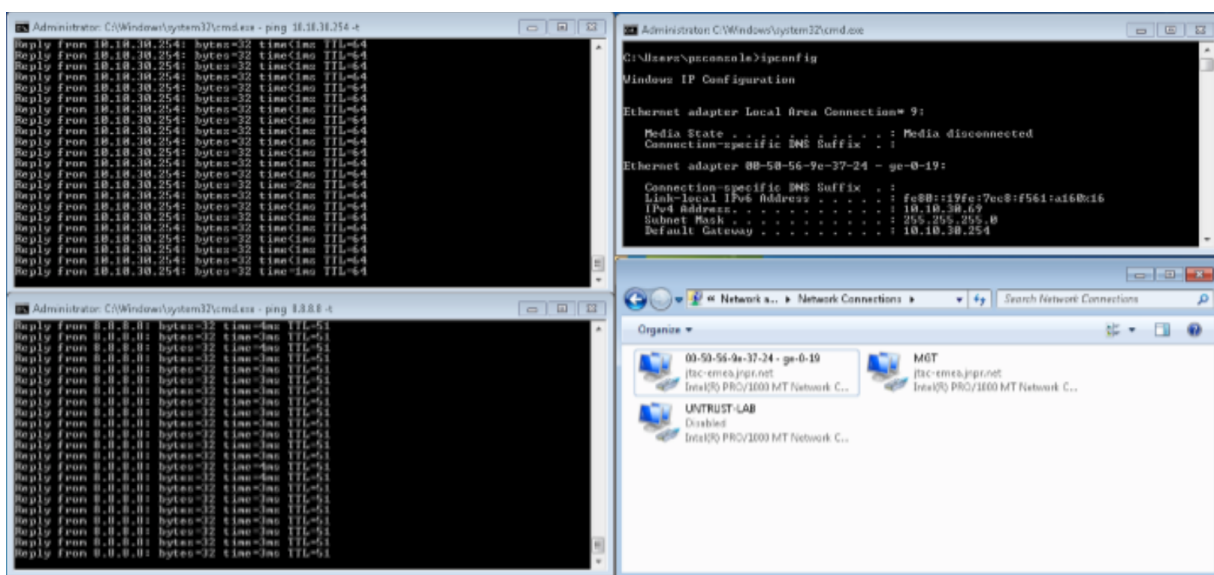
- Confirm that Windows Supplicant is authenticated and in User VLAN (vlan31).

```
user@host> show vlans 31
Name Tag Interfaces
vlan31 31 ge-0/0/0/18.0*, ge-0/0/0/19.0*
```

```
user@host>
```

- Confirm that the endpoint 10.10.30.69 can ping to Internet (IP address 8.8.8.8) and Layer 2 connected default gateway (10.10.30.254). Before the attack, the endpoint starts continuous pings to other endpoints on the LAN and Internet.

Figure 95: Confirming Ping from Windows Supplication Before the Attack



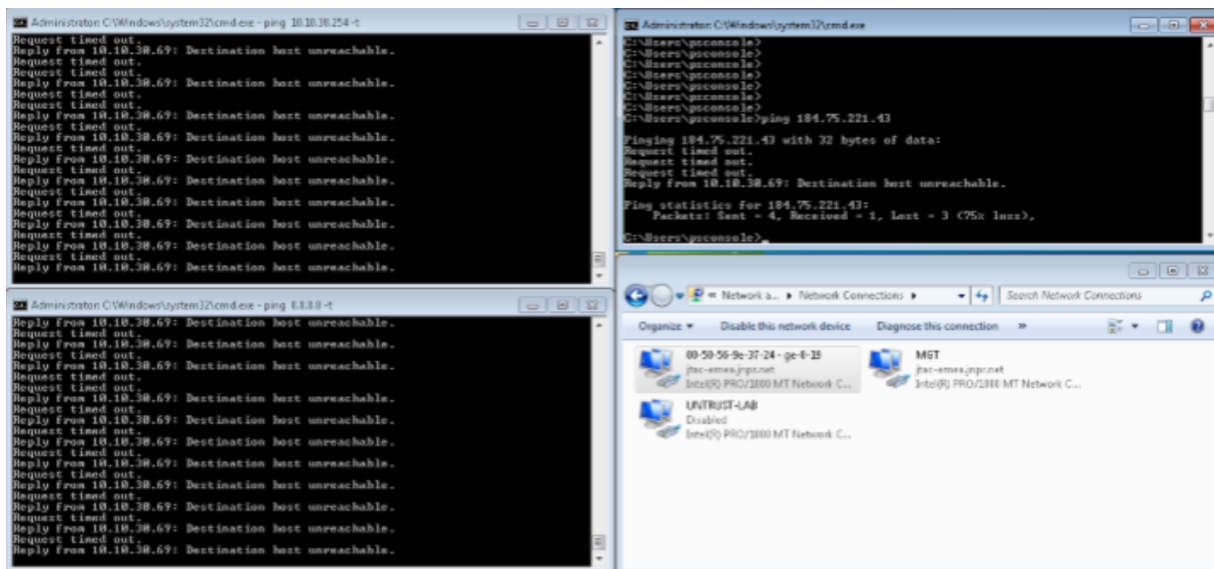
The endpoint pings the C&C server on the Internet from Windows Supplication (in this example from the IP address 184.75.221.43).

After the attack, the 802.1X session is terminated with RADIUS CoA on the EX4300 switch initiated by ForeScout CounterACT.

Confirm the following:

- Confirm that Windows Supplicant re-authenticates and is automatically moved into Quarantine VLAN (vlan32). As a result, the Windows Supplicant cannot connect to the Internet or the LAN anymore.

Figure 96: Confirm Traffic is Moved to Quarantine VLAN After Attack



- After the RADIUS CoA disconnect message and re-authentication, confirm that the Windows Supplicant is now in Quarantine VLAN (vlan32).
- Confirm that further authentication requests are rejected by ForeScout CounterACT.

```
user@host> show vlans default
```

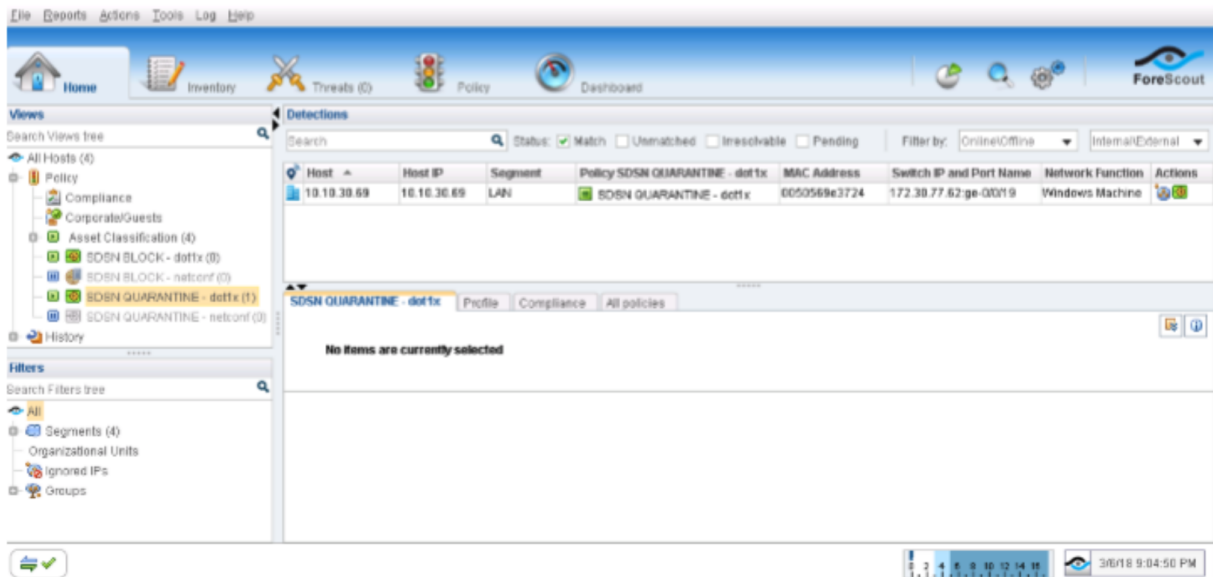
```
Name Tag Interfaces
default ge-0/0/0/19.0*
user@host>
```

```
user@host> show vlans 32
```

```
Name Tag Interfaces
vlan32 32 ge-0/0/0/19.0*
user@host>
```

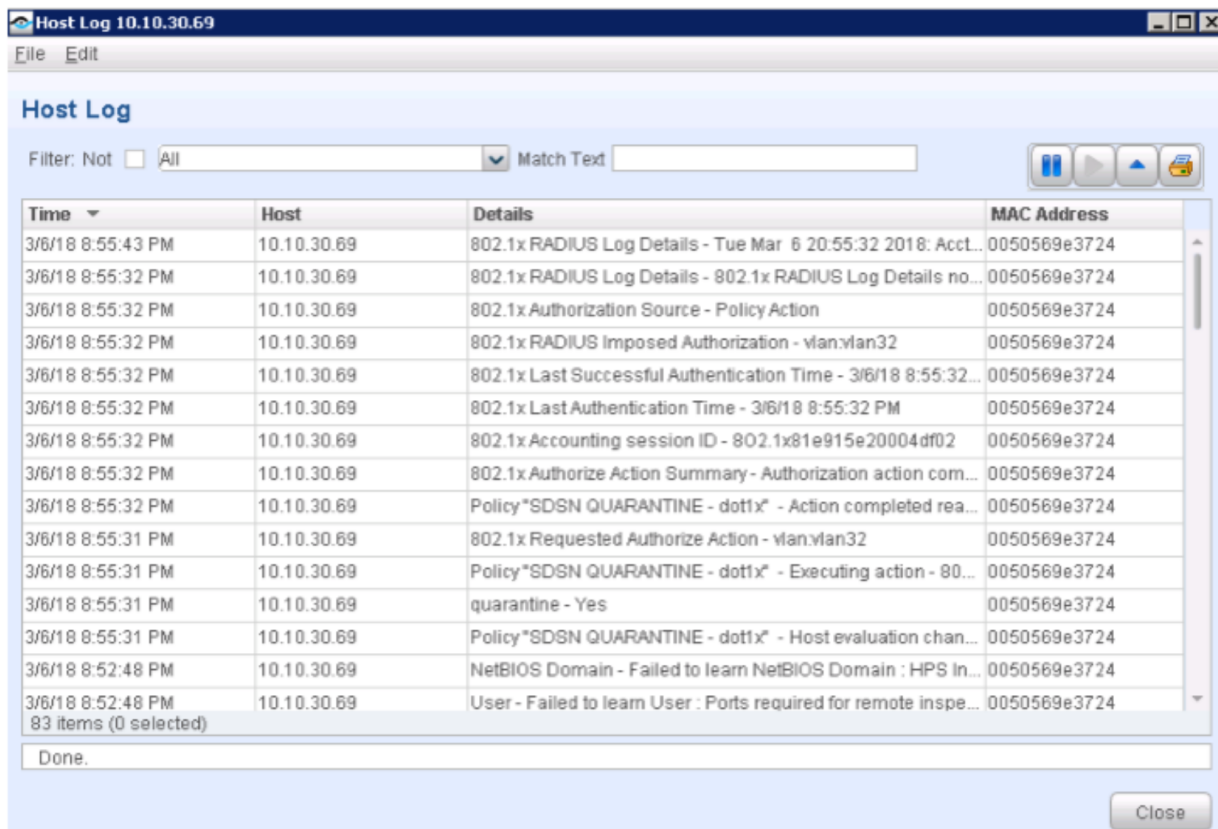
- Confirm the SDN QUARANTINE (dot1x) policy match and automated threat remediation action details by navigating to *ForeScout CounterACT > Home*.

Figure 97: 802.1X SDSN Quarantine Policy Match



- Navigate to *Log > Host Log*. Review the details for the SDSN QUARANTINE (dot1x) policy.

Figure 98: 802.1X SDSN Quarantine Host Log



- Confirm that the Windows Supplicant's IP address was also added to the Infected-Hosts Feed on the SRX Series device to block Internet access.

```
user@vSRX_L3> show security dynamic-address category-name Infected-Hosts
```

```
No.  IP-start  IP-end  Feed      Address
1   10.10.30.69 10.10.30.69 Infected-Hosts/1 ID-2150001a
Total number of matching entries: 1
user@vSRX_L3>
```

- In the ATP Cloud portal, navigate to *Monitor > Hosts*. Confirm the host IP address (10.10.30.69), MAC-ID, and switch port of the Windows Supplicant.

Figure 99: Confirming Host Details in ATP Cloud

The screenshot displays the ATP Cloud portal interface. At the top, there's a navigation bar with 'Monitor / Hosts'. Below it, a table lists hosts. The first host is 'n/a@10.10.30.69' with a threat level of 9. The table columns include Host Identifier, Host IP, Threat Level, Infected Host Feed, Threat First Seen, Threat Last Seen, C&C Hits, Malware, Policy, and State of Investigation.

Below the table, the details for the selected host 'n/a@10.10.30.69' are shown. The 'General' section includes fields for Host Identifier (n/a@10.10.30.69), Host IP (10.10.30.69), MAC Address (0050569e3724), Switch, port (172.30.77.62:ge-0/0/19), and Host Status (High threat level, recommend blocking host and investigating further). The 'Threat Settings' section shows the Investigation Status as 'Open'.

Meaning

The output shows that the ATP Cloud infected host feed containing the Windows Supplciant's IP address 10.10.30.69 has been successfully downloaded, resulting in the SRX device taking an action to quarantine the IP address.

The *Hosts* page lists compromised hosts and their associated threat levels. The output confirms that ATP Cloud and Security Director have detected and quarantined the infected host. You can monitor and mitigate malware detections on a per host basis. You can also drill down and verify why the host is marked as infected (for this use case, the C&C server IP address). For malware, details of the downloaded file display.

Verify ForeScout CounterACT Functionality to Block Infected Endpoint (with NETCONF)

Purpose

Test the ForeScout CounterACT integration and functionality when an endpoint is infected. In this example, you verify when the enforcement policy is NETCONF, and it is configured block the infected host.

Action

NOTE: A client VM or physical PC is required to trigger an attack.

Before the attack, confirm the following:

- On the *Policy Enforcer > Threat Prevention Policy* page, change infected host profile actions to *Drop connection silently*. Click OK.

Figure 100: Drop Connection Silently Option

Modify Threat Prevention Policy ?

☒ Include infected host profile in policy

Select an action to apply to infected hosts.

Actions

Drop connection silently ▾

☒ Include malware profile in policy

HTTP File Download ? ☒

Select a file scanning device profile and threat score ranges to apply to HTTP and HTTPS traffic.

Scan HTTPS ? ☐

Device profile

default_profile

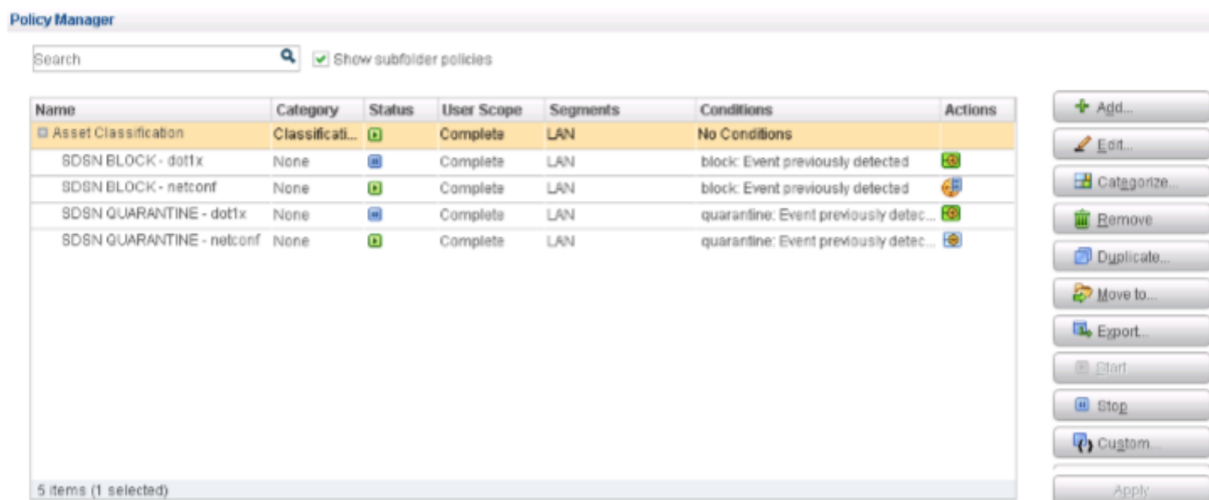
Change

Cancel

OK

- Navigate to the Policies tab. From the Console, stop both SDSN BLOCK-dot1x and SDSN QUARANTINE-dot1x polices, and start both SDSN BLOCK-NETCONF and SDSN QUARANTINE-NETCONF policies.

Figure 101: Policies Tab in Policy Manager



- Confirm that the Linux host is in User VLAN (vlan31) with IP address 10.10.30.99.

Figure 102: Linux Host Confirmation

```
[root@BATPLANE ~]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:50:56:94:32:19
          inet addr:10.10.30.99  Bcast:10.10.30.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe94:3219/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2744588  errors:1688  dropped:0  overruns:0  frame:0
          TX packets:2290151  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:288738294 (275.3 MiB)  TX bytes:182048224 (173.6 MiB)
          Interrupt:67  Base address:0x2080

[root@BATPLANE ~]#
root@vqfx-re> show ethernet-switching table

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C - Control MAC
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)

Ethernet switching table : 4 entries, 4 learned
Routing instance : default-switch

```

vlan name	MAC address	MAC flags	Age	Logical interface	NH Index	RTR ID
vlan31	00:50:56:94:00:d4	D	-	xe-0/0/0.0	0	0
vlan31	00:50:56:94:32:19	D	-	xe-0/0/1.0	0	0
vlan31	00:50:56:94:47:cc	D	-	xe-0/0/0.0	0	0
vlan31	00:50:56:9e:37:24	D	-	xe-0/0/0.0	0	0

```

{master:0}
root@vqfx-re> show vlans vlan31

Routing instance      VLAN name      Tag      Interfaces
default-switch       vlan31        31       xe-0/0/0.0*
                   xe-0/0/1.0*

{master:0}
root@vqfx-re> █

```

- Confirm that the endpoint 10.10.30.99 can ping to Internet (IP address 8.8.8.8) and Layer 2 connected default gateway (10.10.30.254). Before the attack, the endpoint starts continuous pings to other endpoints on the LAN and Internet.

Figure 103: Internet Ping

```
[root@BATPLANE ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=8.00 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=7.77 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=8.03 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=8.49 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 7.775/8.080/8.497/0.261 ms
[root@BATPLANE ~]# ping 10.10.30.254
PING 10.10.30.254 (10.10.30.254) 56(84) bytes of data.
64 bytes from 10.10.30.254: icmp_seq=1 ttl=64 time=4.59 ms
64 bytes from 10.10.30.254: icmp_seq=2 ttl=64 time=11.6 ms
64 bytes from 10.10.30.254: icmp_seq=3 ttl=64 time=4.38 ms
64 bytes from 10.10.30.254: icmp_seq=4 ttl=64 time=4.54 ms

--- 10.10.30.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 4.386/6.300/11.678/3.107 ms
[root@BATPLANE ~]# █
```

The endpoint pings the C&C server on the Internet from the Linux host (in this example from the IP address 184.75.221.43).

Figure 104: C&C Server Ping

```
[root@BATPLANE ~]# ping 184.75.221.43
PING 184.75.221.43 (184.75.221.43) 56(84) bytes of data.

--- 184.75.221.43 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9001ms
```

After the attack, ForeScout CounterACT applies ACL on the QFX switch using NETCONF. Confirm the following:

- Confirm that the Linux host cannot connect to the Internet or the LAN anymore.

Figure 105: Confirming Disconnected Linux Host

```

root@vqfx-re> show configuration firewall | display set
set firewall family ethernet-switching filter forescout_acl term rule1 from source-mac-address 00:50:56:94:32:19/48
set firewall family ethernet-switching filter forescout_acl term rule1 then discard
set firewall family ethernet-switching filter forescout_acl term rule2 then accept
{master:0}
root@vqfx-re> █

[root@BATPLANE ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 10.10.30.99 icmp_seq=2 Destination Host Unreachable
From 10.10.30.99 icmp_seq=3 Destination Host Unreachable
From 10.10.30.99 icmp_seq=4 Destination Host Unreachable
From 10.10.30.99 icmp_seq=6 Destination Host Unreachable
From 10.10.30.99 icmp_seq=7 Destination Host Unreachable
From 10.10.30.99 icmp_seq=8 Destination Host Unreachable

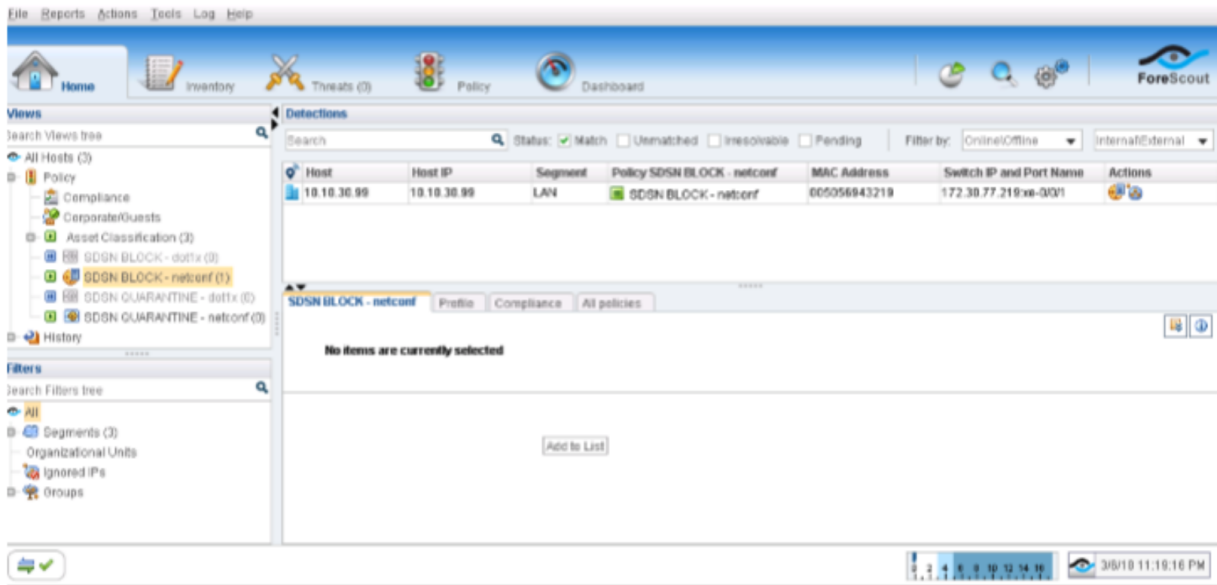
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7999ms
, pipe 3
[root@BATPLANE ~]# ping 10.10.30.254
PING 10.10.30.254 (10.10.30.254) 56(84) bytes of data.
From 10.10.30.99 icmp_seq=2 Destination Host Unreachable
From 10.10.30.99 icmp_seq=3 Destination Host Unreachable
From 10.10.30.99 icmp_seq=4 Destination Host Unreachable
From 10.10.30.99 icmp_seq=6 Destination Host Unreachable
From 10.10.30.99 icmp_seq=7 Destination Host Unreachable
From 10.10.30.99 icmp_seq=8 Destination Host Unreachable

--- 10.10.30.254 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7000ms
, pipe 3
[root@BATPLANE ~]# █

```

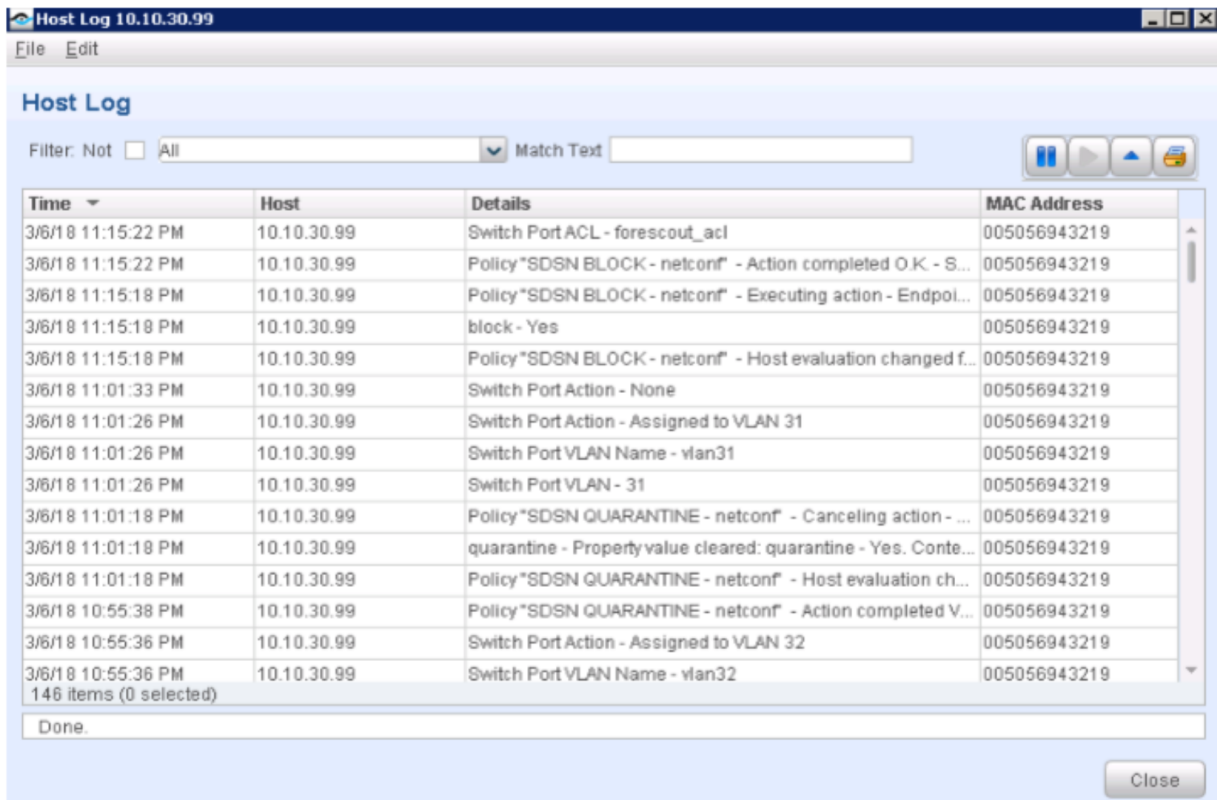
- Confirm the SDSN BLOCK (NETCONF) policy match and automated threat remediation action details by navigating to *ForeScout CounterACT > Home*.

Figure 106: Confirming Policy Match and Automated Threat Remediation Details



- Navigate to *Log > Host Log*. Review the details for the SDSN BLOCK (NETCONF) policy.

Figure 107: SDSN Block Host Log



- Confirm that the Linux host's IP address was also added to the Infected-Hosts Feed on the SRX Series device to block Internet access.

```

user@vSRX_L3> show security dynamic-address category-name Infected-Hosts
No.  IP-start  IP-end  Feed      Address
1   10.10.30.99 10.10.30.99 Infected-Hosts/1 ID-2150001a
Total number of matching entries: 1
user@vSRX_L3>

```

- In the ATP Cloud portal, navigate to *Monitor > Hosts*. Confirm the host IP address (10.10.30.99), MAC-ID, and switch port of the Linux host.

Figure 108: Confirming Host Information in ATP Cloud Portal

The screenshot displays the ATP Cloud portal interface. At the top, the breadcrumb navigation shows 'Monitor / Hosts'. Below this, the 'Hosts' section header is visible. A table lists host information, with one entry selected: 'n/a@10.10.30.99'. The table columns include Host Identifier, Host IP, Threat Level (indicated by a red circle with a '9'), Infected Host Feed (Included), Threat First Seen (27 Feb 2018 18:20), Threat Last Seen (9 Mar 2018 22:14), C&C Hits (17), Malware (0), Policy (Use configured policy), and State of Investigation (Open). Below the table, the 'Host n/a@10.10.30.99' details are shown. The 'General' section includes fields for Host Identifier (n/a@10.10.30.99), Host IP (10.10.30.99), MAC Address (005056943219), Switch, port (172.30.77.219:xe-0/0/1), and Host Status (High threat level, recommend blocking host and investigating further). The 'Threat Settings' section shows the Investigation Status as 'Open'.

Monitor / Hosts

Hosts

Export Select Policy Override Select Investigation Status

Host Identifier	Host IP	Threat Level	Infected Host Feed	Threat First Seen	Threat Last Seen	C&C Hits	Malware	Policy	State of Investigation
n/a@10.10.30.99	10.10.30.99	9	Included	27 Feb 2018 18:20	9 Mar 2018 22:14	17	0	Use configured policy	Open

Monitor / Hosts

Host n/a@10.10.30.99

General

Host Identifier Save Reset

Host IP

MAC Address

Switch, port

Host Status

Threat Settings

Investigation Status

Meaning

All ping sessions show that the traffic is blocked after the threat was detected, confirming that the automated threat remediation use case is working properly.

The *Hosts* page lists compromised hosts and their associated threat levels. The output confirms that ATP Cloud and Security Director have detected the infected host. You can monitor and mitigate malware detections on a per host basis.

Verify ForeScout CounterACT Functionality to Quarantine Infected Endpoint (with NETCONF)

Purpose

Test the ForeScout CounterACT integration and functionality when an endpoint is infected. In this example, you verify when the enforcement policy NETCONF, and it is configured to quarantine the infected host.

Action

NOTE: A client VM or physical PC is required to trigger an attack.

Before the attack, confirm the following:

- Release the infected host on the ATP Cloud portal or in Security Director (*Monitor > Threat Prevention > Hosts*).
- Ensure that Internet or LAN access is restored for the Linux host.
- On the *Policy Enforcer > Threat Prevention Policy* page, change infected host profile actions to *Quarantine* and add the VLAN ID as `vlan32`. Click *OK*.

Figure 109: Changing Threat Prevention Policy to Quarantine

Modify Threat Prevention Policy ?

Actions Drop connection silently (recommended) ▾

☒ Include infected host profile in policy

Select an action to apply to infected hosts.

Actions Quarantine ▾

vlan32

☒ Include malware profile in policy

HTTP File Download ? ☒

Select a file scanning device profile and threat score ranges to apply to HTTP and HTTPS traffic.

Cancel OK

- Confirm that the Linux host is in User VLAN (vlan31) with IP address 10.10.30.99.

Figure 110: Confirming Linux Host Details

```
[root@BATPLANE ~]# ifconfig eth1
eth1      Link encap:Ethernet  Hwaddr 00:50:56:94:32:19
          inet addr:10.10.30.99  Bcast:10.10.30.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe94:3219/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2744588 errors:1688 dropped:0 overruns:0 frame:0
          TX packets:2290151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:288738294 (275.3 MiB)  TX bytes:182048224 (173.6 MiB)
          Interrupt:67 Base address:0x2080

[root@BATPLANE ~]#

root@vqfx-re> show ethernet-switching table

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned, P - Persistent static, C - Control MAC
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC, O - ovsdb MAC)

Ethernet switching table : 5 entries, 5 learned
Routing instance : default-switch

```

Vlan name	MAC address	MAC flags	Age	Logical interface	NH Index	RTR ID
vlan31	00:50:56:94:00:d4	D	-	xe-0/0/0.0	0	0
vlan31	00:50:56:94:32:19	D	-	xe-0/0/1.0	0	0
vlan31	00:50:56:94:47:cc	D	-	xe-0/0/0.0	0	0
vlan31	00:50:56:9e:37:24	D	-	xe-0/0/0.0	0	0
vlan31	06:50:56:94:66:00	D	-	xe-0/0/0.0	0	0

```
{master:0}
root@vqfx-re> show vlans

Routing instance      VLAN name      Tag      Interfaces
default-switch       default       1
default-switch       vlan31       31
                     xe-0/0/0.0*
                     xe-0/0/1.0*
default-switch       vlan32       32

{master:0}
root@vqfx-re>

root@vqfx-re> show configuration interfaces xe-0/0/1 | display set
set interfaces xe-0/0/1 unit 0 description Linux_Host_vSWITCH
set interfaces xe-0/0/1 unit 0 family ethernet-switching interface-mode access
set interfaces xe-0/0/1 unit 0 family ethernet-switching vlan members vlan31

{master:0}
root@vqfx-re>
```

- Confirm that the endpoint 10.10.30.99 can ping to Internet (IP address 8.8.8.8) and Layer 2 connected default gateway (10.10.30.254). Before the attack, the endpoint starts continuous pings to other endpoints on the LAN and Internet.

Figure 111: Confirming Internet Connectivity

```
[root@BATPLANE ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=8.00 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=7.77 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=8.03 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=8.49 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 7.775/8.080/8.497/0.261 ms
[root@BATPLANE ~]# ping 10.10.30.254
PING 10.10.30.254 (10.10.30.254) 56(84) bytes of data.
64 bytes from 10.10.30.254: icmp_seq=1 ttl=64 time=4.59 ms
64 bytes from 10.10.30.254: icmp_seq=2 ttl=64 time=11.6 ms
64 bytes from 10.10.30.254: icmp_seq=3 ttl=64 time=4.38 ms
64 bytes from 10.10.30.254: icmp_seq=4 ttl=64 time=4.54 ms

--- 10.10.30.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 4.386/6.300/11.678/3.107 ms
[root@BATPLANE ~]# █
```

The endpoint pings the C&C server on the Internet from the Linux host (in this example from the IP address 184.75.221.43).

Figure 112: Confirming Connection to C&C Server

```
[root@BATPLANE ~]# ping 184.75.221.43
PING 184.75.221.43 (184.75.221.43) 56(84) bytes of data.

--- 184.75.221.43 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9001ms
```


After the attack, ForeScout CounterACT changes the VLAN configuration of the interface connecting the Linux host from User VLAN (vlan31) to Quarantine VLAN (vlan32) on the QFX switch using NETCONF.

Confirm the following:

- Confirm that the Linux host cannot connect to the Internet or the LAN anymore.

Figure 113: Confirming Linux Host Cannot Connect to Internet or LAN

```

root@vqfx-re> show configuration interfaces xe-0/0/1 | display set
set interfaces xe-0/0/1 unit 0 description Linux_Host_vSWITCH
set interfaces xe-0/0/1 unit 0 family ethernet-switching interface-mode access
set interfaces xe-0/0/1 unit 0 family ethernet-switching vlan members vlan32

{master:0}
root@vqfx-re> █

root@vqfx-re> show vlans

Routing instance      VLAN name      Tag      Interfaces
default-switch        default        1
default-switch        vlan31         31       xe-0/0/0.0*
default-switch        vlan32         32       xe-0/0/1.0*

{master:0}
root@vqfx-re> █

[root@BATPLANE ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 10.10.30.99 icmp_seq=2 Destination Host Unreachable
From 10.10.30.99 icmp_seq=3 Destination Host Unreachable
From 10.10.30.99 icmp_seq=4 Destination Host Unreachable
From 10.10.30.99 icmp_seq=6 Destination Host Unreachable
From 10.10.30.99 icmp_seq=7 Destination Host Unreachable
From 10.10.30.99 icmp_seq=8 Destination Host Unreachable

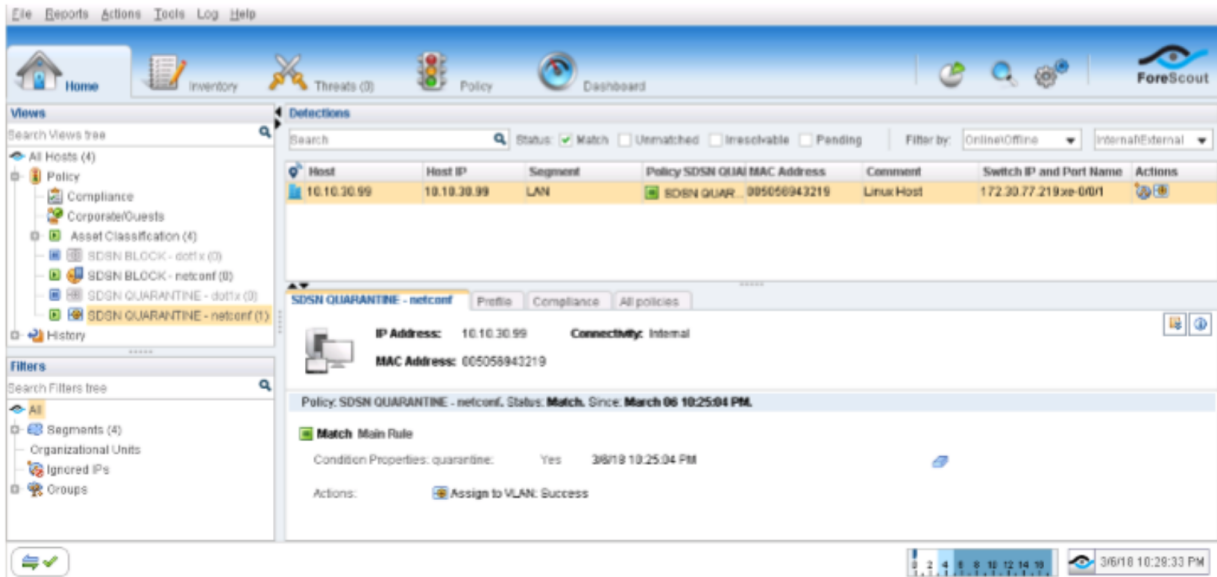
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7999ms
, pipe 3
[root@BATPLANE ~]# ping 10.10.30.254
PING 10.10.30.254 (10.10.30.254) 56(84) bytes of data.
From 10.10.30.99 icmp_seq=2 Destination Host Unreachable
From 10.10.30.99 icmp_seq=3 Destination Host Unreachable
From 10.10.30.99 icmp_seq=4 Destination Host Unreachable
From 10.10.30.99 icmp_seq=6 Destination Host Unreachable
From 10.10.30.99 icmp_seq=7 Destination Host Unreachable
From 10.10.30.99 icmp_seq=8 Destination Host Unreachable

--- 10.10.30.254 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7000ms
, pipe 3
[root@BATPLANE ~]# █

```

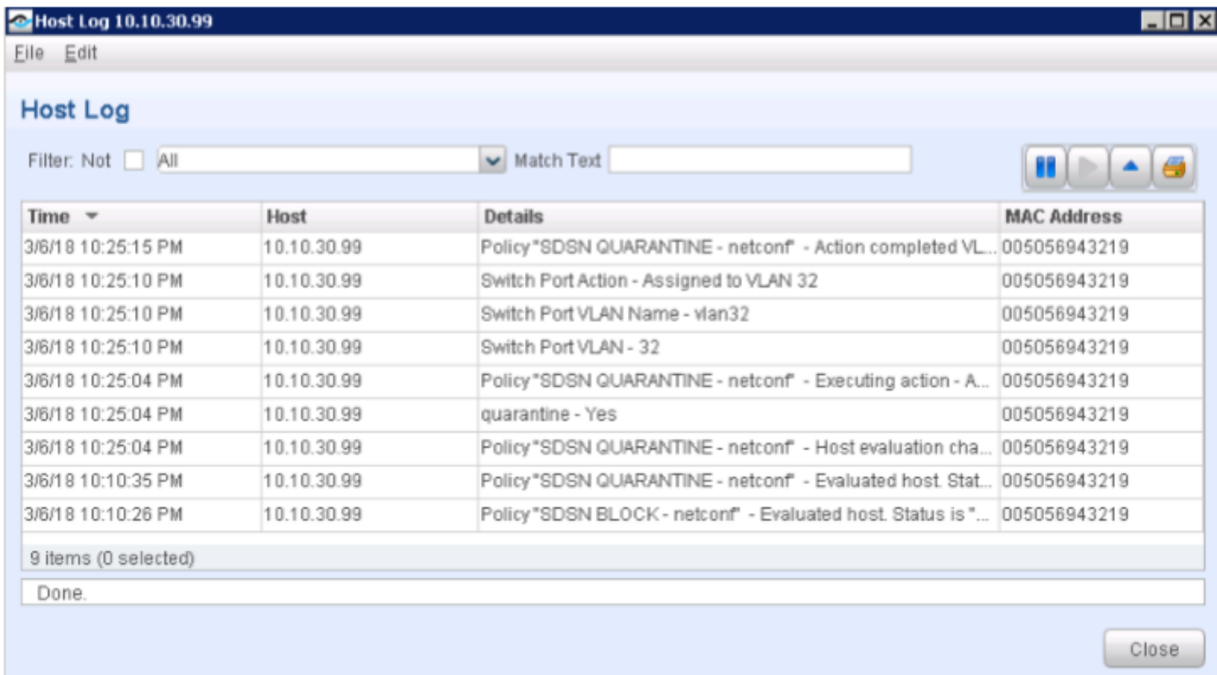
- Confirm the SDSN QUARANTINE (NETCONF) policy match and automated threat remediation action details by navigating to *ForeScout CounterACT > Home*.

Figure 114: Confirming Policy Match and Automated Threat Remediation Details



- Navigate to *Log > Host Log*. Review the details for the SDSN BLOCK (NETCONF) policy.

Figure 115: SDSN Block Policy Host Log



- Confirm that the Linux host's IP address was also added to the Infected-Hosts Feed on the SRX Series device to block Internet access.

```
user@vSRX_L3> show security dynamic-address category-name Infected-Hosts
```

```
No.  IP-start  IP-end  Feed      Address
```

```
1   10.10.30.99 10.10.30.99 Infected-Hosts/1 ID-2150001a
```

```
Total number of matching entries: 1
```

```
user@vSRX_L3>
```

- In the ATP Cloud portal, navigate to *Monitor > Hosts*. Confirm the host IP address (10.10.30.99), MAC-ID, and switch port of the Linux host.

Figure 116: Confirming Host Details in ATP Cloud Portal

Monitor / Hosts

Hosts ?

Export Select Policy Override Select Investigation Status

Host Identifier	Host IP	Threat Level	Infected Host Feed	Threat First Seen	Threat Last Seen	C&C Hits	Malware ...	Policy	State of Investigation
n/a@10.10.30.99	10.10.30.99	9	Included	27 Feb 2018 18:20	9 Mar 2018 22:14	17	0	Use configured policy	Open

Monitor / Hosts

Host n/a@10.10.30.99 ?

General

Host Identifier ?

n/a@10.10.30.99

Save

Reset

Host IP

10.10.30.99

MAC Address

005056943219

Switch, port

172.30.77.219:xe-0/0/1

Host Status ?

High threat level, recommend blocking host and investigating further

Threat Settings

Investigation Status

Open

Meaning

The output shows that the ATP Cloud infected host feed containing the Linux host's IP address 10.10.30.99 has been successfully downloaded, resulting in the SRX device taking an action to quarantine the IP address.

The *Hosts* page lists compromised hosts and their associated threat levels. The output confirms that ATP Cloud and Security Director have detected and quarantined the infected host. You can monitor and mitigate malware detections on a per host basis.

Appendix A: Device Configurations

IN THIS SECTION

- [CLI Configuration for SRX Series Device | 136](#)
- [CLI Configuration for EX4300 Switch | 141](#)
- [CLI Configuration for QFX Switch | 142](#)

This section provides the following device configurations:

CLI Configuration for SRX Series Device

```
set version 15.1X49-D110.4
set system host-name vSRX_L3
set system time-zone Europe/Amsterdam
set system root-authentication encrypted-password "$ABC123"
set system name-server 172.29.143.60
set system services ssh max-sessions-per-connection 32
set system services netconf ssh
set system services dhcp-local-server group wan-dhcp interface ge-0/0/1.0
set system services web-management http interface fxp0.0
set system syslog user * any emergency
set system syslog file messages any any
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any info
set system syslog file default-log-messages match "(requested 'commit'
operation)|(requested 'commit synchronize' operation)|(copying configuration to
juniper.save)|(commit complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU
insertion)|(link UP)|transitioned|Transferred|transfer-file|(license add)|(license
```

```

delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU Offline)|(plugged
in)|(unplugged)|GRES"
set system syslog file default-log-messages structured-data
set system license autoupdate url https://ael.juniper.net/junos/key_retrieval
set system ntp boot-server 172.30.77.162
set system ntp server 172.30.77.162
set services application-identification
set services ssl initiation profile aamw-ssl trusted-ca aamw-secintel-ca
set services ssl initiation profile aamw-ssl trusted-ca aamw-cloud-ca
set services ssl initiation profile aamw-ssl client-certificate aamw-srx-cert
set services ssl initiation profile aamw-ssl actions crl disable
set services security-intelligence url https://172.30.77.104:443/api/v1/manifest.xml

set services security-intelligence authentication auth-token
22QDFN29DJQXK7ZD3V8Q21X34THWKBC7
set services security-intelligence profile POLICY_CC category CC
set services security-intelligence profile POLICY_CC rule Rule-1 match threat-level
1
set services security-intelligence profile POLICY_CC rule Rule-1 match threat-level
2
set services security-intelligence profile POLICY_CC rule Rule-1 match threat-level
3
set services security-intelligence profile POLICY_CC rule Rule-1 match threat-level
4
set services security-intelligence profile POLICY_CC rule Rule-1 then action permit

set services security-intelligence profile POLICY_CC rule Rule-1 then log
set services security-intelligence profile POLICY_CC rule Rule-2 match threat-level
5
set services security-intelligence profile POLICY_CC rule Rule-2 match threat-level
6
set services security-intelligence profile POLICY_CC rule Rule-2 match threat-level
7
set services security-intelligence profile POLICY_CC rule Rule-2 then action permit

set services security-intelligence profile POLICY_CC rule Rule-2 then log
set services security-intelligence profile POLICY_CC rule Rule-3 match threat-level
8
set services security-intelligence profile POLICY_CC rule Rule-3 match threat-level
9
set services security-intelligence profile POLICY_CC rule Rule-3 match threat-level
10
set services security-intelligence profile POLICY_CC rule Rule-3 then action block
drop

```

```

set services security-intelligence profile POLICY_CC rule Rule-3 then log
set services security-intelligence profile POLICY_Infected-Hosts category
Infected-Hosts
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match
threat-level 1
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match
threat-level 2
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match
threat-level 3
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match
threat-level 4
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match
threat-level 5
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 match
threat-level 6
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 then
action permit
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-1 then
log
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 match
threat-level 7
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 match
threat-level 8
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 match
threat-level 9
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 match
threat-level 10
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 then
action block drop
set services security-intelligence profile POLICY_Infected-Hosts rule Rule-2 then
log
set services security-intelligence policy POLICY_CC POLICY_CC
set services security-intelligence policy POLICY_Infected-Hosts
POLICY_Infected-Hosts
set services advanced-anti-malware connection url
https://srxapi.eu-west-1.sky.junipersecurity.net
set services advanced-anti-malware connection authentication tls-profile aamw-ssl

set services advanced-anti-malware policy POLICY http inspection-profile
default_profile
set services advanced-anti-malware policy POLICY http action block
set services advanced-anti-malware policy POLICY http notification log
set services advanced-anti-malware policy POLICY verdict-threshold 8
set services advanced-anti-malware policy POLICY fallback-options action permit

```

```

set services advanced-anti-malware policy POLICY fallback-options notification log

set services advanced-anti-malware policy POLICY default-notification log
set services advanced-anti-malware policy POLICY whitelist-notification log
set services advanced-anti-malware policy POLICY blacklist-notification log
set security log mode stream
set security log format sd-syslog
set security log report
set security log source-address 10.10.10.251
set security log stream TRAFFIC category all
set security log stream TRAFFIC host 10.10.10.250
set security log stream TRAFFIC host port 514
set security pki ca-profile aamw-ca ca-identity deviceCA
set security pki ca-profile aamw-ca enrollment url
http://ca.junipersecurity.net:8080/ejbca/publicweb/apply/scep/SRX/pkiclient.exe
set security pki ca-profile aamw-ca revocation-check disable
set security pki ca-profile aamw-ca revocation-check crl url
http://va.junipersecurity.net/ca/deviceCA.crl
set security pki ca-profile aamw-secintel-ca ca-identity JUNIPER
set security pki ca-profile aamw-secintel-ca revocation-check crl url
http://va.junipersecurity.net/ca/current.crl
set security pki ca-profile aamw-cloud-ca ca-identity JUNIPER_CLOUD
set security pki ca-profile aamw-cloud-ca revocation-check crl url
http://va.junipersecurity.net/ca/cloudCA.crl
set security address-book global address IPSUBNET_10.10.30.0/24 10.10.30.0/24
set security screen ids-option untrust-screen icmp ping-death
set security screen ids-option untrust-screen ip source-route-option
set security screen ids-option untrust-screen ip tear-drop
set security screen ids-option untrust-screen tcp syn-flood alarm-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood attack-threshold 200
set security screen ids-option untrust-screen tcp syn-flood source-threshold 1024

set security screen ids-option untrust-screen tcp syn-flood destination-threshold
2048
set security screen ids-option untrust-screen tcp syn-flood queue-size 2000
set security screen ids-option untrust-screen tcp syn-flood timeout 20
set security screen ids-option untrust-screen tcp land
set security nat source rule-set OutBoundInternetTraffic from zone trust
set security nat source rule-set OutBoundInternetTraffic to zone untrust
set security nat source rule-set OutBoundInternetTraffic rule natALL match
source-address 0.0.0.0/0
set security nat source rule-set OutBoundInternetTraffic rule natALL match
destination-address 0.0.0.0/0
set security nat source rule-set OutBoundInternetTraffic rule natALL then source-nat

```

```

interface
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1
  match source-address IPSUBNET_10.10.30.0/24
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1
  match destination-address any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1
  match application any
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1
  then permit applicationservices security-intelligence-policy POLICY
set security policies from-zone trust to-zone untrust policy PolicyEnforcer-Rule1-1
  then permit applicationservices advanced-anti-malware-policy POLICY
set security policies from-zone trust to-zone untrust policy default-permit match
  source-address any
set security policies from-zone trust to-zone untrust policy default-permit match
  destination-address any
set security policies from-zone trust to-zone untrust policy default-permit match
  application any
set security policies from-zone trust to-zone untrust policy default-permit then
  permit
set security policies global policy PolicyEnforcer-Rule1-1 match source-address
  IPSUBNET_10.10.30.0/24
set security policies global policy PolicyEnforcer-Rule1-1 match destination-address
  any
set security policies global policy PolicyEnforcer-Rule1-1 match application any
set security policies global policy PolicyEnforcer-Rule1-1 then permit
  application-services securityintelligence-policy POLICY
set security policies global policy PolicyEnforcer-Rule1-1 then permit
  application-services advanced-antimalware-policy POLICY
set security zones security-zone trust tcp-rst
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/1.0
set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust host-inbound-traffic system-services all

set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone untrust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 description LOGGING-INTERFACE-VLAN10
set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.251/24
set interfaces ge-0/0/1 description LAN-VLAN31
set interfaces ge-0/0/1 vlan-tagging
set interfaces ge-0/0/1 unit 0 vlan-id 31
set interfaces ge-0/0/1 unit 0 family inet address 10.10.30.254/24

```



```

set interfaces ge-0/0/2 description INTERNET-MANAGEMENT
set interfaces ge-0/0/2 unit 0 family inet address 172.30.77.230/23
set interfaces fxp0 unit 0
deactivate interfaces fxp0
set snmp trap-group space targets 172.30.77.106
set routing-options static route 0.0.0.0/0 next-hop 172.30.77.1
set access address-assignment pool wan-1 family inet network 10.10.30.0/24
set access address-assignment pool wan-1 family inet range wan-1-range low
10.10.30.60
set access address-assignment pool wan-1 family inet range wan-1-range high
10.10.30.100
set access address-assignment pool wan-1 family inet dhcp-attributes
maximum-lease-time 86400
set access address-assignment pool wan-1 family inet dhcp-attributes name-server
8.8.8.8
set access address-assignment pool wan-1 family inet dhcp-attributes name-server
172.30.77.162
set access address-assignment pool wan-1 family inet dhcp-attributes router
10.10.30.254

```

CLI Configuration for EX4300 Switch

```

set version 15.1R5.5
set system host-name abernathy
set system services ssh root-login allow
set system services ssh protocol-version v2
set system services ssh max-sessions-per-connection 32
set system services netconf ssh
set system ntp server 172.30.255.62
set interfaces ge-0/0/1 description PORT_TO_ESXi_vmnic0_vSRX_LOGGING
set interfaces ge-0/0/1 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members LOGGING
set interfaces ge-0/0/18 description PORT_TO_ESXi_vmnic1_vSRX_vQFX_LAN
set interfaces ge-0/0/18 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/18 unit 0 family ethernet-switching vlan members vlan31
set interfaces ge-0/0/19 description PORT_TO_ESXi_vmnic2_WINDOWS7_DOT1x
set interfaces ge-0/0/19 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/19 unit 0 family ethernet-switching vlan members default
set interfaces ge-0/0/20 description
SPAN_PORT_TO_ESXi_vmnic3_COUNTERACT_EXPERIMENTAL
set interfaces ge-0/0/20 unit 0 family ethernet-switching port-mode access
set interfaces ge-0/0/20 unit 0 family ethernet-switching vlan members default

```

```

set interfaces me0 unit 0 family inet address 172.30.77.62/23
set routing-options static route 0.0.0.0/0 next-hop 172.30.77.1
set protocols igmp
set protocols dot1x authenticator authentication-profile-name CounterACT
set protocols dot1x authenticator interface ge-0/0/19.0 supplicant multiple
set protocols rstp
set access radius-server 172.30.77.100 dynamic-request-port 3799
set access radius-server 172.30.77.100 secret "$ABC123"
set access radius-server 172.30.77.100 source-address 172.30.77.62
set access profile CounterACT authentication-order radius
set access profile CounterACT radius authentication-server 172.30.77.100
set access profile CounterACT radius accounting-server 172.30.77.100
set access profile CounterACT radius options nas-identifier 172.30.77.100
set access profile CounterACT accounting order radius
set ethernet-switching-options analyzer mirror_traffic input ingress interface
ge-0/0/18.0
set ethernet-switching-options analyzer mirror_traffic input ingress interface
ge-0/0/19.0
set ethernet-switching-options analyzer mirror_traffic input egress interface
ge-0/0/18.0
set ethernet-switching-options analyzer mirror_traffic input egress interface
ge-0/0/19.0
set ethernet-switching-options analyzer mirror_traffic output interface ge-0/0/20.0

set ethernet-switching-options secure-access-port vlan vlan31 examine-dhcp
set vlans LOGGING description LOGGING
set vlans LOGGING vlan-id 10
set vlans vlan31 description LAN-VLAN31
set vlans vlan31 vlan-id 31
set vlans vlan32 description QUARANTINE
set vlans vlan32 vlan-id 32
set poe interface all

```

CLI Configuration for QFX Switch

```

set system host-name vqfx-re
set system root-authentication encrypted-password "$ABC123"
set system root-authentication ssh-rsa "ssh-rsa
AAAAB3NzaClyc2EAAAABIwAAAQEA6NF8iallvQp22MDK1krtp9eW6A8Yr+kz4TjGye7gHzIw+niNltCEFHZD8+v1I2YU6oXevct1YeS0c9H
ZyNlQ9cgGzUftdCKLv6IedplqPkmf0aYct2PKEDo3MlTBckFXPTAMzF8dUSIFo9D8HfdOV0IAkx407PtixWKn5y2hMNG0zQPyeq4pzC6ki

```

```

vAlHyFhILFR6IRGL+QFXQ2MZWfYbAGjyiYhAmCP3NOTB0jMZEhKdUvzhMhBYSdEtKlrRgm+R4LOzFUGhQhDLKX+FlPKcF96hruCxcwYlBl
bEgE980HlnVYCzRdK8j1qm8tehUc9c9WhQ== vagrant insecure public key"
set system login user vagrant uid 2000
set system login user vagrant class super-user
set system login user vagrant authentication ssh-rsa "ssh-rsa
AAAAB3NzaClyc2EAAAABIWAAQEA6NF8iallvQp22MDk1kyrtvp9eW6A8Yr+kz4TjGye7ghZTw+niNltGEFHzD8+v1I2YJ6oxevct1YeS0c9H

ZyNlQ9ggCgzUFTdCKLv6IedlqgPkmlF0ayEt2PkEDo3MlTBckFXPTtAmZF8dUSIFo9D8HfdOV0IAck407PtixWKn5y2hMNG0zQPyUecp4pzC6ki

vAlHyFhILFR6IRGL+QFXQ2MZWfYbAGjyiYhAmCP3NOTB0jMZEhKdUvzhMhBYSdEtKlrRgm+R4LOzFUGhQhDLKX+FlPKcF96hruCxcwYlBl
bEgE980HlnVYCzRdK8j1qm8tehUc9c9WhQ== vagrant insecure public key"
set system services ssh root-login allow
set system services ssh max-sessions-per-connection 32
set system services netconf ssh
set system services rest http port 8080
set system services rest enable-explorer
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system syslog file default-log-messages any any
set system syslog file default-log-messages match "(requested 'commit'
operation)|(requested 'commit synchronize' operation)|(copying configuration to
juniper.save)|(commit complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU
insertion)|(link UP)|transitioned|Transferred|transfer-file|(license add)|(license
delete)|(package -X update)|(package -X delete)|(FRU Online)|(FRU Offline)|(plugged
in)|(unplugged)|QF_NODE|QF_SERVER_NODE_GROUP|QF_INTERCONNECT|QF_DIRECTOR|QF_NETWORK_NODE_GROUP|(Master
Unchanged, Members Changed)|(Master Changed, Members Changed)|(Master Detected,
Members Changed)|(vc add)|(vc delete)|(Master detected)|(Master changed)|(Backup
detected)|(Backup changed)|(interface vcp-)"
set system syslog file default-log-messages structured-data
set system extensions providers juniper license-type juniper deployment-scope
commercial
set system extensions providers chef license-type juniper deployment-scope
commercial
set interfaces xe-0/0/0 description UPLINK-via-ESXi-vmnic1-to-EX4300
set interfaces xe-0/0/0 unit 0 family ethernet-switching interface-mode trunk
set interfaces xe-0/0/0 unit 0 family ethernet-switching vlan members vlan31
set interfaces xe-0/0/1 unit 0 description Linux_Host_vSWITCH
set interfaces xe-0/0/1 unit 0 family ethernet-switching interface-mode access
set interfaces xe-0/0/1 unit 0 family ethernet-switching vlan members vlan31
set interfaces em0 unit 0 family inet address 172.30.77.219/23
set interfaces em1 unit 0 family inet address 169.254.0.2/24

```

```

set forwarding-options storm-control-profiles default all
set routing-options static route 0.0.0.0/0 next-hop 172.30.77.1
set protocols igmp-snooping vlan default
set vlans default vlan-id 1
set vlans vlan31 vlan-id 31
set vlans vlan32 vlan-id 32
set poe interface xe-0/0/1

```

Appendix B: Troubleshooting Adding Third-Party Connector

IN THIS SECTION

- [Troubleshooting Policy Enforcer | 144](#)
- [Troubleshooting ForeScout CounterACT | 145](#)

If you encounter problems while adding the third-party connector, review the following log files for troubleshooting information.

This section covers the following third-party connector issues:

Troubleshooting Policy Enforcer

To troubleshoot Policy Enforcer, review these logs:

- `/srv/feeder/connectors/forescout/logs/forescout_connector.log`
- `/srv/feeder/log/controller.log`
- If the following log message displays in the `forescout_connector.log` file:

```

DEBUG response content of API:
{"status": "NOT_FOUND", "code": 404, "message": "failed to read properties file
/usr/local/forescout/plugin/webapi/local.properties"}

```

Then navigate to the ForeScout CounterACT CLI and enter this command:

```
chmod 777 /usr/local/forescout/plugin/webapi/local.properties
```

Troubleshooting ForeScout CounterACT

To enable debugging on the CLI for the DEX (eds) and Web API plugins, enter the following commands:

- **fstool eds debug 10**
- **fstool webapi debug 10**

Review the following log files:

- **/usr/local/forescout/log/plugin/eds**
- **/usr/local/forescout/log/plugin/webapi**

RELATED DOCUMENTATION

[Use Case Overview: Threat Remediation of Infected Hosts with Forescout CounterACT | 25](#)

[Juniper Connected Security Building Blocks | 9](#)

[Components of Juniper Connected Security | 13](#)

[Benefits of Juniper Connected Security | 11](#)