

Juniper Advanced Threat Prevention Appliance

Operator's Guide

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. and/or its affiliates in the United States and other countries. All other trademarks may be 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 Advanced Threat Prevention Operator's Guide
Copyright© 2018 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 document 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 <http://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

CONTENTS

About the Documentation

Documentation and Release Notes	i
Requesting Technical Support	i
Self-Help Online Tools and Resources	i
Opening a Case with JTAC	ii

Introduction

Juniper ATP Appliance's Adaptive Detection Fabric: Defense-in-Depth	2
Advanced Threat Analytics (ATA)	5
Single Pane View of Advanced Persistent Threats (APTs)	5
Juniper ATP Appliance Cyber Threat Kill Chain Progressions	5
Context-Aware Detection and Juniper ATP Appliance Intel	7
Juniper ATP Appliance Multi-Platform Product Suite	8
Juniper ATP Appliance Traffic Collectors	10
Traffic Collector Performance, Confidence and Diagnostics Displays	11
Web UI Cyber Kill Chain Progression Mappings	12
Integrated Network Endpoint Mitigation	12
CrowdStrike Endpoint Integration	12
SMB Lateral Detection	13
Lateral Detection Enhancements: SSH Honeypot	13
Incidents Tab Kill Chain, Correlation & Lateral Spreads	14
Kill Chain Stages	16
Juniper ATP Appliance Progression Mappings Per Kill Chain Stages	18
YARA Rules and Lateral Detection	18
Juniper ATP Appliance HTTP API	19
Juniper ATP Appliance Global Security Services (GSS)	20
Machine Learning Model Updates	20
Static Analysis Signature Updates	20
One-Way vs Two-Way GSS Service Options	21
Quick Link to More Juniper ATP Appliance GSS Information	22
Juniper ATP Appliance Dashboard Threat View	22
Operations Dashboard	23
Research Dashboard	23
Traffic Collectors Dashboard	26
Events Timeline Dashboard	28
Email Detection Enhancements	28
Email Threat Mitigation: Gmail and Office 365 Quarantine Options	30
Email URL Reputation Detection	30
Threat Metric Prioritization Mapping	31
Incident vs Event Context Detailing and Reporting	31
False Negative False Positive Reporting on the Incidents Tab	32
Auto-Mitigation with Existing Security Infrastructure	33
PAN Firewall Integration	34

URL Blocking Support for Palo Alto Networks Firewall Integration	34
Centralized Panorama Integration for PAN Firewall Devices	34
SRX Series Device Integration	34
Cisco ASA Firewall Integration	35
Check Point Firewall	35
BlueCoat ProxySG Integration	36
Endpoint Mitigation with Carbon Black Response	36
CEF, QRadar LEEF Logging Support for SIEM	37
Virtual Collector, Virtual Core for AWS, and vCore [OVA] Deployments	37
Clustered Core Deployment	38
Virtual Core for Amazon EC2 AWS	39
Small Footprint Virtual Traffic Collector	39
Management Traffic Proxy Support	39
Span-Traffic Proxy Data Path Support	40
Set Proxy Inside	40
Set Proxy Outside	40
Single Sign On SAML Authentication	41
YARA Rules Support	41
YARA Rules for Detecting Lateral Spread within a Customer Network	41
Custom SNORT Rules Support	41
Email Correlation and Mitigation	41
Reverse SSH Tunneling for Optimizing Customer Technical Support	42
Manager of Central Managers (MCM) Virtual or Hardware Device	42

Getting Started

Before you Begin	48
Juniper ATP Appliance Network Information	48
Management Network	49
Internal Servers	49
Management Port eth0	49
Monitoring Port eth1	49
Analysis Engine Exhaust Port eth2	50
Port Scan Detector and SSH Honeypot Port eth3	50
External Servers	50
Juniper ATP Appliance Web UI Support	51
Screen Resolution Support	52
Accessing Juniper ATP Appliance Device Interfaces	52
Launching the Configuration Wizard	52
CONFIGURATION WIZARD	53
Juniper ATP Appliance Web UI Access	57
Login to the Juniper ATP Appliance using SAML Authentication	57
Login to the Juniper ATP Appliance System using AD Authentication	58
Working with the Juniper ATP Appliance Web UI	58
Navigating the CM Web UI	58
Navigating the CM Web UI	59
Summary of the Tabs in the Juniper ATP Appliance Web UI	60
Deploying the Distributed Juniper ATP Appliance System	60

Deployment Scenarios	61
Juniper ATP Appliance Defense in an Enterprise Headquarters	61
Juniper ATP Appliance Defense in a Distributed Enterprise Environment	62
Juniper ATP Appliance Distributed SaaS/OVA Deployment	62
Deployment Guidelines	63
Network Tapping	64
SPAN Port Mirroring	64
Guidelines for Environments with Web Proxies	65
Configuring Collector Email Journaling	65
Configuring Journaling for the Email Collector	65
Email Journaling	65
Creating a Journaling Mailbox on the Exchange Server	66
Configuring a Mailbox Database	66
Configuring Microsoft Exchange Server 2013 Journaling	66
Configuring Exchange-Server Journal Polling from the Web UI	69
Configuring Office 365 Journaling	70
Configuring Gmail Journaling	72
Configuring Gmail Threat Mitigation	75
Delegating domain-wide authority to a Gmail service account	75
Using the Dashboard Views	77
Interacting with Dashboard Views and Components	80
Resetting the Threat View	86
Submitting a Malware File for Analysis	87
To Upload a File for Analysis	88
Configuring Juniper ATP Appliance for Integrated Deployment	88
Deploying Juniper ATP Appliance SaaS Virtual Collectors	89
Virtual Collector Deployment Options	90
Provisioning Requirements	90
OVA vCollector Sizing Options	91
Deploying SaaS Virtual Cores as OVAs	91
To install the Juniper ATP Appliance OVA to a VM	92
Upgrading without Whitelisting	94
Enabling Juniper ATP Appliance Support	94
Managing your Support Account	94
Configuring an Alternate Analysis Engine Interface	95
Requirements for setting up SSH honeypot lateral detection:	95
Configuring Distributed Defense	
Setting Notifications	99
Configuring Alert Settings	99
To create a new alert notification:	99
To display, delete or edit an existing alert configuration:	99
Alert notification configuration options	100
Configuring SIEM Settings	101
To create a new SIEM notification:	102
Using CEF Alert event_id or incident_id to Display Details in Web UI	103
To display, delete or edit an Active SIEM connector configuration:	103

Alert notification configuration options	103
Configuring System Profiles	104
Resetting the Central Manager Password	105
Configuring Role Based Access Controls	106
Default Roles	107
Remote Authentication and Roles	107
Configuring MSSP Multi-Tenancy Zones	107
Configuring User Accounts	109
Adding a New User Configuration	109
Updating a User Account and Setting an API Authorization Key	111
Configuring SAML Settings	112
Login to the Juniper ATP Appliance using SAML Authentication	114
Setting SAML for PingFederate Servers	114
Configuring RADIUS Server Settings	115
About Radius Groups	115
Local/Remote User Authentication and RBAC	116
Configuring RADIUS Settings on the Juniper ATP Appliance	116
Configuring System Settings	118
Configuring System Settings	119
Understanding IVP MSI and Self-Extracting ZIP Options	119
Self-Extracting Zip File IVP Process	120
Configuring Proxy Settings for the Management Network	121
Configuring No Proxy Settings for Local Traffic	122
Configuring Auto-Mitigation	122
Configuring Display Settings	123
Configuring Outgoing Mail Settings	124
Testing Email Notification Settings	124
Managing Certificates	125
Creating a Self-Signed Certificate/CSR	125
Uploading and Installing a User-Provided Certificate	128
Downloading a Certificate or PKCS#12 Bundle	128
Configuring GSS Settings	129
Remote Support	130
Configuring Web Collectors	130
Status of Proxy and deployed Collector: online off line	133
Configuring Email Collectors	133
Adding a New Email Server	134
Editing or Deleting Email Server Settings	135
Configuring Mac OSX or Windows SecondaryCores	135
Using the Secondary Core Web UI Config Options	137
Status of the deployed Secondary Core: online off line	137
Configuring Golden Image VMs	137
Golden Image VM Config Process	138
Step 1: Mount the Custom OS ISO and Boot the VM	139
Step 2: Connect to the VM via VNC & Install Windows OS	140
Step 3: Reboot the Golden Image VM	140

Step 4: Finalize and Enable the Custom Golden Image VM	140
Step 5: Reconnect to VNC to install Adobe Acrobat, if necessary	140
Step 6: Installing Preferred AV Software to Golden Image	141
Viewing Custom Image Results	141
Configuring the ESXi Server to Enable Virtualized HV	141
Setting the Juniper ATP Appliance License Key	142
Configuring Backup and Restore Options	142
Backing up the current configuration	143
Restoring a saved configuration	143
Testing Malware Detection Capabilities	143
Configuring Environmental Settings	144
Configuring Email Mitigation Settings	145
To configure Gmail Quarantine mitigation settings:	145
To configure Exchange Online Quarantine mitigation settings:	146
Configuring Firewall Auto-Mitigation	147
About Auto-Mitigation	148
Configuring a PAN Firewall	148
Configuring a PAN Firewall Tag	148
Configuring a New Auto-Mitigation Rule at the Juniper ATP Appliance CM Web UI ..	148
Implementing an Auto-Mitigation Rule	149
Verifying Auto-Mitigation Rule Operations	150
Configuring a PANORAMA Device for Centralized PAN FW Mitigation Management	150
Configuring Centralized Panorama Integration	150
Implementing the Auto-Mitigation Rule	151
Verifying Auto-Mitigation Rule Operations	152
Configuring Security Policy Address Sets at the SRX CLI	153
Defining a Zone-Defined SRX Configuration at the Juniper ATP Appliance Web UI ..	154
Viewing SRX Activity from the Juniper ATP Appliance Mitigation Tab	156
Generating an SRX SSH public/private key pair	156
Defining a Zone-Attached SRX Configuration at the Juniper ATP Appliance Web UI	157
Configuring a Cisco ASA Firewall	158
Cisco ASA Firewall Configuration	158
Cisco ASA Firewall Configuration Example:	158
Juniper ATP Appliance ASA Firewall Configuration	159
Configurations at the FortiManager Console	159
Configurations at the Juniper ATP Appliance Central Manager	161
Configuring a Check Point Firewall	162
Configuring and Deploying the Check Point Firewall	162
Configuring Juniper ATP Appliance Integration with Check Point	163
Configuring Enterprise Network Asset Values	163
Configuring Anti-Virus Integration	164
Configuring Endpoint Integration: CrowdStrike and Carbon Black Response	166
Configuring Carbon Black Response Endpoint Integration	166
Obtaining the Carbon Black Response API Key	166
Configuring the Carbon Black Response Integration at the Juniper ATP Appliance CM	167
Configuring CrowdStrike Endpoint Integration	167

Configuring BlueCoat ProxySG Integration	167
Configuring Whitelist Rules	168
Updating and Redefining Whitelist Filters from the Incidents Page	171
Configuring YARA Rules	172
To Create a YARA Rule	172
To upload and enable a YARA Rule:	173
Reviewing YARA Rule Malware Detection	174
Configuring Identity	174
Setting Identity Configuration for Splunk	174
Setting Identity Configuration for Active Directory	175
Active Directory Log Ingestion	176
Splunk Universal Forwarder of Active Directory Logs	176
Splunk WMI Forwarding of Active Directory Logs	182
Configuring Active Directory	184
Part 1 - Obtaining a Domain Component Name for a Domain Controller	185
Prerequisites for Active Directory Integration	185
Creating a Domain User or Group	186
Part 2 - Configuring an Active Directory Domain Controller from the Web UI	190
AD Domain Controller Configuration Requirements and Tips	191
Configuration Requirements and Tips	191
Troubleshooting Active Directory	192
Configuring Custom SNORT Rules	192
Sample Snort Rules	192
Setting Anti-SIEM Identity Configurations	193
Setting Identity Configuration for Splunk	194
Setting Identity Configuration for Active Directory	194
Active Directory Log Ingestion	194
Splunk Universal Forwarder of Active Directory Logs	195
Splunk WMI Forwarding of Active Directory Logs	202
Carbon Black Response - Splunk Integration	204
Carbon Black Response Direct Log Ingestion: Event Forwarder of JSON Logs	205
Carbon Black Response Integration via Splunk Forwarder	206
Carbon Black Response Ingestion Reporting at Juniper ATP Appliance	209
Configuring Anti-SIEM Splunk Ingestion	209
Juniper ATP Appliance Side - Splunk Integration Configuration	209
Splunk Side - Splunk Configuration	210
Integrating Anti-Siem External Event Collectors	211
Anti-SIEM Firewall [PAN: Log Collector Splunk Ingestion]	211
PAN Log Collector Configuration - Juniper ATP Appliance Side	211
PAN-Side Direct Ingestion Settings	212
Direct Ingestion PAN Event Filtering	214
PAN and Splunk Integration Configuration	214
Splunk Side Configuration for PAN	215
Splunk Integration Event Filtering	218
Incident Reporting for PAN Syslog Ingestion	218
Anti-SIEM Web Gateway [Bluecoat: Log Collector Splunk Ingestion]	219

Configuring a Bluecoat Secure Web Gateway Log Collector	219
Configuring Splunk to Bluecoat Integration	220
Juniper ATP Appliance Side Configuration	221
Bluecoat Side Configuration	221
Splunk Side Configuration	221
Configuring Bluecoat to Juniper ATP Appliance Integration	221
Juniper ATP Appliance Side Setup	221
Bluecoat Side Setup	222
Configuring Bluecoat Secure Web Gateway Splunk Ingestion	224
Anti-SIEM Endpoint AV [ESET McAfee ePO Symantec: Log Collector Splunk Ingestion]	225
Configuring ESET Endpoint AV Log Collection	225
Configuring McAfee ePO Endpoint AV Log Collection	226
Configuring Symantec EP Endpoint AV Log Collection	226
Configuring McAfee ePO Endpoint AV Splunk Ingestion	226
McAfee ePO Splunk integration: Splunk-Side Configuration	227
McAfee ePO Direct Log Ingestion: McAfee ePO Side Configuration	228
Anti-SIEM Endpoint Response [Carbon Black Response: Log Collector Splunk Ingestion]	229
Configuring Carbon Black Response Log Events via Splunk	229
Splunk Side Configuration for Carbon Black Response	229
Configuring Carbon Black Response via Direct Log Ingestion	229
Carbon Black Response - Splunk Integration	230
Carbon Black Response Direct Log Ingestion: Event Forwarder of JSON Logs	231
Carbon Black Response Integration via Splunk Forwarder	232
Carbon Black Response Ingestion Reporting at Juniper ATP Appliance	235
Managing Incidents	
Understanding Threats and Incidents	238
Context-Aware Kill Chain Stage and Progression per Incident	239
Threats and the Attack Life Cycle	239
Understanding Severity	239
Severity Risk Colors	239
Severity Range	239
Severity and the Kill Chain	240
Severity and Risk Calculations	240
Interpreting Context-Aware Incident Details	241
Navigating the Incidents Page	241
Setting Incident Status and Entering User Comments	242
Details Summary	242
Viewing Golden Image Results in Incidents Summary	243
Object Rescans History Timestamps on Incidents Page	243
Custom Time Range Filtering	243
Malware Download Naming Conventions	244
Mitigation and Reporting	
Network Mitigation Options	246
Blocking Threats at Firewalls	246
Blocking Threats at Secure Web Gateways	247
Blocking Threats at the IPS/NextGen Firewall	247

Verifying Threats on the Endpoint	247
Using Whitelists	248
Mitigation Options from the Incidents Tab	250
Updating Whitelist Filtering Rules	250
Generating Reports	250
Report Types and Options	251
Customizing Reports	252
Executive Report	252
Technical Report	253
System Audit Report	253
System Health Report	254
Sample Executive Report Segments	254
Traffic Statistics	254
Malware Statistics	255
File Statistics by Operating System	255
Malware Types	256
Malware Vector & Detection Engine	256
Kill Chain Breakdown	257
Top Malware Serving Countries	257
Malware Detections Breakdown (Part 1)	258
Malware Targets (Part 1)	258
System Information and Updates	
Checking Appliance Health	260
Upgrading Juniper ATP Appliance Software and Security Content	261
CEF Logging Support for SIEM	262
syslog Trap Sink Server	262
CEF Format	262

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes. Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>.
- Search for known bugs: <https://prsearch.juniper.net/>.
- Find product documentation: <http://www.juniper.net/documentation/>.
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>.
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>.
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>.
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>.
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>.

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).
- For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>

CHAPTER 1

Introduction

The following topics are in this chapter:

- Juniper ATP Appliance's Adaptive Detection Fabric: Defense-in-Depth
- Advanced Threat Analytics (ATA)
- Single Pane View of Advanced Persistent Threats (APTs)
- Juniper ATP Appliance Cyber Threat Kill Chain Progressions
- Context-Aware Detection and Juniper ATP Appliance Intel
- Juniper ATP Appliance Multi-Platform Product Suite
- Juniper ATP Appliance Traffic Collectors
- Traffic Collector Performance, Confidence and Diagnostics Displays
- Web UI Cyber Kill Chain Progression Mappings
- Integrated Network | Endpoint Mitigation
- CrowdStrike Endpoint Integration
- SMB Lateral Detection
- Incidents Tab Kill Chain, Correlation & Lateral Spreads
- Kill Chain Stages
- Juniper ATP Appliance HTTP API
- Juniper ATP Appliance Global Security Services (GSS)
- Machine Learning Model Updates
- Juniper ATP Appliance Dashboard Threat View
- Threat Metric Prioritization Mapping
- Incident vs Event Context Detailing and Reporting
- Auto-Mitigation with Existing Security Infrastructure
- Endpoint Mitigation with Carbon Black Response
- CEF, QRadar LEEF Logging Support for SIEM
- Virtual Collector, Virtual Core for AWS, and vCore [OVA] Deployments
- Clustered Core Deployment
- Virtual Core for Amazon EC2 AWS

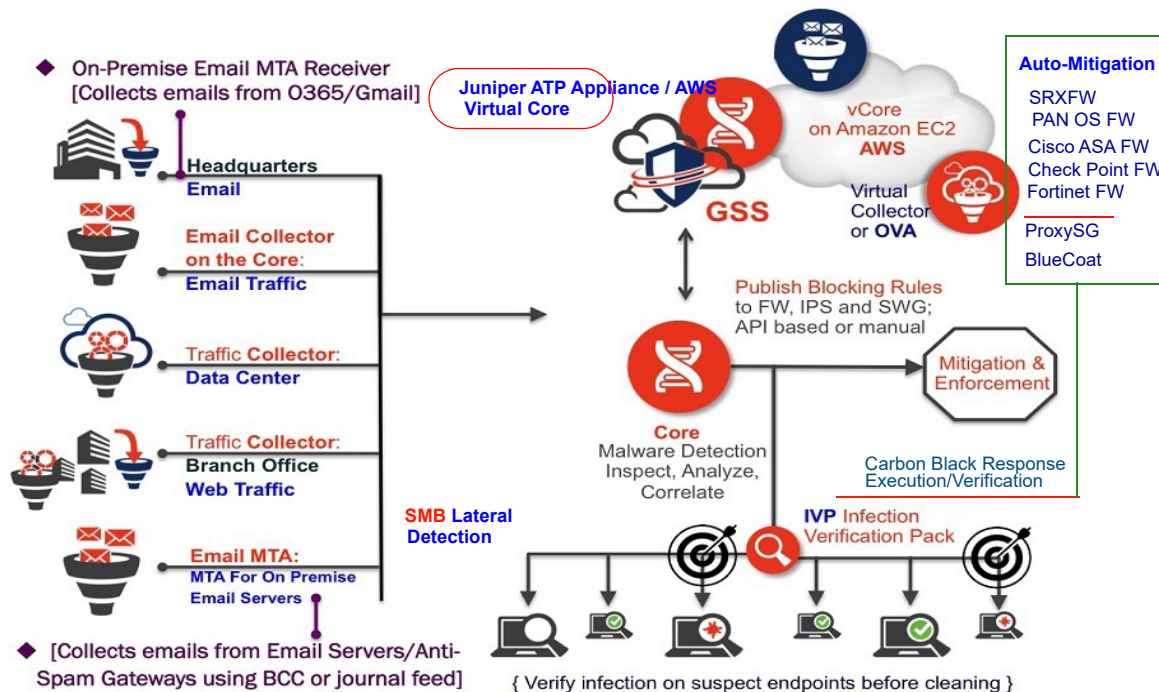
- Small Footprint Virtual Traffic Collector
- Management Traffic Proxy Support
- Span-Traffic Proxy Data Path Support
- Single Sign On SAML Authentication
- YARA Rules Support
- YARA Rules for Detecting Lateral Spread within a Customer Network
- Custom SNORT Rules Support
- Email Correlation and Mitigation
- Reverse SSH Tunneling for Optimizing Customer Technical Support
- Manager of Central Managers (MCM) Virtual or Hardware Device

Juniper ATP Appliance's Adaptive Detection Fabric: Defense-in-Depth

Security experts agree that cyber threat solutions are not keeping pace with emerging criminal ecosystems. Evolving threat strategies employ stealthier and more insidious mechanisms for infiltrating networks and stealing intellectual property and proprietary data. The increasing use of cloud computing, BYOD and social media in multi-platform enterprise environments means that the industry-wide requirement for “defense in depth” is just getting deeper and deeper.

Juniper ATP Appliance's continuous traffic monitoring and seamless, extensible, multi-thread, multi-platform malware detonation engine Cores provide truly actionable, context-aware detection and intelligence. This is Juniper ATP Appliance's Adaptive Detection Fabric. Juniper ATP Appliance products detect evasive threats that cause breaches using a unique combination of Smart Core Technology: behavioral analysis and machine learning that empowers each enterprise's incident response team with prioritized alerts that eliminate overload and significantly reduce response time.

ADAPTIVE DETECTION FABRIC & SMART CORE TECHNOLOGY



Juniper ATP Appliance is the industry's first distributed threat protection solution deployed wide and deep to provide a context-aware, multi-platform advanced threat detection and mitigation system, stopping targeted and zero-day attacks along all web and email Kill Chain vectors. With adaptive, anti-evasion detection, Juniper ATP Appliance intelligence and analysis information evolves with advanced threats.

- Web-borne Threats**
 The Juniper ATP Appliance Web Traffic Collector protects an enterprise against web-borne threats. Web Traffic Collectors provide continuous monitoring and inspection of network traffic either through a mirror/monitor port on a switch, a network tap, or a load balancer. The Juniper ATP Appliance Web Collector analyzes network traffic and communications, performing packet captures and assessing for indications of malware. Following the initial inspection and analysis phase, the Web Collectors deliver all network objects for detonation inside the Juniper ATP Appliance Core detection engines, identifying and testing the characteristics of detected malware using instrumented virtualization and emulation technologies. The Traffic Collector extracts payload along with envelope information which is sent to the Core. Web collectors also detect command and control (CnC) communications.
- Email-borne Threats and Email Phishing Correlation**
 Juniper ATP Appliance also provides protection against email attack vectors, defending against spear-phishing attacks by detecting and preventing advanced malware from infecting the endpoint via attachments and URLs in emails intended to compromise a host and/or initiate CnC extraction of sensitive organizational data. The Email Traffic Collector can be configured for BCC or Email Journaling via a Mail Transfer Agent (MTA) Juniper ATP Appliance Receiver.
- Core Windows & Mac OSX Threat Detonation Engines**
 As part of the Juniper ATP Appliance Core, multi-phase, multi-OS detonation engines perform detailed, context-aware forensic analysis of advanced malware, zero-day, and targeted APT attacks embedded in common file formats, email attachments, URLs binaries, and web objects. The Core and Mac OSX Secondary Core also perform callback analysis to track advanced malware and exfiltrations.

- Flexible Appliance-based, Software-Only, VCore for Amazon Web Services (AWS), or OVA VM Distributed Deployments
The Juniper ATP Appliance scalable threat protection system via Juniper ATP Appliance deployments, SaaS or VM options, is designed to integrate with, and leverage, existing infrastructure and network security services. Juniper ATP Appliance allows you to customize its technology and components to match your network environment.
- SMB Lateral Detection Support
Via the Juniper ATP Appliance Advanced license, monitoring and analysis of the SMB protocol stack includes extraction of file transmissions between clients or between clients and servers, similarly to the way Juniper ATP Appliance currently monitors HTTP traffic. With SMB lateral detection, the endpoint that downloads malware is the target endpoint, and the host that serves the malware is the threat source. The incident uses each of these hosts' IP addresses. This "east-west" traffic monitoring, in addition to established "north-south" monitoring of ingress and egress traffic, helps identify malware as it spreads to other hosts within an enterprise, tracking the progression from "patient zero." Because HTTP is rarely used to communicate between endpoints within an organization, SMB ([See SMB Lateral Detection on page 13](#)) is a proven candidate for malware transmission within the organization and across file shares.
- Network and Endpoint Mitigation with Remediation Prioritization
Juniper ATP Appliance generates actionable intelligence and provides mitigation options for each determined threat; this is a large part of the Juniper ATP Appliance advanced defense system. Prioritization of mitigation actions in the network path and at the enterprise endpoint, specifically for the threats that matter the most to your enterprise, are derived from a combination of threat intelligence assessments referred to as the Juniper ATP Appliance Threat Metric:
 - › [Threat Severity](#) — The behavior and goal of the detected malware
 - › [Threat Progression](#) — The stage of the attack's Kill Chain
 - › [Threat Relevance](#) — Whether the malware was recognized or blocked by static analysis scanners like VirusTotal; whether the targeted OS was available on the targeted endpoint; whether execution of a download took place at the endpoint; and whether the custom-configured asset value for the network segment that was attacked represents a significant risk to the enterprise

For more information, refer to [Threat Metric Prioritization Mapping on page 31](#) of this guide.
- Open API Platform Incident Tracking
The Juniper ATP Appliance Central Manager also provides a comprehensive open platform HTTP-based API for accessing all threat and processing data as well as device and software configuration. [See Juniper ATP Appliance HTTP API on page 19.](#)

Juniper ATP Appliance's architecture allows for faster, more accurate detection. The Juniper ATP Appliance system employs four cooperative dimensions of malware analysis with correlated machine learning:

- Network
- Static
- Reputation
- Dynamic (Behavioral)

Juniper ATP Appliance detection and analysis is context-aware and identifies infected endpoints while providing actionable intelligence about each infection. Juniper ATP Appliance catches zero-day threats, including armored and VM-resistant malware against more file types and more platforms, with more behavioral traces than any other technology, using real machine learning as opposed to heuristic shortcuts.

Juniper ATP Appliance products provide details of the threat incidents detected for a specific attack vector and supports notification, reporting, and real-time integration with blocking mitigation and security analysis work flows.

Advanced Threat Analytics (ATA)

Juniper ATP Appliance's Advanced Threat Analytics features are critical to incident response, providing a comprehensive view of threat activities. While many organizations have implemented security information and event management (SIEM) platforms, the lack of unified threat context limits the effectiveness of the operational intelligence that allows immediate, informed responses to threats. Juniper ATP Appliance ATA enables your security team to maximize the value of the intelligence captured by your existing security tools, allowing analysts to optimize their ability to analyze and respond to data from SIEM systems while providing a better understanding of the incident context associated with SIEM events.

Juniper ATP Appliance ATA is a holistic view of threat activity from diverse information sources such as:

- Active Directory
- Endpoint Anti-Virus,
- Firewalls
- Secure Web Gateways
- Intrusion detection systems
- Endpoint Detection and Response Tools

Traditional security devices collect valuable information, but most of it goes unused as the devices are not specifically looking for advanced threats. Juniper ATP Appliance's ATA looks at data from different sources, identifies advanced malicious traits and correlates the events to provide complete visibility into the kill chain of a threat. This becomes especially useful in the case of noisy devices such as intrusion prevention systems. And customers that do not use SIEM also benefit because ATA ingests data directly from other security devices in their network to secure them from cyber attack.

Juniper ATP Appliance ATA focuses on the day to day workflow of Tier 1 and Tier 2 security analysts who work on triaging and investigating malware incidents. A host and user timeline is provided to the security analyst to reveal the specific events that occurred on the targeted host. Within minutes, a Tier 1 analyst—who is not a detection expert—can easily determine the course of action necessary for the incident. With ATA, analysts have comprehensive information to determine the exact nature of the threat and whether it is an advanced threat that requires escalation to Tier 2 teams for mitigation. The Tier 2 analyst is freed up to focus on vetted advanced threats and to use the timeline view provided by ATA to perform detailed investigations on the host and user. This holistic view of information results in providing response teams with rich data that includes the threat context, the host identity, and the end user identity—with no manual data aggregation and analysis required.

Single Pane View of Advanced Persistent Threats (APTs)

By providing a single-pane-of-glass view of advanced threats coming from both the enterprise perimeter as well as laterally from within an enterprise network, Juniper ATP Appliance's visibility and correlated intel uniquely identify the next generation of threats (that often evade other solutions) so an administrator or incident response team can quickly mitigate the threat to the enterprise.

Juniper ATP Appliance Cyber Threat Kill Chain Progressions

A "Kill Chain" is defined as those attack vectors and attack stages that characterize a cyber threat. Juniper ATP Appliance detects and analyzes all extended links in the cyber threat Kill Chain — providing a distinctive cyber security solution that offers comprehensive and actionable visibility into all relevant network traffic and data along the kill chain and its associated attack vectors.

Table 1-1 Links of the Cyber Threat Kill Chain Monitored and Analyzed by Juniper ATP Appliance

Exploits	XP	Activity that could expose users to malicious objects.
Downloads	DL	Download of an object identified as malicious.
User Uploads	UP	A data upload performed at an endpoint.
Executions	EX	Execution of malicious code on the enterprise endpoint [identified through Carbon Black Response API integration]
Infections	IN	Identified evidence of infection (CnC, IVP verification).

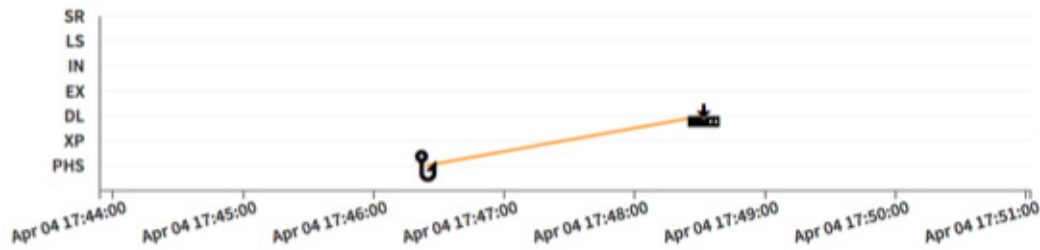
Table 1-1 Links of the Cyber Threat Kill Chain Monitored and Analyzed by Juniper ATP Appliance

Exploits	XP	Activity that could expose users to malicious objects.
Lateral Spread	LS	Detected spread across enterprise hosts within the east-west traffic.
Phishing	PHS	Email with malicious URL (often correlated with Download(s))

Juniper ATP Appliance Kill Chain Detection Designations

XP + UP + DL + EX + IN + LS + PHS

Figure 2 Sample Kill Chain Progression for Email Phishing Correlation



NOTE Refer also to [Incidents Tab Kill Chain, Correlation & Lateral Spreads on page 14](#) and the section [Graphical Kill Chain Progression Display on page 285](#) for information about the interactive Kill Chain, Email Correlation and Lateral Spread displays.

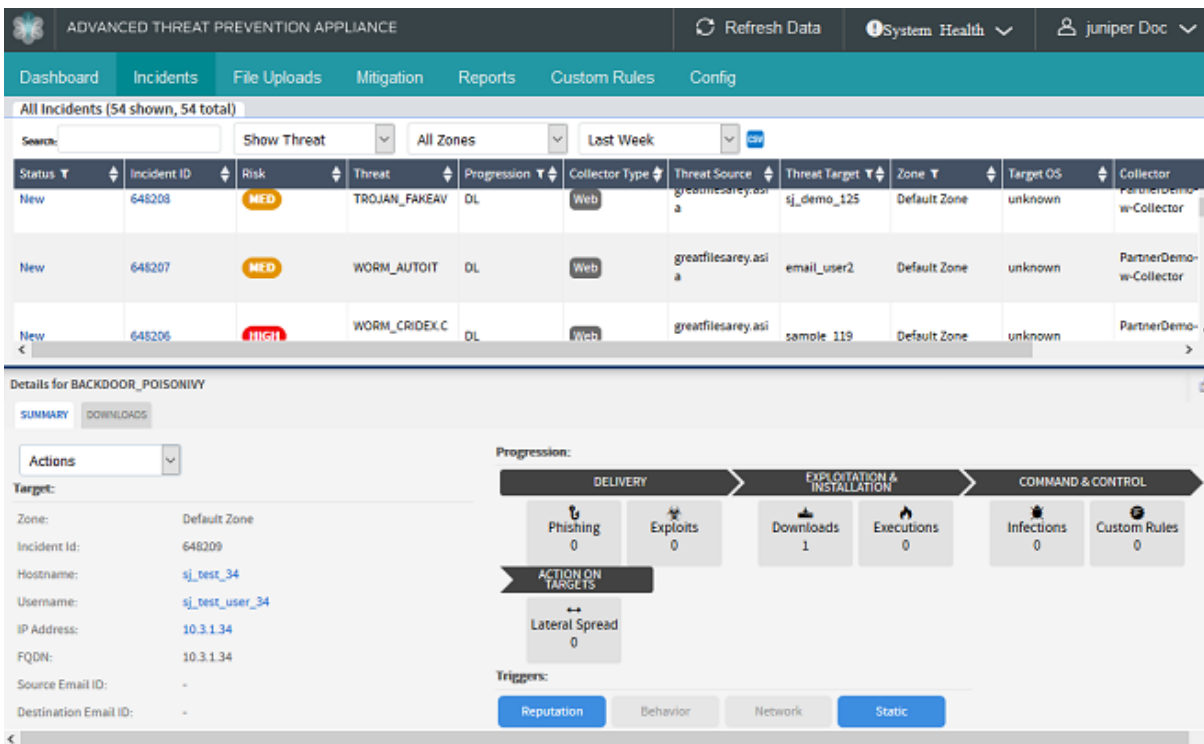
Juniper ATP Appliance's one-of-a-kind hierarchical reasoning and machine learning engines employ virtualized as well as emulated object analysis, combined with Juniper ATP Appliance's distributed big data correlation engines, to accurately and dynamically detect advanced malware threats in network traffic and generate actionable intelligence about the threats that matter to your particular organization.

Juniper ATP Appliance's multi-OS detection engines (Windows and Mac OS X) provide malware detonation as well as detailed, context-aware coverage of all attack vectors with deep analysis of all attack stage activities along the Threat Kill Chain. Immediate verification and auto-mitigation is also provided via Palo Alto Networks (PAN), Juniper SRX Firewall, Cisco ASA, Check Point firewalls, Fortinet firewalls and BlueCoat Proxy SG integrations along the network path, in addition to Carbon Black Response integration at the network endpoint. Juniper ATP Appliance's on-demand endpoint IVP (Infection Verification Package) brings Juniper ATP Appliance's advanced threat protection full circle to secure your enterprise's entire infrastructure.

Juniper ATP Appliance's distributed architecture is designed to break the Threat Kill Chain while adapting to literally any enterprise network architecture. Juniper ATP Appliance separates continuous inspection of traffic data and network objects from threat detection and analytics, using Juniper ATP Appliance's unique object-based Traffic Collector technology. The distributed Juniper ATP Appliance system is a significant advantage over existing analysis and detonation technologies because it allows for the deployment of various traffic Collectors throughout the network, in

a substantially cost-effective manner, incurring less latency during dynamic behavioral-analysis cycles, and greater visibility and coverage of the breadth of an enterprise network and its kill chain vulnerabilities.

Figure 3 Kill Chain Progression Mapping on the Juniper ATP Appliance Incidents Tab



Juniper ATP Appliance threat intelligence pinpoints and highlights:

- The threat aspects that constitute kill chain progression
- The attack location in the “kill chain”
- The in-context metrics about how close the malware is to achieving an intended kill and posting kill exposure

Context-Aware Detection and Juniper ATP Appliance Intel

Recently there has been a marked increase in advanced payload delivery mechanisms that use advanced evasion techniques. These threats are stealthily designed to bypass network security solutions by changing dynamically during an on-going attack and becoming stackable through parallel executions on multiple protocol layers, making it difficult for traditional security solutions to detect them. Also, the delivery of a payload is mostly distributed across multiple platforms such as Mobile or Web, or over an extended period of time.

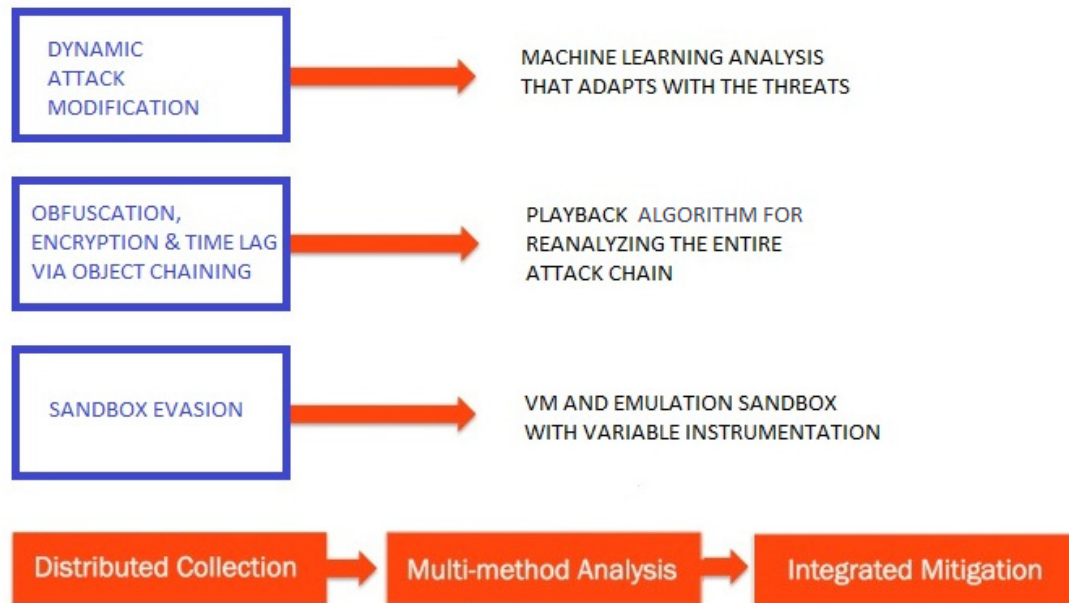
Evasive attacks are successful due to the lack of contextual awareness and full visibility by current security solutions. The challenge in detecting advanced evasive threats at an early stage is tied to the fact the security solutions and analysts have to find numerous low-level signals and correlate the appropriate pieces of various threats against each other. This breeds complexity since the data is a combination of structured and unstructured signals combined with various levels of meta-data from different network segments. Considering the scale and complexity of most enterprise infrastructures, the task of validating, prioritizing and mitigating relevant threats requires Juniper ATP Appliance's distributed architecture coverage and context-aware, object-focused intelligence.

The prerequisite to detecting advanced threats is establishing full visibility by leveraging a distributed architecture combined with “long” data analysis combined with in-depth assessment of the threat's impact on the full

ecosystem. Understanding how various aspects of a threat relate to each other is required for stopping determined adversaries.

The Juniper ATP Appliance product suite provides a unique solution that combines intelligence technology from the Web/Email Traffic Collectors and detonation engines to provide a defense-in-depth architecture. This end to end correlation protects the entire enterprise network and performs as a protective layer against attacks that employ advanced malware.

Figure 4 Juniper ATP Appliance Correlates Situational Awareness and Context with Threat Defense Analysis



When operating in concert, the context-aware Juniper ATP Appliance product suite complements the effectiveness of other layers of the enterprise architecture while supporting existing security infrastructure. The following figure shows a distributed enterprise deployment with appliances in each of the available configurations, and with Juniper ATP Appliance Central Manager deployed for centralized collection and detection management.

Juniper ATP Appliance Multi-Platform Product Suite

Juniper ATP Appliance's multi-OS product solutions are designed to monitor and defend the entire enterprise against malicious attacks from all threat vectors. Many threats use different channels and incremental stages to bypass traditional protections. An attack might enter the network when a user clicks a URL, causing an array of drive-by downloads that assault the browser while searching for vulnerabilities. The Juniper ATP Appliance product suite components works together to detect and stop such blended threats.

Table 1-1 Juniper ATP Appliance Products and Components

Product Component	Deployment Location(s)	Model Options
Juniper ATP Appliance Core Engine (Windows)	Locate anywhere in the enterprise network, in a clustered deployment, and/or in remote branch office(s)	Juniper ATP700 Appliance

Table 1-1 Juniper ATP Appliance Products and Components

Product Component	Deployment Location(s)	Model Options
Juniper ATP Appliance Virtual or Secondary Core Engine (Windows)	Locate anywhere in the enterprise network and/or in remote branch office(s); Connected logically to the Primary Core.	Juniper ATP Appliance, OVA VM, vCore for AWS, or Software-only
Juniper ATP Appliance Central Manager	Locate anywhere in the enterprise network as part of the [Primary] Core; Manages traffic collector objects and multi-platform Detonation engine detection, analysis and reporting (Web UI).	Packaged with the Core Engine [Primary Core in the case of clustered deployments]
Juniper ATP Appliance Web Traffic Collector	Locate at any network location; most typical: Internet (or network) egress. If a web proxy is present, refer to optional deployment scenarios in the next chapter.	Juniper ATP Appliance Web Collector Appliance, Virtual, OVA or Software-only
Juniper ATP Appliance Email Traffic Collector	Locate between the anti-spam gateway and the network's internal mail server(s), such as MS-Exchange. The Email Collector does not parse email messages out of a SPAN port; deployment requires an account to login to a special email account (Journaled or BCC) to get email for analysis using POP or IMAP.	A component of the Juniper ATP Appliance Core or All-in-One System
Juniper ATP Appliance Secondary Core (Mac OSX Detection)	Locate anywhere in the enterprise network and/or in remote branch office(s); Connected logically to the Primary Core.	Juniper ATP Appliance software for Mac Mini Devices
Juniper ATP Appliance All-In-One	Locate anywhere in the enterprise network. Logically connect a Mac Mini Secondary Core for Mac OSX Detection coverage. (Central Manager Core (Windows) Collector)	Juniper ATP700 Appliance
Global Security Services (GSS)	Configured for any of the Juniper ATP Appliance CM/ Core appliances or All-in-One appliances.	Service
clustered or virtual	Software and Cloud-based deployment: Virtual Collector, Virtual Core for AWS, and vCore (OVA)	Many options; refer to respective Juniper ATP Appliance Quick Start Guide

Juniper ATP Appliance Core and Secondary Core Detonation Engines

Juniper ATP Appliance's Core integrates Windows platform malware analysis with Mac OS X monitoring and malware detection.

The Juniper ATP Appliance Windows detonation engine resides on the Core (regardless of whether you are implementing an All-in-One deployment, or a clustered or virtual or physical Core/CM deployment in the enterprise network or in the Amazon cloud).

The Juniper ATP Appliance MAC OS X detonation chamber (Secondary Core) runs on a Mac Mini (not supplied by Juniper) and is for detecting both known and unknown threats in web and email traffic.

The Juniper ATP Appliance Core Central Manager coordinates all detection and intelligence data in its Web UI displays and threat views, in concert with Juniper ATP Appliance's GSS, Global Security Services.

Juniper ATP Appliance detonation engines fully execute suspicious traffic objects: code, attachments, files, and URLs. Juniper ATP Appliance Collector automation moves suspicious traffic through a series of known-rules static, reputation, network and behavioral reasoning sequences with machine learning adaptation as the traffic is moved into and through Juniper ATP Appliance's instrumented execution engines.

In the Core Windows and Mac OS X, suspected malware is executed in the virtualization environment and fully examined. In Juniper ATP Appliance's Core Windows and Mac OS X environment, real-world malware is allowed to trigger zero-day assaults, escalations, and other next-generation functions so that Juniper ATP Appliance can examine and assess its full threat potential.

Following detonation in the virtualization chamber, the malware is next run through its paces using emulation. For example, the internal Core Windows and Mac OS X of the Juniper ATP Appliance Web appliance emulates the browser (client) side of suspicious web transactions between actual network users and web servers to determine if the web server is attempting to infect the browser. Suspicious code is replayed into and analyzed inside the emulation engine, enabling it to discover polymorphic or zero-day malware that may not have been seen before. Real threats to the enterprise are identified and stopped in their tracks by Juniper ATP Appliance's malware protection system engines, and analyses are available as detailed reports in the Central Manager Dashboard, Incidents Tab and Mitigation pages for malware remediation and forensics teams.

Juniper ATP Appliance detonation engines accumulate detailed information about the examined threat: malware analysis results provide the IP addresses associated with the malware, the network protocols employed, specific ports that are targeted, and intelligence about how attackers cloak, communicate, and distribute payloads. Using this data, Juniper ATP Appliance captures callbacks and all data exchange between the malware and its remote command and control (CnC) center. With detailed context-driven malware analyses and threat metric reporting, administrators can select real time mitigation options available from the Central Manager, including Juniper ATP Appliance's integrated PAN OS, SRX, Cisco ASA, Check Point, Fortinet and BlueCoat ProxySG mitigations, endpoint infection verification (Juniper ATP Appliance IVP), and the Carbon Black Response Juniper ATP Appliance-partner response system for real time endpoint mitigations inside, as well as outside, the enterprise network perimeter.

Quick Links to More Juniper ATP Appliance Core Information

- Refer to the Juniper ATP Appliance Quick Start Guides for your products for information about initial installation and configuration of Juniper ATP Appliance Cores:
 - › Juniper ATP Appliance All-in-One System Quick Start Guide
 - › Juniper ATP Appliance Core/CM Quick Start Guide
 - › Juniper ATP Appliance Virtual Core for AWS Quick Start Guide

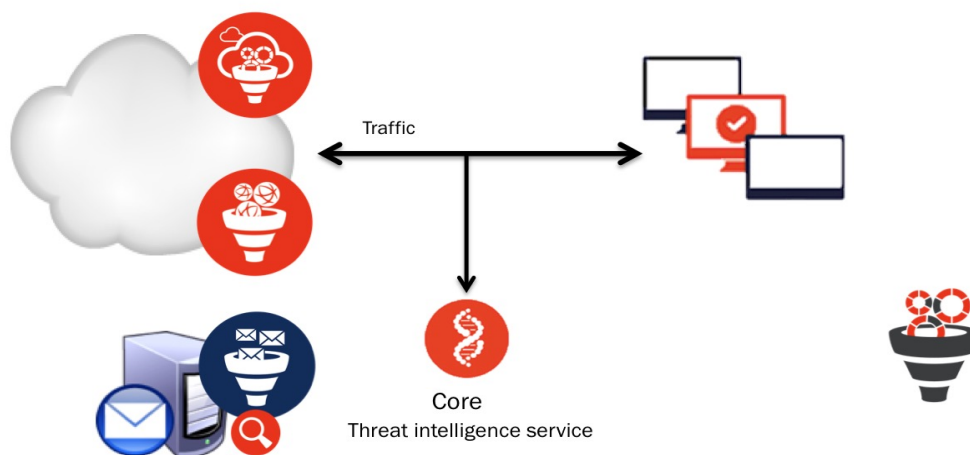
Juniper ATP Appliance Traffic Collectors

The Juniper ATP Appliance Traffic Collector appliance scans and analyzes web objects and emails to identify malicious threats. Web Collectors inspect network callbacks and perform object collection, including user session data and link tracebacks. Email Collectors perform email attachment collection and email metadata inspection.

Juniper ATP Appliance Collectors can be deployed as a physical appliance, as a software-only ISO, or as a VM OVA. Collectors connect to the network switch SPAN/TAP port.

NOTE For multi-tenancy MSSPs, Juniper ATP Appliance Traffic Collectors can be deployed for tenant-specific MSSP sites. Refer to [Multi-Tenancy Web Collector Zones: Managed Security Service Provider \(MSSP\) Support on page 11](#) for more information.

Figure 2 Juniper ATP Appliance Traffic Collector Deployments



1. Continuously monitor command and control traffic for persistent threats
2. Coverage across networks, VMs and cloud
3. Early mitigation before breach happens
4. Protection from infected mobile users, partners and customers

Multi-Tenancy Web Collector Zones: Managed Security Service Provider (MSSP) Support

Juniper ATP Appliance integrates Traffic Collector deployments at tenant sites. Each tenant-configured Collector is connected to the Juniper ATP Appliance Core Cluster hosted at the MSSP site. All management of incidents is performed by the MSSP; tenants do not have access to the Core cluster.

A configured Zone is defined at the Juniper ATP Appliance Central Manager Web UI to identify and correlate incidents and events per tenant. The MSSP defines a Zone per tenant and groups all Collectors associated with a tenant to a tenant-specific Zone, which is then added to the Juniper ATP Appliance CM Web UI Zones configuration page. Thereafter, all event correlation progressions track events per originating Zone, and correlate events within the same Zone. In this way, the multi-tenant MSSP manages incidents per Zone/Tenant using the Juniper ATP Appliance Central Manager.

Traffic Collector Performance, Confidence and Diagnostics Displays

Traffic Collector performance metrics are provided in the new Central Manager Web UI Collector Dashboards (Web and Email).

Top-level health indicator summaries are color coded to indicate total Collector health. For example:

- › The indicator for an Offline Collector is RED.
- › The indicator for a Degraded Collector is YELLOW.
- › When all elements are nominal, the indicator is GREEN.

Clicking on a health-indicator on a Collector Dashboard page opens the System Dashboard. The System Health page summarizes all system alerts.

- No user configuration or action is required.

Web UI Cyber Kill Chain Progression Mappings

The Log Event Extended Format (LEEF) is a customized event format for IBM® Security QRadar®. Juniper ATP Appliance supports the sending of SIEM threat alerts for malware events in LEEF format for QRadar integration.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.20	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.222.234.2.119	0	10.1.1.20	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	106.179.26.151	0	126.125.249.182	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	103.106.172.140	0	10.1.1.24	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	187.17.38.219	0	10.1.1.4	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	202.214.216.27	0	10.1.1.42	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	196.199.243.109	0	10.1.1.40	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	90.69.64.52.196	0	10.1.1.2	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.21.170.165.131	0	10.1.1.48	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	113.47.49.191	0	10.1.1.44	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	10.2.20.47	0	10.1.1.5	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.4	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	10.2.20.47	0	10.1.1.5	0	N/A	100
Infected Host	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.2.20.47	0	10.1.1.5	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	74.208.164.106	0	10.1.1.26	0	N/A	100
Malicious Email	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Mail Attachment	235.190.83.195	0	235.190.83.149	0	N/A	100
Malicious Email	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Mail Attachment	10.2.20.47	0	10.2.20.47	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.2	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.26	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.24	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.36	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.48	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.44	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.48	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.42	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.54	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.52	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	202.214.216.27	0	10.1.1.42	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.58	0	N/A	100
A malicious file was downloaded	tap47.eng.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	100.104.104.103	0	10.1.1.45	0	N/A	100

NOTE Installation of the DSM-Juniper ATP Appliance extension plugin on the QRadar server is required.

- For configuration information, refer to [Configuring SIEM Settings on page 101](#), and the [Juniper ATP Appliance CEF LEEF and Syslog Support for SIEM User's Guide](#).

Integrated Network | Endpoint Mitigation

Object-based end-to-end malware defense is performed in two parts: detection and mitigation. The blocking of web-based threats requires that the Juniper ATP Appliance Core be integrated during configuration with the network IPS/Next Gen Firewall, Proxy or Web Gateway. In addition endpoint protection is secured with Carbon Black Response and CrowdStrike Endpoint integrations as well as the Juniper ATP Appliance IVP, Infection Verification Package. The Juniper ATP Appliance Threat View on the Central Manager Web UI Dashboard, Incidents and Mitigation pages enable real time incident response. And malicious CnC callbacks are also actively detected and blocked on the outbound with these integrated systems in place.

Juniper ATP Appliance uses its in-depth threat intelligence to detail and prioritize defensive actions using an enterprise's existing security infrastructure: integrated auto-mitigation with existing FW, SWG and IPS. In this way, Juniper ATP Appliance can push malicious content per host IP address to existing blocking rules in Palo Alto Networks firewalls, Cisco ASA, Check Point, Fortinet or Juniper SRX firewall equipment, for example, or push URLs associated with detected threats to the PAN firewall or a BlueCoat ProxySG.

Juniper ATP Appliance Endpoint Mitigation Options:

- Juniper ATP Appliance Global Security Services (GSS)
- Integration with existing security and blocking infrastructure, including automatic and proactive mitigation options and URL blocking
- False Positive (FP) and False Negative (FN) Reporting via the Central Manager Web UI.
- SIEM integration and CEF Logging Support
- Juniper ATP Appliance blocking and enforcement support with selected network and endpoint vendors/partners such as Carbon Black Response and CrowdStrike.
- Juniper ATP Appliance Infection Verification Package (IVP)

CrowdStrike Endpoint Integration

Juniper ATP Appliance's "CrowdStrike Endpoint Integration" supplements Juniper ATP Appliance's

established Carbon Black Response integration for endpoint threat detections and mitigation. Specifically, CrowdStrike endpoint integration determines whether a binary that Juniper ATP Appliance detected over an enterprise network is executed at an endpoint. Juniper ATP Appliance incidents are then marked "EX" to indicate a higher threat risk in order to help an incident response team to assess their response.

To configure CrowdStrike integration at the Juniper ATP Appliance Central Manager Web UI, users need to enter:

- › CrowdStrike Falcon API server hostname
- › CrowdStrike Falcon API user
- › CrowdStrike Falcon API key

At the Juniper ATP Appliance Central Manager Web UI Incidents page, an exploit (EX) flag is displayed if an endpoint has executed detected malware. The Web UI self-updates to display information from the endpoint agent when a certain file is executed on an endpoint host.

NOTE: AD integration must be enabled as a prerequisite for CrowdStrike Endpoint Integration.

- Refer to [Configuring Endpoint Integration: CrowdStrike and Carbon Black Response on page 166](#) for configuration information.

SMB Lateral Detection

Juniper provides support for monitoring the SMB network file sharing protocol version 2.1. This allows for the extraction of file transmissions between clients, or between clients and servers, similarly to the way Juniper ATP Appliance currently monitors HTTP traffic. Juniper ATP Appliance's support of lateral "east-west" SMB traffic monitoring and detection, in addition to the monitoring of "north-south" ingress and egress traffic, helps identify malware as it spreads to other hosts within an organization from an infected endpoint. Because HTTP is rarely used to communicate between endpoints within an organization, SMB is a significant vector for malware transmission and infection proliferation within an enterprise.

NOTE Support includes Windows 7 Windows Server 2008 R2 Version 2.1 and Windows 7 Windows Server 2008 R2 Samba Server 2.1. This means that either the client or the server must be running Windows 7 or Windows Server 2008 R2, and on the other end, either the client or the server must be running Windows 7/Windows Server 2008 R2 or later. On Linux platforms, for SMB lateral detections, run Samba Server Version 2.1 on one end, and Windows 7/Windows Server 2008 R2 on the other end.

An Advanced License Key must be installed to activate SMB support.

To view SMB detections from the Central Manager Web UI, refer to [Viewing SMB Lateral Detections on page 283](#) in the Incidents Tab Downloads summary tables.

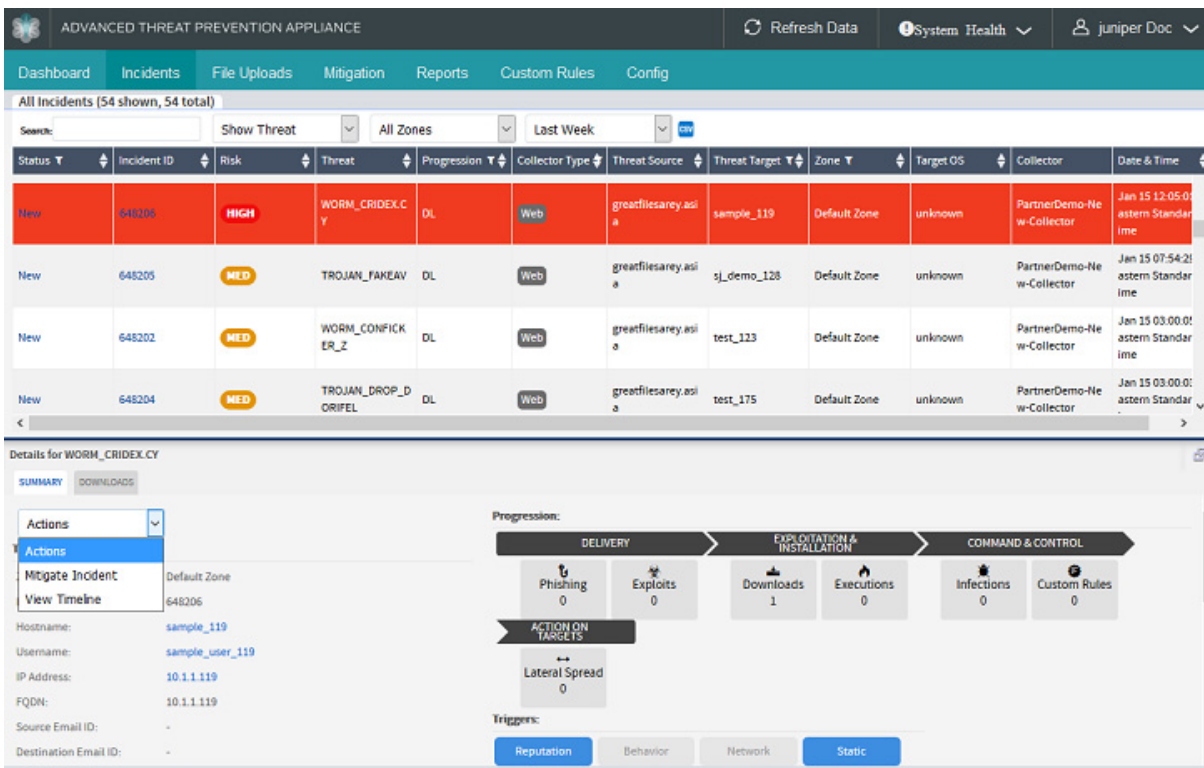
Juniper ATP Appliance also supports SSH Honeypot lateral detections; refer to the next section, as well as [Lateral Detection Enhancements: SSH Honeypot on page 13](#) for more information.

Lateral Detection Enhancements: SSH Honeypot

The Juniper ATP Appliance Central Manager Web UI Incidents tab includes results for its SSH Honeypot feature. A honeypot deployed within a customer enterprise network can be used to detect network activity generated by malware attempting to infect or attack other machines in a local area network. Attempted SSH login honeypots are used to supplement detection of lateral spread. A honeypot can be deployed on a customer Traffic Collector from which event information is sent to the Juniper ATP Appliance Core for processing. Customers can place a honeypot on any local network they desire.

Juniper ATP Appliance's interactive graphical Kill Chain includes Lateral Spread displays on the Incidents tab Summary Details page.

Figure 4 Details Summary Progression Map



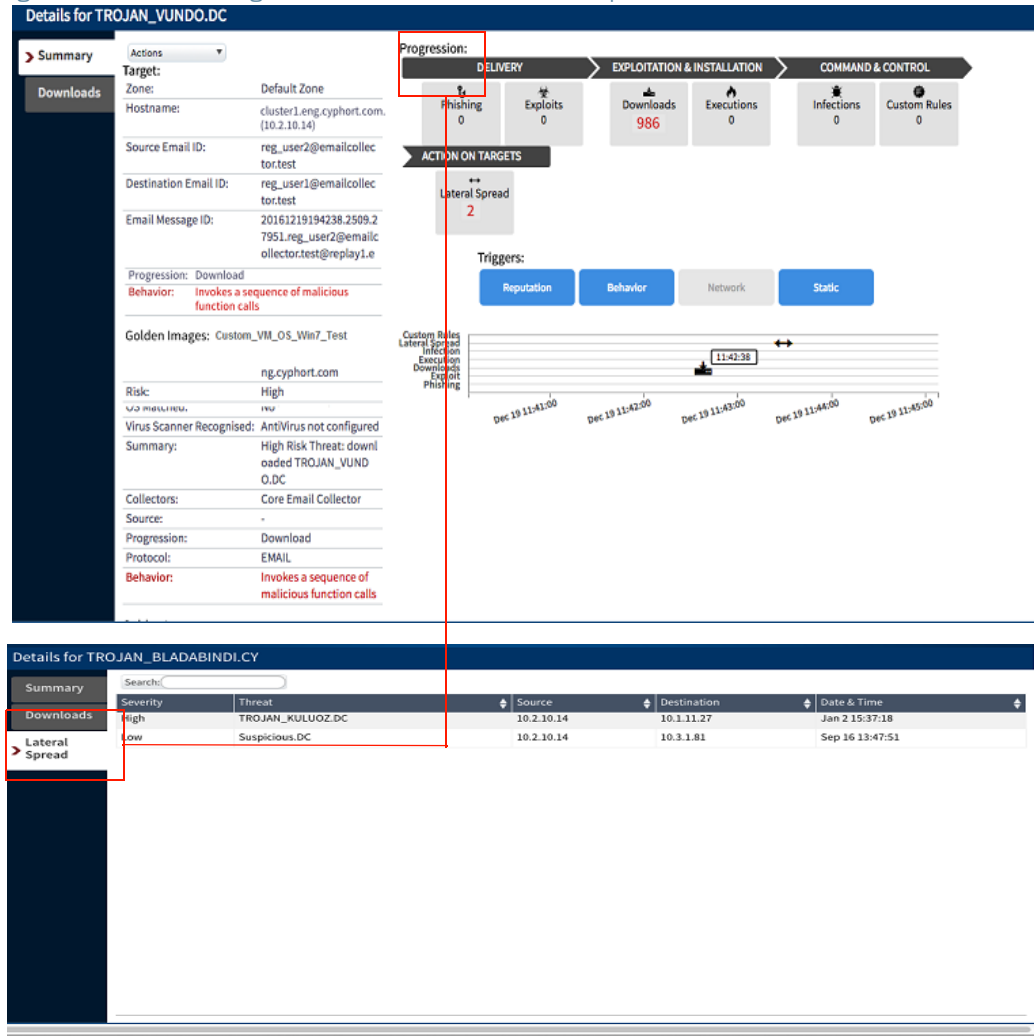
The Kill Chain Progression graph shows dated occurrence mapping of LS (Lateral Spread), IN (infection), DL (downloads), XP (Exploits), Lateral Spread (LS), Phishing (PHS), and so on. The Kill Chain icons help administrators, at a glance, determine quickly what event(s) took place and at which stage in the Kill Chain at which time.

TIP Clicking on a Kill Chain Progression button opens its corresponding page of detailed information; for example, Clicking the Infections button opens the Infections Details page.

The detection Triggers for this Kill Chain incident are displayed directly above the Progression graph. Those triggers displayed in blue were actively triggered during monitoring and analysis. The Triggers include: Reputation | Behavior | Network | Static.

When the Kill Chain Progression display shows Lateral Spread activity, as in the example below, you can click the interactive Lateral Spread button icon in the Kill Chain to open the Lateral Spread Details page:

Figure 5 Kill Chain Progression Indicates Two Lateral Spread Events



NOTE Downloads and Lateral Spread events can look similar on the Juniper ATP Appliance Web UI Incidents page. The difference is specific to whether the host IP is the malware source or destination. If the malware source is a lateral spread event that targets a recipient, in other words, the hJuniper ATP Appliance is receiving the malware, then it is considered a download.

No configuration is required. Refer to [Graphical Kill Chain Progression Display on page 285](#) for more information.

With endpoint identity integration, the Lateral Spread graph displays the endpoint hostname as the node name if it's available; otherwise, the endpoint IP address is supplied.

Kill Chain Stages

Juniper ATP Appliance's Central Manager Web UI Incidents page includes kill chain progression mapping showing incident alignment with the Gartner kill chain stages.

Figure 6 CM Web UI Kill Chain Progression Mappings: Mouseover or Click to Display Descriptions

All Incidents (500 shown, 12431 total)

Search: Show Threat All Zones Last Month CSV

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Target OS	Collector	Date & Time
New	102502	MAX	Phishing	PHS	EMAIL	systest_user2@mailcollector.test	systest_user1@mailcollector.test		Core Email Collector	Dec 12, 2018 10:11:14 AM
New	102501	MAX	Phishing	PHS	EMAIL	systest_user2@mailcollector.test	systest_user1@mailcollector.test		Core Email Collector	Dec 12, 2018 10:11:14 AM
New	102500	MAX	Phishing	PHS	EMAIL	systest_user2@mailcollector.test	systest_user1@mailcollector.test		Core Email Collector	Dec 12, 2018 10:11:14 AM
New	102499	MAX	Phishing	PHS	EMAIL	systest_user2@mailcollector.test	systest_user1@mailcollector.test		Core Email Collector	Dec 12, 2018 10:11:14 AM

Details for Phishing

Details for TROJAN_MIUREF.DC

SUMMARY EXPLOITS DOWNLOADS EXTERNAL SOURCES

Actions:

Target:

Zone: Default Zone

Incident ID: 5428

Hostname: NICK-LAPTOP

Username: nick

IP Address: 1.1.1.14

FQDN: nick.eng.cyphart.com

Source Email ID: systest_user2@mailcollector.test

Source Email ID: systest_user2@mailcollector.test

Destination Email ID: systest_user1@mailcollector.test

Progression:

DELIVERY	EXPLOITATION & INSTALLATION	COMMAND & CONTROL
Phishing 0	Exploits 1	Downloads 1
	Executions 0	Infections 0
		Custom Rules 0

ACTION ON TARGETS

Lateral Spread 0

The different kill chain stages are:

- › Reconnaissance,
- › Weaponization
- › Delivery [Juniper ATP Appliance's progressions start here with the Kill Chain Delivery stage.]
- › Exploitation
- › Installation
- › Command and Control
- › Action on Targets

Juniper ATP Appliance's progressions start with the Delivery stage. The Juniper ATP Appliance Progressions are mapped to the Cyber Kill Chain Stages as shown below:

Juniper ATP Appliance Progression Mappings Per Kill Chain Stages

Delivery >	Phishing, Exploits, Downloads
Exploitation and Installation >	Execution
Command and Control >	Infections, Custom Rules
Action on Targets >	Lateral Spread

- Refer to [Understanding Threats and Incidents on page 273](#) for more information.

YARA Rules and Lateral Detection

Remote Administration Tools (RATs) can be detected using YARA rules. By adding the ability to push YARA rules to Juniper ATP Appliance devices, Juniper ATP Appliance can detect the lateral spread of Remote Administration Tools (RATs) within a network.

Each Juniper ATP Appliance YARA rule includes the following additional information:

- Rule Name
- Rule Description
- Severity (between 0 and 1)
- File Types for which the rule is to be applied

Juniper ATP Appliance's analysis engines test new downloads against each YARA rule, and the YARA results are used by the machine learning components to help generate a final severity score and malware name.

YARA rules are always installed and applied against downloads.

The Juniper ATP Appliance YARA engine uses YARA Version 3 (backwards compatible with version 2). Details of matched YARA rules are shown in the Downloads tab of the Incidents page.

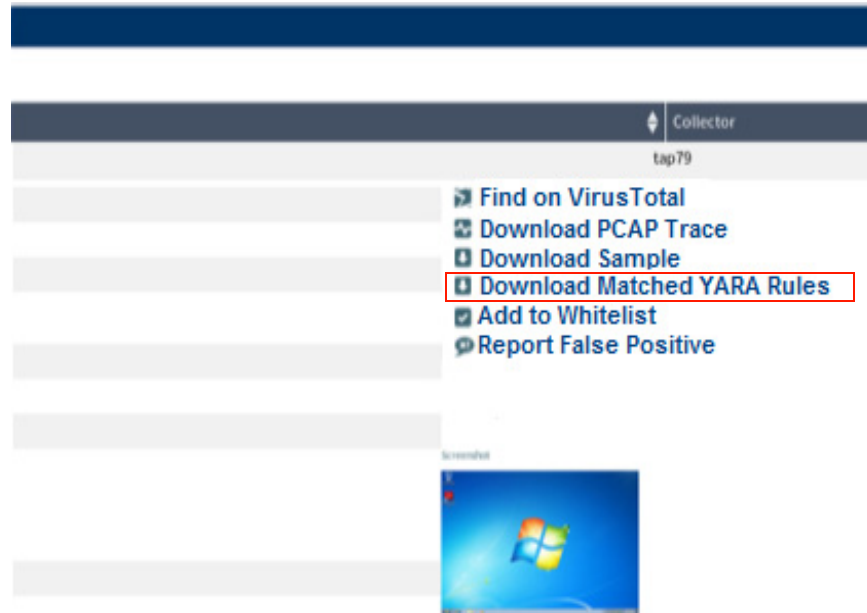
Figure 7 Yara Rule Match for Lateral Detection Download on Incidents>Download Page

The screenshot displays the 'Details for Trojan_Generic.DC' page. The 'Downloads' tab is active, showing file details such as File Size (134,656 (132KB)), File Hashes (MD5, SHA1, SHA256), and Confidence (High). The 'YARA Information' section is highlighted with a red box, showing a match for the 'XtremeRATStrings' rule with a severity of 0.500. The 'Behavior Information' section shows top indicators like 'Creates suspicious file with intention to overwrite on system paths'.

Rule Name	Severity	File Name	Description
XtremeRATStrings	0.500	cyphort/Xtreme.yar	Xtreme

All matched YARA rules can be downloaded from the Incidents page:

Figure 8 Option to Download Matched YARA Rule on Incident Page



An Advanced license is required to enable SMB, but YARA rules are always installed and used regardless of SMB status.

Juniper ATP Appliance HTTP API

The Juniper ATP Appliance Central Manager supports an HTTP API for accessing all threat and system processing data as well as device and software configuration. All functionality available from the Central Manager Web UI is also accessible via the HTTP API.

As part of all API requests, JSON is returned in all responses from the API, including errors.

The Juniper ATP Appliance Smart Core Platform is specifically designed to work seamlessly with existing security infrastructure, providing rules and mitigation options that contribute to full contextual awareness of each enterprise environment, including its enforcement points. This integration helps to prioritize threats and reduce threat response time (blocking and situation-aware mitigation rules) from hours or days to minutes.

Juniper ATP Appliance's built-in API pushes mitigation rules to existing infrastructure, leveraging existing enforcement solutions via firewalls, IPS/IDS (for blocking), or AV. And infection validation using IVP and Carbon Black Response allows the Juniper ATP Appliance platform to become a deeper part of the infrastructure mesh rather than just another security patch point solution.

STIX API Integration

Structured Threat Information Expression (STIX™) is a language used to qualify cyber threat data and intel so it can be exchanged, stored, and analyzed. Juniper ATP Appliance includes an API that allows users to query Juniper ATP Appliance to obtain Indicators of Compromise (IOC) in a standard STIX format.

- Refer to the Juniper ATP Appliance HTTP API Guide for details and usage information.

Juniper ATP Appliance Global Security Services (GSS)

Juniper ATP Appliance global security service (GSS) provides cloud services for Juniper ATP Appliance and its customers. Juniper ATP Appliance's Global Security Service is a cloud-based subscription service that works in conjunction with the Juniper ATP Appliance Advanced Threat Defense Platform to provide enhanced threat detection and mitigation. The Juniper ATP Appliance Global Security Service continually updates all aspects of the Juniper ATP Appliance Advanced Persistent Threat Platform's multi-method detection engine, providing new threat intelligence, machine learning models and static analysis signatures.

The GSS provides:

- System monitoring and reporting services
- Automatic software and security content updates and refreshes
- Automatic report and alert generation

The Core checks for Core image upgrades every day at midnight. Checks also take place for new software and content updates (if enabled) every 30 minutes. To enable GSS updates, refer to [Configuring GSS Settings on page 129](#).

Automatic updates are performed for:

- Machine learning model updates
- Ongoing threat intelligence
- Static analysis updates

Machine Learning Model Updates

Juniper ATP Appliance uses machine learning analytics for analyzing malware behavior and to provide an analysis assessment. The Juniper ATP Appliance Labs team continuously trains the machine-learning engine with millions of new samples of malicious and non-malicious code. This allows Juniper ATP Appliance to increase the efficacy of detection while learning key characteristics of known good objects, allowing Juniper ATP Appliance to flag object behavior that does not conform to norms. As part of GSS, these updates are provided to customers' Juniper ATP Appliance deployments.

Static Analysis Signature Updates

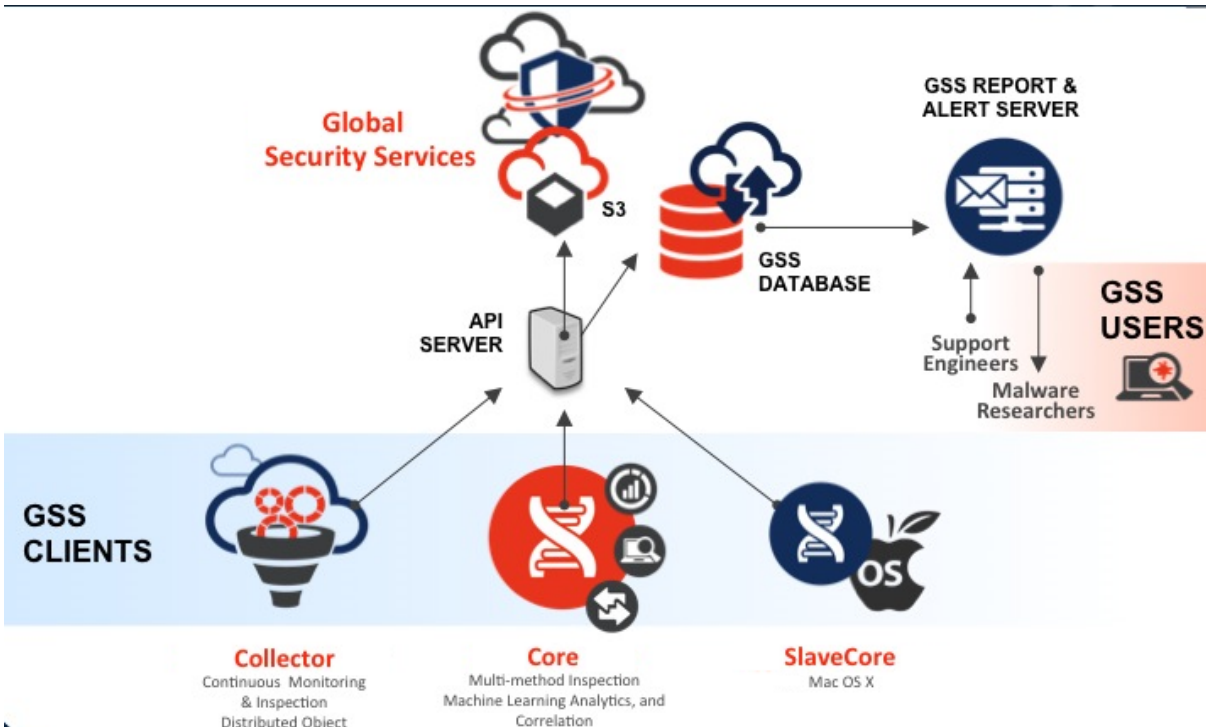
Juniper ATP Appliance continuously adds new signatures for newly found malware across its customer base. These signatures are updated by GSS.

Threat Intelligence Updates

The Juniper ATP Appliance Labs team creates and aggregates threat intelligence from various sources including our crawler network, as well as public and private intelligence feeds. Updated threat intelligence is essential to understanding the detected threats in depth. GSS continually provides the most current threat intelligence to our customers.

NOTE Juniper provides automated refreshing of security content releases.

Figure 9 A Generalized View of the GSS system



NOTE The Juniper ATP Appliance software/security content updates and health and monitoring functionality are incorporated into GSS. Future GSS cloud services will include distributed detonation and analysis handling and remote debugging.

One-Way vs Two-Way GSS Service Options

In order to share the benefits of real-time malware intelligence gathered by local analysis engines around the world, Juniper ATP Appliance has built a global network to distribute auto-generated security intelligence reports about advanced malware worldwide, including any covert call-back channels. As Juniper ATP Appliance analyzes code and traffic for malicious objects, it creates a dynamic fingerprint of all confirmed malware. These malware fingerprints are shared in real-time with subscribers.

Real-time sharing of local malware intelligence is achieved when individual Juniper ATP Appliance Traffic devices connect and share their locally generated malware intelligence, ensuring that the entire Juniper ATP Appliance deployment has protections for the targeted threats designed to infiltrate the enterprise network. When the GSS collects and distributes threat information, it is shared as security content updates:

- All threat data contained in security content is specific only to malware and malicious activities.
- No customer specific data is transferred as part of security content sharing and automatic refreshes.
- The data is transferred over encrypted protocol (HTTPS).

Juniper ATP Appliance GSS is offered in the following two optional ways:

Step 1 Juniper ATP Appliance GSS two-way option

With this option, customers receive all of the benefits of Juniper ATP Appliance GSS and also contribute back to the service by automatically providing to GSS the metadata about new threats found in their

environment. All threat data contained in metadata is specific only to malware and malicious activities. No customer specific data is transferred as part of security content updating.

Step 2 Juniper ATP Appliance GSS one-way option

This option allows customers to benefit from GSS updates without contributing malware information back to the service.

Benefits of two-way sharing:

- Leveraging of the Juniper ATP Appliance Labs threat intelligence to identify and stop threats early in their life cycle
- Keep the machine learning models updated to identify yet unseen threats
- Improve threat categorization and prioritization
- Accelerate threat containment and remediation

Quick Link to More Juniper ATP Appliance GSS Information

- Refer to the [Configuring GSS Settings on page 129](#) for configuration information.
- See also [Configuring System Settings on page 119](#)

Juniper ATP Appliance Dashboard Threat View

The Juniper ATP Appliance Central Manager Web UI Dashboard includes a “Threat View” panel on the Operations Dashboard page, shown below. The Threat View is designed to help users prioritize and focus on the most important attacks within the enterprise network. Implemented as a bubble view, or bubble diagram, the Threat View bubbles graphically represent those threats an admin needs to be most aware of.

Each bubble represents an individual host for which suspicious activity has been observed by Juniper ATP Appliance’s detection and analysis engines. The higher each bubble is displayed on the Y-axis, the more serious is the potential threat; the larger the bubble is in the display, the more correlated or more individual threats have been observed and are in play for that host. The color is another indicator of threat severity, with dark orange representing the greatest threat.

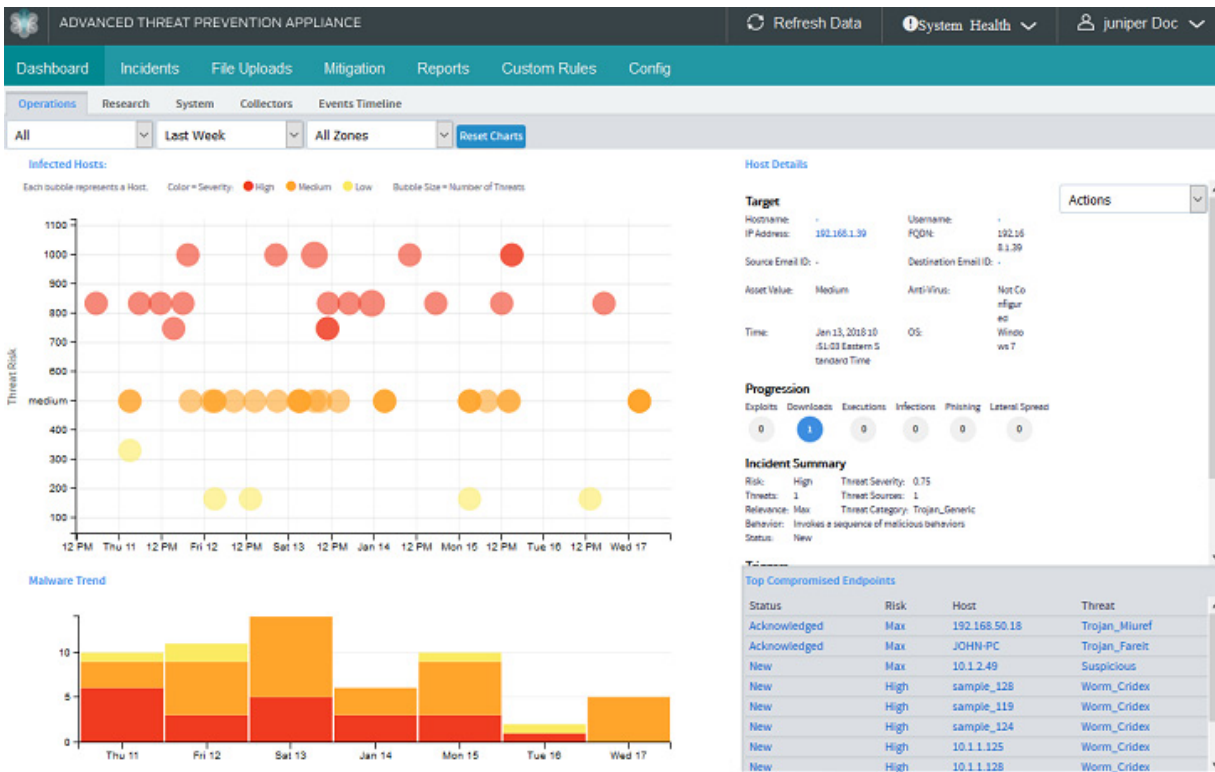
Available Dashboards:

- Operations
- Research
- System
- Collectors
- Events Timeline

Operations Dashboard

The Threat View filters out the noise on the network and displays the threats that matter the most to your enterprise for the time period selected in the dropdown menu above the graphs.

Figure 10 Operations Dashboard



NOTE Threat value colors are translated as:

Critical, High (Red), Medium (Orange), Low (Yellow)

This threat coloring scheme is consistent throughout the Juniper ATP Appliance Central Manager Web UI.

The Infected Hosts area of the Dashboard displays bubble graphs of all host-specific incidents detected by the entire distributed system; the size of the bubbles represents Juniper ATP Appliance's determination of the currently most severe or less severe infections.

Infected Hosts The layout of the Dashboard and its Threat Metric allows you to then drill down into the most critical threats for mitigation or to verify auto-mitigation (if configured).

Click the Reset Charts button to return to the original all-threats view.

To display a bubble's Host Details, click a bubble. Details are immediately displayed to the right of the bubble graph Threat View.

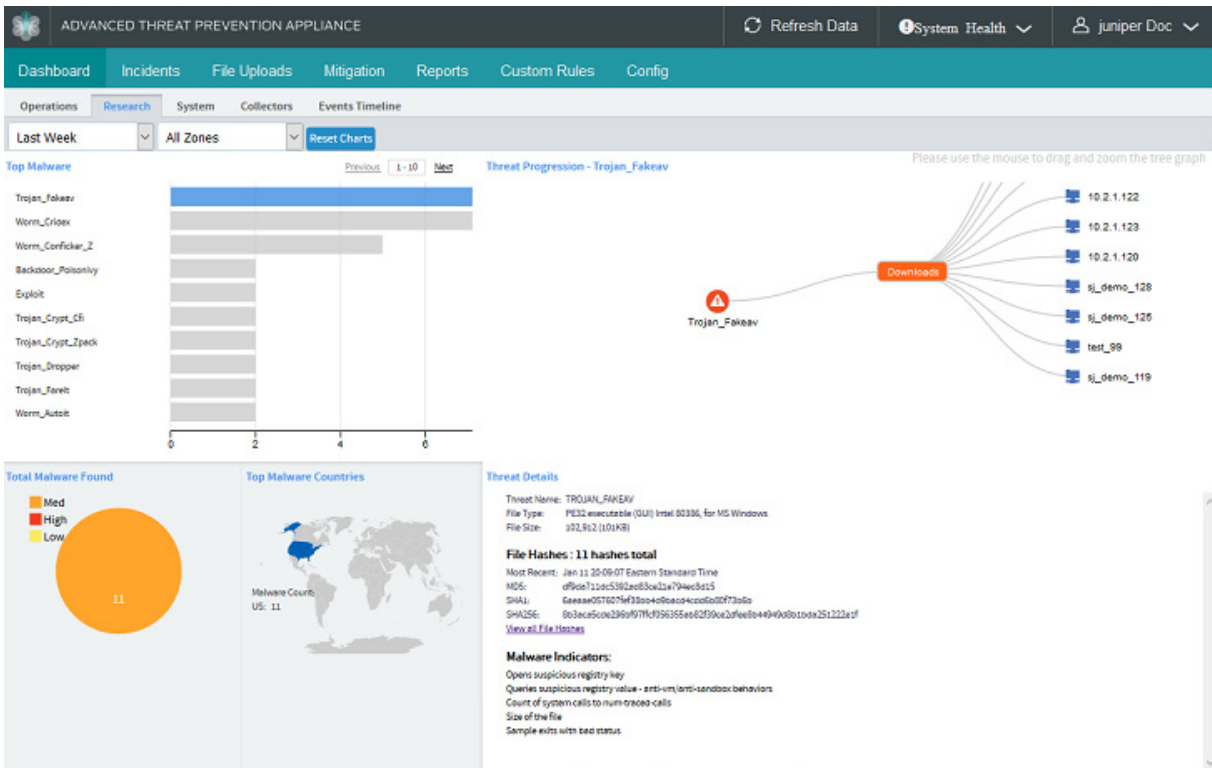
When you double click a bubble in the Threat View, it opens the Incident tab of the Central Manager Web UI to provide a summary and details for the incidents associated with the selected host. In other words, the entire Dashboard UI follows your navigation focus, while detailing threat context and relevance.

- For more usage information, refer to [Using the Dashboard Views on page 113](#).

Research Dashboard

The [Research Dashboard](#) is another context-specific analyst's tool available from the Dashboard tab.

Figure 11 Research Dashboard



The longest line presentation in the Top Malware graph typically represents the greatest threat to the enterprise. When you click on that (or any) single line count in the Top Malware Threat View graph, the Threat Progression array to the right displays the hosts associated with that selected malware threat.

- Drag the threat name in the Threat Progression View to adjust and fan out the array display.
- Click a host IP Address in the array to display Host Details immediately below the array. The host circular-bullet turns orange in the array when selected.

NOTE Select to move and reposition or enlarge/reduce the entire array in order to view all displayed IP addresses.

To recap: when you click on a malware name in the Top Malware graphical list, the Threat Progression View adjusts to display all hosts that have been targeted by that particular malware.

When you double click a Top Malware line in the Top Malware list, it opens the Incident tab of the Central Manager Web UI to provide a summary and details for the incidents associated with that malware. In other words, the entire Dashboard UI follows your navigation focus, while detailing threat context and relevance.

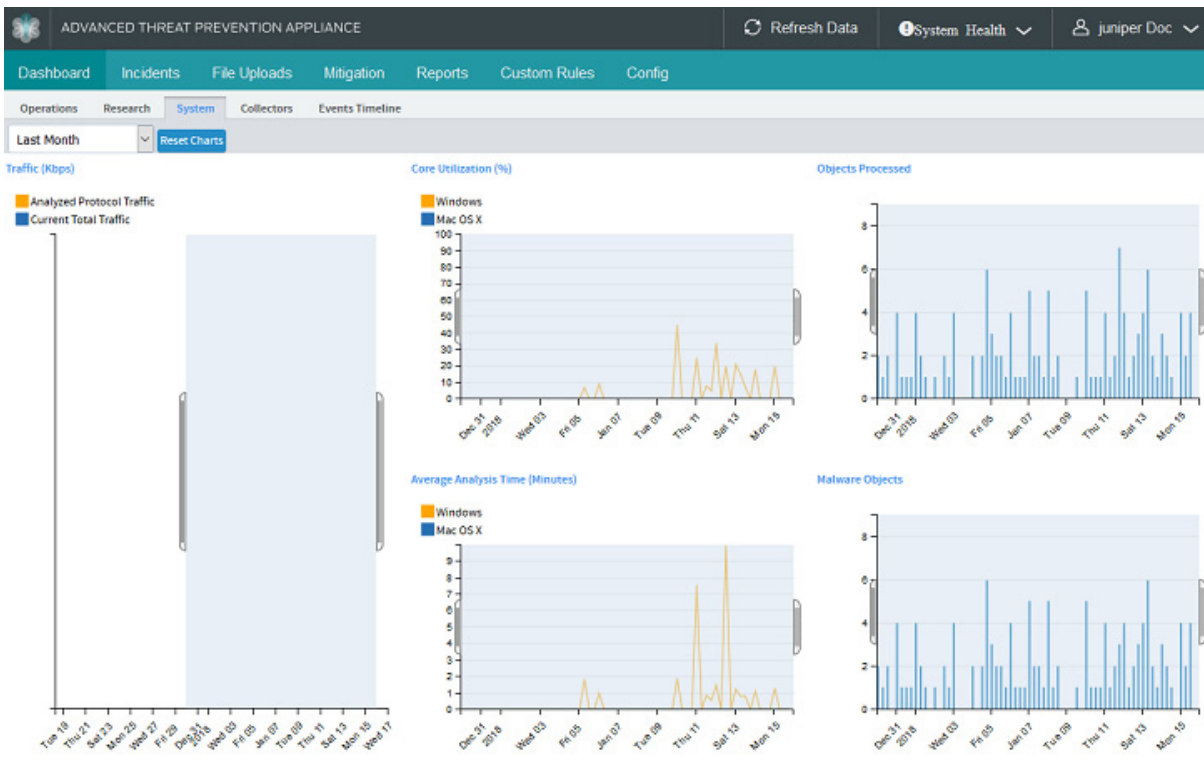
For more usage information, refer to [Using the Dashboard Views on page 113](#).

The Research and Operations Dashboards integrate sets of north-south (ingress-egress) HTTP traffic detection incidents and events as well as lateral east-west incidents and events (detected within the enterprise via SMB monitoring). The Juniper ATP Appliance Central Manager Web UI Dashboards help administrators identify an infected endpoint as well as track the vector of a malicious object throughout the enterprise network from host to host. Moreover, lateral spread east-west malware events are carefully correlated with related web-based incidents (downloads, infections, phishing and exploits).

No configuration is required to access Operations and Research Dashboards, but an Advanced license key is required for mapping the SMB lateral monitoring data. For more information about using the redesigned Dashboards, refer to [Using the Dashboard Views on page 113](#). For information about SMB lateral detection incidents, refer to the Incidents tab [Viewing SMB Lateral Detections on page 283](#) of this guide.

System Dashboard

The System Dashboard is also available from the Dashboard tab as well:



The System Dashboard includes metrics for the following:

- Traffic (Mbps)
 - › Total Traffic refers to traffic seen on the wire.
 - › Analyzed Protocol Traffic refers to all traffic that is used for analysis.

Note: In previous releases, traffic was categorized as "Offered" and "Inspected." Offered corresponds to the current Total Traffic metric. However inspected is not the same as Analyzed Protocol Traffic. Analyzed traffic includes all HTTP traffic, including the bytes that do not form objects. So there may be an expected increase in this metric than measured in the past.

- Core Utilization (Windows and Mac OSX)
- Objects Processed
- Average Analysis Time (in Minutes) (Windows and Mac OSX)
- Malware Objects

System Charts can be displayed for:

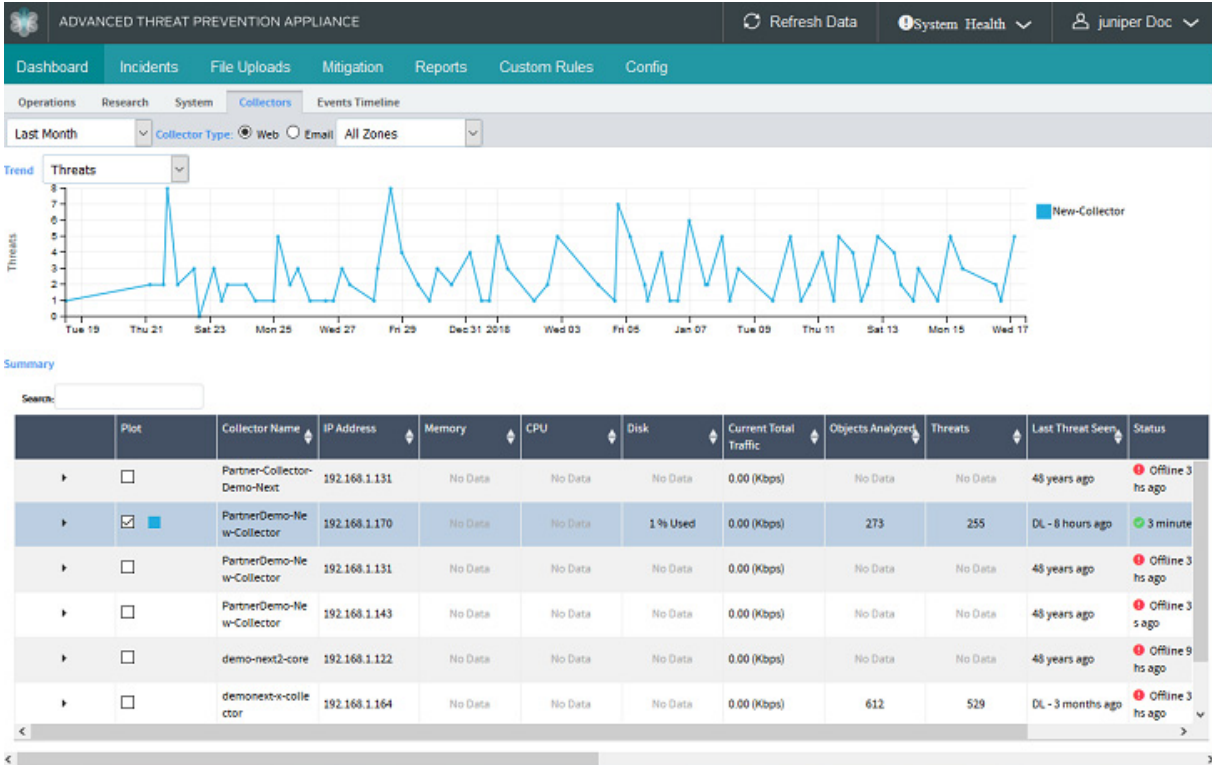
Last 24 Hours | Last Week | Last Month | Last 3 Months | Last Year

For more usage information, refer to [Using the Dashboard Views on page 113](#).

Traffic Collectors Dashboard

The Collectors Dashboard is another dashboard set available from the Dashboard tab:

Select Web or Email Collector views to display graphical trends and details.



Up to 5 Web or Email Collectors can be selected for comparison graphical-trend plotting at the same time.

The Collectors Dashboard includes metrics for the following Trend displays (options are select from the Trend dropdown menu):

- Current Total Traffic (Mbps)
- CPU Usage
- Memory Usage
- Links Analyzed
- Objects Analyzed
- Threats

There is also a Collector Services section provided in the Details; scroll down the Collector Dashboard page to view Services. This section contains data about services that are down or affecting the health of the Collector. If all services are up and running as expected, then an "OK" line is printed:

Graphical data charts can be displayed for Last 24 Hours | Last Week | Last Month

Table 1 The Collectors Dashboard Summary table provides configured and statistical information in the following columns:

Summary Column	Description
Plot	Click to display [multiple] plots for comparisons in the graph above; colors are displayed for each selected graphical plot line
Collector Name	Name of the installed Traffic Collector
IP Address	IP Address of the Collector
Memory	Memory Usage statistics
CPU	CPU usage statistics
Disk	Disk Usage
Current Total Traffic	Total Traffic Scanned in Kbps or Mbps - all the traffic seen on the wire from various Collectors at any instant (not cumulative)
Objects Analyzed	Objects analyzed - cumulative
Links Analyzed	URL extraction and analysis
Threats	Malware Objects detected that account for all types of threat - exploit, malware download, infection - cumulative
Last Seen	Last malware incident detected and analyzed
Status	Last status check on the Collector (example: "83 seconds ago")
Enabled	Green checkmark indicates that the Collector is currently enabled; a red X indicates that the Collector is disabled or offline.

Refer to [Interacting with Dashboard Views and Components on page 116](#) and [Navigating the CM Web UI on page 92](#) for more information about Juniper ATP Appliance Dashboards and usage options.

Events Timeline Dashboard

The Events Timeline Dashboard is a recent addition to the product dashboard views available from the Dashboard tab:

Figure 12 Events Timeline Dashboard



The Event Collector displays every event and action taken to protect a given endpoint or host along a timeline for each integrated vendor as well as for Juniper ATP Appliance detections and actions. You can expand a Timeline view to see how and when the enduser enacted a malicious download.

The Events Timeline Dashboard includes event metrics for the following vendors (for a HOSTNAME | ENDPOINT IP | USERNAME | or EMAIL option that you select from the dropdown menu, specify in the corresponding field, then click GO to process for events display along the timeline view):

- Bluecoat Secure Web Gateway
- Carbon Black Response
- PAN Next Gen Firewall
- Symantec EP
- McAfee ePO

Email Detection Enhancements

Juniper ATP Appliance-MTA-Receiver and Juniper ATP Appliance-MTA-Cloud

Juniper ATP Appliance offers several significant enhancements of email-borne malware detection and mitigation. Both Juniper ATP Appliance Cloud Email Deployment and On-Premise Juniper ATP Appliance-MTA-Receiver Email Deployment scenarios are supported in this release.

NOTE A Juniper ATP Appliance Advanced License is required for all Email Detection configurations.

On-Premise Juniper ATP Appliance-MTA-Receiver Deployments

Juniper ATP Appliance MTA Receiver deployments support receiving emails from different servers including Office 365, Gmail and MS Exchange. It also supports any other email servers/anti-spam gateways that support adding additional SMTP receivers to send emails to the Juniper ATP Appliance MTA Receiver (without adding any SMTP envelop headers to make the original email an attachment). The admin must configure the supported servers to direct the email stream to the Juniper ATP Appliance MTA Receiver using the email address setup on the MTA Receiver (for example: CustomerX@MTA-IP or

CustomerX@DomainName. When using a domain name, the MX records should be resolvable by the servers). In all cases, Juniper ATP Appliance's On-Premise MTA Receiver extracts objects/URL links and submits them to the Juniper ATP Appliance Core for analysis.

Figure 13 On-Premise Juniper ATP Appliance-MTA-Receiver Email Deployment for Office 365, Gmail Analysis

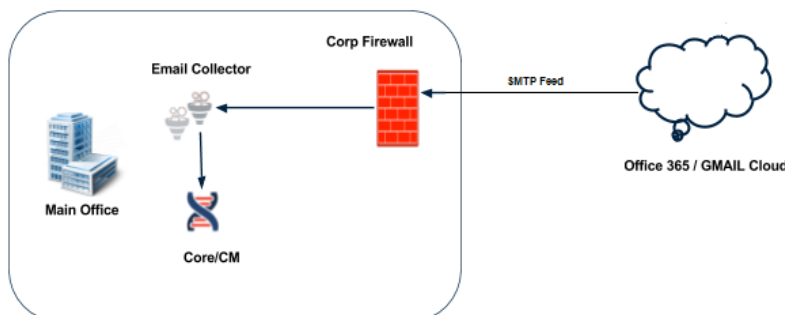
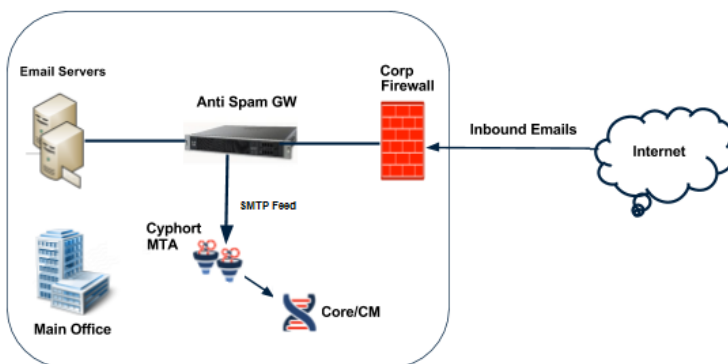


Figure 14 On-Premise Juniper ATP Appliance-MTA-Receiver Email Deployment with Anti-Spam Gateway



Again: this release supports 1) On Premise MTA for Cloud emails, and 2) On Premise MTA for Microsoft Exchange, Ironport, Barracuda etc. For On-Premise Email Deployments, the supported Mail Solutions are:

- Office 365
- Gmail
- MS Exchange
- Cisco Ironport
- Barracuda
- Any mail solution that provides a journaling output using SMTP

Note: An admin must configure their email solution to direct the journaling stream to the Juniper ATP Appliance MTA Collector deployed on-premise at the customer's site (for example: CustomerX@Collector-IP or CustomerX@Collector-hostname). Juniper ATP Appliance's On-Premise MTA Collector extracts objects/URL links for analysis from the email received and redirects the email stream to the Juniper ATP Appliance Core for processing.

- For more information, refer to:
 - › [Configuring Journaling for the Email Collector on page 101](#)
 - › [Configuring Office 365 Journaling on page 106](#)
 - › [Configuring Gmail Journaling on page 108](#)
 - › [Configuring Email Detection Mitigations on page 111](#)
 - › [Configuring Gmail Threat Mitigation on page 111](#)
 - › [Configuring Email Collectors on page 187](#)

Email Threat Mitigation: Gmail and Office 365 Quarantine Options

With Juniper ATP Appliance, you can quarantine emails that are detected as malicious by using Office 365 APIs or Gmail APIs.

Note that all content on the Juniper ATP Appliance email cloud is encrypted; email quarantine options require encryption of email attachments saved on the disk using a Mitigation Key provided by the user. The Juniper ATP Appliance Central Manager includes a form for user-input of the required mitigation encryption key.

NOTE A Juniper ATP Appliance Advanced license is required for advanced Email Detection configurations.

- For more information, refer to:
 - › [Configuring Email Detection Mitigations on page 111](#)
 - › [Configuring Email Mitigation Settings on page 145](#) for information about setting the Gmail JSON Key file and generating new Azure Key Credentials.
 - › [Configuring Office 365 Journaling on page 106](#)
 - › [Configuring Gmail Journaling on page 108](#)
 - › [Configuring Email Detection Mitigations on page 111](#)
 - › [Configuring Gmail Threat Mitigation on page 111](#)

Email URL Reputation Detection

Additionally, threat detection and mitigation is supported by the sending of malicious URLs to the Juniper ATP Appliance reputation server for analysis. When there is an URL link in an email, Juniper ATP Appliance submits it to the reputation server and performs a reputation lookup. In this way, Juniper ATP Appliance can proactively identify a URL as malicious or as a threat without waiting for an actual download and exploit to happen. On the Juniper ATP Appliance Central Manager Web UI Incidents page, suspicious or malicious URLs are represented by the label “[Malicious URL detected by Juniper ATP Appliance ATA.](#)”

URL Reputation Results are categorized as follows:

- **Malware:** The URL is known to host malicious payloads.
- **Benign:** The URL is known to be clean or the URL is not known.
- No configuration is required. Refer to [Proactive Email URL Reputation Inspections on page 297](#) for more information.

Threat Metric Prioritization Mapping

Because “malware severity” on its own does not always reveal deep context and actionable threat relevance, Juniper “threat metrics” that combine threat severity with other relevance factors to help prioritize and identify whether the threat poses a risk specific to a given enterprise environment. These factors include:

- **Asset Value** — A customizable value that allows admins to prioritize the value of assets in their enterprise, based on IP address ranges, so that malware detected in high asset network segments can be immediately recognized and remediated.
- **OS Relevance** — A threat metric based on an understanding of whether the threat contains the potential to compromise the target endpoint's Operating System. For example, a significant threat may be reported in the Dashboard Threat View with a low severity because it is a Windows virus that was downloaded to a Mac OSX host—an OS Mismatch will cause an adjustment in the severity rating.
- **Virus Scanner Relevance** — Determines whether the configured virus scanner recognizes the identified threat at the time of a download.
- **Execution Relevance** — Bi-directional Carbon Black Response integration helps identify whether a malicious object actually executed on the target endpoint.
- **Progression** — A threat metric that displays which triggers of the kill chain have been identified: XP+UP+DL+EX+IN
- **New Severity Range**— In the previous release, the severity range was a positive integer value between 1-4. The range is a value (including decimals) between 0 and 1.

All factors are used to determine the final threat metric. Threat values are translated as Critical, High (**Red**), Medium (**Orange**), Low (**Yellow**), and Clean (**Green**) in the Juniper ATP Appliance Central Manager Web UI.

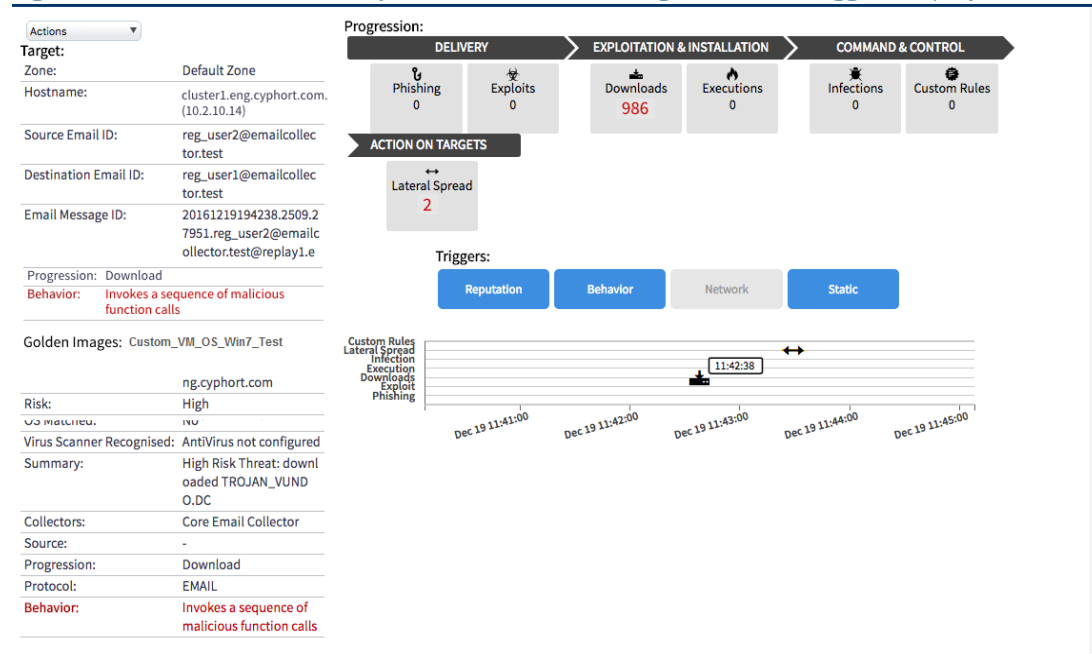
Incident vs Event Context Detailing and Reporting

Juniper ATP Appliance transitioned from an “events” based model to an “incidents” model early on in its technology development process, meaning that in order to more closely represent attack processes, Juniper ATP Appliance now combines multiple related events into a single incident.

The Juniper ATP Appliance defines “incidents” as a group of events that share the same endpoint. In other words, an incident contains events that the Juniper ATP Appliance threat detection system has determined are likely part of the same attack. Currently, the grouping of events into an incident is primarily a measure of time; the events occurred at or from the same endpoint within a 5-minute timespan.

Previously, Juniper ATP Appliance represented each download as an individual threat line item, but in this release and going forward, Juniper ATP Appliance now integrates related items into a single incident to realistically represent related events. This change provides greater context when viewing some attacks that may generate a large number of downloads, CnC activities or events.

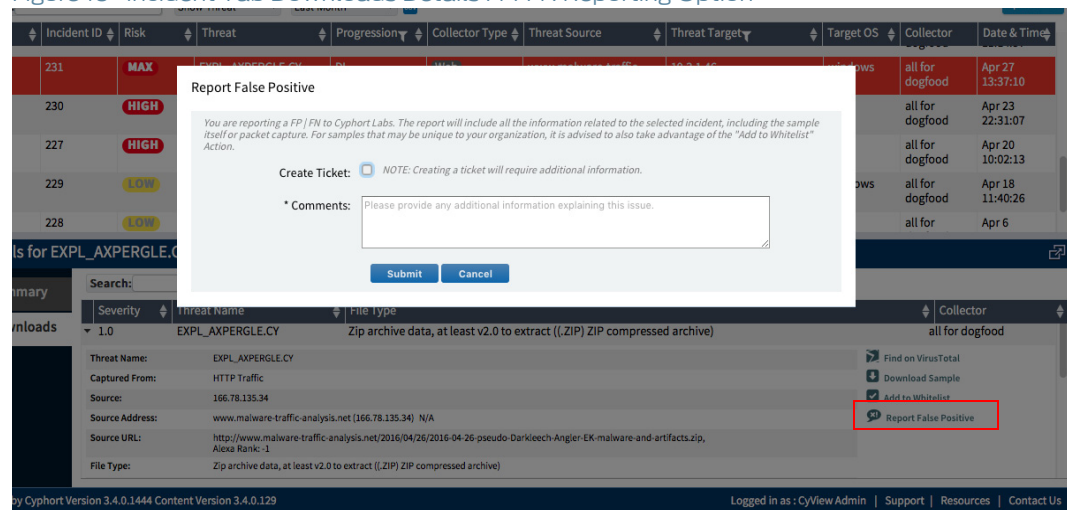
Figure 15 Incidents Tab Summary View with Kill Chain Progression and Triggers Displays



False Negative | False Positive Reporting on the Incidents Tab

Juniper ATP Appliance Central Manager Web UI reporting of False Positive (FP) and False Negative (FN) detections is available from the Incidents Tab. This feature facilitates customer reporting of FPs and FNs from the product Web UI, and automatically attaches all related details about the event required for analysis by the Juniper ATP Appliance Technical Support team.

Figure 16 Incident Tab Downloads Details FP/FN Reporting Option



The option to Report False Positive is available from the Incidents page. For incidents that are benign, the reporting link option displays Report False Negative.

No configuration is required. For more information, refer to [Reporting False Positive or False Negative Incidents on page 288](#).

Auto-Mitigation with Existing Security Infrastructure

Threat intelligence is translated into prevention in real time using your enterprise's existing security infrastructure. With Auto-Mitigation, an admin can configure the following integrated auto-mitigations as part of its malware analysis response:

- **Palo Alto PAN Firewall Integration** — IP addresses of hosts determined to contain malicious objects can be delivered to Palo Alto Networks appliances, where the IP can be blocked. Blocking based on URLs to Palo Alto Networks firewalls is also available. URL-based blocking allows more precise blocking control.
- **Juniper SRX Firewall Integration** — IP addresses of hosts determined to be infected can be delivered to Juniper SRX appliances, where the IP can be blocked.
- **Cisco ASA Firewall Integration** — In addition to Juniper ATP Appliance's established firewall integration support, Cisco ASA Firewall support is available. Now, enterprises using ASA Firewalls, are able to push IP addresses to the Cisco ASA Firewall platform for malware blocking. Juniper ATP Appliance uses a REST interface to communicate to the ASA Firewall.
- **Fortinet Firewall Integration** — Fortinet Firewall and management platform is also supported. This integration includes submission of blocking information using Fortinet's Management APIs, including IP addresses and URLs as appropriate.
- **CrowdStrike Integration** — Juniper ATP Appliance's "CrowdStrike Endpoint Integration" supplements Juniper ATP Appliance's established Carbon Black Response integration for endpoint threat detections and mitigation.
- **Check Point Firewall Integration** — Check Point Firewall integration is also available. The Juniper ATP Appliance communicates with configured Check Point appliances whenever a Juniper ATP Appliance administrator chooses to mitigate a particular threat or remove a previously propagated mitigation. Communication takes place via the SSH interface through which Check Point users may also access the CLI of the Check Point device.

Blocking information is submitted using Check Point APIs. This release supports pushing malicious IP addresses to integrated Check Point appliances. Similar to Juniper ATP Appliance's established PAN and Juniper integration support, an administrator identifies threats in the Firewall or Secure Web Gateway, and submits the selected objects to the configured Check Point Firewall from the Central Manager Web UI.

NOTE Check Point Firewall integration requires Check Point GAiA operating system release R76, R77, or later. Check Point IPSO and Secure Platform (SPLAT), which are predecessors of GAiA, are not supported.

- **BlueCoat ProxySG Integration** — Malicious URLs associated with threats can be sent to BlueCoat's ProxySG equipment so that users can take desired actions (including blocking).

NOTE Blocking does not need to be part of an auto-mitigation operation.

TIP Integration Requirements

- › Requires Microsoft Exchange 2010+ for the Email Collector
- › Junos version 12.1-X47.x for Juniper Firewall
- › Palo Alto Firewall Version x for Palo Alto

PAN Firewall Integration

Configuration of PAN integration for auto-mitigation is a two-step process;

1. First, configure Juniper ATP Appliance recognition on the vendor equipment.
2. Next, configure auto-mitigation from the Juniper ATP Appliance Central Manager (CM) Web UI Config tab.

See complete procedural information at [Configuring Firewall Auto-Mitigation on page 147](#) of this guide.

URL Blocking Support for Palo Alto Networks Firewall Integration

Integration with Palo Alto Networks (PAN) Firewalls uses IP addresses for malware blocking as well as provides blocking based on URLs to Palo Alto Networks firewalls. URL-based blocking is also supported and allows more precise blocking control. In addition, centralized PAN FW mitigation management is also supported via Juniper ATP Appliance and Palo Alto Network's PANORAMA integration.

For configuration information, refer to:

- [Configuring Firewall Auto-Mitigation on page 147](#)
- [Configuring a PANORAMA Device for Centralized PAN FW Mitigation Management on page 150.](#)

Centralized Panorama Integration for PAN Firewall Devices

The Juniper ATP Appliance platform monitors and detects malicious IP addresses and the URLs that link to malware. In previous releases, Juniper ATP Appliance's integration with Palo Alto Networks (PAN) firewalls allowed Juniper ATP Appliance to block malicious URLs and IPs by pushing those IP addresses and URLs to individual PAN FW devices. But because some enterprises utilize an array of PAN firewalls deployed in various locations, integration of each PAN FW with Juniper ATP Appliance could become cumbersome. Therefore, Juniper ATP Appliance offers integration with Palo Alto Network's Panorama, a network security management device that controls the distributed network of PAN firewalls from a central location. Juniper provides the flexibility to either configure integration with individual PAN-OS FWs as usual, or configure integration with a centralized Panorama device as part of Juniper ATP Appliance's Firewall and Secure Gateway auto mitigation options.

Refer to [Configuring a PANORAMA Device for Centralized PAN FW Mitigation Management on page 150.](#)

SRX Series Device Integration

Configuration of Juniper SRX Firewall integration for auto-mitigation is a two-step process;

1. First, configure the Juniper SRX firewall: Create an address set to contain all mitigated IP addresses to be pushed by the Juniper ATP Appliance Central Manager (CM). Then enable remote configuration via the NETCONF protocol. Also, gather the appropriate user credentials that the Juniper ATP Appliance CM will use to configure the SRX. Configure the security policy address book and address sets from the SRX CLI.

Address sets and zone-defined or zone-attached policies are discussed in the configuration section of this guide as well as in the Juniper Junos SRX documentation.

2. Next, configure auto-mitigation from the Juniper ATP Appliance Central Manager (CM) Web UI Config>Environmental Settings>Firewall Mitigation Settings tab.

Figure 17 Firewall Mitigation Settings

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications System Profiles Environmental Settings Email Mitigation Settings Firewall Mitigation Settings Asset Value Anti-Virus Configuration Endpoint Integration Settings BlueCoat Configuration Whitelist Rules YARA Rule Upload SNORT Rule Upload Identity Configuration Splunk Configuration External Event Collectors

Mitigation Type: ☐ ASA ☐ Check Point ☐ Fortinet ☐ PAN ☒ SRX

Hostname/IP: 192.168.1.

SRX Key Pair Authentication: ☐ Enabled ☐ Generate New SSH Key Pair

SRX Address Book Mode: ☐ Zone Attached ☒ Zone Defined

Address Book Name: untrust

Address Set: aset2

Username: admin

Password: *****

Save Cancel

Current Auto Mitigation Rules

Description	Actions
SRX: 192.168.1.	Disable Delete Edit Test

Cisco ASA Firewall Integration

With integrated Cisco ASA Firewall support, enterprises with deployed ASA Firewalls are able to push IP addresses from Juniper ATP Appliance products to the Cisco ASA Firewall platform for malware blocking. Juniper ATP Appliance uses a REST interface to communicate with the ASA Firewall.

Refer to [Configuring a Cisco ASA Firewall on page 158](#) for more information.

Check Point Firewall

Configured Check Point Firewall integration allows Juniper ATP Appliance products to communicate and perform threat mitigation in concert with Check Point firewalls. A Juniper ATP Appliance administrator can choose to block a particular threat or remove a previously propagated mitigation via Check Point Firewall integration. Communication takes place via the SSH interface through which Check Point users may also access the CLI of the Check Point device.

Blocking information is submitted using Check Point APIs. By pushing malicious IP addresses to integrated Check Point appliances, similar to Juniper ATP Appliance's established PAN and Juniper integration support, an administrator identifies threats at the Firewall or Secure Web Gateway, and submits the selected objects to the configured Check Point Firewall from the Central Manager Web UI.

Juniper ATP Applianceyphort firewall blocking corresponds to Check Point CLI SAM commands, as follows:

```
fw sam -J any <blocked_address>
# Drop and close

fw sam -C -i any <blocked_address>
fw sam -C -j any <blocked_address>

fw sam -s <sam_server> -S <SIC_name> -f
<fw_host> -[ i | j | I | J ] any
<blocked address>
fw_host can be All, localhost, Gateways, or a group or object name
fw sam -s <sam_server> -S <SIC_name> -f
```

```
<fw_host> -C -i any <blocked_address>  
fw sam -s <sam_server> -S <SIC_name> -f  
<fw_host> -C -j any <blocked_address>
```

The Check Point “FW SAM CLI Reference” guide is available online.

After configuring the Check Point server, set up integration with Juniper ATP Appliance products from the Central Manager Config>Environmental Settings>Firewall Mitigation Settings page:

Refer to [Configuring a Check Point Firewall on page 162](#) for more information.

BlueCoat ProxySG Integration

For BlueCoat ProxySG integration, Juniper ATP Appliance publishes a “web page” with a list of URLs to which the BlueCoat device is directed. ProxySG polls the malicious URL list periodically to collect blocking details.

BlueCoat can be configured to apply various rules to the Juniper ATP Appliance list, including blocking, as desired.

Refer to [Configuring BlueCoat ProxySG Integration on page 167](#) for more information.

Endpoint Mitigation with Carbon Black Response

Juniper provides comprehensive closed-loop integration between its threat analysis and detonation services, and the enterprise endpoint via Carbon Black Response partner service.

Juniper ATP Appliance and Carbon Black Response integration combine Juniper ATP Appliance’s network-based threat defense with Carbon Black Response’s next-generation endpoint and server security service to provide bi-directional visibility and mitigation support.

While Juniper ATP Appliance detects malware on the network, Carbon Black Response is assessing where the detected malware landed, if it executed, and how many host machines in the enterprise were affected. This real-time visibility enables security analysts to filter out non-actionable events, prioritize high-impact alerts faster, and improve response times to potential intrusions.

Juniper ATP Appliance confirms the location, scope and severity of a threat, and simultaneously queries Carbon Black Response to determine if the malicious file was executed at the endpoints. In this way, the Juniper ATP Appliance Platform can efficiently determine exactly where an attack sits in the kill chain and if a download progressed to infection, expediting targeted enterprise remediation.

In addition, if mobile users download potential malware objects while outside the boundaries of their organization, Carbon Black Response software running at the endpoint can use its blacklist to allow or deny opening of the file. However, in case of a zero-day threat, the blacklist entry does not exist. In such a scenario, the Carbon Black Response solution can submit the file to the Juniper ATP Appliance Core and get a verdict before allowing execution of the file and thus protect the mobile user.

Also, as new files arrive on your endpoints and servers, Carbon Black Response can submit them—on-demand or automatically— for analysis by Juniper ATP Appliance. If Juniper ATP Appliance determines that the file is malicious, Carbon Black Response will stop it from executing and can block the execution of this file across the enterprise’s entire user base. As a result, additional users downloading the same malware objects are automatically protected from malware infections.

Juniper ATP Appliance integration with Carbon Black Response provides significant threat defense benefits:

- Continuous, real-time visibility into what’s happening on every computer
- Real-time threat detection, without relying on signatures
- Instant response by seeing the full “kill chain” of any attack
- Prevention that is proactive and customizable

NOTE Refer to [Configuring Endpoint Integration: CrowdStrike and Carbon Black Response on page 238](#) for more information, and the [Juniper ATP Appliance/Carbon Black Response Integration Guide](#).

CEF, QRadar LEEF Logging Support for SIEM

Juniper ATP Appliance's detection of malicious events generates incident and alert details that can be sent to connected SIEM platforms in CEF and QRadar LEEF format.

The Juniper ATP Appliance Central Manager WebUI Config>System Settings>SIEM Settings provides the option to configure event, incident and alert notifications for rSYSLOG, LEEF or CEF-based SIEM servers. The servers, in turn, must be configured to receive the Juniper ATP Appliance notifications in CEF or LEEF format.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.20	0	N/A	High
Infected Host	1047.ang.opphort.com	12	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.222.234.2.119	0	10.1.1.20	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.198.176.26.151	0	10.1.1.20	0	N/A	High
Infected Host	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.193.106.172.145	0	10.1.1.20	0	N/A	High
Infected Host	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.187.17.28.219	0	10.1.1.20	0	N/A	High
Infected Host	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.222.214.214.27	0	10.1.1.20	0	N/A	High
Infected Host	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.198.198.203.108	0	10.1.1.20	0	N/A	High
Infected Host	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.193.64.52.196	0	10.1.1.20	0	N/A	High
Infected Host	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.191.170.165.131	0	10.1.1.20	0	N/A	High
Infected Host	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.187.48.191	0	10.1.1.20	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	10.2.20.47	0	10.1.1.5	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.4	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	10.2.20.47	0	10.1.1.5	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	10.2.20.47	0	10.1.1.5	0	N/A	High
Infected Host	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Malware Infection	10.74.208.164.168	0	10.1.1.20	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	235.190.83.195	0	235.190.83.149	0	N/A	High
Malicious Email	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Mail Attachment	10.2.20.47	0	10.2.20.47	0	N/A	High
Malicious Email	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Mail Attachment	10.2.20.47	0	10.2.20.47	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.2	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.26	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.34	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.24	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.38	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.40	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.44	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.48	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.42	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.34	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.52	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	10.222.214.214.27	0	10.1.1.42	0	N/A	High
A malicious file was downloaded	1047.ang.opphort.com	1	Jan 20, 2017, 12:53:47 AM	Hostile Software Download	172.16.0.1	0	10.1.1.56	0	N/A	High

NOTE Installation of the DSM-Juniper ATP Appliance extension plugin on the QRadar server is required.

Identity information is sent as part of SIEM, and SIEM events are sent for Email detections for Downloads+Phishing (DL + PHS), Download (DL), and Phishing (PHS).

- For configuration information, refer to [Configuring SIEM Settings on page 101](#), and the [Juniper ATP Appliance CEF LEEF and Syslog Support for SIEM User's Guide](#). Refer also to the document [Juniper ATP Appliance CEF, LEEF & Syslog Support for SIEM](#).

Virtual Collector, Virtual Core for AWS, and vCore [OVA] Deployments

The Juniper ATP Appliance Core-CM and Traffic Collector products can be deployed as a virtual machine Virtual Core (vCore) and/or Virtual Collector (vCollector) using VMWare vSphere (initially) via thick or thin provisioning. This feature extends the Juniper ATP Appliance product footprint to allow deployment in virtualized environments.

The virtual deployment is provided as an .OVA for simple deployment, or .ISO for custom deployments, or vCore for Amazon EC2 AWS (Amazon Web Services).

NOTE vCenter is no longer a requirement for the virtual collector deployment. Although Juniper still provides an .ova for customers who use vCenter, in addition, Juniper also generates an .ovf and a .vmdk file for every build. The .ovf and .vmdk are bundled into a .tar file that you download and expand.

For customers who do not want to use vCenter for the virtual collector deployment: download the .tar file and expand both the OVF and the VMDK into the same directory. Then, from the vSphere client, click on File

-> Deploy OVF Template. Choose the .ovf file and then complete the deployment of the ovf wizard. The configuration wizard prompts for collector/core properties such as IP address, hostname, device key. Log in to the CLI and configure each setting.

OVA vCore deployments contain the full deployment package (including detonation engines).

Customers deploy Virtual Core and Virtual Collector(s) separately.

NOTE Virtual Core performance is comparable to equally equipped physical appliances (generally same CPUs, Memory, etc). But unlike physical appliances, Juniper ATP Appliance is unable to provide MS Windows licenses for Virtual Cores due to Microsoft Licensing restrictions. Customers must supply Windows licenses for the vCore and vCore for AWS system. For an overview of vCore for AWS, see [Virtual Core for Amazon EC2 AWS on page 39](#).

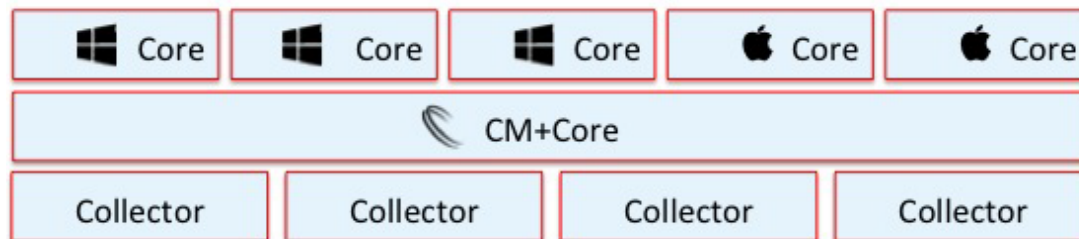
For installation and configuration instructions, refer to:

- › Juniper ATP Appliance Core-CM Quick Start Guide
- › Juniper ATP Appliance Virtual Core for AWS Quick Start Guide
- › Juniper ATP Appliance Traffic Collector Quick Start Guide

Clustered Core Deployment

The Clustered Core feature allows multiple Core detection engines to run in tandem to support larger networks and provides a magnitude improvement in scale of the Juniper ATP Appliance Core. Clustering improves scalability by allowing multiple cores to perform malware analysis simultaneously. Juniper ATP Appliance supports Windows-based Secondary Cores (in addition to the Mac-Mini Secondary Cores already available in previous and current releases).

Figure 18 Clustered Mac OSX and Windows Cores



Clustering allows multiple appliances to be configured as analysis cores to increase analysis workload; the process works for both physical and virtual appliances. In fact, virtual appliances can be cloned and restarted to instantly improve capacity.

NOTE The Central Manager Web UI Dashboard indicates when a cluster requires more cores.

The installation procedures for clustering are the same installation procedures set for non-clustered devices.

- The first Core install (perhaps an existing device currently deployed) is automatically registered as the Primary and will drive the Central Manager whenever another Secondary Core installation takes place.

- A second (or additional) Secondary Core or Mac OSX Secondary Core, when installed, automatically becomes a(nother) Secondary Core.

Refer to the Juniper ATP Appliance Core-CM Quick Start Guide for installation and configuration instructions. See

Virtual Core for Amazon EC2 AWS

Juniper ATP Appliance technology integrates with Amazon Web Services (AWS) by providing Virtual Core images that can be run on the Amazon EC2 AWS platform. The Virtual Core (vCore) is provided in an AMI (Amazon Machine Image) format that is launched as an AWS EC2 instance. The AWS Core provides performance capability similar to the R320+ and R720/R730 appliance models.

An Amazon AMI provides the information required to launch a configured Juniper ATP Appliance vCore instance as a virtual server in the Amazon Cloud. Many Juniper ATP Appliance AMI vCore instances as needed can be launched from an AMI, and vCore instances can be launch from as many different AMIs as needed.

With Juniper ATP Appliance vCore for AWS, both the Primary Core (i.e., Core + Central Manager (CM)) and the connected Secondary Cores are installed and run from the AWS platform. Each vCore instance status is displayed at the AWS management console, and all connectivity status is shown at the Juniper ATP Appliance CM Web UI.

Configuration is required at the AWS Management Console as well as the Juniper ATP Appliance Central Manager Web UI and CLI. Refer to Juniper ATP Appliance Virtual Core for AWS Quick Start Guide for more installation and configuration information.

Small Footprint Virtual Traffic Collector

Juniper ATP Appliance offers a small footprint Traffic Collector for virtual deployments. Standard Virtual Collector deployments require 512GB hard disk drive space plus 4 minimum cores and 16 GB RAM. The low-resources Collector provides a VM Collector instance requiring only 16 GB HDD, 1 Core and 4 GB of RAM, supporting 25Mbps of traffic.

Configuration is required by customers. Refer to Juniper ATP Appliance Traffic Collector Quick Start Guide for more information. See also [Configuring a Cisco ASA Firewall on page 158](#).

This small, extremely affordable portable form factor Traffic Collector is ideal for Juniper ATP Appliance partners and small business remote offices and branch offices. The small form factor Collector is also suitable for small businesses such as retailers and consulting businesses and/or financial services organizations for which there are relatively small bandwidth requirements (~ 150 Mbps traffic data collection).

Refer to Juniper ATP Appliance Traffic Collector Quick Start Guide for more information.

Management Traffic Proxy Support

Many customers still rely on proxies and gateways to provide rudimentary security for their endpoints. In such environments, the CM/Core must be able to function and communicate with external services similarly to an unproxied environment. This communication includes uploads and downloads for GSS, as well as software, security content and signature updates, and all other necessary communications. Juniper ATP Appliance Cores deployed in HTTP and/or HTTPS proxy environments can be configured to function and communicate with Juniper ATP Appliance GSS and other Internet services.

For more information, refer to [Configuring Proxy Settings for the Management Network on page 121](#) for Web UI configurations, and the Juniper ATP Appliance CLI Command Reference for CLI-based configurations from server mode.

Span-Traffic Proxy Data Path Support

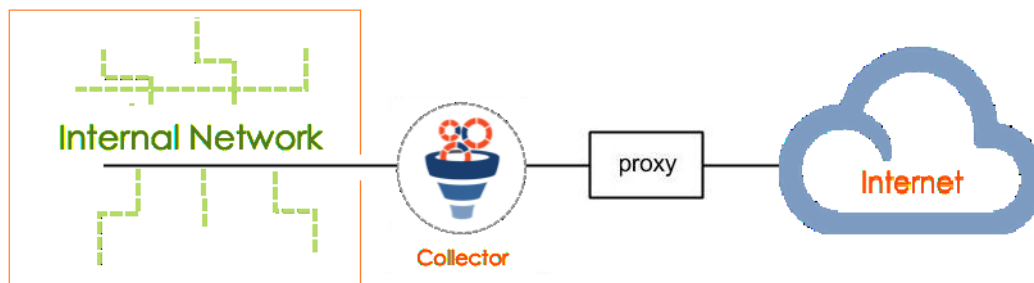
Juniper ATP Appliance now facilitates deployment of Traffic Collectors in locations where the monitoring interface is (1) placed between the proxy and the egress network for customer environments in which the proxy supports XFF (X-Forwarded-For), or (2) [the more typical deployment scenario], the Collector is placed between the proxy and the internal network using FQDN (if available) to identify the threat source for all types of incidents.

Now, the Juniper ATP Appliance Traffic Collector can monitor all traffic and correctly identify source and destination hosts for each link in the kill chain wherever the data allows for it. Note that if the “X-Forwarded-For” header is provided in the HTTP request, detection will identify threat targets when deployed outside of the proxy (customers can choose to disable the XFF feature in the proxy setting, if desired).

Set Proxy Inside

When the web proxy is between the Internet and the Juniper ATP Appliance Traffic Collector monitoring interface, use the CLI command `collector>set proxy inside` for adding/removing the proxy IP address. The following diagram illustrates this deployment scenario:

Figure 19 Juniper ATP Appliance Collector is “inside” of the Proxy



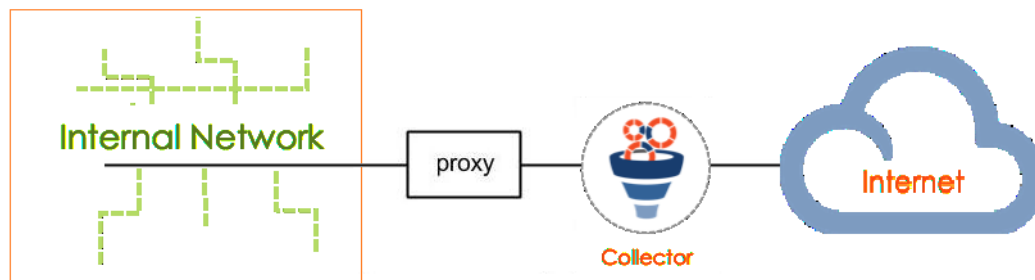
The following example sets an inside data path proxy:

```
Juniper ATP Appliance (collector)# set proxy inside add 10.1.1.1 8080
```

Set Proxy Outside

Alternatively, when the proxy is between the internal networks and the Juniper ATP Appliance Traffic Collector monitoring interface, use the CLI command `collector>set proxy outside` for adding/removing the proxy IP address. The following diagram illustrates this deployment scenario:

Figure 20 Juniper ATP Appliance Collector is “outside” of the Proxy



The following example sets an outside data path proxy:

```
Juniper ATP Appliance (collector)# set proxy outside add 10.2.1.1
```


Single Sign On SAML Authentication

SAML (Security Assertion Markup Language) standardizes the functions involved in receiving, transmitting, and sharing security assertion information. Juniper ATP Appliance supports SAML authentication for web browser single sign-on (SSO) operations. More information about SAML can be found at https://en.wikipedia.org/wiki/SAML_2.0.

YARA Rules Support

Juniper ATP Appliance supports the use of YARA rules for malware analysis. Using YARA, an open source static analysis tool, security analysts can define byte-level rules used to quickly analyze numerous object and traffic files for relevant matches. If a byte-pattern match is identified, then analysts can specify that byte-pattern as a YARA rule and upload to the Juniper ATP Appliance Central Manager to be used to detect related malicious files during Juniper ATP Appliance malware detonation and analysis cycles.

You can choose to define YARA rules as malware families based on textual or binary patterns obtained from samples of identified families. Rule descriptions consist of a set of strings and a Boolean expression that establishes the rule's logic. In addition, YARA integration results show whether an object can be classified as malicious. YARA rules are also used to classify malware samples.

YARA rule files are uploaded and enabled from the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>YARA Rule Upload page, where a wide variety of available YARA file formats are accepted and integrated. For configuration information, refer to [Configuring YARA Rules on page 172](#).

YARA Rules for Detecting Lateral Spread within a Customer Network

Remote Administration Tools (RATs) can allow remote control of an enterprise system as if physical access is established. Although there are certainly legal application of RATs, this software is often associated with criminal or malicious activity via software installed without the target's awareness. Remote Administration Tools can be detected using YARA rules. Juniper provides the ability to push YARA rules to Juniper ATP Appliance devices to detect the lateral spread of RATs inside the customer network. These Lateral spread rules are packaged in the Juniper ATP Appliance product. Details of matched YARA rules are displayed in the Juniper ATP Appliance Central Manager Web UI "Incidents" tab; matched YARA rules can be downloaded from the Web UI as well.

An Advanced license is required to enable SMB lateral monitoring, but YARA rules can be installed and applied regardless of SMB use.

For more information about YARA Rules for lateral detections, refer to [YARA Rules and Lateral Detection on page 18](#).

Custom SNORT Rules Support

Support is provided for customers to upload Snort Rules that will be matched against network traffic monitored by Juniper ATP Appliance Collectors, with match results displayed in the Juniper ATP Appliance Central Manager Web UI. Additionally, Juniper ATP Appliance correlates triggered rules with incidents that were active at the time of the trigger. All triggered SNORT rules are displayed in their own main Web UI Custom Rules tab

Refer to [Configuring Custom SNORT Rules on page 192](#) for more information.

Email Correlation and Mitigation

Malicious Email Correlation features are implemented to analyze not only email attachments (as has been available in previous releases), but to also detect phishing by analyzing malicious URLs within enterprise emails. Correlation between HTTP/SMB incidents and email events is performed when an URL is first identified in an incoming email and then later also visited by an endpoint. Email alerts are generated for phishing event mitigation.

NOTE Email Correlation requires an Active Directory configuration.

Refer to [Email Phishing Correlation on page 294](#) for more information.

Reverse SSH Tunneling for Optimizing Customer Technical Support

Juniper ATP Appliance offers a Reverse SSH Tunneling feature to allow for direct debugging by a remote Juniper ATP Appliance technical support team of a Core/CM installation running in a customer network. From the Core/CM, technical support could then SSH into component Secondary Cores and Web Collectors in the same subnet.

Configuration is required; customers enable/disable this functionality and specify the duration for the reverse ssh tunnel operation. For more information, refer to [Configuring GSS Settings on page 129](#).

Manager of Central Managers (MCM) Virtual or Hardware Device

The Juniper ATP Appliance Manager of Central Managers (MCM) is a device that provides a centralized Web UI for Juniper ATP Appliance customers that deploy multiple Core/Central Managers (CMs) in various geographic locations including multi-tenant MSSP sites. The MCM allows customers with distributed enterprises to consolidate viewing of detected malware incidents occurring on multiple CMs registered to the central MCM.

The MCM Platform device type is represented as “mcm” in the Juniper ATP Appliance CLI. The MCM receives incident data from multiple secondary Central Manager (CM) appliances and displays that data in the primary MCM Web UI.

The MCM Web UI is a subset of the larger Juniper ATP Appliance Central Manager Web UI and includes only the Incidents tab and the Config tab for System Profile configurations, in addition to a device Refresh and Logout tab options.

Figure 21 Manager of CMs (MCM) Web UI

The screenshot displays the MCM Web UI interface. At the top, there's a header for 'All Incidents (5 shown, 5 total)' with search and filter options. Below this is a table of incidents with columns: Status, Incident ID, Risk, Threat, Progression, Collector Type, Threat Source, Threat Target, Zone, Target OS, and Collector. Three incidents are listed, all with a 'HIGH' risk level. The first incident is 'TROJAN_AGENT.DC' with a 'User' collector type. The second is 'TROJAN_GENOME.DC' with a 'User' collector type. The third is 'TROJAN_VAWTRAK.DC' with a 'User' collector type. Below the table, there's a detailed view for 'TROJAN_GENOME.DC' showing target information (Hostname, Username, IP Address, FQDN, Source Email ID, Destination Email ID) and triggers (Reputation, Behavior, Network, Static). The risk is 'High' and the threat category is 'Trojan_Generic'.

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector
New	8	HIGH	TROJAN_AGENT.DC	UP	User	switch-56.corp.cyphort.com	switch-56.corp.cyphort.com	Default Zone		Core File Upload Collector
New	7	HIGH	TROJAN_GENOME.DC	UP	User	switch-54.corp.cyphort.com	switch-54.corp.cyphort.com	Default Zone		Core File Upload Collector
New	9	HIGH	TROJAN_VAWTRAK.DC	UP	User					Core File Jun 24

Details for TROJAN_GENOME.DC

Target:

Hostname: -
 Username: -
 IP Address: -
 FQDN: -
 Source Email ID: -
 Destination Email ID: -
 Risk: High
 Threat Category: Trojan_Generic
 Asset Value: Medium

Triggers:

Reputation Behavior
 Network Static

Note that the **CM Name** column details the name of each incident's originating Central Manager.

Refer to the Juniper ATP Appliance Manager of Central Managers (MCM) User's Guide and the Juniper ATP Appliance CLI Command Reference.

Advanced Threat Analytics (ATA): External Event Collectors and New Events Timeline Dashboard

ATA expedites analysis efforts by security teams that must sort through multitudinous alerts to determine which events are important, which threats are related, and which incidents deserve immediate attention from the incident response (IR) team. Juniper ATP Appliance Advanced Threat Analytics solves this problem by automatically filtering and linking all related events from other security infrastructure sources in the network, identifying the infected user, and presenting a consolidated timeline view of the entire security apparatus. This empowers security teams to accelerate incident response and process more meaningful security incidents each day.

You can configure each external event collectors for Direct Ingestion of syslogs to a Juniper ATP Appliance Core, or for Splunk Ingestion.

Raw logs are filtered and displayed on the Juniper ATP Appliance Incidents Web UI page, and a detailed host view is available from the Juniper ATP Appliance Events Timeline Dashboard.

For example, the following Incidents page example shows Juniper ATP Appliance event correlation with an external source event:

Figure 22 Juniper ATP Appliance Incidents External Sources PAN Ingestion Showing RAW LOG Detection Event

All Incidents (46 shown, 46 total)

Search:

Show Threat

Last Month

On

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Target OS	Collector	Date & Time
New	47	HIGH	TROJAN_SILCON.DC	DL	Web LOG	74.0.0.10	172.16.2.101	unknown	2 Collectors	Jun 23 16:24:06 DT
New	45	LOW	Download		LOG	74.0.0.10	172.16.2.101		Core External Event Collector	Jun 23 16:07:07 DT
New	46	HIGH	TROJAN_SILCON.DC	DL	Web	172.16.1.111	host-1-11.private.cysphort.com	unknown	Eng2-Collector	Jun 23 16:06:38 DT
New	44	LOW	Download		LOG	74.0.0.10	172.16.2.101		Core External Event Collector	Jun 23 15:59:07 DT
New	43	LOW	Download		LOG	74.0.0.10	172.16.2.101		Core External Event Collector	Jun 23 15:40:45 DT

Details for TROJAN_SILCON.DC

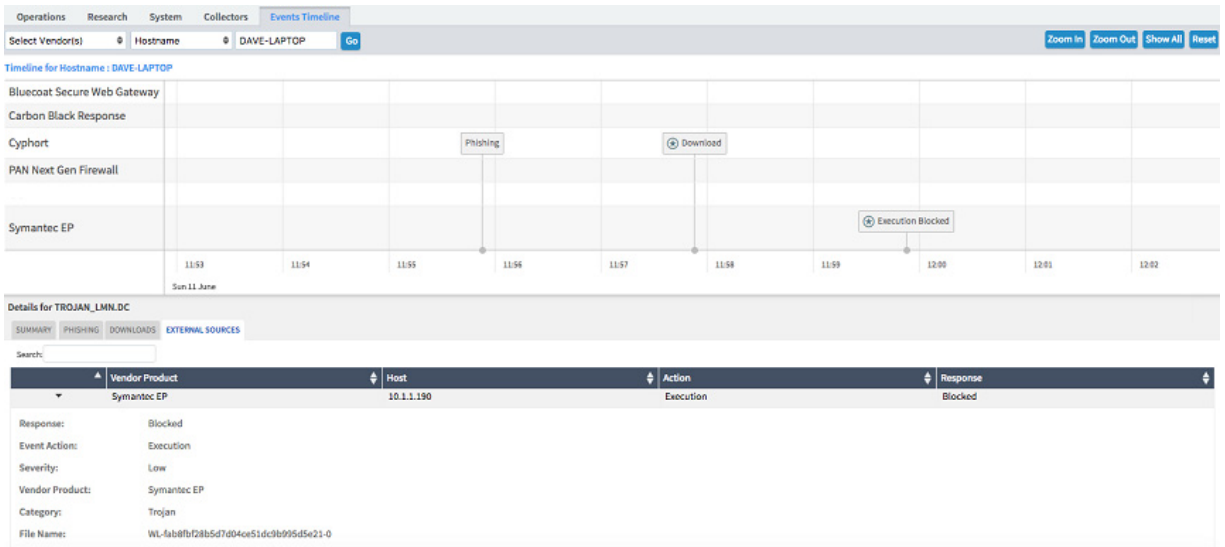
SUMMARY

DOWNLOADS

EXTERNAL SOURCES

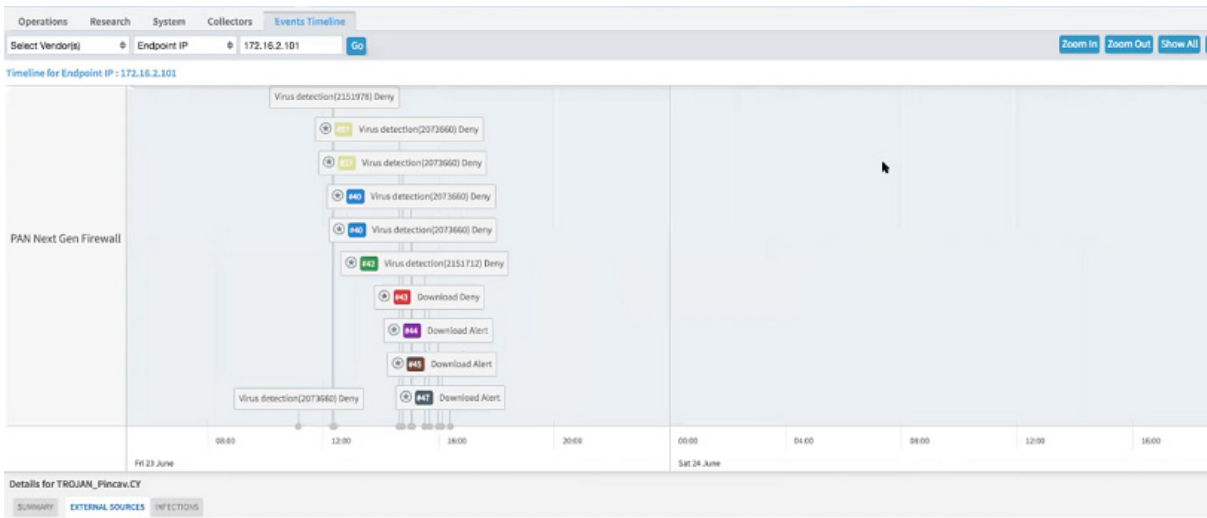
Search:

Vendor Product	Host	Action	Response
Detection Method:	Trust-untrust		
Vendor Product:	PAN Next Gen Firewall		
File Name:	f5dab95505492b20cd60418fbc725a031193c4e3dfabe546d2d9338059adb3		
Raw Log:	1,2017/06/23 16:24:01.001606020919,THREAT,wildfire,0,2017/06/23 16:24:01,74.0.0.10,172.16.2.101,0.0.0.0,0.0.0.0,trust-untrust,,web-browsing,xsys,1,untrust,trust,ethernet1/2,ethernet1/2,,yslog-1,2017/06/23 16:24:01,3005,1,80,25582,0,0,0,30000,tcp,alert,7f6dab95505492b20cd60418fbc725a031193c4e3dfabe546d2d9338059adb3,Windows Executable (XXI)32020,malicious,medium,server-to-client,8050,640,JIS,172.16.0.0-172.31.255.255,0,0,6dab95505492b20cd60418fbc725a031193c4e3dfabe546d2d9338059adb3(ya-1,wildfire.paloaltonetworks.com,1,pe,,,,6014729370		



malicious download:

Figure 25 Events Timeline Dashboard Showing PAN Download Event, Juniper ATP Appliance Detection Event



For configuration information specific to all third-party vendors, refer to [Integrating Anti-Siem External Event Collectors on page 211](#).

- Splunk Integration for Anti-SIEM Event Logs and Event Data Management.
 - › Juniper ATP Appliance-Side Configuration
 - › Splunk-Side Configuration

For configuration information, refer to [Configuring Anti-SIEM Splunk Ingestion on page 209](#).

- Identity Configuration Options for Carbon Black Response and Active Directory via Splunk Ingestion

Identity configuration options allow for the import of all Carbon Black Response logs sent to Juniper ATP Appliance via Splunk, and all AD users' access details via Splunk for even more detailed endpoint event reporting. This feature supplements Juniper ATP Appliance's existing support of direct log ingestion from Carbon Black Response to a Juniper ATP Appliance Core, adding the Splunk forwarding options for enterprises that use Splunk deployments for log and event handling.

Several configurations are required:

You will need to perform several configurations:

- Configure Splunk from the Juniper ATP Appliance Web UI Juniper ATP Appliance Config>Environmental Settings>Splunk Integration.
- Configure Carbon Black Response from the Juniper ATP Appliance Config>Environmental Settings>External Event Collectors.
- Configure Identity for AD and Splunk from the Juniper ATP Appliance Config>Environmental Settings>Identity Configurations.
- Improved Representation of Malware Behavior

To improve assessments and determination about the intent of threats and malware, the behavioral analysis improvements categorize malware indicators into groups based on the malicious traits that they exhibit.

CHAPTER 2

Getting Started

The following topics are in this chapter:

- [Before you Begin](#)
- [Juniper ATP Appliance Network Information](#)
- [Management Network](#)
- [Juniper ATP Appliance Web UI Support](#)
- [Accessing Juniper ATP Appliance Device Interfaces](#)
- [Accessing Juniper ATP Appliance Device Interfaces](#)
- [Juniper ATP Appliance Web UI Access](#)
- [Login to the Juniper ATP Appliance using SAML Authentication](#)
- [Login to the Juniper ATP Appliance System using AD Authentication](#)
- [Deploying the Distributed Juniper ATP Appliance System](#)
- [Deployment Guidelines](#)
- [Guidelines for Environments with Web Proxies](#)
- [Configuring Collector Email Journaling](#)
- [Configuring Journaling for the Email Collector](#)
- [Using the Dashboard Views](#)
- [Submitting a Malware File for Analysis](#)
- [Configuring Juniper ATP Appliance for Integrated Deployment](#)
- [Deploying Juniper ATP Appliance SaaS Virtual Collectors](#)
- [Deploying Juniper ATP Appliance SaaS Virtual Collectors](#)
- [Deploying SaaS Virtual Cores as OVAs](#)
- [Enabling Juniper ATP Appliance Support](#)
- [Configuring an Alternate Analysis Engine Interface](#)
- [Review all deployment prerequisites in the Juniper ATP Appliance Quick Start Guide for your SSH Honeypot Requirements](#)

Before you Begin

Before installing Juniper ATP Appliance products, be sure that you meet the following installation, setup, safety, and site requirements:

1. Read the Juniper ATP Appliance Release Notes for the current release.
2. Familiarize yourself with the appliance, AWS, SaaS or VM OVA by reading the Juniper ATP Appliance Quick Start Guide specific to your product(s).
3. Gather the information and equipment outlined in [Juniper ATP Appliance Network Information on page 48](#), including the following items:
 - › Juniper ATP Appliance information
 - › Network information
 - › Client information.
4. Follow the guidelines listed in [Accessing Juniper ATP Appliance Device Interfaces on page 52](#).

Juniper ATP Appliance Network Information

For hardware specifications and set up instructions, refer to the **JATP700 Appliance Hardware Guide**.

Before you connect and configure the appliance, collect the information about your network outlined in Table 2-1 below.

Table 2-1 Network Information Requirements

Network Item	Information Needed
Juniper ATP Appliance	<ul style="list-style-type: none"> • IP address • Subnet Mask
DNS (Domain Name Service) Service (Optional)	IP address of one or more DNS server
NTP (Network Time Protocol) Service (Optional)	IP address of one or more NTP servers
Remote Management (Optional)	<p>If you want to access the Juniper ATP Appliance CLI remotely, the remote system must have one of the following:</p> <ul style="list-style-type: none"> • SSH client <p>NOTE: Always use the latest version of Putty for SSH operations, if using Putty as an SSH client.</p>
CM (Central Manager)	<ul style="list-style-type: none"> • Default Gateway address • Default IPS/Next Gen Firewall address • SIEM device addresses • Carbon Black address • PAN OS Firewall IP Address, Juniper ATP Appliance-tag and configured Dynamic Address Group (DAG) • Juniper SRX Firewall port 830 • Cisco ASA Firewall • Check Point Firewall • Bluecoat ProxySG IP Address

Management Network

The following table summarizes all port and protocol configurations for the Juniper ATP Appliance and CM connectivity. Note that the admin interface on all appliances is eth0 by default. All auto-updates for GSS are handled exclusively by the Core/CM or All-in-One System.

Communication ports and protocols must be opened during installation for both internal and external servers and services.

IMPORTANT: Primary Core/CM and Secondary Cores/Mac Cores must be on the same network, and allow all ports, with no Port Address (PAT) or Network Address Translation (NAT).

The following tables delineate all internal and external ports and protocols.

Internal Servers

Table 2-2 Communication Protocols and Ports

Description	Protocol	Source	Destination	Port
CLI Management	TCP	admin workstation	Core/Collector/Secondary Core admin interface	22
CM Web UI Management	TCP	admin workstation	CM admin interface	443
DNS Queries	TCP/UDP	Core/Collector/Secondary Core admin interface	Internal DNS servers	53
NTP	UDP	Appliance admin interface	NTP Servers	123
Syslog	UDP	Appliance admin interface	SIEM/Syslog CEF server	514
CM Connection	TCP	Collector and Secondary Core admin interface	CM admin interface	443

Management Port eth0

Use the management port eth0 interface to administer and use the distributed Juniper ATP Appliances. This is the port through which the Juniper ATP Appliance exchanges security content and through which integration with the CM is managed. The management interface must be network routable with the Juniper ATP Appliance IP/hostname access over the following ports:

- DNS (UDP/53)
- HTTPS (TCP/443)
- SSL/TLS Port 443 should be open between Collectors and the Core/CM for traffic inspection and malware behavior analysis.

Always use the latest version of Putty for SSH operations, if using Putty as an SSH client.

NOTE For setting up the IP address and DNS for the management interface, the name management interface is used (instead of eth0).

Monitoring Port eth1

Use a network tap to send a copy of network traffic from a network segment to the eth1 network monitoring port of a Juniper ATP Appliance Collector. The tap does not interfere with traffic and, if shut down, allows traffic to pass through unhindered. See [Network Tapping on page 64](#) and [SPAN Port Mirroring on page 64](#) for more information.

Analysis Engine Exhaust Port eth2

The option is available to configure an alternate interface to move analysis engine traffic exhaust and CnC communications during detection detonation processes off the management network eth0 and to a separate interface eth2.

An eth2 interface can be configured for the primary Core+CM, All-in-One Core, and Mac Mini secondary Cores. The Mac Mini requires a USB-to-NIC adapter to set up the alternate interface.

Port Scan Detector and SSH Honeypot Port eth3

There is also an option to configure the eth3 port for all outbound Collector traffic.

NOTE A Juniper ATP Appliance Advanced License is required for SSH Honeypot Lateral Detection configurations. The honeypot interface always enumerates as eth3.

External Servers

The following table lists the ports and protocols per external server for which the Juniper ATP Appliance system requires outgoing connectivity.

Description of External Server Relative to the Juniper ATP Appliance Core or vCore	Source	Destination Hostname/ IP Address	Dest. Port	Protocol
SIEM/ Syslog Server	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-One Core/CM 	IP address of SIEM/ Syslog Server	514	UDP
DNS Server(s)	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-One Core/CM 	Customers' DNS server IP address	53	TCP/UDP
Ping Test	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-One Core/CM 	8.8.8.8		ICMP
Juniper ATP Appliance Software and Content	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-one Core/CM 	gss.cloud.cyphort.com update.cloud.cyp hort.com	443	TCP
Juniper ATP Appliance GSS Reporting Server	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-one Core/CM 	gss.cloud.cyphort.com filestore.cloud.cyp hort.com	443	TCP
Reputation Server Juniper ATP Appliance	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-one Core/CM 	rep.cloud.cyphort.com	443	TCP
Juniper SRX Firewall Note: For Mitigation via SRX Firewall	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-one appliances CM/Core appliances 	Customer's configured SRX appliance and security policies	830	TCP

Description of External Server Relative to the Juniper ATP Appliance Core or vCore	Source	Destination Hostname/ IP Address	Dest. Port	Protocol
Palo Alto Networks PAN appliance or Panorama, Cisco ASA, Checkpoint, Fortinet or FortiManager Note: For Mitigation via integrated Firewall	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-one appliances CM/Core appliances 	Customer's configured PAN appliance	443	TCP
CrowdStrike and/or Carbon Black Response Server Note: For Mitigation/ Validation through Carbon Black Response	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-one appliances CM/Core appliances 	Customer's configured Carbon Black server	443	TCP
BlueCoat ProxySG Note: For Mitigation via BlueCoat Proxy	<ul style="list-style-type: none"> Juniper ATP Appliance All-in-one appliances CM/Core appliances 	Customer's configured BlueCoat proxy		TCP

In summary, be sure to configure Core/CM outgoing internet connectivity to:

- Configure outgoing access from the Juniper ATP Appliance management interface eth0 to the enterprise SMTP server, DNS servers, and logging/SIEM servers.
- The Core engine connects to a separate Mac Mini OSX or other Secondary Core using TCP port 22, be sure to open this port when installing a distributed Mac OS X Engine. All communications take place on eth0. Other ports are reserved in this release (See also [Analysis Engine Exhaust Port eth2 on page 50](#) and [Configuring an Alternate Analysis Engine Interface on page 95](#)).
- If you configure Juniper ATP Appliance Email Collector(s), ports used to access the email server(s) must also be opened. All communications occur across the Juniper ATP Appliance management network via eth0. Other ports are reserved in this release (See [Analysis Engine Exhaust Port eth2 on page 50](#) and [Configuring an Alternate Analysis Engine Interface on page 95](#)).

Primary Core/CM and Secondary Cores/Mac Cores must be on the same network, and allow all ports, with no Port Address (PAT) or Network Address Translation (NAT).

Management interface eth0 requires a static IP address or reserved DHCP address and net mask. However, if this is a CM-connected appliance, use only a static IP address and net mask. See additional Central Manager (CM) communications information below.

NOTE Note: Do not use ZeroConf on the primary interface

NOTE Always use the latest version of Putty for SSH operations, if using Putty as an SSH client.

Juniper ATP Appliance Web UI Support

The browsers supported by the Juniper ATP Appliance Web UI are as follows:

Windows Users

- Internet Explorer 11.0 or higher
- Firefox® 31 or higher
- Google Chrome 36 or higher

Mac Users

- Safari 7.0.2
- Google Chrome 36 or higher
- FireFox® 31 or higher

Screen Resolution Support

The Juniper ATP Appliance Web UI supports use of the following screen resolutions:

Table 2-3 Juniper ATP Appliance Supported GUI Screen Resolutions

• 1152 x 864 pixels	• 1600 x 900 pixels
• 1280 x 1024 pixels	• 1680 x 1050 pixels
• 1280 x 800 pixels	• 1920 x 1080 pixels
• 1360 x 768 pixels	• 1920 x 1200 pixels
• 1366 x 768 pixels	• Other high resolutions
• 1440 x 900 pixels	

Accessing Juniper ATP Appliance Device Interfaces

You can gather information and interact with Juniper ATP Appliances using the following interfaces:

- Command Line Interface (CLI)
- Juniper ATP Appliance Central Manager Web UI

For more information about the CLI and CLI command syntax and usage, refer to the Juniper ATP Appliance CLI Command Reference.

Launching the Configuration Wizard

To launch the configuration wizard, enter the CLI command wizard.

```
JATP# wizard
```

- › At the CLI prompt, enter your username and password. By default, the admin user name is admin and the password is 1JATP234.
Be sure to change the default password for the admin account after initial setup; the password must be at least 8 characters in length.
- › Enter yes to use the configuration wizard when prompted, and then respond as shown below.

CONFIGURATION WIZARD

Configuration Wizard Prompts	Customer Response from <u>All-in-One</u>	Customer Response from <u>Core</u> or <u>Mac Mini</u>	Customer Response from <u>Collector</u>
<p>Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)?</p> <p>Note: Only if your DHCP response is no, enter the following information when prompted:</p> <p>a. IP address</p> <p>b. Netmask</p> <p>c. Enter a gateway IP address for this management (administrative) interface:</p> <p>d. Enter primary DNS server IP address.</p> <p>e. Do you have a secondary DNS Server (Yes/No).</p> <p>f. Do you want to enter the search domains?</p> <p>g. Enter the search domain (separate multiple search domains by space):</p> <p>Restart the administrative interface (Yes/No)?</p>	<p>We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.</p> <p>Recommended: Respond with no:</p> <p>a. Enter an IP address</p> <p>b. Enter a netmask using the form 255.255.255.0.</p> <p>c. Enter a gateway IP address.</p> <p>d. Enter the DNS server IP address</p> <p>e. If yes, enter the IP address of the secondary DNS server.</p> <p>f. Enter yes if you want DNS lookups to use a specific domain.</p> <p>g. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com</p> <p>Enter yes to restart with the new configuration settings applied.</p>	<p>We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.</p> <p>Recommended: Respond with no:</p> <p>a. Enter an IP address</p> <p>b. Enter a netmask using the form 255.255.255.0.</p> <p>c. Enter a gateway IP address.</p> <p>d. Enter the DNS server IP address</p> <p>e. If yes, enter the IP address of the secondary DNS server.</p> <p>f. Enter yes if you want DNS lookups to use a specific domain.</p> <p>g. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com</p> <p>Enter yes to restart with the new configuration settings applied.</p>	<p>We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.</p> <p>Recommended: Respond with no:</p> <p>a. Enter an IP address</p> <p>b. Enter a netmask using the form 255.255.255.0.</p> <p>c. Enter a gateway IP address.</p> <p>d. Enter the DNS server IP address</p> <p>e. If yes, enter the IP address of the secondary DNS server.</p> <p>f. Enter yes if you want DNS lookups to use a specific domain.</p> <p>g. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com</p> <p>Enter yes to restart with the new configuration settings applied.</p>
Enter a valid hostname (enter a unique name)	Type a hostname when prompted; do not include the domain; for example: juniperatp1	Type a hostname when prompted; do not include the domain; for example: juniperatp1	Type a hostname when prompted; do not include the domain; for example: juniperatp1

Configuration Wizard Prompts	Customer Response from All-in-One	Customer Response from Core or Mac Mini	Customer Response from Collector
<p>[OPTIONAL]</p> <p>If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p>	<p>Refer to Configuring an Alternate Analysis Engine Interface on page 95 for more information.</p> <p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>	<p>Refer to Configuring an Alternate Analysis Engine Interface on page 95 for more information.</p> <p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>	<p>[Traffic Collectors do not send or receive Core analysis engine CnC network traffic, so no eth2 interface is needed.]</p>
<p>Regenerate the SSL self-signed certificate (Yes/No)?</p>	<p>Enter yes to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.</p> <p>If you decline the self-signed certificate by entering no, be prepared to install a certificate authority (CA) certificate.</p>	<p>Enter yes to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.</p> <p>If you decline the self-signed certificate by entering no, be prepared to install a certificate authority (CA) certificate.</p>	<p>Not applicable to Collector.</p>

Configuration Wizard Prompts	Customer Response from <u>All-in-One</u>	Customer Response from <u>Core</u> or <u>Mac Mini</u>	Customer Response from <u>Collector</u>
Enter the following server attributes: Is this a Central Manager device:	Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in-One IP address.	Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in-One IP address.	Enter No; the system will request that you enter the CM IP address now.
Device Name: (must be unique)	Enter the Juniper ATP Appliance Collector Host Name; this identifies the Collector in the Web UI.	Enter a Juniper ATP Appliance Mac Mini or Core/CM Host Name; this identifies the Mac OS X or Core Engine in the Web UI.	Enter the Juniper ATP Appliance Collector Host Name; this identifies the Collector in the Web UI.
Device Description	Enter a device Description	Enter a device Description	Enter a device Description
Device Key PassPhrase NOTE: Remember this passphrase and use it for all distributed devices!	Enter a user-defined PassPhrase to be used to authenticate the Core to the Central Manager.	Enter the same PassPhrase used to authenticate the Core or Mac Mini to the Central Manager.	Enter the same PassPhrase used to authenticate the Collector to the Central Manager.

Configuration Wizard Prompts	Customer Response from All-in-One	Customer Response from Core or Mac Mini	Customer Response from Collector
<p>[OPTIONAL]</p> <p>If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p> <p>...Restarting alternate-exhaust (eth2) interface</p> <p>...A complete network interface restart can take more than 60 seconds</p> <p>...Restarting os_engine_eth2 interface</p> <p>Waiting for os_engine_eth2 to get ready (MAXWAIT is 32 seconds).</p>	<p>Refer to Configuring an Alternate Analysis Engine Interface on page 95 for more information.</p> <p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>	<p>Refer to Configuring an Alternate Analysis Engine Interface on page 95 for more information.</p> <p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>	<p>Traffic Collectors do not send or receive Core analysis engine CnC network traffic.</p>

- After all the questions are answered, the wizard summarizes the answers. To change an answer, enter the step number. To save changes and exit, press <enter>.
- To return to the configuration wizard to make changes to the configuration, use the following CLI command:

```
JATP# wizard
```

NOTE Be sure to use the double quotation marks in CLI parameters using special characters.

- Refer to the Juniper ATP Appliance CLI Command Reference for command syntax and usage.

Juniper ATP Appliance Web UI Access

The Juniper ATP Appliance Web UI is a secure web-based defense system configuration and malware analysis management interface. You can access it by pointing your web browser to the configured IP address of the appliance using HTTPS. For example, if the configured IP address of the appliance is 10.8.20.2, then you would access the appliance GUI by pointing your browser to `https://10.8.20.2`.

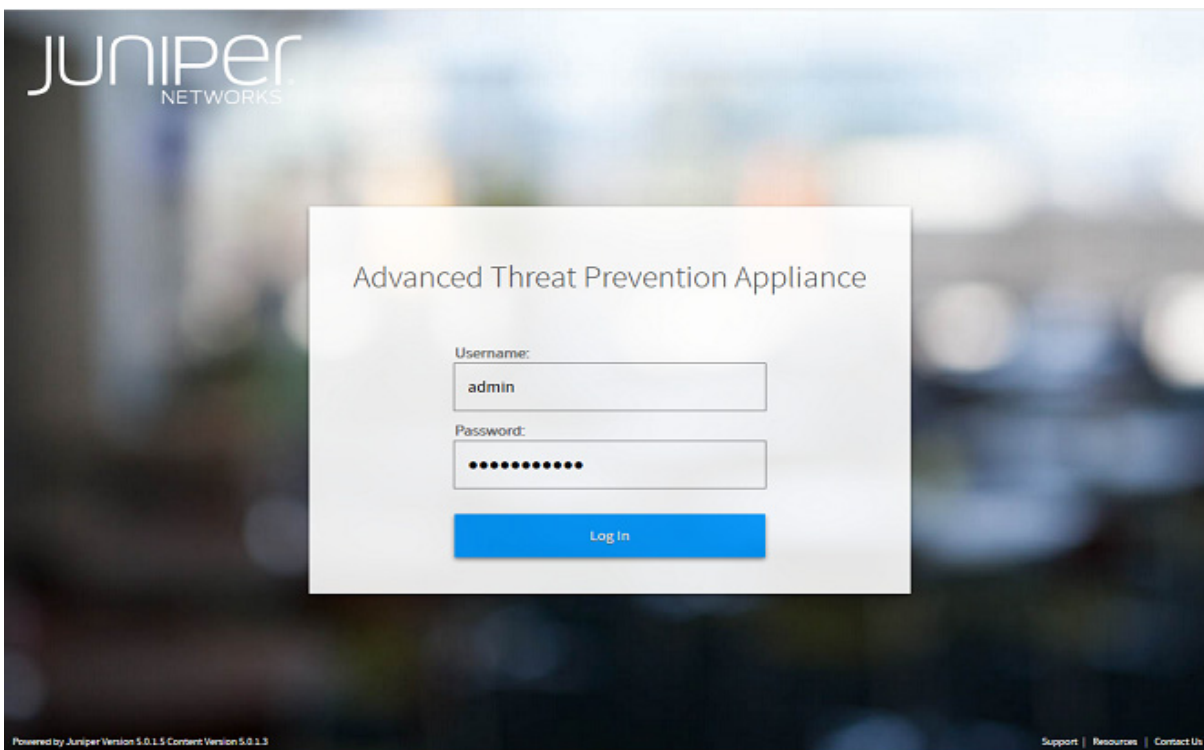
At the login screen, shown in the following figure, enter the default username and password.

- The default username is `admin` and the password is `juniper`. Be sure to reset this default password after initial login.

The CM Web UI supports passwords up to 32 characters, and at least 8 characters. Letters (uppercase/lowercase), numbers, and special characters can be used with the exception of double-quotes (`"`), spaces, or backslash characters (`\`) in passwords.

NOTE The Juniper ATP Appliance Web UI login username and password are separate from the CLI admin username and password.

Figure 3 Central Manager Web UI Login Access



Login to the Juniper ATP Appliance using SAML Authentication

When SAML settings are configured, users for which SAML authentication is assigned are automatically redirected to the enterprise's IdP login page when they try to access the Juniper ATP Appliance. For more information about SAML authentication, refer to [Configuring SAML Settings on page 155](#) and [Configuring User Accounts on page 151](#).

For more information about the Juniper ATP Appliance Central Manager Web UI, refer to [“Working with the Juniper ATP Appliance Web UI” in the next section.](#)

Login to the Juniper ATP Appliance System using AD Authentication

When AD authentication is configured, users are authenticated via Active Directory (AD) servers using the RADIUS protocol in customer networks.

For more information about AD authentication, refer to [Configuring RADIUS Server Settings on page 115](#) and [Configuring Active Directory on page 184](#).

Working with the Juniper ATP Appliance Web UI

This section describes how to navigate the appliance Web UI and describes its tabs:

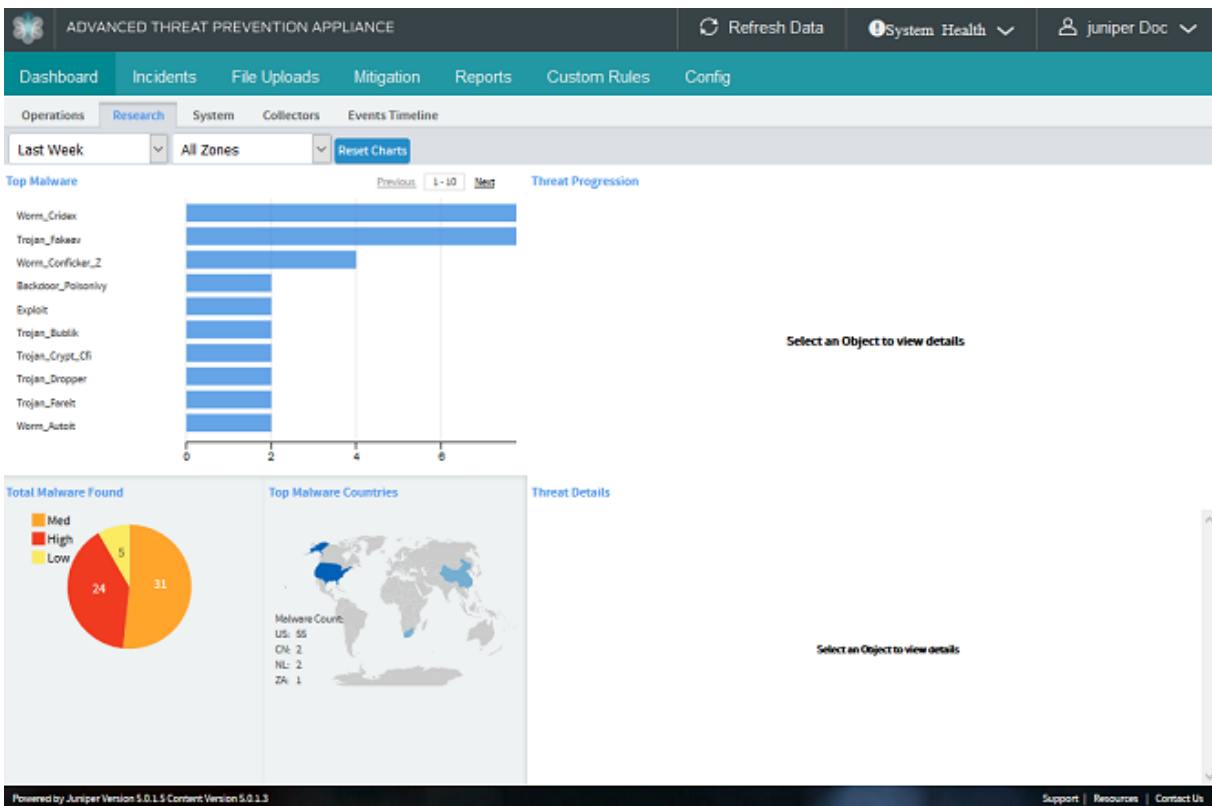
- Navigating the CM Web UI
- Summary of Tabs

Navigating the CM Web UI

To navigate through the appliance Web UI:

- Use the tabs to access the main pages of the Web UI.
- Use links such as the path links under a tab or the left panel links under the Config tab to navigate to other linked pages.

Figure 4 Navigating the Juniper ATP Appliance Central Manager Web UI



Navigating the CM Web UI

- To set an initial view, select a time period from the dropdown for which the Juniper ATP Appliance Dashboard or Incidents tab should display detection results and malware analysis details. All graphs and tabular displays are synchronized by the time period selection control. available time period options include:
 - › 24 hours (hourly)
 - › 1 week (weekly)
 - › 1 month (monthly)
 - › 3 months (quarterly)
 - › 1 year (yearly)
- Select the results type to display in the Incidents table: show threats | show suspicious | show benign.
- Perform a search of the Incidents table by entering search criteria in the Search field; you may search for SHA1, MD5 sums, Collector names, Threat Name, Threat Source, and so on.
- Click a header at the top of a table column in the Incidents tab, for example, to sort the table by that column. Click again to change the sort order from descending to ascending.

The screenshot displays the Juniper ATP Appliance CM Web UI. At the top, there's a navigation bar with tabs: Dashboard, Incidents, File Uploads, Mitigation, Reports, Custom Rules, and Config. The 'Incidents' tab is active. Below the navigation bar, there's a search bar and filters for 'Show Threat', 'All Zones', and 'Last Week'. A table lists incidents with columns: Status, Incident ID, Risk, Threat, Progression, Collector Type, Threat Source, Threat Target, Zone, Target OS, and Collector. Three incidents are visible, all with a risk level of 'HIGH' or 'MED'. The first incident, 'WORM_CRIDEX.CY', is selected, and its details are shown in a panel below. The details panel includes a 'SUMMARY' tab and a 'DOWNLOADS' tab. The 'SUMMARY' tab shows metadata like Risk (High), Threat Category (Trojan_Generic), Asset Value (Max), Target OS (unknown), Relevance (Medium), Progression (Download), Protocol (HTTP), OS Matched (No), and Virus Scanner Recognised (Recognized by Selected AntiVirus). A graph on the right shows the progression of the threat over time, with a peak around Jan 15 12:05:00. The bottom of the screen shows the version information: 'Powered by Juniper Version 5.0.1.5 Content Version 5.0.1.3' and links for Support, Resources, and Contact Us.







- Click a row in the Incidents table to display generalized information about the threat in the left panel Summary table below. Click the subset of tabs under the Summary tab, in turn, to view event details. And expand the row for greater details by clicking the arrow.
- Use the left panel menu options on the Config page to open configuration windows for Notifications, System Settings and Environmental Settings.
- On the configuration pages, enter information in the fields provided.

Summary of the Tabs in the Juniper ATP Appliance Web UI

The Juniper ATP Appliance Central Manager Web UI

The purpose of each Web UI Tab is described as follows:

- **Dashboard**—Displays appliance status information as well as detected threats and incident trends. Context-specific Threat Views on the Operations Dashboard and Research Dashboard prioritize the threats that affect your enterprise the most, according to your configurations. The System Dashboard and Collector Dashboards (Web and Email) provide information about System and Collector health status and trends. The Event Timeline Dashboard displays Advanced Threat Analytics (ATA) data per event for a given vendor and Endpoint IP, Hostname, Username or Email.
- **Incidents**—Displays levels of detailed information about malicious or suspicious downloads or infections, at various kill chain stages, in your network. See also [Navigating the Incidents Page on page 241](#) for more information.
- **File Uploads**—Provides detailed information about all file upload malware analysis results, whether malicious or benign, in one Web UI location. File Upload Handling capabilities from the Central Manager Web UI include uploads from a new File Uploads tab. The enhanced file uploads API accepts additional meta-data for third party integrations such as Carbon Black Response to provide seamless integration with incidents. For more information, refer to [Submitting a Malware File for Analysis on page 87](#).
- **Mitigation**—Presents mitigation options for specific detected threats such as Auto-Mitigation, blocking callbacks from the Gateway or IPS/Next Gen Firewall, or deploying the Juniper ATP Appliance Infection Verification Package (IVP) or Carbon Black Response integration to confirm infection on the targeted endpoint. For more information, refer to [Configuring Firewall Auto-Mitigation on page 147](#).
- **Reports**—Allows you to generate or schedule consolidated and detailed executive summary reports, or system Audit Reports. Refer to [Generating Reports on page 250](#) for more information.
- **Custom Rules**—Displays custom Snort rule matches in the Juniper ATP Appliance Central Manager Web UI Custom Rules Tab; correlated Snort Rule matches are available on the Incidents Tab. Refer to [Configuring Custom SNORT Rules on page 192](#) for information about adding rules to the system.
- **Config**—Allows you to configure appliance and software system settings as well as configure analysis, notifications and mitigation settings.
- **Refresh**—Performs a refresh of the CM browser display. Always perform a refresh following a software or security content update.
- **Health**—Displays health indicator checks for Juniper ATP Appliance static and dynamic detonation engines and analysis systems. All indicators should display the green checkmark which indicates that the systems are in good health. If a red indicator displays, then troubleshooting actions are required. .

		
Behavior Engine		Core Detonation Engine
Static Engine		Static Analysis
Correlation		Event Correlation Engine
Web Collectors		Connection status of the enabled Web Collectors
Secondary Cores		Connection status of configured Secondary Cores (Mac OSX)

- **Log Out**—Performs a log out of the current Central Manager Web UI user.

Deploying the Distributed Juniper ATP Appliance System

Deploying the Juniper ATP Appliance Advanced Threat Protection system is covered in the following sections:

- [“Deployment Scenarios” in the next section](#)
- [Deployment Guidelines on page 63](#)
- [Network Tapping on page 64](#)

- [SPAN Port Mirroring on page 64](#)
- [Guidelines for Environments with Web Proxies on page 65](#)
- [Configuring Journaling for the Email Collector on page 65](#)
- [Deploying Juniper ATP Appliance SaaS Virtual Collectors on page 89](#)
- [Deploying Juniper ATP Appliance SaaS Virtual Collectors on page 89](#)
- [Deploying SaaS Virtual Cores as OVAs on page 91](#)

NOTE For information about validating Juniper ATP Appliance deployment, refer to the Juniper ATP Appliance CLI Command Reference.

Deployment Scenarios

Three Juniper ATP Appliance advanced threat protection deployment scenarios are described in this section:

- Juniper ATP Appliance Deployment in an Enterprise Headquarters
- Juniper ATP Appliance Defense in a Distributed and/or Clustered Enterprise Environment
- Juniper ATP Appliance Distributed SaaS/OVA or Virtual Deployment

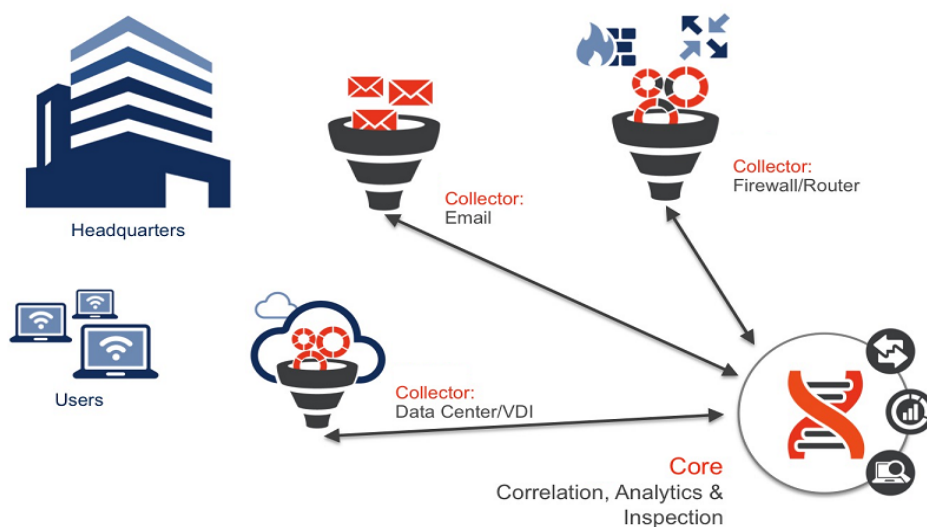
Juniper ATP Appliance Defense in an Enterprise Headquarters

In this scenario (see Figure 5 below), a Core|CM system is installed in an enterprise headquarters with three physical Traffic Collectors deployed for wide traffic coverage and service integration.

- Collector 1 positioned for Data Center coverage
- Collector 2 positioned for Web traffic coverage
- Collector 3 positioned at the firewall for coverage and mitigation/blocking

In this deployment scenario the Traffic Collectors provide network coverage and integrate with existing infrastructure, and the Core|CM provides web and email incident detection while performing risk-aware mitigation and blocking at the firewall.

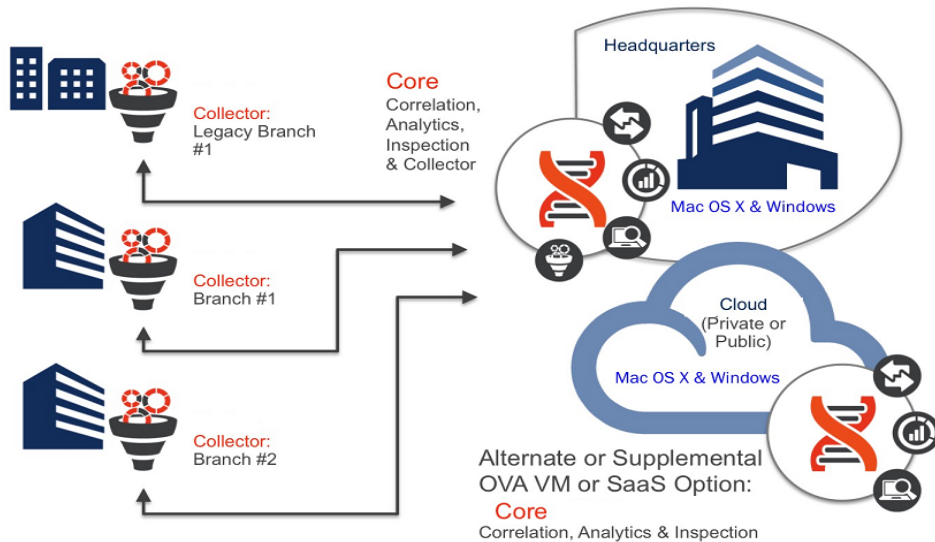
Figure 5 Juniper ATP Appliance Defense in an Enterprise Headquarters Deployment



Juniper ATP Appliance Defense in a Distributed Enterprise Environment

A distributed enterprise requires a distributed threat defense scenario (see Figure below). In this scenario, various physical and virtual Collectors are deployed remotely at branch offices for continuous inspection and extended network visibility.

Figure 6 Juniper ATP Appliance Defense in a Distributed Enterprise Environment



Traffic analysis takes place at the distributed Collectors and objects are then delivered to the Core|CM, deployed at enterprise headquarters, where network objects are subjected to multi-OS detonation chamber execution for final threat assessment and mitigation.

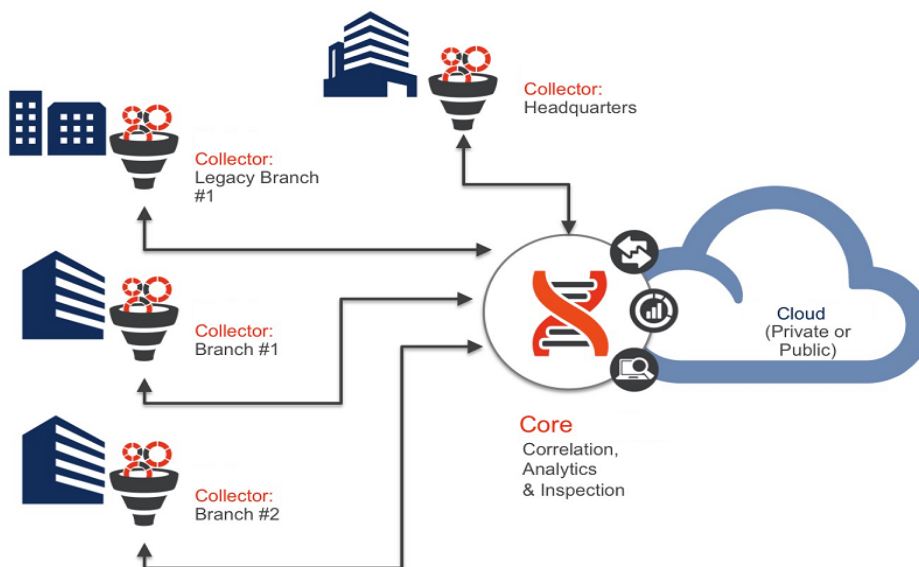
Alternatively, the Core|CM in this distributed deployment could also be configured as an OVA VM or SaaS deployment. In addition, a supplemental Juniper ATP Appliance Core could be deployed in a public or private enterprise cloud.

Juniper ATP Appliance Distributed SaaS/OVA Deployment

In a distributed SaaS/OVA deployment, Traffic Collectors are deployed in several branch offices at critical monitoring locations with the Core|CM at headquarters and a Collector installed as a VM OVA in the cloud to inspect and analyze all content and trigger mitigation actions at configured enforcement servers, such as a PAN or SRX Firewall, for example.

NOTE The Juniper ATP Appliance Core can be deployed in a public, hybrid or private cloud.

Figure 7 Juniper ATP Appliance Distributed SaaS/OVA Deployment



Deployment Guidelines

The following section provides an overview of details you should review to successfully deploy a Distributed Core|CM or All-in-One Juniper ATP Appliance system. Review these guidelines before deploying devices and/or virtual (software-only or OVA) devices as well to avoid troubleshooting issues post-deployment.

1. Obtain the estimated bandwidth traffic, including average/peak information for optimal sizing of the Juniper ATP Appliance Advanced Threat Protection solution. The bandwidth can be acquired from an upstream router or firewall in the network path. Discuss your enterprise network bandwidth and topology requirements with Juniper ATP Appliance Customer Support.
2. The Web Traffic Collector can be deployed at any headquarters or remote location.
3. A network switch with a switch mirror (SPAN) or TAP port should be available to connect to the Traffic Collector. The SPAN/TAP feed should carry live HTTP and non-HTTP end-user network traffic.
4. If NAT (Network Address Translation) or Web proxies that obscure originating IP addresses are used in your environment, the Traffic Collector must be able to see the internal side of your NAT or proxy traffic.
5. The Juniper ATP Appliance Core or All-in-One can be deployed at any location in the enterprise network, but is often deployed in a management VLAN.
6. Have an SSH client on the remote admin system ready for remote CLI access to the Juniper ATP Appliance Traffic Collector and Core or All-in-One system.

NOTE Always use the latest version of Putty for SSH operations, if using Putty as an SSH client.

7. Check for network proxies in the management path between the Juniper ATP Appliance Core and the remote admin system, and then configure the proxy appropriately. Refer to [Configuring Proxy Settings for the Management Network on page 121](#) for information about configuring and managing proxy settings from the Juniper ATP Appliance Web UI, and the Juniper ATP Appliance CLI Command Reference for information about configuring proxies from the Juniper ATP Appliance CLI.

NOTE Since malware may propagate using a number of methods, and botnet Command and Control (C&C) channels may use virtually any port, there should be no special restrictions/ACLs on the traffic fed to the Juniper ATP Appliance device.

8. Be sure to configure Email Journaling or Gmail BCC handling for the Juniper ATP Appliance Email Collector.

NOTE Review all deployment prerequisites in the **Juniper ATP Appliance Quick Start Guide** for your products.

9. On the first boot of a virtual core (either AMI or OVA) with two disks configured, the appliance takes time to set up the second disk to be used. During this process, the system is not yet ready for use. This process may take up to 10 minutes.
10. Juniper provides integration with firewalls, secure web gateways, and many other security devices. A large advantage of distributed defense is that Juniper ATP Appliance leverages your existing security infrastructure for mitigation and monitoring. Please note the following integration requirements:
 - › Requires Microsoft Exchange 2010+ for the Email Collector
 - › Junos version 12.1-X47.x for Juniper Firewall
 - › Palo Alto Firewall Version x for Palo Alto
 - › Cisco ASA Firewall - be sure to review the "ASA REST API Compatibility" section of the "Cisco ASA Compatibility" document to determine if the REST API is supported on a particular ASA hardware platform.
 - › Check Point Firewall integration requires Check Point GAiA operating system release R76, R77, or later. Check Point IPSO and Secure Platform (SPLAT), which are predecessors of GAiA, are not supported.
 - › Fortinet Firewall integration - latest release.
 - › Carbon Black Response - latest release
 - › McAfee ePO and Symantec - latest releases

Network Tapping

A tap is a device that permits unimpeded traffic flow while simultaneously copying all the traffic from a full-duplex link and sending the information to Juniper ATP Appliance Collectors for object analysis. Tap mode uses an external fiber tap (for GBIC ports) or a built-in internal tap (for 10/100/1000 Monitoring ports). In tap mode, the Juniper ATP Appliance Collector monitors the packet information as it traverses the full-duplex network segment. Like SPAN mode, Tap mode is passive.

Use a network tap to send a copy of network traffic from a network segment to the eth1 network monitoring port of the Juniper ATP Appliance Collector. The tap does not interfere with traffic and, if shut down, allows traffic to pass through unhindered.

SPAN Port Mirroring

The Switch Port Analyzer (SPAN) port on a switch is designed for security monitoring. It allows a connected Juniper ATP Appliance to receive a copy of every packet from all incoming and outgoing traffic moving through the switch. This is port forwarding or port mirroring; a passive non-intrusive packet capture method.

Configure a switch with port mirroring capability to forward a copy of incoming and outgoing traffic passing between selected ports to SPAN ports on the switch. Then, connect the SPAN port to the Juniper ATP Appliance (labeled eth1).

The Juniper ATP Appliance can be configured in SPAN mode by configuring a switch with port mirroring capability to forward a copy of incoming and outgoing traffic passing between selected ports to SPAN ports on the switch. Then connect the SPAN ports to the Collector (ports eth1).

Guidelines for Environments with Web Proxies

The following additional guidelines apply to environments with web proxies:

NOTE Refer to [Configuring Proxy Settings for the Management Network on page 121](#) for information about configuring and managing management network proxy settings from the Juniper ATP Appliance Web UI, and the Juniper ATP Appliance CLI Command Reference for information about configuring proxies from the Juniper ATP Appliance CLI.

Refer to [Span-Traffic Proxy Data Path Support on page 40](#) for more information about SPAN-Traffic proxy configurations.

- If your environment contains web proxies or other NAT devices that obscure originating IP addresses, the Juniper ATP Appliance must be deployed in such a way that it sees web traffic from the internal (or LAN) side of the proxy. If misconfigured, the appliance reports the malicious site as being the LAN IP of the proxy. Misconfiguration may also obscure a compromised endpoint if the LAN IP address of the endpoint is not visible to the Juniper ATP Appliance. If your web proxy supports X-Forwarded-For (XFF) headers, the Juniper ATP Appliance Collector may be placed in front of or behind the proxy. You must make sure that the Collector has X-Forwarded-For support enabled via the CLI. Support for X-Forwarded-For headers is enabled by default.
- The appliance must be able to see web (HTTP) traffic and traffic for other network protocols:
 - Botnet remote command and control traffic, as well as some types of exploits, may use protocols other than HTTP, so it is imperative to have visibility into non-web traffic. Support for this type of proxy is pending.
 - The Juniper ATP Appliance Collector is not able to decrypt SOCKS tunneled traffic, so if you use SOCKS proxies in your environment, the Juniper ATP Appliance Traffic Collector should SPAN a network segment that is outside the SOCKS proxy in order to monitor non-HTTP traffic.

Configuring Collector Email Journaling

After installing a Juniper ATP Appliance Core or All-in-One system, both of which contain an Email Traffic Collector in the Core component, you will need to configure an exchange server journal account for the Collector to poll, and set Postfix to forward Gmail Bcc (blind carbon copies) of all mail traffic to the Collector as a default forwarding mechanism.

Configuring Journaling for the Email Collector

Email Journaling

Juniper ATP Appliance Traffic Collectors continuously monitor and inspect all network traffic for malware objects; extracting and sending objects to the Core for distribution to the Windows or Mac Detection Engines.

For Windows traffic, Microsoft Exchange Server journaling can be configured to record a copy (a journal) of enterprise email messages, and then periodically send them to a journal mailbox on the Exchange Server.

NOTE No email or email data is stored on the Traffic Collector. On the Juniper ATP Appliance Core, extracted objects and some meta data (such as source and destination email addresses, timestamp data, etc., are stored and Juniper ATP Appliance logs email header info in the log file. No text from the email is retained (except for the attachment(s) for malware detonation and analysis)

Exchange Server 2010 can be configured to support envelope journaling only. This means that a copy is made of each email message body and its transport information. The transport information is essentially an envelope that includes the email sender and all recipients.

The Juniper ATP Appliance Email Collector polls the Exchange Server for journal entries and as-scheduled, pulls all the emails in the journal account from the exchange server to the Collector. The Email Collector uses journaling for initial traffic analysis and email attachment monitoring/inspection. All email traffic (and email attachments) are sent from the Email Collector to the Juniper ATP Appliance Core for detonation in the Windows or Mac OS X detection engines.

When email-based malware or malicious email attachments are detected, the journal entry is incorporated into the analysis results by the Juniper ATP Appliance Central Manager and sent out as a notification to the Juniper ATP Appliance administrator, with corresponding mitigation and/or infection verification actions detailed in the Central Manager Web UI.

NOTE Juniper ATP Appliance supports journaling for Exchange 2010 and later.

To setup Email Collector Journaling, follow these procedures:

- › “Creating a Journaling Mailbox on the Exchange Server” in the next section
- › Configuring Microsoft Exchange Server 2013 Journaling on page 66
- › Configuring Exchange-Server Journal Polling from the Web UI on page 69
- › Configuring Office 365 Journaling on page 70
- › Configuring Gmail Journaling on page 72
- › Configuring Gmail Threat Mitigation on page 75

Creating a Journaling Mailbox on the Exchange Server

NOTE See also Configuring Microsoft Exchange Server 2013 Journaling.

1. Launch Microsoft Exchange Management Console.
2. Expand Recipient Configuration node and click on Mailbox node.
3. Select New Mailbox... from the Actions pane.
4. Select User Mailbox option and click Next.
5. Select New user option and click Next.
6. New user mailbox details
7. Enter the ‘User information’ details for the Collector to which the new journaling mailbox will be assigned and click Next.
8. Enter an ‘Alias’ for the journaling mailbox and click Next.
9. Click Next again and review the new mailbox summary for the new mailbox to create, then click New.
10. Now that the journaling mailbox is created, configure standard journaling by configuring a Mailbox Database.

Configuring a Mailbox Database

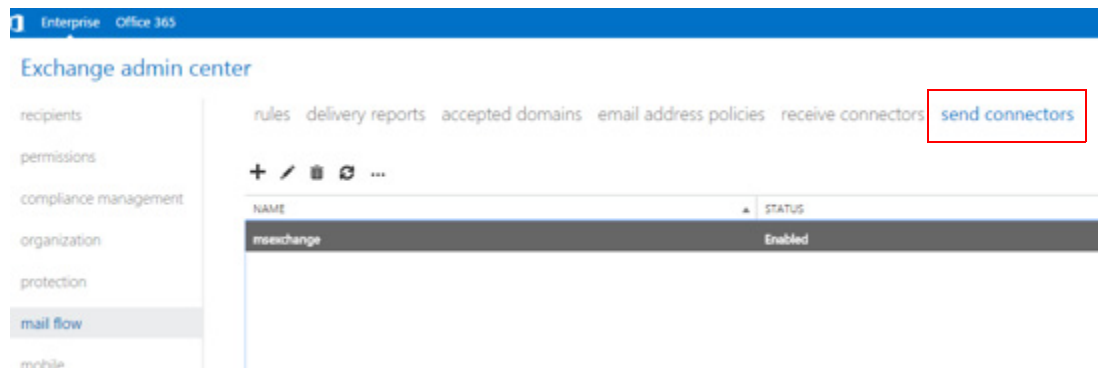
- In the Microsoft Exchange Management Console>Server Configuration, click on Mailbox database.
- In the Toolbox Actions of Selected Mailbox Database, click on Properties.
- In the Mailbox Database Properties page, go to the General tab and select the Journal Recipient checkbox, BUT, before selecting the checkbox, first click on Browse and choose which mailbox will get all messages from the mailbox database. After checking Journal Recipient, click OK to finish.

Configuring Microsoft Exchange Server 2013 Journaling

1. Login to the MS Exchange Server Admin Center at: <https://exchageserverip/ecp/>

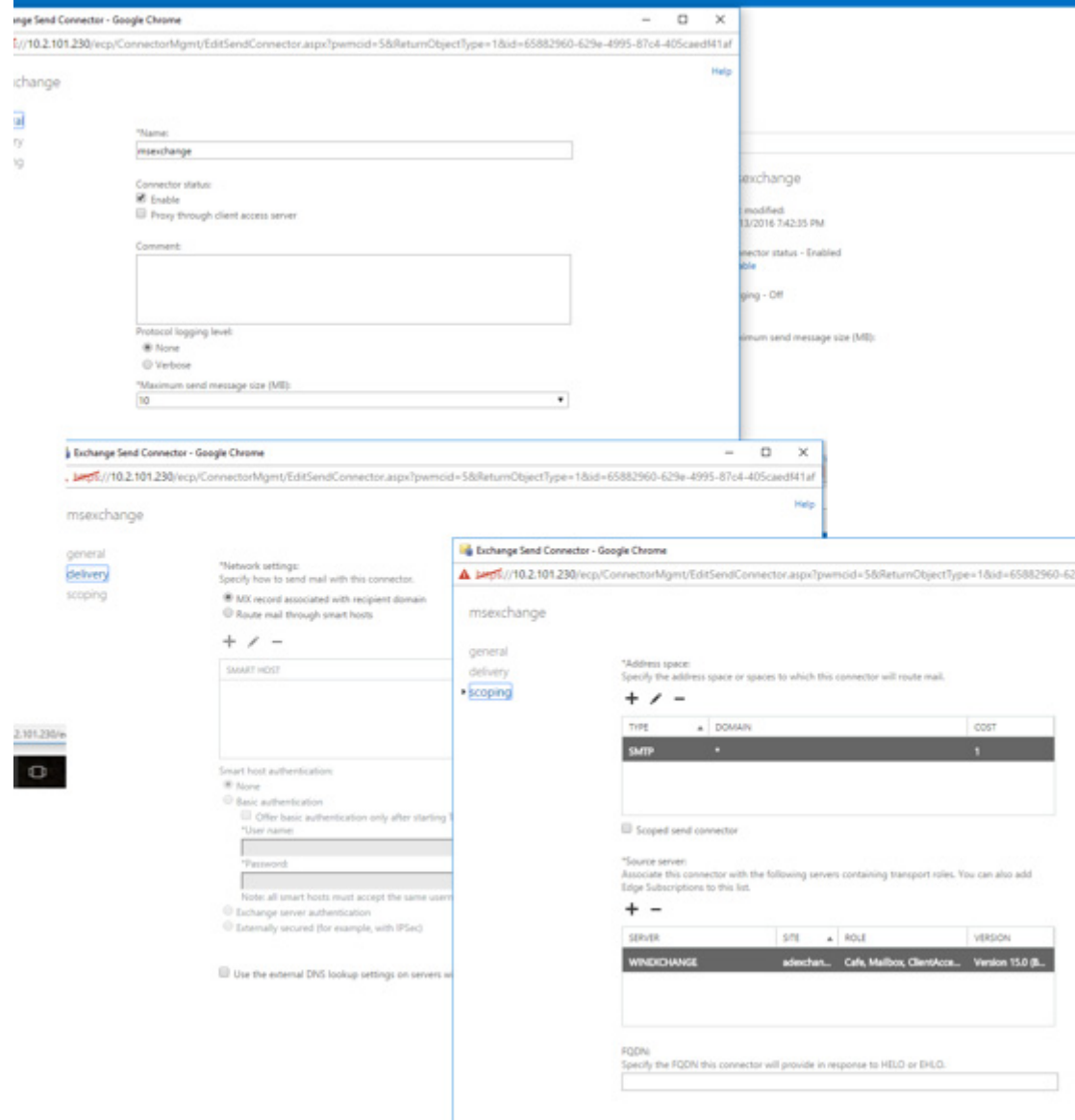
2. Select the Send Connectors tab.

Figure 8 Exchange Admin Center



3. Navigate to mail flow>>send connectors and enter Send Connector settings:

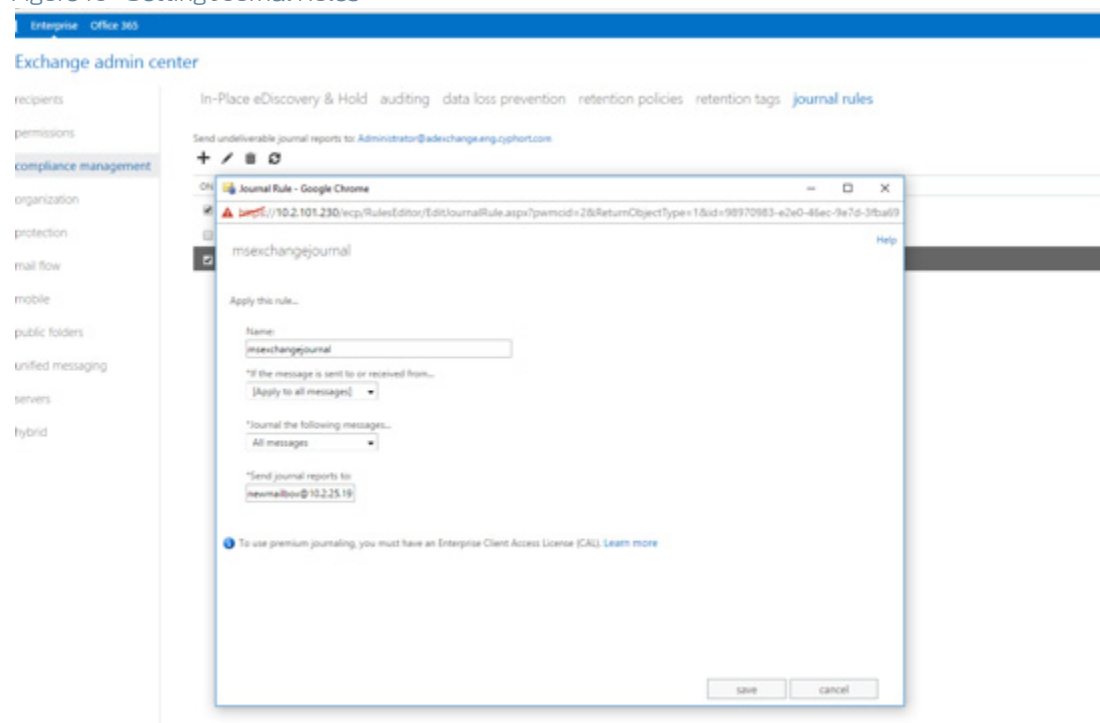
Figure 9 Send Connector Settings



4. Save the connector settings.
5. Navigate to Compliance Management>>Journal Rules to configure Journal rules.

6. Provide the mailboxname and ip address in the “Send Journal Reports To” field .
Note: This should match the mailbox name configured at the Juniper ATP Appliance Email Collector Config>System Profiles>Email Collector Web UI page.

Figure 10 Setting Journal Rules



Refer to [Configuring Email Collectors on page 133](#) for information about configuring Email Collectors.

Configuring Exchange-Server Journal Polling from the Web UI

1. From the Juniper ATP Appliance Central Manager Config>EmailNavigate to compliance management>>Journal rules Collector page, click the Add New Email Collector button, or click Edit for an existing Collector listed in the Current Email Collectors table.
2. Enter and select the email journaling settings in the displayed configuration fields: Email Server [IP], Protocol, SSL, Mailbox Name, Password, Poll Interval (in minutes), Keep Mail on Server, and Enabled. [See following figure].

2. From the Office 365 Admin Center, select Admin Centers > Exchange.

Figure 11 Navigating to the Microsoft Office 365 Admin Center

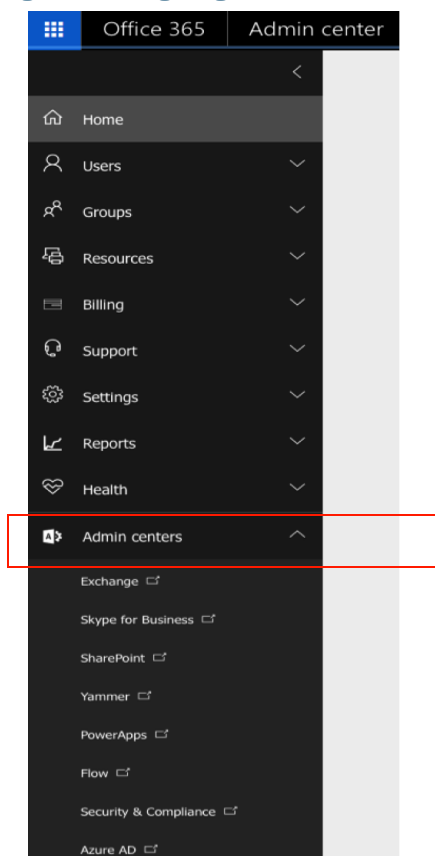
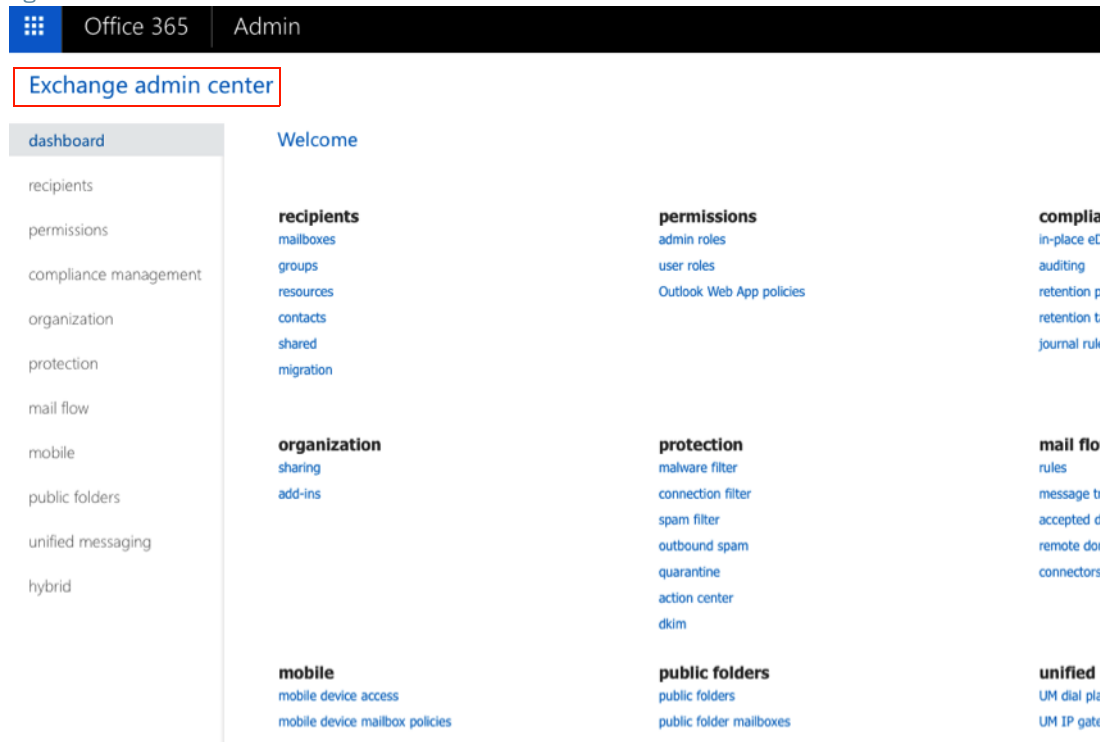


Figure 12 Microsoft Office 365 Admin Center



3. Select Compliance Management > Journal Rules.
 - › Click on the + sign to add a new Journal Rule.
 - › Complete the new journal rule form fields.

Configuring Gmail Journaling

Use the following procedure to configure email journaling for Gmail:

1. Navigate to the Google Admin Home site at <https://admin.google.com/AdminHome>.
2. From the Google Admin Console Dashboard, navigate to Apps->G Suite->Gmail->Advanced Settings.

NOTE To view Advanced Settings, scroll to the bottom of the Gmail page.

3. Navigate to the Compliance Section and click Add Another Compliance Rule to setup deliver to the Juniper ATP Appliance MTA.

Figure 13 Google Gmail Admin Home Journaling Settings

Settings for Gmail > Advanced settings

Hosts Default routing

Search settings

Content compliance
Disabled
Locally applied

Content compliance
Disabled
Locally applied

Content compliance
Disabled
Locally applied

Content compliance
Locally applied

Comprehensive mail

Add setting

Content compliance [Help](#)

Required: enter a short description that will appear within the setting's summary.

1. Email messages to affect

- ☐ Inbound
- ☐ Outbound
- ☐ Internal - sending
- ☐ Internal - receiving

2. Add expressions that describe the content you want to search for in each message

If ANY of the following match the message ▾

Expressions	ADD
No expressions added yet. Add	

3. If the above expressions match, do the following

[CANCEL](#) [ADD SETTING](#)

4. Select the options as displayed in the sample screenshot below (Setting 1 and 2):

Figure 14 Journaling Criteria required by Juniper ATP Appliance MTA

Settings for Gmail > Advanced settings

Hosts Default routing

Search settings

Disabled
Locally applied

Content compliance
Disabled
Locally applied

Content compliance
Locally applied

Content compliance
Locally applied

Comprehensive mail storage
Not configured yet

Edit setting

1. Email messages to affect

- ☒ Inbound
- ☒ Outbound
- ☒ Internal - sending
- ☒ Internal - receiving

2. Add expressions that describe the content you want to search for in each message

If ANY of the following match the message ▾

Expressions	ADD
Matches: "@"	

3. If the above expressions match, do the following

Modify message ▾

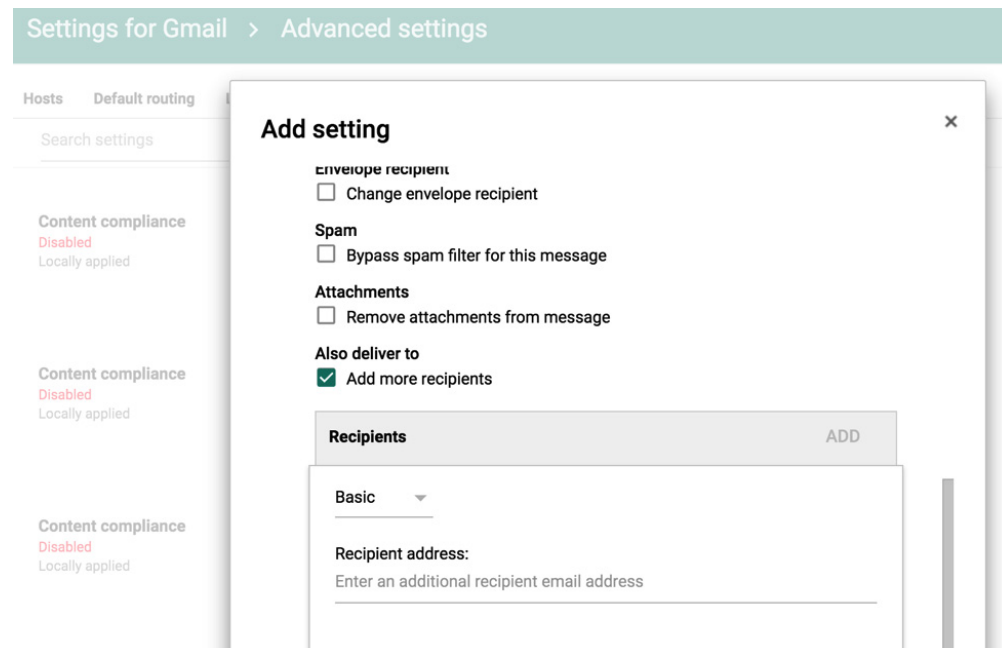
Headers

☐ Add X-Gm-Original-To header

CANCEL SAVE

5. Be sure to add the Recipient information (this is the Juniper ATP Appliance MT); for example: JATP_mta@FQDN or JATP_mta@ip.

Figure 15 Setting the Juniper ATP Appliance MTA as the Gmail Recipient: JATP_mta@FQDN



Configuring Email Detection Mitigations

You can configure Gmail and/or Office 365 for Juniper ATP Appliance Email threat event Mitigations. Mitigation Keys allow you to quarantine emails that are detected as malicious by using Gmail APIs or Office 365 APIs.

- [“Configuring Gmail Threat Mitigation” in the next section](#)
- [Configuring Office 365 Journaling on page 70](#)

Configuring Gmail Threat Mitigation

For enterprise environments using a Google Apps domain, an administrator of the Google Apps domain can authorize an application to access user data on behalf of users in the Google Apps domain. Authorizing a service account to access data on behalf of users in a domain is sometimes referred to as "delegating domain-wide authority" to a service account.

Delegating domain-wide authority to a Gmail service account

To delegate domain-wide authority to a Gmail APIs Service Account, first enable domain-wide delegation for an existing service account from the Google APIs Service Accounts page, or create a new service account with domain-wide delegation enabled.

To create a new Gmail Service Account:

1. Navigate to the Google APIs Service Accounts page.

2. Select an existing Project or Create A New Project from under the Project drop-down menu at the top left corner.

Figure 16 Navigate to the Google APIs Service Account page

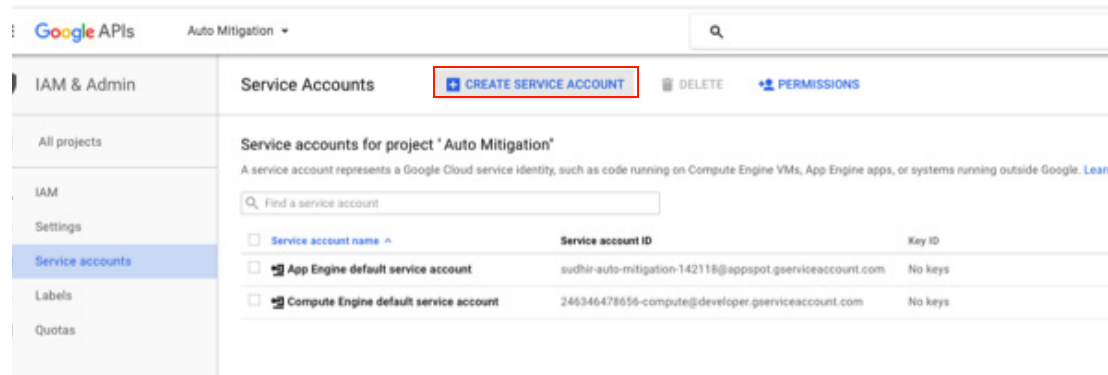
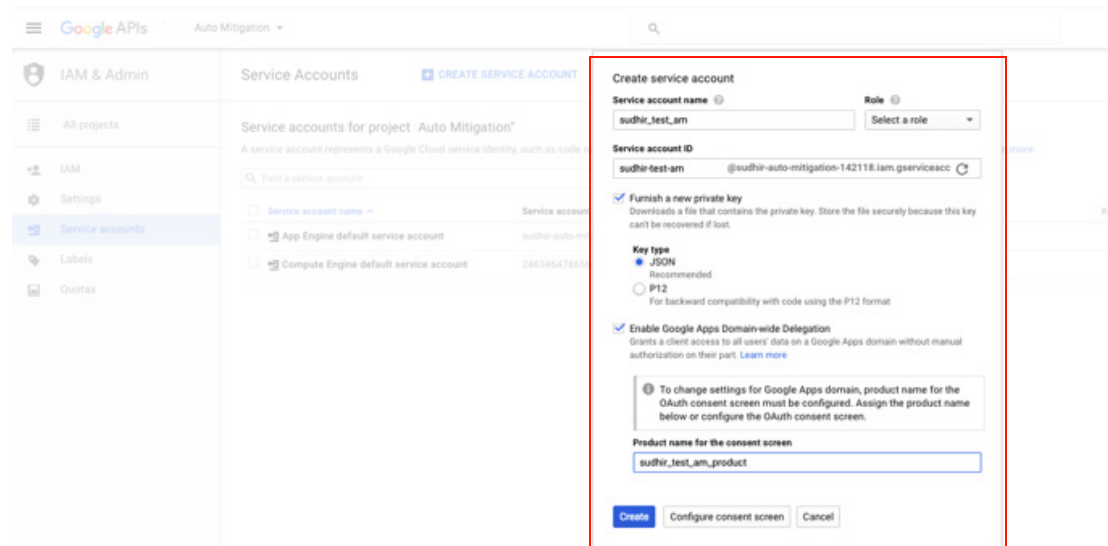


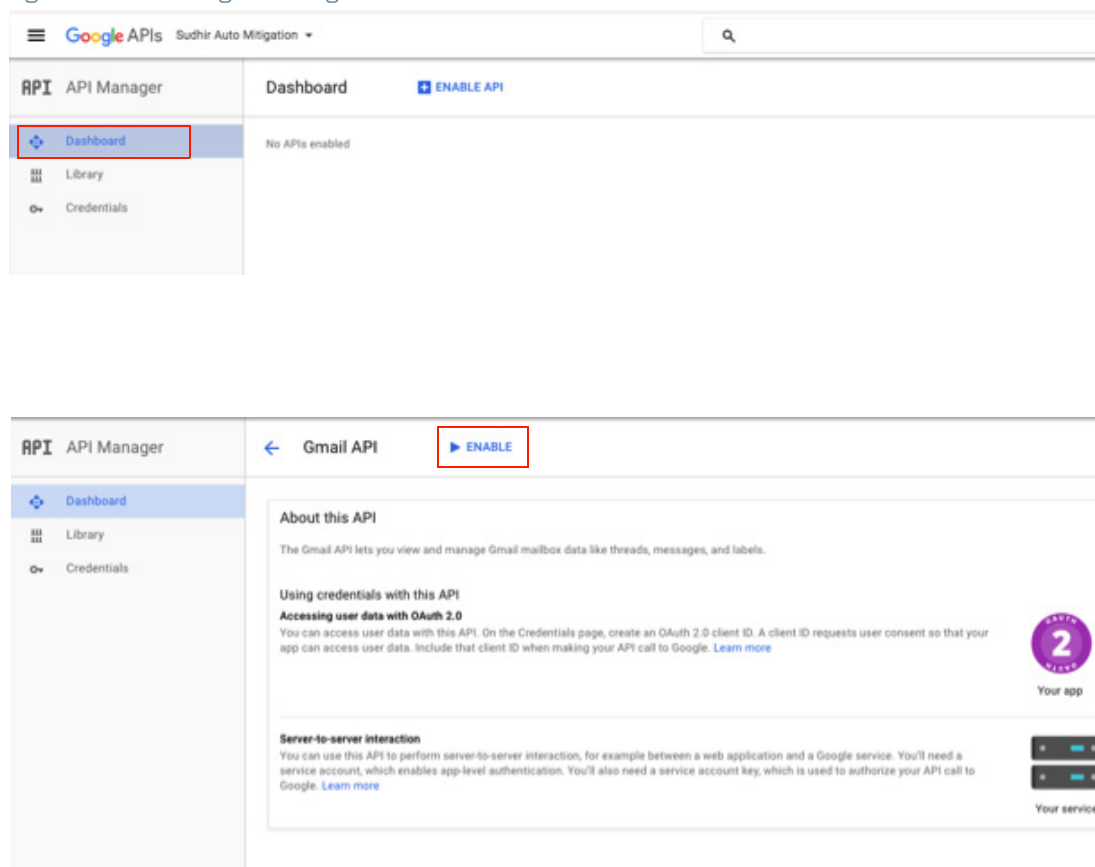
Figure 17 Creating a New Google APIs Service Account



3. Next, navigate to your Google Apps domain's Admin console.
4. Select Security from the list of controls. If Security is not listed, select More controls from the gray bar at the bottom of the page, then select Security from that list of controls. If no controls are available, then be sure you are signed in as an administrator for the domain.
5. Select Show More, then Advanced Settings from the list of options.
6. Select Manage API Client Access in the Authentication section.
7. In the Client Name field, enter the Service Account's Client ID. You can find your Service Account's client ID in the Service Accounts page.

8. In the One or More API Scopes field, enter the list of scopes to which your application should be granted access. For example, if your application requires domain-wide access to the GMAIL API, enter: `https://mail.google.com/`.

Figure 18 Accessing the Google APIs Dashboard



9. Click Authorize.

NOTE Be sure to Enable GMAIL APIs by navigating to the Admin Console and clicking “ENABLE API” at the Dashboard under API Manager for the relevant project. Select GMAIL API and click Enable.

Using the Dashboard Views

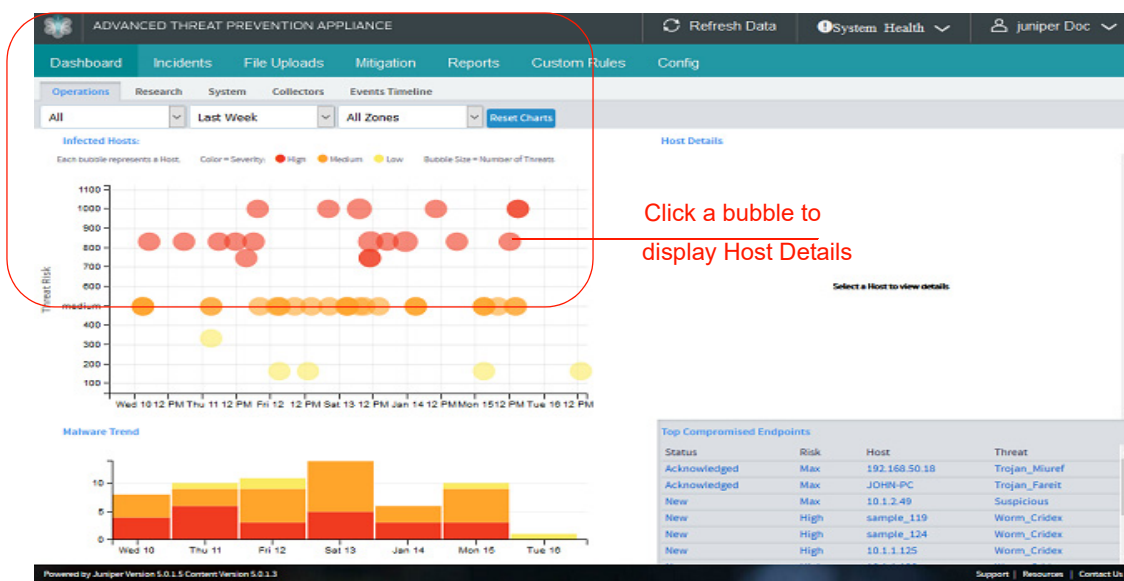
The Dashboard tab includes four interactive, graphical sub-tab Dashboards:

- The Operations Dashboard depicts malware statistics for infected hosts (bubble chart threat view) and trends, including host details triggers, Golden Image compromise (if any), and top compromised endpoints.
- The Research Dashboard shows top malware by name and total malware found, as well as malware progression for infections and downloads (both HTTP “north-south” and SMB “east-west” lateral) throughout the enterprise, with complete threat details per host IP address.
- The System Dashboard shows traffic and performance information, including analyzed protocol traffic , current total traffic, Core utilization, objects processed, average analysis time and malware object statistics.
- The Web and Email Collectors Dashboards show Juniper ATP Appliance Web and Email Traffic Collector trends as a measure of current total traffic, CPU usage, memory usage, objects analyzed, and overall threats. It also displays graphical per-Collector statistics plots, including Collector name, IP address, memory, CPU, Disk statistics, total current traffic, objects analyzed, threats, last threat seen, status (online/offline) and whether enabled/disabled.

- The Event Timeline Dashboard displays Advanced Threat Analytics (ATA) data that focuses on the day to day workflow of Tier 1 and Tier 2 security analysts who work on triaging and investigating malware incidents. A host and user timeline depicts the details and context for the events that occurred on a host or user. Within minutes, a Tier 1 analyst—who is not a detection expert—can easily determine the course of action necessary for the incident. With ATA, analysts have comprehensive information to determine the exact nature of the threat and whether or not it is an advanced threat that requires escalation to Tier 2 teams for mitigation. The Tier 2 analyst is freed up to focus on vetted advanced threats and to use the timeline view provided by ATA to perform detailed investigations on the host and user. This holistic view of information results in provisioning the response teams with rich data that includes the threat context, the host identity, and the end user identity—with no manual data aggregation and analysis required.

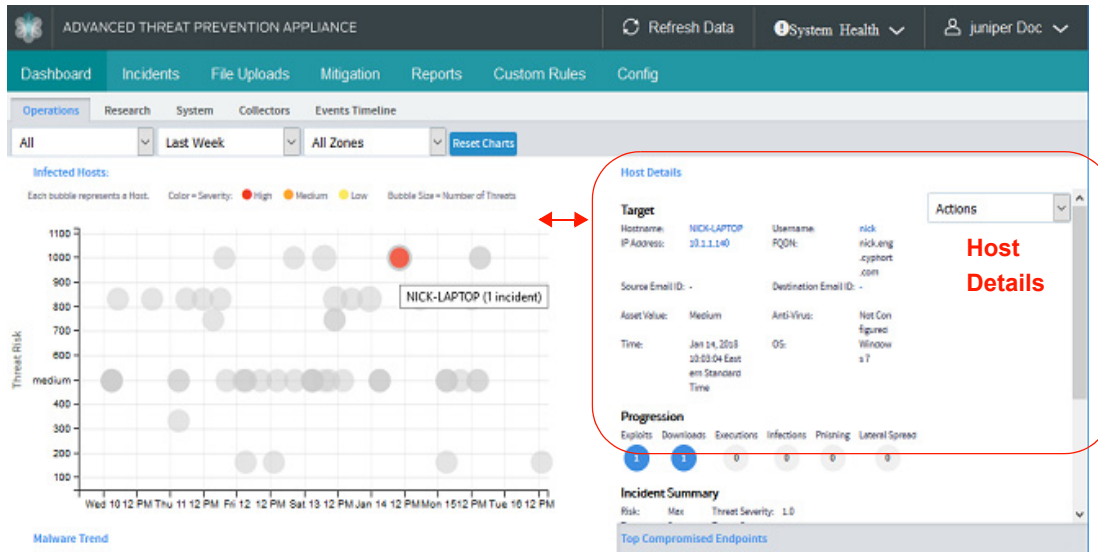
The Operations Dashboard provides a context-specific graphical Threat View that includes statistical depictions of threat events, metrics, trends and severity scoring. The Infected Hosts section reports the total infected hosts and total number of incidents that have been observed on the monitored network for the time period selected as a bubble graph where each bubble represents a threat, and the bubble size indicates a number of threats.

Figure 19 Juniper ATP Appliance Central Manager Web UI Operations Dashboard Tab



NOTE The Zone dropdown on the Operations Dashboard is displayed only when at least one zone is created. All Collectors are designated for the "Default Zone" initially but they must be formally assigned via the Central Manager Web UI Config>System Profiles>Web Collector pages.

Figure 20 Juniper ATP Appliance Central Manager Web UI Operations Dashboard Host Details



Use the Operations Dashboard Threat View interactivity to drill down into a selected host or malware incident's statistics.

- › Click a Bubble to view Host Details in the section to the right of the bubble graph.
- › Double click a bubble [host] to open the Incidents tab with a focus on the selected host.

NOTE To submit a malware file for analysis, use the Upload File option on the Incidents page.

- For more information, refer also to:
 - › Operations Dashboard on page 46,
 - › Research Dashboard on page 47,
 - › System Dashboard on page 49,
 - › Traffic Collectors Dashboard on page 50,
 - › Understanding Risk Severity on page 276,
 - › Viewing SMB Lateral Detections on page 283
 - › Graphical Kill Chain Progression Display on page 285

Interacting with Dashboard Views and Components

This section describes the Dashboard components for Dashboard tabs — the Operations, Research, System and Collectors Dashboard tabs, and describes how to interact with the various views and adjustable statistics and displays.

Table 2-1 Juniper ATP Appliance Dashboard Graphical Components

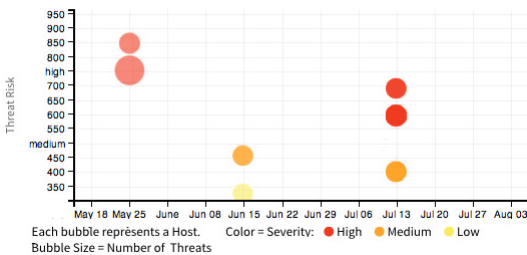
Operations Filter	Filter threat view results by selecting one of the available filters from the drop down menu: All New Only Ack'd & In Progress Complete	Make a selection from the dropdown menu.
Time Period (Operations Dashboard, Research Dashboard, System Dashboard, Collectors Dashboard, Events Timeline)	All Dashboard graphs are synchronized by the time period you select from the dropdown menu at the top of the table. Time period options include: Last 24 Hours Last Week Last Month Last 3 Months Last Year	Make a selection from the dropdown menu.
Reset Charts (both Malware Dashboard & System Dashboard)	Resets all the graphs on the Dashboard to their original state for the time period selected.	Mouse click
Infected Hosts (Operations Dashboard)	<p>This bubble chart is the heart of the Threat View and depicts all infected hosts for the given time period. One bubble represents one infected host.</p> <p>The x axis of the chart represents the time period.</p> <p>The y axis represents the determined severity of the infection.</p> <p>The color of the bubble represents the tiered severity of the malware found on the host along the following spectrum: High (Red), Medium (Orange), Low (Yellow)</p> <p>The size of the bubble represents the total number of threats found on the host.</p> <p>Infected Hosts:</p> 	<p>Mouse-Hover Over a Bubble “Host”</p> <ul style="list-style-type: none"> Shows infected host’s IP address and name, and the total number of malware found on that host in the format: “ip/name (x threats)” <p>Mouse-Click Over a Bubble “Host”</p> <ul style="list-style-type: none"> The bubble becomes highlighted and the Host Details data is displayed, including data for malware Target, Kill Chain, Incident Summary and Triggers. Also, the Malware Trend chart adjusts to show when the selected host was compromised. And, Top Compromised Endpoints Malware data is displayed. Double click a bubble to open the Incidents tab for further details and mitigation options.

Table 2-1 Juniper ATP Appliance Dashboard Graphical Components

<div>Host Details (Operations Dashboard)</div>	<div><p>When an individual bubble is selected in the Threat View bubble graph, the Host Details data is displayed for that host, including data for malware Target, Kill Chain Stage Progression, Incident Summary and Triggers.</p><p>The Kill Chain Progression contains more interactive data.</p></div>	<div><p>Mouse click:</p><ul style="list-style-type: none">Click the highlighted blue result in the Kill Chain Stage Progression to display more information:</div> <div><div>Progression</div><div><div>Exploits</div><div>Downloads</div><div>Executions</div><div>Infections</div><div>Phishing</div></div><div><div>1</div><div>4</div><div>0</div><div>0</div><div>0</div></div></div> <div><p>When a Kill Chain Progression bubble is clicked, the Incidents page is opened displaying the data for the specific Exploit(s), Download(s), Execution(s), Infection(s) and/or Phishing.</p></div>
<div>Malware Trend (Operations Dashboard)</div>	<div><p>Shows the malware trend for any give malware with given time frame.</p><div><div>Trend</div><div><div>High</div><div>Med</div><div>Low</div></div><div><div>30</div><div>20</div><div>10</div><div>0</div></div><div><div>May 18</div><div>May 25</div><div>Jun 01</div><div>Jun 08</div><div>Jun 15</div><div>Jun 22</div><div>Jun 29</div><div>Jul 06</div><div>Jul 13</div><div>Jul 20</div><div>Jul 27</div><div>Aug 03</div><div>Aug 10</div></div></div></div>	<div><p>Select a bubble in the Threat View bubble graph to adjust Trend Malware timeline.</p></div>
<div>Total Malware Found (Research Dashboard)</div>	<div><p>A pie chart that shows malware severity percentages in High (Red), Medium (Orange) and Low (Yellow)</p><div><div>Total Malware Found</div><div><div>High</div><div>Low</div><div>Med</div></div><div><div>7</div></div></div></div>	<div><p>No interactivity</p></div>
<div>Top Malware Countries (Research Dashboard)</div>	<div><p>A geographical graph that displays the incidence of currently-detected malware across the globe.</p><div><div>Top Malware Countries</div><div><div>Malware Count:</div><div>US: 29</div><div>CN: 2</div><div>DE: 2</div><div>RU: 2</div><div>EU: 1</div><div>VG: 1</div><div>GB: 1</div></div></div></div>	<div><p>Opens Incidents Details page</p></div>

Table 2-1 Juniper ATP Appliance Dashboard Graphical Components

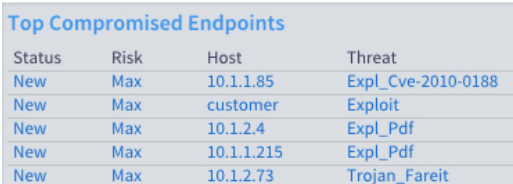
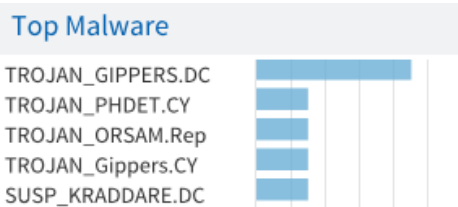

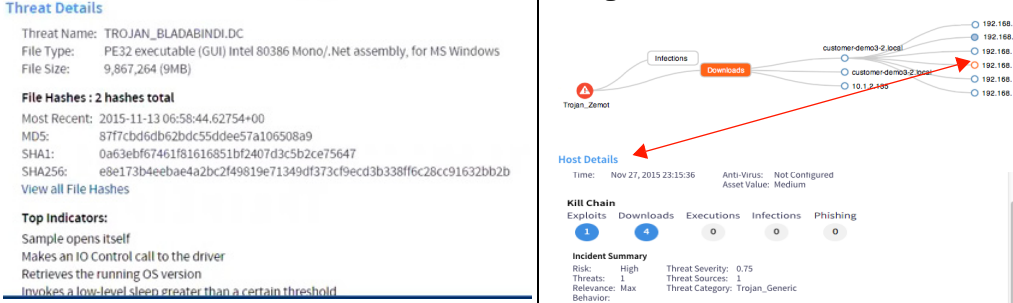
<p>Top Compromised Endpoints (Operations Dashboard)</p>	<p>Displays Status, Risk, Host and Threat per compromised endpoint represented..</p> 	<p>No interactivity</p>
<p>Top Malware (Research Dashboard)</p>	<p>Lists the top set of malware incidents by malware name for the selected time period. The x axis represents the number of infections; the y axis is the malware name.</p> 	<p>Mouse Click:</p> <p>Highlight a malware name in the Top Malware graph to see the Threat Progression graph display for that malware per endpoint host. The Threat Progression includes:</p> <ul style="list-style-type: none"> • Infections • Downloads
<p>Threat Progression (Research Dashboard)</p>	<p>Displays an interactive map of Infections and Downloads per malware selection.</p>  <p>loads to consecutive hosts across the enterprise is shown in the example below.</p>	<p>Mouse Clicks:</p> <ul style="list-style-type: none"> • Click Infections to display infected endpoint progressions. • Click Downloads to display endpoints (indicated by IP address) from which downloads of the selected malware occurred. • Click an endpoint IP address to display Host Details for that endpoint. The circle bullet for the selected endpoint turns orange when clicked.
<p>Threat Details (Research Dashboard)</p>	<p>Displays generalized threat details for the currently selected malware. But, when an endpoint is selected from the Threat Progression map, the displays adjusts to provide Host Details.</p> 	<p>Mouse click:</p> <p>Click an endpoint IP address to display Host Details for that endpoint. The circle bullet for the selected endpoint turns orange when clicked.</p>

Table 2-1 Juniper ATP Appliance Dashboard Graphical Components

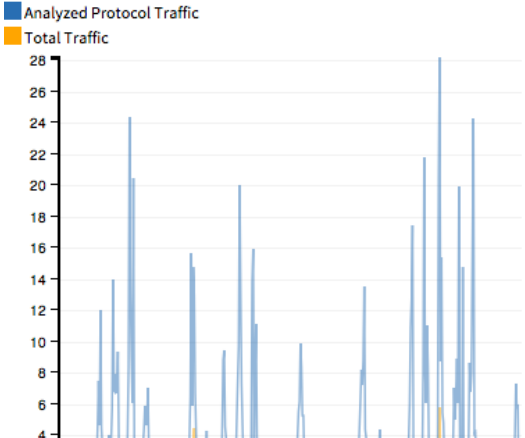
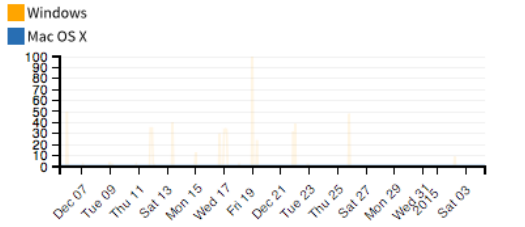
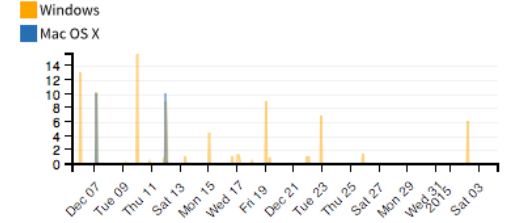
Traffic (System Dashboard)	Displays the total network traffic relative to the Analyzed Protocol Traffic processed in Kbps within the selected time period. The x axis represents the time period in months; the y axis indicates Kbps.	Mouse Hover: Perform a mouse hover over any part of the chart; the mouse pointer will turn into a crosshair: drag the mouse inside the chart to change the interval (x axis) for each of the three components.
Core Utilization (%) (System Dashboard)	<p>Traffic (Mbps)</p>  <p>Core Utilization (%)</p> 	Mouse Hover: Perform a mouse hover over any part of the chart; the mouse pointer will turn into a crosshair: drag the mouse inside the chart to change the interval (x axis) for each of the three components.
Average Analysis Time (Minutes) (System Dashboard)	<p>Average Analysis Time (Minutes)</p> 	Mouse Hover: Perform a mouse hover over any part of the chart; the mouse pointer will turn into a crosshair: drag the mouse inside the chart to change the interval (x axis) for each of the three components.

Table 2-1 Juniper ATP Appliance Dashboard Graphical Components

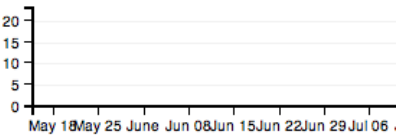
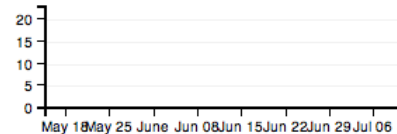
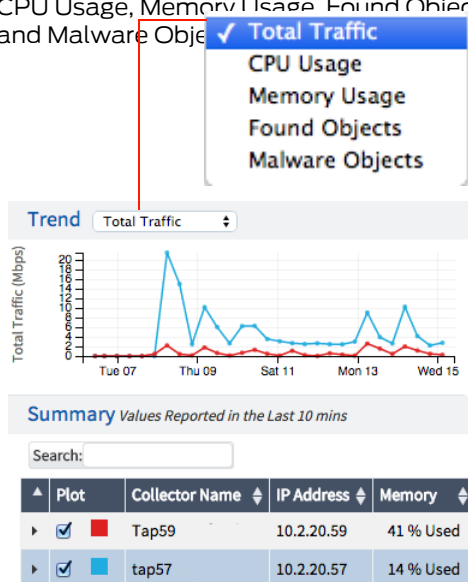
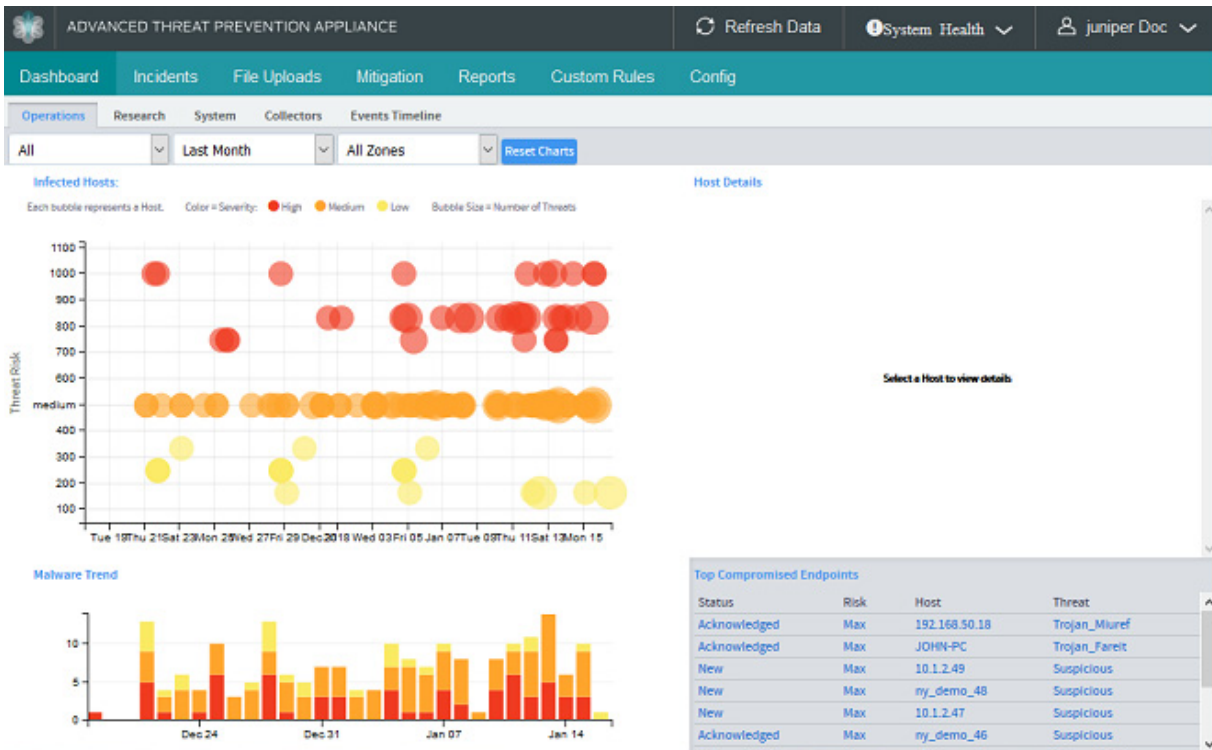
<p>Objects Processed (System Dashboard)</p>	<p>Displays the network objects processed within the selected time period.</p> <p>The x axis represents the time period in months; the y axis indicates number of objects.</p> <p>Objects Processed</p> 	<p>Mouse Hover:</p> <p>Perform a mouse hover over any part of the chart; the mouse pointer will turn into a crosshair: drag the mouse inside the chart to change the interval (x axis) for each of the three components.</p>
<p>Malware Objects (System Dashboard)</p>	<p>Displays the malware objects processed within the selected time period.</p> <p>The x axis represents the time period in months; the y axis indicates number of objects.</p> <p>Malware Objects</p> 	<p>Mouse Hover:</p> <p>Perform a mouse hover over any part of the chart; the mouse pointer will turn into a crosshair: drag the mouse inside the chart to change the interval (x axis) for each of the three components.</p>

Table 2-1 Juniper ATP Appliance Dashboard Graphical Components

<div>Trend</div> <div>(Collectors Dashboard)</div>	<div>Displays stats for Collector(s) activity and trends.</div> <div>Display options are selected from the Trend dropdown menu and include Total Traffic, CPU Usage, Memory Usage, Found Objects and Malware Objects</div> <div></div> <div><table><thead><tr><th>Plot</th><th>Collector Name</th><th>IP Address</th><th>Memory</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>Tap59</td><td>10.2.20.59</td><td>41 % Used</td></tr><tr><td><input checked="" type="checkbox"/></td><td>tap57</td><td>10.2.20.57</td><td>14 % Used</td></tr></tbody></table></div>	Plot	Collector Name	IP Address	Memory	<input checked="" type="checkbox"/>	Tap59	10.2.20.59	41 % Used	<input checked="" type="checkbox"/>	tap57	10.2.20.57	14 % Used	<div>Select the Collectors to track from the Summary table below the plot.</div> <div>Values are updated every 10 minutes for each Collector.</div> <div>Click the Plot column(s) checkbox to plot the graphical information for selected Collectors.</div>
Plot	Collector Name	IP Address	Memory											
<input checked="" type="checkbox"/>	Tap59	10.2.20.59	41 % Used											
<input checked="" type="checkbox"/>	tap57	10.2.20.57	14 % Used											
<div>Vendor</div> <div>(Events Timeline Dashboard)</div>	<div>Select a Vendor from your security infrastructure and view all correlated events for a specified Endpoint IP, Hostname, Username or Email:</div>													

Resetting the Threat View

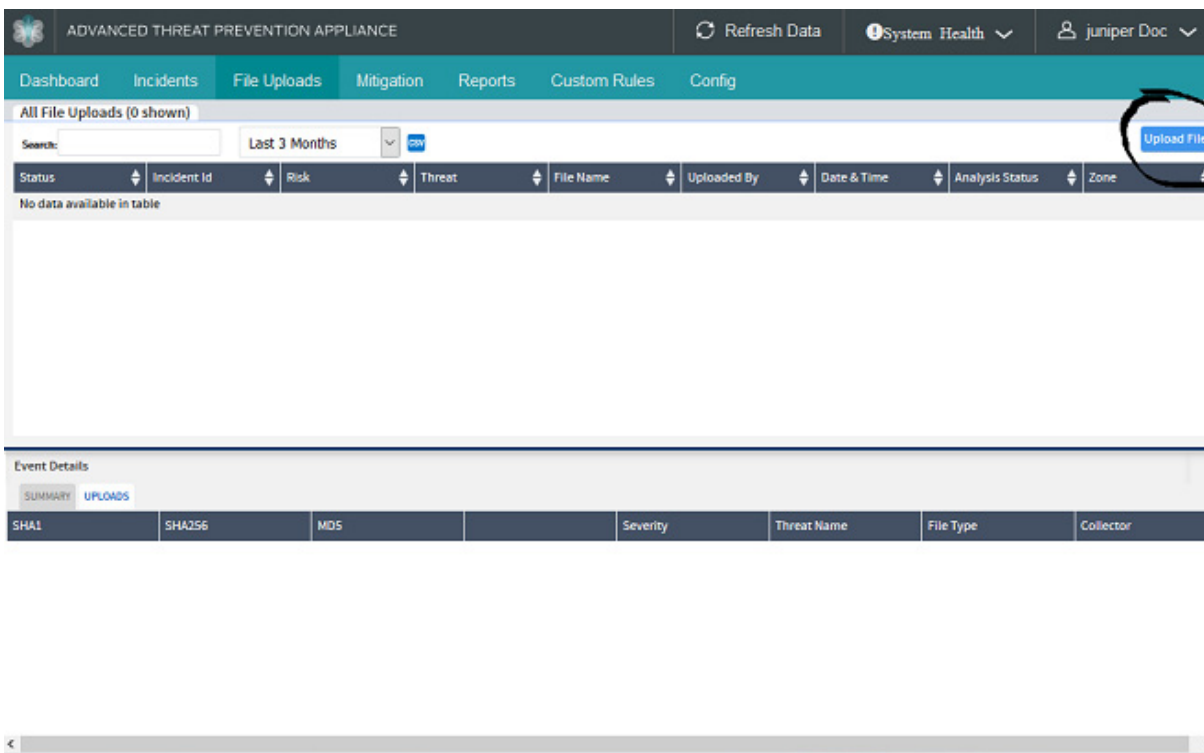
Reset the Dashboard to its original all-hosts, all-threats state by clicking Reset Charts.



Submitting a Malware File for Analysis

The File Uploads tab provides a mechanism for uploading malware files for analysis. The malware analysis results are generated and returned for display in the Details Uploads table, which also includes results for all files uploaded for malware analysis via the Juniper ATP Appliance API.

Figure 3 Upload File Button (Upper Right) and Malware Analysis Results on File Uploads Tab



The File Uploads tab presents all uploaded files and analysis results (malicious and benign).

An enhanced file uploads API accepts additional meta-data for third party integrations such as Carbon Black to provide seamless integration with incidents.

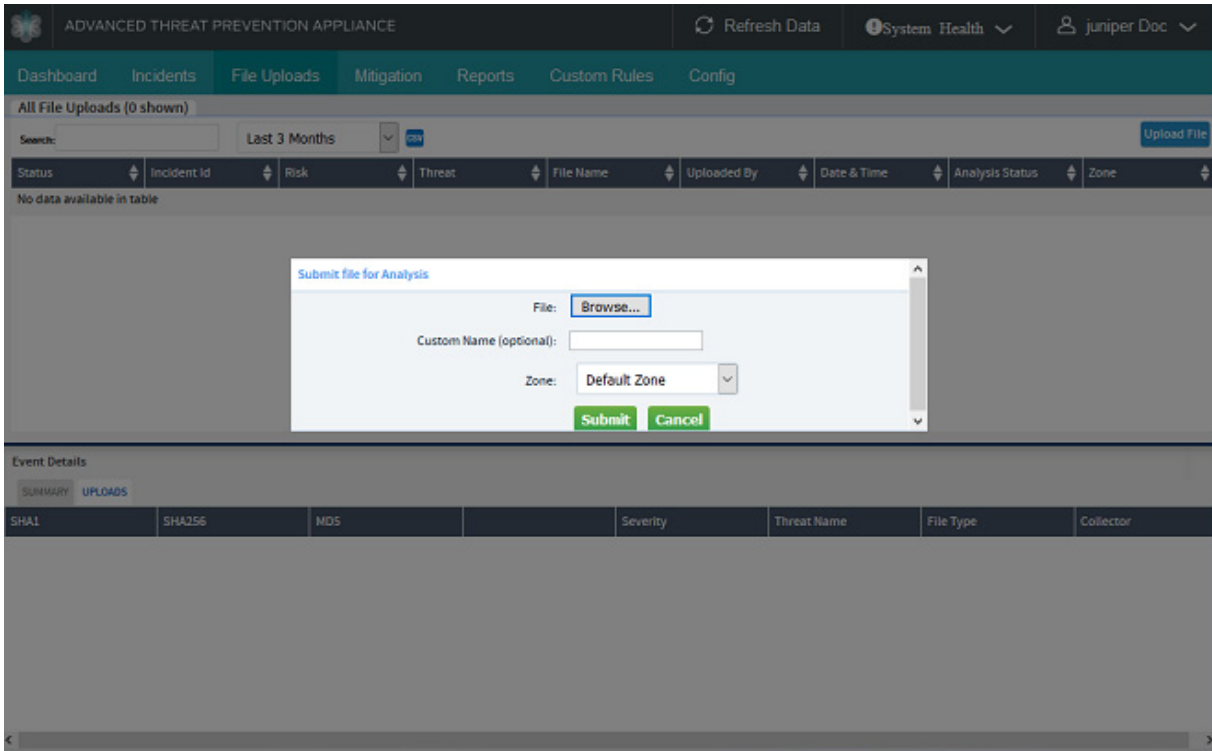
Refer to the Juniper ATP Appliance HTTP API Guide for more information about the File Upload API.

When metadata is available and uploaded with the file to be analyzed, data points such as Target IP Address, Target OS, Source Address, and so on, then this metadata can be used in the analysis profile to create a true incident. In this case, such a file submission can instantiate a Download type of incident that contains all of the information available if the Traffic Collector had inspected the download directly.

To Upload a File for Analysis

- Click the File Uploads tab, and in the “Submit file for analysis” window, select the file to upload for analysis and click the Submit file button.

Figure 4 Submitting a File for Malware Analysis from the Incidents Tab



Upon file submission, a SHA1 is displayed.

The Upload File feature calls the “file_submit” API and then, following analysis, displays the results returned from the API in Central Manager Web UI File Uploads tab. The results are also displayed in the Incidents page table with the Kill Chain Progression designation: UP along with the incident sha1sum and filename.

NOTE You may also use the Juniper ATP Appliance HTTP API directly to submit files for analysis and get results and incident details via the API JSON outputs. Refer to the Juniper ATP Appliance HTTP API Guide for more information.

TIP The Juniper ATP Appliance limits the upload to the actual processing limit and throws an error if the file is greater than 16MB.

Regardless of whether a file is submitted to the Core for malware analysis from the HTTP API or via the Central Manager File Uploads page, the analysis results are always displayed on the File Uploads page.

Configuring Juniper ATP Appliance for Integrated Deployment

Juniper ATP Appliance is designed to integrate with and leverage your existing enterprise security infrastructure. Integrating Juniper ATP Appliance configurations with Firewalls, Proxies, Secure Web Gateways, and other services and devices, requires use of the Central Manager Web UI Config tab options as well as access to the other device or service’s Web UI or CLI to complete the integration.

- Refer to the chapter on Configuring Distributed Defense for all Juniper ATP Appliance-side Web UI-based configuration procedures.

- To integrate Enterprise network segments with Juniper ATP Appliance malware analysis and defense technologies, refer to [Configuring Firewall Auto-Mitigation on page 147](#).
- For Anti-Virus static analysis integration, refer to [Configuring Anti-Virus Integration on page 164](#).
- To configure data theft custom rules, refer to [Configuring Anti-Virus Integration on page 164](#).
- For PAN Firewall Auto-Mitigation integration, refer to [Configuring Firewall Auto-Mitigation on page 147](#).
- For Juniper SRX Firewall integration, refer to [Defining a Zone-Defined SRX Configuration at the Juniper ATP Appliance Web UI on page 154](#).
- For Cisco ASA Firewall Auto-Mitigation integration, refer to [Configuring Firewall Auto-Mitigation on page 147](#).
- For Check Point Firewall Auto-Mitigation integration, refer to [Configuring Firewall Auto-Mitigation on page 147](#).
- For Proxy integration, refer to [Configuring BlueCoat ProxySG Integration on page 167](#).
- For Carbon Black endpoint mitigation integration, refer to [Configuring Carbon Black Response Endpoint Integration on page 166](#).
- For Crowdstrike endpoint integration, refer to [Configuring Crowdstrike Endpoint Integration on page 167](#).

Deploying Juniper ATP Appliance SaaS Virtual Collectors

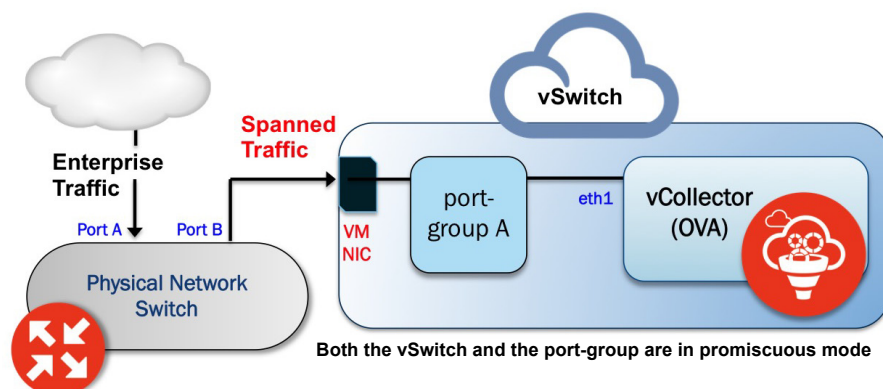
Juniper ATP Appliance's extensible deployment options include a Virtual Collector (vCollector) product: an Open Virtual Appliance, or OVA, that runs in virtual machines. Specifically, a Juniper ATP Appliance OVA-packaged image is available for VMware Hypervisor for vSphere 5.1 and 5.5 via thin provisioning. This includes a 50 Mbps, 100 Mbps, 500 Mbps, 1.0 Gbps and 2.5 Gbps Virtual Collector model to Juniper ATP Appliance product support and services.

See Also: [Deploying SaaS Virtual Cores as OVAs on page 91](#).

An OVF package consists of several files contained in a single directory with an OVF descriptor file that describes the Juniper ATP Appliance virtual machine template and package: metadata for the OVF package, and a Juniper ATP Appliance software image. The directory is distributed as an OVA package (a tar archive file with the OVF directory inside).

RECOMMENDATION: Juniper advises use of a dedicated physical NIC assigned to the vCollector for best collection results.

Figure 5 Juniper ATP Appliance vCollector Architecture



Virtual Collector Deployment Options

Two types of vCollector deployments are supported for a network switch SPAN/TAP:

1. Traffic that is spanned to a vCollector from a physical switch. In this case, traffic is spanned from portA to portB. ESXi containing the Juniper ATP Appliance vCollector OVA is connected to portB. This deployment scenario is shown in the figure above.
2. Traffic from a virtual machine that is on the same vSwitch as the vCollector. In this deployment scenario, because the vSwitch containing the vCollector is in promiscuous mode, by default all port-groups created will also be in promiscuous mode. Therefore, 2 port groups are recommended wherein port-groupA (vCollector) in promiscuous mode is associated with the vCollector, and port-groupB (vTraffic) represents traffic that is not in promiscuous mode.

NOTE Traffic from a virtual machine that is not on the same vSwitch as the vCollector is not supported. Also, a dedicated NIC adapter is required for the vCollector deployment; attach the NIC to a virtual switch in promiscuous mode (to collect all traffic). If a vSwitch is in promiscuous mode, by default all port-groups are put in promiscuous mode and that means other regular VMs are also receiving unnecessary traffic. A workaround for that is to create a different port-group for the other VMs and configure without promiscuous mode.

TIP There are two available options to deploying a Virtual Collector (regular as well as small form factor Collector): (1) Use the OVA installation method using vCenter; (2) Use OVF + VMDK without vCenter by directly installing on ESXi. (The .ovf and .vmdk are bundled into a .tar file that you download and expand.) There is no wizard available for deploying the vCollector using the second method; configure the collector from the CLI.

Provisioning Requirements

The following table details resource and hardware provisioning required for an OVA vCollector deployment.

Table 2-1 vCollector Provisioning Requirements

VM vCenter Version Support	Recommended vCollector ESXi Hardware	vCollector CPUs	vCollector Memory
VM vCenter Server Version: 5.5.0 vSphere Client Version: 5.5.0 ESXi version: 5.5.0 and 5.5.1	Processor speed 2.3-3.3 GHz As many physical CORES as virtual CPUs Hyperthreading: either enable or disable	CPU Reservation: Default CPU Limit: Unlimited Hyperthreaded Core Sharing Mode: None (if Hyperthreading is enabled on the ESXi)	Memory Reservation: Default Memory Limit: Unlimited

NOTE VDS and DVS are not supported in this release.

OVA vCollector Sizing Options

The sizing options available for a vCollector deployment are provided below.

Table 2-2 Sizing options available for a vCollector deployment

Model	Performance	Number of vCPUs	Memory	Disk Storage
vC-v50M	50 Mbps	1	1.5 GB	16 GB
vC-v100M	100 Mbps	2	4 GB	16 GB
vC-v500M	500 Mbps	4	16 GB	512 GB
vC-v1G	1 Gbps	8	32 GB	512 GB
vC-v2.5G	2.5 Gbps	24	64 GB	512 GB

NOTE It is important to reserve CPU and memory for any virtual deployment. Refer to the Juniper ATP Appliance Traffic Collector Quick Start Guide for OVA Deployment vSwitch Setup instructions and information about installing the Juniper ATP Appliance OVA to a VM.

After installing the OVA vCollector, follow instruction in the Quick Start Guide for configuring the Web or Email vCollector using the Juniper ATP Appliance CLI and configuration wizard.

TIP On the first boot of a virtual core (either AMI or OVA) with two disks configured, the appliance takes time to set up the second disk to be used. During this process, the system is not yet ready for use. This process may take up to 10 minutes.

NOTE Some of the configuration process is optional and can be skipped because several settings are addressed during OVA deployment of the VM vSwitch.

Deploying SaaS Virtual Cores as OVAs

Juniper ATP Appliance's extensible deployment options now include a Virtual Core (vCore) detection engine product, as an Open Virtual Appliance, or OVA, that runs in virtual machines. Specifically, a Juniper ATP Appliance OVA-packaged image is available for VMware Hypervisor for vSphere 5.1 and 5.5 via thin provisioning. This release supports a 500 Mbps and a 1.0 Gbps Virtual Core model to Juniper ATP Appliance product support and services. An OVF package consists of several files contained in a single directory with an OVF descriptor file that describes the Juniper ATP Appliance virtual machine template and package: metadata for the OVF package, and a Juniper ATP Appliance software image. The directory is distributed as an OVA package (a tar archive file with the OVF directory inside).

NOTE It is important to reserve CPU and memory for any virtual deployment. When initially deploying an OVA, the smaller size OVA is configured by default. Use the sizing guide to increase CPUs, memory and so on to the larger size as desired. Sizing information is provided on the previous page.

TIP See the Juniper ATP Appliance Traffic Collector Quick Start Guide for information about the small footprint virtual collector option.

To install the Juniper ATP Appliance OVA to a VM

1. Download the Juniper ATP Appliance OVA file from the location specified by your Juniper support representative to a desktop system that can access VMware vCenter. See TIP at end of this section to optionally avoid the use of vCenter.
2. Connect to vCenter and click on File>Deploy OVF Template.
3. Browse the Downloads directory and select the OVA file, then click Next to view the OVF Template Details page.
4. Click Next to display and review the End User License Agreement page.
5. Accept the EULA and click Next to view the Name and Location page.
6. The default name for the Virtual Core is Juniper ATP Appliance Virtual Core Appliance. If desired, enter a new name for the Virtual Core.
7. Choose the Data Center on which the vCore will be deployed, then click Next to view the Host/Cluster page.
8. Choose the host/cluster on which the vCore will reside, then click Next to view the Storage page.
9. Choose the destination file storage for the vCore virtual machine files, then click Next to view the Disk Format page. The default is THIN PROVISION LAZY ZEROED which requires 512GB of free space on the storage device. Using Thin disk provisioning to initially save on disk space is also supported. Click Next to view the Network Mapping page.
10. Set up the vCore interface:
 - Management (Administrative): This interface is used for management and to communicate with the Juniper ATP Appliance Traffic Collectors. Assign the destination network to the port-group that has connectivity to the CM Management Network IP Address.
 - Click Next to view the Juniper ATP Appliance Properties page.
11. IP Allocation Policy can be configured for DHCP or Static addressing-- Juniper recommends using STATIC addressing. For DHCP instructions, skip to Step 12. For IP Allocation Policy as Static, perform the following assignments:
 - IP Address: Assign the Management Network IP Address for the vCore.
 - Netmask: Assign the netmask for the vCore.
 - Gateway: Assign the gateway for the vCore.
 - DNS Address 1: Assign the primary DNS address for the vCore.
 - DNS Address 2: Assign the secondary DNS address for the vCore.
12. Enter the Search Domain and Hostname for the vCore.
13. Complete the Juniper ATP Appliance vCore Settings:

New Juniper ATP Appliance CLI Admin Password: this is the password for accessing the vCore from the CLI.

14. Complete the Juniper ATP Appliance vCore Settings:
 - New Juniper ATP Appliance CLI Admin Password: this is the password for accessing the vCore from the CLI.
 - Juniper ATP Appliance Central Manager IP Address: If the virtual core is stand-alone (no clustering enabled) or Primary (clustering is enabled), the IP address is 127.0.0.1. If the virtual core is a Secondary, the Central Manager IP address will be the IP address of the Primary.
 - Juniper ATP Appliance Device Name: Enter a unique device name for the vCore.
 - Juniper ATP Appliance Device Description: Enter a description for the vCore.
 - Juniper ATP Appliance Device Key Passphrase: Enter the passphrase for the vCore; it should be identical to the passphrase configured in the Central Manager for the Core/CM. Click Next to view the Ready to Complete page.

15. Do not check the Power-On After Deployment option because you must first (next) modify the CPU and Memory requirements (depending on the vCore model--either 500Mbps, or 1Gbps; refer to [OVA vCollector Sizing Options on page 91](#) for sizing information).
16. To configure the number of vCPUs and memory:
 - A. Power off the vCore.
 - B. Right click on the vCore -> Edit Settings
 - C. Select Memory in the hardware tab. Enter the required memory in the Memory Size combination box on the right.
 - D. Select CPU in the hardware tab. Enter the required number of virtual CPUs combination box on the right. Click OK to set.
17. To configure CPU and memory reservation:
 - A. For CPU reservation: Right click on vCore-> Edit settings:
 - B. Select Resources tab, then select CPU.
 - C. Under Reservation, specify the guaranteed CPU allocation for the VM. It can be calculated based on Number of vCPUs *processor speed.
 - D. For Memory Reservation: Right click on vCore -> Edit settings.
 - E. In the Resources tab, select Memory.
 - F. Under Reservation, specify the amount of Memory to reserve for the VM. It should be the same as the memory specified by the Sizing guide.
18. If Hyperthreading is enabled, perform the following selections:
 - A. Right click on the vCore -> Edit settings.
 - B. In the Resources tab, select HT Sharing: None for Advanced CPU.
19. Power on the Virtual Core (vCore). NOTE: For future reference, whitelist rules rely on normal service shutdown to be backed up. Powering off a VM or Virtual Core directly will lose the current whitelist state because the rules cannot be saved in that case.

Log into the CLI and use the server mode "show uuid" command to obtain the UUID; send to Juniper ATP Appliance to receive your license.

When an OVA is cloned to create another virtual Secondary Core, the value for column "id" in the Central Manager Appliance table is the same by default. Admins must reset the UUID to make it unique. A new Virtual Core CLI command "set id" is available to reset the UUID on a cloned Virtual Core from the CLI's core mode. Refer to the Juniper ATP Appliance CLI Command Reference to review the new Core mode "set id" and "show id" commands.

Upgrading of software and security content is automatic when upgrades are configured from the Central Manager Web UI Config>System Settings>System Settings page.

- To enable automatic upgrades, check the "Software Update Enabled" and/or "Content Update Enabled" options on the System Settings page.

All automatic updates from all Juniper ATP Appliance components are coordinated and implemented by the Juniper ATP Appliance Core. Ongoing updates take place on a regular schedule:

- The Core software and content update (if enabled) checks for available updates every 30 minutes and pushes new files to the Collectors and/or Secondary Cores.
- The Core detonation engine image upgrade check occurs daily at midnight.

To upgrade a Mac OS X Detection Engine running on a Mac Mini, refer to the Juniper ATP Appliance CLI Command Reference [use the **upgrade** command from the Mac Mini CLI].

A successful upgrade progression:

Ready to upgrade. The process can take up to 30 minutes and should not be

```
interrupted. Do you want to continue (Yes/No)? yes
Running release upgrade on the base system...
98%
Waiting for the kernel upgrade...
Kernel upgrade is done.
Release upgrade is done. Please reboot the machine for all the updated changes.
```

Upgrading without Whitelisting

- Juniper ATP Appliance continues to reduce its operational footprint and no longer requires an extensive set of whitelist external IP addresses for upgrades, telemetry, content updates and other services.
- Firewall ports opened previously for specific services can be closed after a Release upgrade is complete.
- Note that most modern firewalls support domain whitelists.
- Customers can optionally allow just outbound access to the Core/CM device* (not collectors) on HTTPS (port 443); no domain whitelist is required in this case.
- *Juniper ATP Appliance has always recommended allowing un-fettered outbound communications for the Core/CM appliance (or All-in-One) in order to allow for kill-chain correlation in sandbox detonations.
- Customers concerned about a comprehensive whitelist on port 443 can restrict the whitelist to just Amazon AWS and S3 CIDRs - but note that this is still a quite large range of IP addresses.

Enabling Juniper ATP Appliance Support

SSH remote access to Juniper ATP Appliances for troubleshooting is available via JATP Support— the only user account available for remote SSH login for diagnosing and troubleshooting product issues, if necessary.

NOTE Always use the latest version of Putty for SSH operations, if using Putty as an SSH client.

The Juniper ATPS support account can be disabled by customers (either through the Central Manager Web UI Config>System Settings>System Settings page, or via the CLI).

NOTE A Juniper ATP Support account is created only when a product license key is uploaded from the CM Web UI during a product installation.

After an upgrade, an existing Juniper ATP Support account will be maintained; no user action is necessary.

Note that if you disable an enabled Juniper ATP Support account, the change will automatically propagate to connected Collectors and Secondary Core Mac OSX Detection Engines.

NOTE When a system is installed from AMI, OVA or ISO, the support password is not enabled by default, but rather is set during licensing, then enabled manually. When installing Juniper ATP Appliance AMI, OVA or ISO software, first upload the license and then enable **support** and **support localmode** access from the CLI.

TIP Adding a license manually does not enable support.

Managing your Support Account

- To enable or disable the Support account from the CM Web UI, refer to [Configuring System Settings on page 165](#) where you can select the checkbox “Enable Junper ATP Appliance Support Account”, then click Submit.
- To enable the Support account from the CLI: log in to the CLI, enter server mode, then use the **set support** command. To check Support status from the CLI, use the **show support** command.

- Changes to a JATP Support account password can be handled in the following ways:
 - › A support password can be reset temporarily to a default password from the CLI. It will be reset back to the customer-based password within 5 minutes
 - › The JATP Support account password can also be changed by installing a new license key. The password change will take effect on the connected Traffic Collectors and Secondary Core Mac OSX detection engines as well.

NOTE Any JATP Support changes, such as enable/ disable or password reset (even those triggered by a newly installed license key) may take at most 5 minutes to take effect on the Collector/ Mac OSX Secondary Core.

Configuring an Alternate Analysis Engine Interface

When network objects are detonated during detection procedures in Core analysis engines, some of them generate network traffic to malicious CnC servers. An optional eth2 interface can be configured for a primary and/or secondary Core (Mac Mini) or a Virtual Core in order to transmit CnC-specific generated traffic via a different network as an alternate exhaust option.

NOTE Review all deployment prerequisites in the Juniper ATP Appliance Quick Start Guide for your SSH Honeypot Requirements

The SSH Honeypot feature detects any attempts to connect to an SSH server in the enterprise network.

A honeypot deployed within a customer enterprise network can be used to detect network activity generated by malware attempting to infect or attack other machines in a local area network. Attempted SSH login honeypots are used to supplement detection of lateral spread. Multiple honeypots can be deployed on a customer Traffic Collector from which event information is sent to the Juniper ATP Appliance Core for processing. Customers can place honeypots on any local network they desire.

A malicious actor attempting to perform brute force SSH entry, or execute targeted SSH access to a “root” account, will also be detected by the Juniper ATP Appliance SSH Honeypot feature.

The Juniper ATP Appliance Central Manager Web UI Incidents tab includes results for the SSH Honeypot feature.

Results of SSH Honeypot detections are displayed on the Central Manager Web UI Incidents page, and included in generated Reports. Data sent to the Juniper ATP Appliance GSS for honeypot detection events include “Threat Target” and a detailing of all attempted “SSH sessions” (including username and password) with timestamps.

Requirements for setting up SSH honeypot lateral detection:

- Be sure the honeypot Collector has a minimum of four interfaces (eth0, eth1, eth2, eth3 [honeypot])
- Place an SSH server on a network
- Log any attempts to connect to the server
- Enable the SSH honeypot feature from the Juniper ATP Appliance CLI
- If enabling honeypot functionality during an UPGRADE of Juniper ATP Appliance software, the upgrade must be performed twice to ensure that the virtualization emulator is fully updated to the correct version.

NOTE SSH Honeypot detections are not relevant for TAP mode Collector deployments.

To configure and monitor SSH honeypot incidents:

- Refer to the Juniper ATP Appliance CLI Command Reference for information about configuring SSH Honeypot.
- Refer to the Juniper ATP Appliance Traffic Collector Quick Start Guide for information about using the eth3 port for all outbound Collector traffic.

CHAPTER 3

Configuring Distributed Defense

The following topics are in this chapter:

- Setting Notifications
- Configuring Alert Settings
- Configuring System Profiles
- Configuring MSSP Multi-Tenancy Zones
- Configuring System Settings
- Managing Certificates
- Configuring GSS Settings
- Configuring Web Collectors
- Configuring Email Collectors
- Configuring Mac OSX or Windows SecondaryCores
- Configuring Golden Image VMs
- Setting the Juniper ATP Appliance License Key
- Configuring Backup and Restore Options
- Testing Malware Detection Capabilities
- Configuring Environmental Settings
- Configuring Email Mitigation Settings
- Configuring Firewall Auto-Mitigation
- Configuring Enterprise Network Asset Values
- Configuring Anti-Virus Integration
- Configuring Endpoint Integration: Crowdstrike and Carbon Black Response
- Configuring BlueCoat ProxySG Integration
- Configuring Whitelist Rules
- Configuring YARA Rules
- Configuring Identity
- Configuring Active Directory
- Part 1 – Obtaining a Domain Component Name for a Domain Controller

- [Part 2 - Configuring an Active Directory Domain Controller from the Web UI](#)
- [Configuring Custom SNORT Rules](#)
- [Setting Anti-SIEM Identity Configurations](#)
- [Carbon Black Response - Splunk Integration](#)
- [Configuring Anti-SIEM Splunk Ingestion](#)
- [Integrating Anti-Siem External Event Collectors](#)

NOTE To use the command-line interface to configure and manage the Juniper ATP Appliance, refer to the [Juniper ATP Appliance CLI Command Reference Guide](#).

Setting Notifications

Use the Config>Notifications page to set or edit Alert Settings or SIEM Settings.

Configuring Alert Settings

Configure Alert Settings in order to have Events or System Audit notifications sent to designated email recipients as alerts.

Figure 3 Setting Alert Notifications

Description	Delivery	Actions
Events, HTML, All malware	12:00 am on mon,tue,wed,thu,fri,sat,sun	Display Delete Edit

To create a new alert notification:

1. Navigate to the Config>Notifications page and select Alert Settings from the left panel menu.
2. Click Create New Notification to set up a new Events or System Audit or System Health alert.
3. Select from the available options (see descriptions further below) and click Add to complete the configuration and add the new alert configuration to the Current Notifications list.

To display, delete or edit an existing alert configuration:

1. To display, delete or edit an existing alert notification configuration, click Display, Delete or Edit in the Current Notification table for a selected alert.
2. Edit, modify or delete the current settings and fields as desired, then click Save.
 - A sample of an Alert report Display is provided below:

Alert notification configuration options

Descriptions of Events, System Audit and System Health alert settings are provided in the following tables..

Table 3-1 Events Settings

Type	Select the type of alert notification to be configured: Event System Audit System Health
Max Num Results	For Event-based alerts, enter the number of rows of results to include in the alert notification [default is 25].
Format	Select HTML or PDF as the notification output format.
Malware Severity	To filter the report notification by malware severity results, choose either: All Malware Critical, High or Med Critical or High
Generate On	Select Trigger or By Schedule to set the method by which an alert is generated. If "By Schedule" is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.

Table 3-1 System Health Settings

Type	Note: Selecting the System Health event type will add email alerts for the following four event instances: <ul style="list-style-type: none"> › Lost connection to another appliance for more than 10 minutes (for example: if the Central Manager loses connection to a Web Collector or Mac OSX Secondary Core) › Low network traffic threshold configured via the CLI. By default, this alert is not generated unless enabled via the CLI. › Network Interface Down. on Engine went down
Overall Health Processing Delay	For System Health alerts, select either overall health metrics alerting or processing-delays-specific alerting.
Format	Select HTML or PDF as the notification output format.
Generate On	Select Trigger or By Schedule to set the method by which an alert is generated. If "By Schedule" is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.
Recipient's Email	Enter the email address(es) of the alert notification recipient(s).

Table 3-2 Example Alert Configurations: System Audit Alert Settings

Type	Select the type of alert notification to be configured: System Audit
Event Type	Select the event type(s) to include in the alert notification: Login/Logout Failed logins Add/Update Users Mitigation Whitelist System Settings Restarts Remote Support (for ATA analytics) Alerts are resent every two hours if the condition persists. An example of the alert text in generated email alerts: Tue, 05 Aug 2014 21:45:18 -0700 n/a jatp(10.1.1.1) received 0 KB of monitor traffic over last 1 days, 16 hours, 31 Mon, 11 Aug 2014 10:57:26 -0700 n/a Behavior Engine is not running Mon, 11 Aug 2014 10:57:26 -0700 n/a Link eth1 on jatp(10.1.1.1) is down Mon, 11 Aug 2014 10:57:26 -0700 n/a Lost connection to web_collector jatp(10.1.1.1) for 2 days, 5 hours, 11 minutes
Users	Select All Users or Current User for the notification report.
Date Range	To filter the report notification by time period, select one: Last Day Last Week Last Month Last Year
Max Num Results	Enter the number of rows of results to include in the alert notification [default is 25].
Format	Select HTML or PDF as the notification output format.
Generate On	Select Trigger or By Schedule to set the method by which an alert is generated. If "By Schedule" is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.
Recipient's Email	Enter the email address(es) of the alert notification recipient(s).

- To Test Email Notification Settings, refer to [Testing Email Notification Settings on page 124](#).

Configuring SIEM Settings

Configure SIEM Settings in order to have Events or System Audit notifications sent to designated hosts as logs in either CEF, LEEF or Syslog format.

Figure 4 Setting SIEM Notification

The screenshot shows the 'Config' tab of the Juniper ATP Appliance interface. The left sidebar contains a 'Notifications' section with 'Alert Settings' and 'SIEM Settings'. The main panel is titled 'SIEM Settings' and contains the following configuration options:

- Data Type:** Radio buttons for Events (selected), System Audit, and System Health.
- Format:** Radio buttons for CEF, LEAF (selected), and Syslog.
- Message Severity:** Radio buttons for All malware (selected), Critical, high or low, and Critical or high.
- Generate On:** Radio buttons for By Schedule (selected) and Trigger.
- Host Name:** A text input field.
- Port Number:** A dropdown menu.
- Days:** Checkboxes for Mon, Tue, Wed, Thu, Fri, Sat (checked), and Sun.
- Time:** A time selection field set to 12:00 am.

A 'Cancel' button is located below the configuration fields. At the bottom, there is a section titled 'Active SIEMs' with a table structure:

Description	Delivery	Actions

Note that if selecting Syslog as the SIEM setting when configuring System Health alerts, you can choose to include the Hostname or Process name in the Syslog messages that are sent from the Juniper ATP Appliance: Show Hostname and Show Process Name:

To create a new SIEM notification:

1. Navigate to the Config>Notifications page and select SIEM Settings from the left panel menu.
2. Click Add New SIEM Connector to set up a new Events, System Audit or System Health log notification in CEF or Syslog format.
3. Select from the available options (see descriptions further below) and click Add to complete the configuration and add the new SIEM connector configuration to the Active SIEMs list.

Using CEF Alert event_id or incident_id to Display Details in Web UI

Given an incident_id or event_id, you can use the following URLs to display relative details in the Juniper ATP Appliance Web UI.

Replace "JUNIPERATPAPPLIANCE_HOSTNAME_HERE" with your Juniper ATP Appliance host name, and replace "0000000" with the event_id or incident_id.

- https://JATPAPPLIANCE_HOSTNAME_HERE/admin/index.html?incident_id=0000000
- https://JATPAPPLIANCE_HOSTNAME_HERE/admin/index.html?event_id=0000000

NOTE The system will prompt for login/password if no login session is currently active.

To display, delete or edit an Active SIEM connector configuration:

1. To display a recent report, or delete or edit an existing SIEM configuration, click Display, Delete or Edit, respectively, in the Active SIEM table for a selected configuration row.
2. Edit, modify or delete the current settings and fields as desired, then click Save.

Alert notification configuration options

Alert notifications for SIEM events or system audits are available only if Outgoing Mail Settings are configured from the Config>System Settings menu.

Descriptions of Events alert settings are provided in the following tables.

Table 3-1 Events SIEM Settings

Event Type	Select the type of SIEM connector notification to be configured: Login/Logout Failed Logins Add/Update Users Mitigation Whitelist System Settings Restarts Remote Support
Format	Select CEF, LEEF or Syslog as the notification output format.
Malware Severity	To filter the log notification by malware severity results, choose either: All Malware Critical, High or Med Critical or High
Generate On	Select Trigger or By Schedule to set the method by which a SIEM Events log is generated. If "By Schedule" is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.
Host Name	Enter the host name of the CEF, LEEF or Syslog server.
Port Number	Enter the port number of the CEF, LEEF or Syslog server.

Table 3-2 System Audit SIEM Settings

Data Type	Select the type of SIEM notification to be configured: System Audit
Format	Select CEF or Syslog as the notification output format.
Event Type	Select the event type(s) to include in the alert notification: Login/Logout Failed logins Add/Update Users Mitigation Whitelist System Settings Restarts Remote Support
Format	Select CEF, LEEF or Syslog as the log output format.
Generate On	Select Trigger or By Schedule to set the method by which a SIEM System Audit log is generated. If "By Schedule" is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.

Table 3-3 System Health SIEM Settings

Type	Select the type of SIEM connector log to be configured: System Health
Health	Select the health report type(s) to include in the SIEM log: Overall Health Processing Delay
Format	Select CEF, LEEF or Syslog as the log output format. Note that if selecting Syslog as the SIEM setting when configuring System Health alerts, you can choose to show or hide the Hostname or Process name in the Syslog messages that are sent from the Juniper ATP Appliance: show Hostname and Show Process Name.
Generate On	Select Trigger or By Schedule to set the method by which a SIEM System Audit log is generated. If "By Schedule" is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.

Configuring System Profiles

Use the [Config>System Profiles](#) page to perform Central Manager Web UI password resets, configure users, modify display settings, and set system functions and variables.

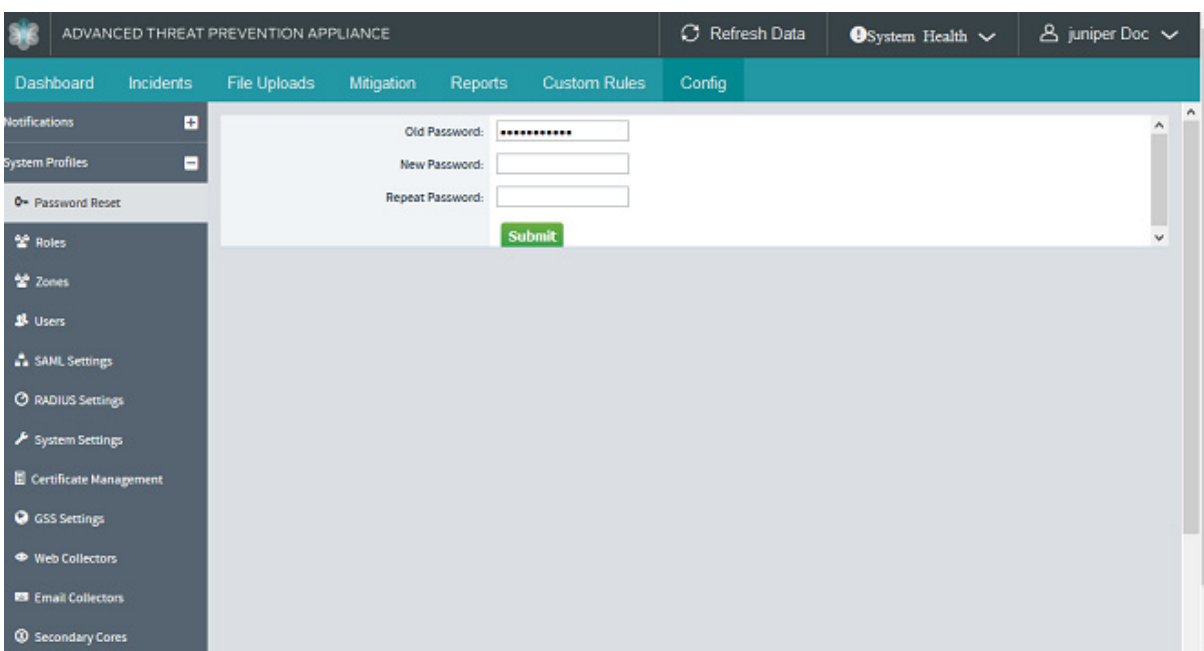
- [Resetting the Central Manager Password on page 105](#)
- [Configuring Role Based Access Controls on page 106](#)
- [Configuring MSSP Multi-Tenancy Zones on page 107](#)
- [Configuring User Accounts on page 109](#)
- [Configuring SAML Settings on page 112](#)
- [Configuring RADIUS Server Settings on page 115](#)
- [Configuring System Settings on page 119](#)

- [Managing Certificates on page 125](#)
- [Configuring Display Settings on page 123](#)
- [Configuring Outgoing Mail Settings on page 124](#)
- [Testing Email Notification Settings on page 124](#)
- [Configuring GSS Settings on page 129](#)
- [Configuring Web Collectors on page 130](#)
- [Configuring Email Collectors on page 133](#)
- [Configuring Mac OSX or Windows SecondaryCores on page 135](#)
- [Configuring Golden Image VMs on page 137](#)
- [Setting the Juniper ATP Appliance License Key on page 142](#)
- [Configuring Backup and Restore Options on page 142](#)
- [Testing Malware Detection Capabilities on page 143](#)

Resetting the Central Manager Password

Use the Password Reset configuration window to reset the administrator password used to access the Juniper ATP Appliance Central Manager Web UI.

Figure 4 Password Reset Configuration



The screenshot displays the Juniper ATP Appliance Central Manager Web UI. The top navigation bar includes the title "ADVANCED THREAT PREVENTION APPLIANCE", a "Refresh Data" button, a "System Health" status indicator, and a user profile dropdown for "juniper Doc". Below this is a teal navigation menu with tabs for "Dashboard", "Incidents", "File Uploads", "Mitigation", "Reports", "Custom Rules", and "Config". The "Config" tab is active. On the left side of the "Config" tab, there is a sidebar menu with options: "Notifications", "System Profiles", "Password Reset" (selected), "Roles", "Zones", "Users", "SAML Settings", "RADIUS Settings", "System Settings", "Certificate Management", "GSS Settings", "Web Collectors", "Email Collectors", and "Secondary Cores". The main content area shows the "Password Reset" form, which includes three input fields: "Old Password:" (masked with asterisks), "New Password:", and "Repeat Password:". A green "Submit" button is located below the "Repeat Password:" field.

To reset the Central Manager password:

1. Navigate to the Config>System Profiles>Password Reset page.
2. Enter the current password in the Old Password field.
3. Enter a new password in the New Password field, and re-enter that password in the Repeat Password field.
4. Click Submit

Configuring Role Based Access Controls

Juniper provides the option for an enterprise to restrict Juniper ATP Appliance product users to roles and privileges specific to the data they need to perform their jobs. In addition, remote authentication as well as RADIUS / SAML configurations support Juniper ATP Appliance's role based access control (RBAC) options.

With roles configuration, all new users in a system must be associated with a role, and access to various functions in a Juniper ATP Appliance product are controlled by defined user privileges. Although several default roles are available, more roles can be created as required. Existing users are migrated automatically to the new RBAC system.

Following role configuration, when a user successfully logs in to a Juniper ATP Appliance product, user access to features is controlled according to the mapped privileges assigned to that user (via the role associated with the user during user configuration).

NOTE Remote User Authentication (RADIUS / SAML) is also supported for RBAC. Only one type of remote authentication (RADIUS or SAML) is supported at any given time on a Juniper ATP Appliance.

To configure new roles for an established user:

1. Navigate to the Config>System Profiles>Roles page.

NOTE Navigate to the Config>System Profiles>Users page to create a new user before defining that user's access roles.

Figure 5 Roles Page for Configuring User Role-Based Access Controls

Role Name	Remote Group Name	Admin	Privileges	Actions
admin	dddd	Yes	All	Delete Edit
Default Admin Role	-	Yes	All	Delete Edit
Default Non-Admin Role	-	No	Access to Dashboard and Incidents Access to Upload Files Access to Detection Artifacts Access to Mitigation Access to Whitelist	Delete Edit
grant	test	Yes	All	Delete Edit
Test	-	No	Access to Upload Files	Delete Edit

2. Click Add New Roles to define a new role.
3. In the Add New Roles window, enter a "Role" name.

NOTE Two default roles are available: Default Admin Role and Default Non-Admin Role

4. Enter a Remote Group Name (optional).

NOTE Remote Group Name is specific to the name defined for remote authentication via your SAML or RADIUS configuration.

5. Click “Yes” or “No” to assign Administrator status to the new role.

NOTE If Administrator status is “No”, the Privileges options are displayed; an administrator is assigned all privileges by default so this list is not displayed when Administrator status is set to “Yes.”

6. If Administrator status is “No”, click to select the set of Privileges to be assigned to the new role.
7. Click Add to complete the role configuration. The new role is added to the Current Roles Configured table.

NOTE Navigate to [Adding a New User Configuration on page 109](#) to add the configured role to a user account.

8. Click the Delete button to remove a role configuration from the Current Roles Configured table.

NOTE You cannot delete a role to which users are actively mapped.

9. Click the Edit button to modify the configuration.

Default Roles

The following default roles are available for local and remotely authenticated Juniper ATP Appliance users:

Table 3-1 Default Roles

Default Admin Role	Access to all Features and Functionality
Default Non-Admin Role	Access to Dashboard and Incidents Access to Upload Files Access to Mitigation

Remote Authentication and Roles

Juniper ATP Appliance's Remote Authentication features support role-based access controls (RBAC).

- To enable SAML configuration for remote authentication, refer to [Configuring SAML Settings on page 112](#). The Remote Group Name must be mapped to a valid Role you've configured for the Juniper ATP Appliance system.
- To configure RADIUS for remote authentication and RBAC, refer to [Configuring RADIUS Server Settings on page 115](#).

NOTE Only one type of remote authentication (SAML or RADIUS) can be used at a time on a Juniper ATP Appliance. Remember also that the Remote Group Name must be mapped to valid roles you've configured for the Juniper ATP Appliance. Remote Group Name is specific to the name defined for remote authentication via your SAML or RADIUS configuration.

- See also [Configuring Active Directory on page 184](#).

Configuring MSSP Multi-Tenancy Zones

Use the Zones configuration page to configure multi-tenancy Web Collector Zones for Managed Security Service Provider (MSSP) support.

This feature configures Zones for Traffic Collector deployments at tenant sites. All tenant collectors are connected to the Juniper ATP Appliance Core cluster hosted at the MSSP multi-tenancy site. All management of incidents is performed by the MSSP; tenants do not have access to the Core cluster.

A configured Zone identifies incidents and events per tenant. The MSSP defines a Zone per tenant and groups all Collectors associated with a tenant to a tenant-specific Zone. Juniper ATP Appliance's event correlation stages track all events per originating Zone, and correlate events within the same Zone. In this way, the multi-tenant MSSP manages incidents per Zone/Tenant and controls all zoned Juniper ATP Appliance Central Managers per tenant using the Juniper ATP Appliance Manager of Central Managers (MCM).

To configure MSSP tenant-specific Zones:

1. Configure tenants per MSSP and assign Zones.
2. At the Juniper ATP Appliance Central Manager Web UI Config>System Profiles>Zones page, name and describe the MSSP Zones.
3. At the Juniper ATP Appliance Central Manager Web UI Config>System Profiles>Web Collectors page, assign Collectors to a defined Zone.
4. View Zone data from the Juniper ATP Appliance Central Manager Web UI Incidents page.
5. View Juniper ATP Appliance Web UI Operations Dashboard and Research Dashboard displays of Zone data and analytics.
6. Generate Reports that include Zone analytics from the Juniper ATP Appliance Web UI Reports tab.

To configure a Zone for an established MSSP tenant:

1. Click Zones under the Config>System Profiles menu to open the Zones configuration page.

Figure 4 Zones Configuration Page

The screenshot shows the 'Zones Configuration Page' in the Juniper ATP Appliance web interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various system settings and management options. The main content area features a form to add a new zone with fields for 'Zone Name' and 'Zone Description', and a 'Cancel' button. Below the form, a table titled 'Current Zones' lists existing zones with their names, descriptions, and actions (Delete and Edit).

Zone Name	Zone Description	Actions
ABC Corp	Customer_1	Delete Edit
Acme Corp	Customer_2	Delete Edit

2. Enter a Zone Name and Description, then click Add.
3. Click the Edit button to modify the configuration.
4. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>System Profiles>Web Collectors page to assign Collectors to a defined Zone.

NOTE To delete a Zone, click the Delete option in the Current Zones table row for the Zone to be deleted.

Configuring User Accounts

To create user accounts for Juniper ATP Appliance access, open the Config>Users page. The role assigned to each account determines whether the user can administer the appliance or simply perform debugging tasks.

NOTE You must be logged in with the admin role to view and access the Juniper ATP Appliance settings.

The following default roles are defined:

- Default Administrator—Allows full access to all monitoring and administrative functions. The predefined Admin account has this role.
- Debugging—Allows access only to debugging functions. Users with the Debugging role cannot view or access the CLI or the Config options. A user with the Debugging role is included in the system, but is disabled by default.
- Default Non-Administrator—Allows a set of selectable privileges defined by the Config>System Profiles>Roles settings page for user access to all or some of the following:
 - › Access to Juniper ATP Appliance's Web UI Dashboard and Incidents
 - › Access to malware analysis File Uploads
 - › Access to Mitigation options

Use the Juniper ATP Appliance Users configuration window to add, identify, edit, re-configure and/or view settings and status for Juniper ATP Appliance and software administrators and users.

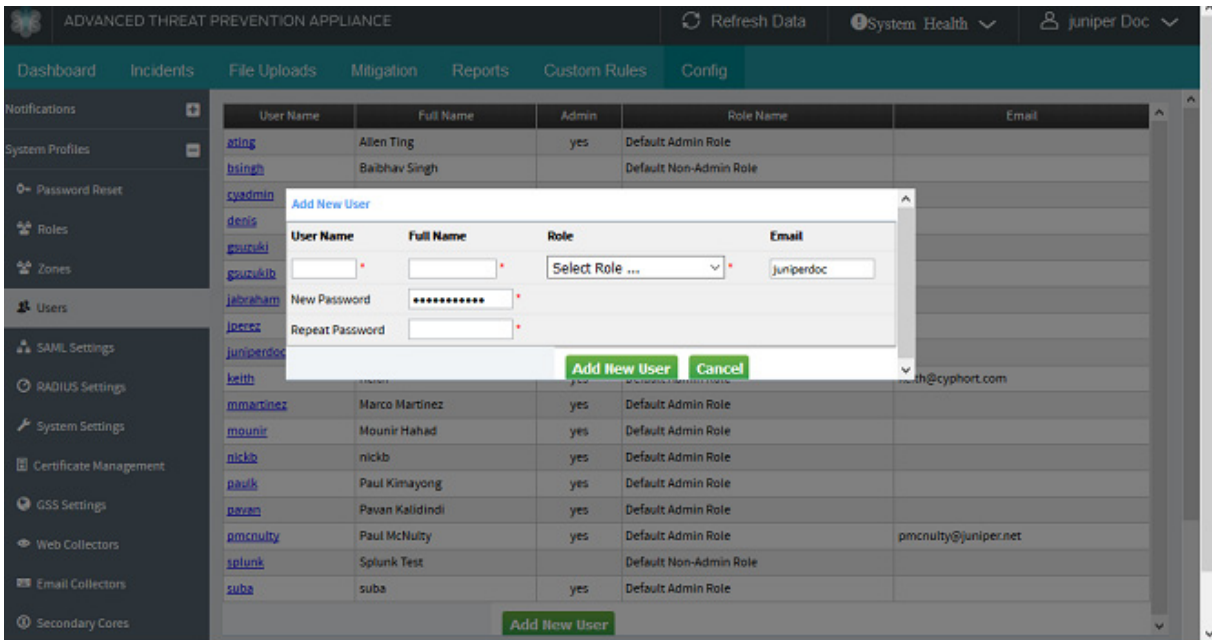
NOTE Click on a User Name in the Juniper ATP Appliance Users table to view, edit or delete existing user information.

Adding a New User Configuration

To add user accounts:

1. Click Users under the Config>System Profiles menu to open the Users page.

Figure 5 Configuring New User Accounts and Assigning Configured or Default Roles



2. Click the Add New User button to configure a new user.

To configure a new Juniper ATP Appliance user, enter settings in the fields [described below] and click Add New User to apply or Cancel to abort the configuration.

Table 3-1 Add New User Settings

User Name	Brief name of the new user; for example: admin.
Authenticate using [SAML configuration] [RADIUS configuration]	<p>Check to use SAML or RADIUS authentication for this user, only if such remote authentication is configured and available.</p> <p>When this option is checked, there is no need to enter passwords in this dialog. User authentication will take place via the "Authenticate using <IdP Name>" option on the Login screen.</p> <p>Refer to Configuring SAML Settings on page 112 or Configuring RADIUS Server Settings on page 115 for remote authentication configuration information.</p>
Full Name	A more descriptive name to identify the new user; for example: CentralManagerAdmin_NYC.
Roles	<p>Select a configured or default Role from the Roles drop down menu.</p> <p>Default roles include either Default Admin or Default Non-Admin. See Default Roles on page 107 for description of privileges assigned to default roles.</p> <p>Enable Debugging to qualify that role for this user.</p>

Table 3-1 Add New User Settings

User Name	Brief name of the new user; for example: admin.
Authenticate using [SAML configuration] [RADIUS configuration]	<p>Check to use SAML or RADIUS authentication for this user, only if such remote authentication is configured and available.</p> <p>When this option is checked, there is no need to enter passwords in this dialog. User authentication will take place via the "Authenticate using <IdP Name>" option on the Login screen.</p> <p>Refer to Configuring SAML Settings on page 112 or Configuring RADIUS Server Settings on page 115 for remote authentication configuration information.</p>
New Password	<p>Enter a Central Manager (CM) Web UI access password for this user.</p> <p>The CM Web UI supports passwords up to 32 characters, and at least 8 characters. Letters (uppercase/lowercase), numbers, and special characters can be used with the exception of double-quotes ("), spaces, or backslash characters (\) in passwords.</p>
Repeat Password	Repeat entry of the new password for this user

Click the Delete button to remove a user configuration.

Updating a User Account and Setting an API Authorization Key

User accounts are modified by clicking on an existing account on the Config>System Profiles>Users page list. Each username in the Users pager table is a link to that user account's details. When you click on a username link, the Update User window displays.

On the Update Users page, you can edit a user's name, password and role, and also create or re-create an API Key (API Authorization Key) for that user.

Generate a new API key to provide authorized programmatic access to the Juniper ATP Appliance REST API. The configured Authorization Key for that user is then applied each time an API request is made by that user.

NOTE Note that this API Key setting removes the requirement for API session logins.

To edit user settings and generate an API Key for a given user, use this two-step procedure.

1. On the Config>System Profiles>Users page, click on an existing user account.
2. If using SAML or RADIUS authentication for this user, click to check Authenticate using [SAML ID] [RADIUS], if configured.

When this option is checked, there is no need to define passwords in this dialog. User authentication will take place via the "Authenticate using <IdP Name>" option on the Login screen. Refer to [Configuring SAML Settings on page 112](#) or [Configuring RADIUS Server Settings on page 115](#) for information about configuring remote authentication and RBAC.

3. In the Update User window, make any needed modifications to the user role or password, and click to check the "Generate New API Key" option. A new API Key will be displayed the next time you open this Update User window.

[To disable a user's API Key, click the Disable API Key option.]

4. Click the Update User button.
5. Open the User Update window one more time to view and copy the new API Key.

- Access the Juniper ATP Appliance API, and as part of each API call, enter the Authorization Key, as shown in the example below.

Example

```
curl -k -H 'Authorization: bbc940ccdc795813d1c2d21c60d51a4b'
'https://localhost/admin/api.php?op=license_details&api_key=bbc940ccdc795813d1c2d21c60d51a4b'
```

Be sure to review the Juniper ATP Appliance HTTP API Guide for more information.

Configuring SAML Settings

Juniper ATP Appliance supports Security Assertion Markup Language (SAML) authentication for web browser single sign-on (SSO) operations in environments where users are allowed to log in with a username and password. More information about SAML can be found at https://en.wikipedia.org/wiki/SAML_2.0.

As part of SAML authentication, before delivering an identity assertion to a Service Provider (SP), an SSO Identity Provider (IdP) requests information from a user (principal) – such as a user name and password – in order to authenticate that principal. SAML configuration specifies the assertions between the interacting parties: the message that asserts identity is then passed from the IdP to the SP.

In SAML, one identity provider may provide SAML assertions to many service providers. Similarly, one SP may rely on and trust assertions from many independent SSO identity providers (IdPs). LDAP, RADIUS, or Active Directory allow users to log in with a user name and password; they act as typical sources of authentication tokens for an identity provider.

NOTE This section describes SAML configuration. To implement, select **Authenticate Using MyIdP** from the Juniper ATP Appliance Central Manager Web UI **Config>System Profiles>Users** page for each user. Refer to [Adding a New User Configuration on page 109](#) for more information.

To configure SAML settings at the Juniper ATP Appliance Central Manager Web UI, enter setting information for the SP and IdP:

- Navigate to the **Config>System Profiles>SAML Settings** page.

The screenshot displays the 'SAML Settings' configuration page in the Juniper ATP Appliance Central Manager Web UI. The page has a dark teal header with navigation tabs: Dashboard, Incidents, File Uploads, Mitigation, Reports, Custom Rules, and Config. The left sidebar contains a list of system settings including Notifications, System Profiles, Password Reset, Roles, Zones, Users, SAML Settings (selected), RADIUS Settings, System Settings, Certificate Management, GSS Settings, Web Collectors, Email Collectors, and Secondary Cores. The main content area is titled 'SP Settings' and contains the following fields and options:

- SP Entity Id:** A text input field with a 'Download SP Metadata' link next to it.
- Username Attribute:** A text input field.
- Authorize only locally configured users:** A checkbox.
- Group Attribute:** A text input field.
- Sign Authentication Requests:** A checkbox.
- Want IdP to sign messages:** A checkbox.
- Submit:** A green button.

Below the SP Settings section is the 'IdP Settings' section, which includes:

- Enable SAML Authentication:** A checkbox.
- * IdP Entity Id:** A text input field.
- * Login URL:** A text input field.
- * IdP Cert:** A large text area for pasting the certificate.

- For SP settings, enter definitions per field, or click the link to Download SP Metadata.

Table 3-2

SP Entity ID	An entity ID is a globally unique name for a SAML entity; the name of the appliance entity id as registered with the IdP. Typically, an SP entity ID is an absolute URL but as a name, not a location (it need not resolve to an actual Web location). Note: the host part of the URL must be a name rooted in the organization's Primary DNS Domain, and the URL must not contain a port number, a query string, or a fragment identifier. Example: "https://sp_name.JATPAppliance.net/sp">
Download Metadata File	Link from which to download the SP's XML (Juniper ATP Appliance) that will be uploaded to the IdP.
Username Attribute	The attribute in the SAML Assertion that contains the Juniper ATP Appliance username. By default, Juniper ATP Appliance uses the NameID field of the SAML response if this field is left undefined.
Group Attribute	The attribute in the SAML Assertion that contains the group name.
Admin User Group	The group (as specified by the attribute) that receives admin privileges. Example: jatp_admin
Sign Authentication Requests	Check if you want Juniper ATP Appliance to sign SAML authentication requests.
Want IdP to sign messages	Check if you want the IdP to sign messages.

- Next, define the IdP settings:

IdP Entity ID	A globally unique name for the IdP (same general naming criteria as SP entity ID) Example: "https://webauthentication.JATP.net/idp"
Login URL	The SSO URL (this field is required to allow the SP to initiate SSO). Example: "https://app.onelogin.com/trust/saml2/http-post/sso/local_login/440761"
IdP Cert	The IdP certificate details. See example in screen shot above.

NOTE When SAML-authenticated users log out of the Juniper ATP Appliance using the "log out" link, they are signing out of the Juniper ATP Appliance but not the IdP.

There are three types of Juniper ATP Appliance users and authentication methods:

Local Users with local passwords	<p>Users login with username and password at Juniper ATP Appliance Web UI login screen.</p> <p>User specific data such as report configurations and other settings are stored locally for this user type.</p>
Local Users Authenticated using SAML	<p>Users are created manually on the Juniper ATP Appliance (Config>System Profiles>Users) but authenticated via SAML. This means the password is not stored on the Juniper ATP Appliance. The SAML assertion controls whether the user is given “admin” privileges; the user privileges can be configured locally or via SAML, with SAML taking higher precedence when both are configured.</p> <p>User specific data such as report configurations and other settings are stored locally for this user type.</p> <p>Such users also can use user-specific features of Juniper ATP Appliance (API Keys, reports, UI customizations).</p>
Non Local Users Authenticated using SAML	<p>These user accounts only exist on the IdP and not on the Juniper ATP Appliance. Consequently, such users do not have access to Juniper ATP Appliance’s user-specific features. No data is stored locally for this user type. Their user role (RBAC) is determined from the information present in the SAML Assertion.</p>

Login to the Juniper ATP Appliance using SAML Authentication

After the SAML SP and IdP details are configured from the Config>System Profiles>SAML Settings page, users for which SAML authentication is checkmarked (from the Config>System Profiles>Users page) are automatically redirected to the IdP’s login page when they try to access the Juniper ATP Appliance. To perform a local login, ensure the parameter “local_login” is present in the IdP URL; for example: `https://10.2.20.100/admin/?local_login`

NOTE An AuditLog will include username with SAML user-id. In addition, Juniper ATP Appliance logs audit messages when SAML settings are changed by a user.

Setting SAML for PingFederate Servers

Some enterprises configure SML using PingFederate (PF) servers for AD authentication. In addition to Juniper ATP Appliance’s enhanced RBAC for allowing deterministic access to Juniper ATP Appliance devices, administrators can configure precedence-based authorization to control access behavior. A few additional settings, in addition to the SAML configuration provided in the previous section, must be configured for initial deployment.

1. Administrators must add authorization control for non-admin role users in the Juniper ATP Appliance Central manager Config>System Profiles>Users>Add New User window. This control involves using the group name for the SAML assertion (which removes any precedence-specific issues).

When Authorize using is enabled, Juniper ATP Appliance will use the remote group from the Role configured. If the Role is not set for a Radius or SAML response, the authorization will fail.

If Authorize using is disabled (unchecked), the Role selected is applied.

2. Navigate to the Central Manager Config>System Profiles>SAML Settings>SP Settings window to allow authorization only for locally configured users; check “Authorize only locally configured users.”

When “Authorize only locally configured users” is selected, authorization is allowed only if the local user is present.

When “Authorize only locally configured users” is selected and the user is present, the authorization checkbox in the user account window is used for authorizing privileges.

NOTE The default value for “Authorize only locally configured users” is unchecked (or disabled) in SP settings. The default value of “Authorize using SAML/Radius” is True (checked).

Options for “Authorize only locally configured users”

- For Simple Local User (Radius and SAML not configured), “Authorize only locally configured users” is not relevant. Access to the Juniper ATP Appliance device is granted per matching Role Name. If a “remote group” in the Role is configured, it is ignored.
- For a user that is present in Juniper ATP Appliance configured with Authentication to SAML or Radius ON, the “Authorize only locally configured users” option in SAML SP Settings should be set.
- For remote authentication and authorization when “Authorize only locally configured users” is unselected, type 3 users are allowed. A temporary user is created based on the successful authentication of the type-3 user if the SAML group assertion matches with the remote group settings in one of the Roles configured.
- Navigate to the Config>System Profiles>SAML Settings>RADIUS Server Settings window and select “Authorize only locally configured users” for these configured users.

Configuring RADIUS Server Settings

Juniper ATP Appliance Release supports remote authentication to Active Directory (AD) servers using the RADIUS protocol in customer networks. This feature integrates Juniper ATP Appliance products and an Active Directory RADIUS configuration on primary and secondary servers in the customer enterprise. This integration between Juniper ATP Appliance products and the RADIUS feature on existing Active Directory servers in a customer's network frees enterprises from having to maintain two access databases: one for network access and one for Juniper ATP Appliance access, while helping to simplify network security and usage.

NOTE Remote User Authentication via RADIUS or SAML is supported for RBAC. But only one type of remote authentication (RADIUS or SAML) is supported at any given time on a Juniper ATP Appliance. Refer to [Configuring Active Directory on page 184](#) for information about setting up a new AD domain controller. Note also that Juniper ATP Appliance Email Phishing Correlation requires an Active Directory configuration.

Implementation of RADIUS support requires that the RADIUS server be configured with Active Directory in addition to configuring RADIUS server settings on the Juniper ATP Appliance system. This implementation assumes there is no NAS between the RADIUS client (the Juniper ATP Appliance) and the RADIUS server. Active Directory authentication is achieved using Radius protocol (RFC 2865).

For the RADIUS server configuration:

1. Add the Juniper ATP Appliance IP to the allowed RADIUS client list.
2. Configure the RADIUS secret on the RADIUS server.
3. Configure the Filter-Id or choose a RADIUS attribute in the RADIUS server policy.
4. Enable PAP and MS-CHAP authentication methods on the RADIUS server.

NOTE Juniper ATP Appliance's RADIUS integration is available for Windows Server 2008 and 2012, with support for primary and secondary RADIUS servers using PAP and MS-CHAP authentication methods. A separate link is available for Local login when RADIUS is configured: https://<JATPDeviceIP>/admin/?local_login

About Radius Groups

With RADIUS configurations, authentication and authorization are coupled. If the Active Directory username is found and the password is correct, the RADIUS server returns an Access-Accept response, including a list of attribute-value pairs that describe the parameters to be used for the session. Since the Group Name specified by AD is not included as part of the Access-Accept response attributes, Juniper ATP Appliance uses the Filter-Id attribute by default, but the choice of attribute is configurable. This attribute must be configured on the RADIUS server with its string value as Group Name for users configured on the Active Directory. For example, RADIUS could

be configured to send the same Filter-Id value string (preferably matching the group name from AD) for multiple users.

Local/Remote User Authentication and RBAC

For local users authenticated through RADIUS, the authenticated user's AD group name will be checked against the user role for applying privileges. Such users can use a set of allowed Juniper ATP Appliance features (as configured on the Juniper ATP Appliance Central Manager Web UI Config>System Profiles>Roles page).

For users not configured on a Juniper ATP Appliance but authenticated through RADIUS, Juniper ATP Appliance accommodates hidden user specifications similar to SAML configurations (Type 3 user). This user will not have access to admin-level features on a Juniper ATP Appliance product. User role is determined based on Group Name received via the Filter-Id value.

NOTE Each user Role is mapped to a configured Group Name for RBAC, as configured on the RADIUS server (the Group Name is returned as a value of the configured Filter-Id attribute).

For example, if you configure the Filter-Id on the RADIUS server as TestGroup1 for a Juniper ATP Appliance Admin Role, and Filter-Id as TestGroup2 for a Juniper ATP Appliance Non-Admin Role, then the Remote Group Name for the Admin Role on the Juniper ATP Appliance side is AccessGroup1, and the Group Name for the Non-Admin Role on the Juniper ATP Appliance side is AccessGroup2. Refer also to [Configuring Role Based Access Controls on page 106](#), [Default Roles on page 107](#) and [Remote Authentication and Roles on page 107](#) for more information about RBAC.

A sample Windows Server 2012 Network Policy Server integration configuration example is provided below. Next, configure the Filter-Id and be sure to enable PAP and MS-CHAP authentication methods.

Configure a secondary RADIUS server, as required. A Secondary Server configuration for failover purposes is optional.

NOTE Failover to a secondary RADIUS server takes place if there is no response from the primary server, or when a shared secret key does not match the one set on the primary server, or when an invalid RADIUS group attribute is contained in the RADIUS response from the primary RADIUS server.

Configuring RADIUS Settings on the Juniper ATP Appliance

For the Juniper ATP Appliance configuration, set the following:

- Hostname/IP:port
- RADIUS secret
- User group attribute
- Time-out value

NOTE Refer to the Juniper ATP Appliance HTTP API Guide for information about configuring the Juniper ATP Appliance-side RADIUS settings using the “set_radius_config” API.

Use the following procedure to configure RADIUS server settings from the Juniper ATP Appliance Central Manager Web UI.

1. Navigate to the Central Manager Config>System Profiles> RADIUS Settings page:

Figure 4 Juniper ATP Appliance Central Manager RADIUS Server Settings Page

2. To enable RADIUS authentication, click the checkbox Enable RADIUS Authentication. Remove the checkbox to disable a RADIUS configuration.
3. Select the RADIUS Authentication Method configured for the server from the dropdown: PAP or MS-CHAP; the default method is PAP.
4. Enter the User Group Attribute; Filter-Id is the default unless a different attribute was configured on the server side. (See [About Radius Groups on page 115](#) for information about mapping the Filter-Id to the Group Name.)

NOTE The User Group Attribute is mapped to the Remote Group Name configured on the Juniper ATP Appliance-side for RBAC using the Juniper ATP Appliance Config>System Profiles>Roles page. The Remote Group Name is case sensitive.

5. Enter the Wait Timeout; the default is 3 seconds. Timeout can be configured for 1-30 seconds.

NOTE Three login attempts by AD/RADIUS users are allowed by default; the timeout between attempts is configurable, as indicated in the step above. If the timeout value is configured to a high value of 30 seconds, and if the RADIUS server is not reachable, the user's browser may display a timeout message while waiting for a response from the Juniper ATP Appliance.

6. Enter the Primary Server Settings:
 - › Enter the Hostname or IP Address of the primary RADIUS server in the RADIUS Server Host field.
 - › Enter the RADIUS Port; 1812 is the default. This is the UDP port used to send the RADIUS access request.
 - › Enter the RADIUS Secret as configured on the server side.

7. (Optional) Enter the configured Secondary Server Settings:

- › Enter the Hostname or IP Address of the secondary RADIUS server in the RADIUS Server Host field.
- › Enter the RADIUS Port; 1812 is the default. Again, this is the UDP port used to send the RADIUS access request.
- › Enter the RADIUS Secret as configured on the server side.
- › When RADIUS login is configured, the behavior of local login is unchanged although a separate URL is used to perform the local login:
https://<JATPDeviceIP>/admin/?local_login

Configuring System Settings

Use the System Settings configuration window to configure and/or revise settings for Juniper ATP Appliance deployment(s) and software display and email settings.

- [Configuring System Settings on page 119](#)
- [Configuring Display Settings on page 123](#)
- [Configuring Outgoing Mail Settings on page 124](#)
- [Testing Email Notification Settings on page 124](#)

Navigate to the Config>System Profiles>System Settings page to configure and perform various setup actions [as described below], and then click Submit to save the configuration.

NOTE The Config>System Profiles>System Settings page contains settings options for baseline system settings as well as Display Settings, Auto-Mitigation Settings, Outgoing Email Settings and Testing Outgoing Mail Settings -- all on the same configuration page. Scroll the System Settings page to see full option sets.

Figure 5 System Settings | Display Settings | Outgoing Mail Settings Page

The screenshot displays the 'System Settings' page of the Juniper ATP Appliance. The interface includes a top navigation bar with 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings categories: Notifications, System Profiles, Password Reset, Roles, Zones, Users, SAML Settings, RADIUS Settings, System Settings, Certificate Management, GSS Settings, Web Collectors, Email Collectors, Secondary Cores, Golden Image VMs, Licensing, Backup/Restore, Test Malware Detection, and Environmental Settings. The main content area is titled 'System Defaults' and contains the following settings:

- System Defaults:**
 - Hostname: PartnerDemo-New
 - Server fully-qualified domain name: PartnerDemo-New.wg.cyphort.com
 - IVP format: ☐ MSI ☒ Self-extracting Zip file [Download MSI](#)
 - Software Update enabled: ☒
 - Content Update enabled: ☒
 - Enable JATP support account: ☐
 - Restart services now: [restart](#)
 - Reboot appliance now: [reboot](#)
 - Clear event database: [clear](#)
 - [Submit](#)
- Proxy Settings:**
 - Proxy Type: ☒ No Proxy ☐ Manual Proxy
 - [Submit](#)
- Auto Mitigation Settings:**
 - Enable for Web: ☒
 - Enable for Email: ☐
 - Mitigation Aggressiveness Level: ☐ Moderate (Only Max and High Threat Confidence Levels) ☒ Aggressive (All Threat Confidence Levels)
 - Max IP Address Threats: (percentage of left blank)
 - Max URL Threats: (percentage of left blank)
 - [Submit](#)

Configuring System Settings

To configure system settings:

1. Navigate to the Config>System Profiles>System Settings page.
2. In the System Settings area at the top of the page, enter the settings in the fields provided (each options is described below), then click Submit to save the configuration settings.

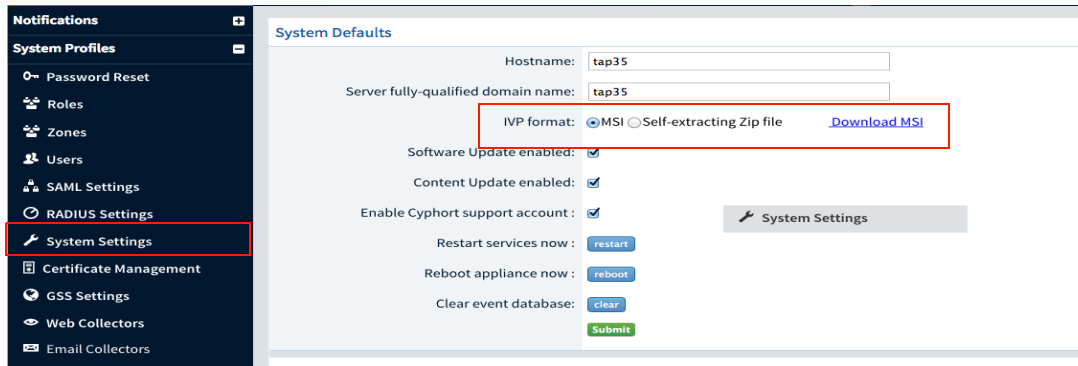
Table 3-1 System Settings Options

Hostname	Enter a name for the Juniper ATP Appliance or software.
Server Fully Qualified Domain Name	Enter the fully qualified domain name for the deployed Juniper ATP Appliance.
IVP Format	<p>Configure the Infection Verification Package (IVP) format for your environment: an MSI installer in .ivp format or a Self Extracting Zip File in .exe format [this is the script customized for the detected malware download (DL) that will test for infection at the enterprise endpoint after the MSI installer is installed at that endpoint.</p> <p>To download the MSI Installer now, click Download MSI. Download MSI downloads the Juniper ATP Appliance-ivp-setup.msi to the endpoint on which you want to run an .ivp file. Executing Juniper ATP Appliance-ivp-setup.msi once on an endpoint will allow the IVP file to run in .ivp format.</p> <p>You can distribute and execute Juniper ATP Appliance-ivp-setup.msi on all systems in your network so that they can natively run the .ivp file. Alternately, you can simply set the format of the IVP to be a self-extracting zip file which all windows machines can run without any modification.</p> <p>Note: Be sure to review the section below Understanding IVP MSI and Self-Extracting ZIP Options on page 119</p>
Software Update Enabled	Click to enable or disable automatic Juniper ATP Appliance software updates.
Content Update Enabled	Click to enable or disable automatic security content updates.
Enable Support Account	Click to enable or disable theSupport access account for troubleshooting and appliance diagnostics.
Restart Services Now	Click Restart to restart Juniper ATP Appliance services.
Reboot Appliance Now	Click Reboot to reboot the Juniper ATP Appliance.
Clear Event Database	Click Clear to clear the Juniper ATP Appliance or software-only event database.

NOTE Click the Submit button to apply the configuration.

Understanding IVP MSI and Self-Extracting ZIP Options

Juniper ATP Appliance's Infection Verification Pack (IVP) verifies whether malware that was downloaded to any endpoint in the enterprise has been executed at that given endpoint. For each download that Juniper ATP Appliance detects, an IVP can be created that searches for Indicators of Compromise (IOCs) on the endpoint device. By verifying infection at the endpoints, remediation teams are able to focus their efforts on specific machines identified and verified as compromised machines, saving time and money on desktop mitigation.



Administrators configure IVP settings from the Juniper ATP Appliance Central Manager Web UI Config>System Settings>System Settings page, as described on the previous page in this guide. Setting options include:

- Self-Extracting Zip File
An IVP Self-Extracting zip file is an executable format that includes two files: the IVP program itself and an input file containing the detected indicators of compromise packaged into a single .exe file.
- MSI
An IVP MSI is a Windows Installer package file format.

Self-Extracting Zip File IVP Process

When an IVP Self-Extracting Zip .exe file is executed, a command window displays information about whether the malware was installed, and prompts if and where a log file is to be saved locally. Results of the IVP are also sent to the Juniper ATP Appliance Central Manager.

MSI File IVP Process

To use IVP in MSI mode, the administrator must first download and install Juniper ATP Appliance-ivp-setup.msi on the endpoint. The Juniper ATP Appliance-ivp-setup.msi file is downloaded by the administrator from the Juniper ATP Appliance Central Manager using the Download MSI hyperlink next to the IVP format selection buttons in Config>System Setting>System Settings. After installing the Juniper ATP Appliance-ivp-setup.msi, the IVP program is installed under

"C:\Program Files\JATP\IVP\JATP-ivp.exe" on the target end system. When IVP mode is set to MSI in the Juniper ATP Appliance Central Manager, a text file with the IOCs are downloaded when an IVP is generated.

The format of the file is *.ivp. When JATP-ivp-setup.msi is properly installed, executing the .ivp file launches the juniprtatp-ivp.exe and the search begins for the IOCs that were detected during malware analysis and delineated in the downloaded .ivp file now executing on the end system. By default, a command prompt displays the results, verifying whether or not an infection has taken place at the endpoint. The user must press any key to exit the command prompt window. Log files in MSI mode are stored in "C:\Program Files\JATP\IVP" and the Juniper ATP Appliance Central Manager is notified of the infection results.

NOTE To search for IOCs at the endpoint without requiring any user interaction, be sure to run IVP in MSI mode. Be sure the Juniper ATP Appliance IVP program is installed, download the IVP file, and then execute IVP using the following syntax:

"C:\Program Files\JATP\IVP\JATP-ivp.exe -i <ivp-input.ivp>".

...where <ivp-input.ivp> is the .ivp downloaded from the Juniper ATP Appliance Central Manager. The arguments for IVP are provided below:

```
C:\temp>JATP-ivp.exe -h
Usage: JATP-ivp.exe [-version] | [[-i <inputfile>] [-o <outputfile>] [-threshold
<float_num>]]
        -version                prints out the version string
        -i <inputfile>          default = ivp-input.txt
        -o <outputfile>         default = ivp-output.txt
        -threshold <floatnum>  default = 1.0
```


Configuring Proxy Settings for the Management Network

Many customers still rely on proxies and gateways to provide rudimentary security for their endpoints. In such environments, the CM/Core management network must be able to function and communicate with external services similarly to an unproxied environment. This communication includes uploads and downloads for GSS, as well as software, security content and signature updates, and all other necessary communications. Configure Juniper ATP Appliance Cores deployed in HTTP and/or HTTPS proxy environments to function and communicate with Juniper ATP Appliance GSS and other Internet services.

Use the Proxy Settings area of the System Settings configuration window to define and configure proxy integration and detailed settings for the Juniper ATP Appliance deployment.

System Settings

Proxy Type: ☒ No Proxy ☐ Manual Proxy

Submit

Auto Mitigation Settings

Enable Auto Mitigation: ☒

Mitigation Aggressiveness Level: ☒ Moderate (Only Max and High Threat confidence levels) ☐ Aggressive (All Threat Confidence Levels)

Max IP Address Threats: (infinite if left blank)

Max URL Threats: (infinite if left blank)

NOTE This proxy configuration from the Central Manager Web UI is applicable only to Core or All-in-One settings. To configure a proxy for SPAN-traffic monitoring via the Web Collector, you must configure the proxy inside IP address / outside IP address configuration from the Collector CLI in collector mode; for example:

```
Juniper ATP Appliance Collector (collector)# set proxy inside add <ip address>
```

Refer to the Juniper ATP Appliance CLI Command Reference for more information.

1. Select a Proxy type: No Proxy or Manual Proxy.

Proxy configuration provides integration with Juniper ATP Appliance's detection of all links in the kill chain, including exploit, download and infection.

2. When you select Manual Proxy as your proxy type, the display area fields on the Proxy Settings page will change to accommodate configuration, as shown below:

Proxy Settings

Proxy Type: ☐ No Proxy ☒ Manual Proxy

Proxy FQDN / IP:

Proxy Port:

No Proxy for: (separate each address with a comma)

Authentication Required: ☐

Username:

Password:

Submit

3. Enter the Proxy FQDN / IP Address in the Proxy FQDN / IP Address field.

Proxy settings for the management network must utilize embedded host name and URL -- the IP address will always reference the proxy server

4. Enter the Proxy Port number in the Proxy Port field.
5. Enter into the No Proxy for field all IP Addresses for which no proxy is required; separate each address with a comma.
6. Check to indicate whether authentication is required for this proxy by clicking Authentication Required checkbox.
7. Enter a Username and Password if authentication is required.
8. Click Submit.

NOTE Refer to the Juniper ATP Appliance CLI Command Reference for information about configuring proxies from the Juniper ATP Appliance CLI server mode. See [Setting proxy IP addresses](#).

Configuring No Proxy Settings for Local Traffic

Local servers situated inside the proxy must be added to the No Proxy rules. The No Proxy rules ensure that outgoing connections targeted for specified network addresses included in the No Proxy rules do not go through the proxy.

The configuration will include the proxy settings for the CM/Core appliance or All-in-one appliances only. The proxy settings for the connected Collectors and Secondary Core(s) will be displayed in the Juniper ATP Appliance Central Manager Web UI Config pages for Web Collectors and Secondary Cores.

NOTE Administrators should check whether their proxy policy filters out the IP addresses of the Juniper ATP Appliance GSS cloud servers, or whether the IP addresses of the Juniper ATP Appliance GSS servers (which include the update, report, and reputation servers) are part of the category of blocked hostnames under existing proxy policy.

Configuring Auto-Mitigation

Auto-mitigation enables users to configure whether they want Juniper ATP Appliance's mitigation intelligence pushed automatically to the enterprise's integrated security infrastructure without user interaction, or manually push a specified mitigation rule to integrated devices.

When auto-mitigation is enabled, the Juniper ATP Appliance administrator is not required to take any action to mitigate a newly discovered threat.

Figure 4 Auto-mitigation Settings page

Auto Mitigation Settings

Enable Auto Mitigation: ☒

Mitigation Aggressiveness Level: ☒ Moderate (Only Max and High Threat confidence levels) ☐ Aggressive (All Threat Confidence Levels)

Max IP Address Threats: (infinite if left blank)

Max URL Threats: (infinite if left blank)

Submit

To configure auto-mitigation:

1. Navigate to the Config>System Profiles> System Settings page in the Central Manager Web UI and scroll down to the Auto Mitigation Settings area as shown above.
2. Click to Enable Auto-Mitigation to enable auto-mitigation blocking to configured security devices. See also [Configuring Firewall Auto-Mitigation on page 147](#).

NOTE When auto-mitigation is enabled, Juniper ATP Appliance's Advanced Threat Analytics (ATA) is also enabled and ATA results can be viewed on the Mitigation tab as "Juniper ATP Appliance ATA" (as opposed to Local security content) under the Threat Source column of the Mitigation table (meaning the threat was detected locally rather than through the Juniper ATP Appliance GSS).

When not enabled, automatic blocking is disabled and mitigating rule is not sent to integrated firewalls without the Juniper ATP Appliance administrator manually pushing the threat from the Mitigation tab.

3. Select a Mitigation Aggressiveness Level: Moderate or Aggressive. Aggressive means all threats reported in the Mitigation tab are automatically pushed. Moderate means only Max and High severity threats listed in the Mitigation tab are automatically pushed.
4. At Max IP Address Threats, enter the maximum number of IP Addresses to send to a firewall. If left unspecified, the Juniper ATP Appliance will not limit the number of threats pushed to devices.

This number is threat confidence-based, not risk-based. Confidence state is determined by the rule complex state.

5. At Max IP URL Threats, enter the maximum number of URLs to send to a firewall. If left unspecified, an infinite number is allowed.
6. View threats and auto-blocking results from the Mitigation tab. .

Configuring Display Settings

Use the Display Settings area of the System Settings configuration window to configure and/or revise Central Manager Web UI login and display settings.

Figure 5 Display Settings

To configure display settings:

1. Navigate to the Config>System Profiles page, select System Settings from the left panel menu, and scroll down to locate the Display Settings configuration area in the System Settings page.
2. Enter or select optional display settings [options are described below].
3. Click Submit to apply the configuration.

Table 3-1 Display Settings Options

Maximum Threats	Enter the maximum number of threats to display in the Central manager Web UI tables [default is 500].
Default Display Period	Select either Last Month Last 3 Months Last Year
Session Timeout	Enter the Web UI session timeout value [default is 15 minutes; minimum Web UI timeout setting is 2 minutes].
Account Lockout Observation	If a user fails to log into the Juniper ATP Appliance Web UI with a valid login, the account lockout observation setting default is 10 minutes before a retry is allowed.

Table 3-1 Display Settings Options

Maximum Threats	Enter the maximum number of threats to display in the Central manager Web UI tables [default is 500].
Account Lockout Threshold	The number of times a user can attempt to log into the Juniper ATP Appliance or service [default is 15].
Account Lockout Duration	Enter the amount of time an unauthorized user is to be locked out of the Juniper ATP Appliance Web UI.

Configuring Outgoing Mail Settings

Use the Outgoing Mail Settings configuration window to configure and/or revise outgoing email notification settings for the Juniper ATP Appliance or software deployment.

The screenshot shows the 'Outgoing Mail Settings' configuration window. It includes the following fields and options:

- SMTP host:** smtp.gmail.com
- SMTP port:** 465
- Use SSL:** ☒ (recommended)
- SMTP login:** gocyph@gmail.com
- SMTP password:** [Redacted] [Important password security information](#)
- 'From' address:** no-reply@cyphort.com
- Test Outgoing Mail Settings:**
 - Email addresses:** bong@cyphort.com (separate addresses with a comma and space) (Note: this test only verifies the ability to send email, not whether the email addresses are valid)
 - Outgoing configuration:** ok
 - TEST** button

To configure Outgoing Mail Settings:

1. Navigate to the Config>System Profiles page, select System Settings from the left panel menu, and scroll down to locate the Outgoing Mail Settings configuration area on the System Settings page.
2. Enter or select email settings [options are described below].then click Submit to apply the configuration.

Table 3-2 Outgoing Mail Setting Options

SMTP Host	Enter the IP of the enterprise mail host
SMTP Port	Enter the SMTP port number [default is 587].
Use SSL	Enabled by default; uncheck to disable use of SSL.
SMTP Login	Enter an SMTP email login for the appliance or service.
SMTP Password	Enter an SMTP password the login account.
From Address	Enter a ""From"" field email address; the default is no-reply@JATP.net.

Testing Email Notification Settings

At the bottom of the Config>System Profiles>System Settings page, in the Test Outgoing Mail Settings area, you can perform a test of the current outgoing mail configuration.

The screenshot shows the configuration interface of a Juniper ATP Appliance. It is divided into three main sections:

- Max IP Address Threats:** A text input field with a placeholder "(infinite if left blank)".
- Max URL Threats:** A text input field with a placeholder "(infinite if left blank)".
- Submit** button.
- Display Settings:**
 - Maximum threats:** 500
 - Default display period:** Last Month (dropdown)
 - Session timeout:** 600 (2 minutes minimum)
 - Account lockout observation:** 10 (minutes)
 - Account lockout threshold:** 600
 - Account lockout duration:** 10 (minutes)
 - Submit** button.
- Outgoing Mail Settings:**
 - SMTP host:** smtp.gmail.com
 - SMTP port:** 465
 - Use SSL:** ☒ (recommended)
 - SMTP login:** gocyp@gmail.com
 - SMTP password:** (empty field) with a link to [Important password security information](#)
 - 'From' address:** no-reply@cyphort.com
 - Submit** button.
- Test Outgoing Mail Settings:**
 - Email addresses:** bong@cyphort.com (Note: this test only verifies the ability to send email, not whether the email addresses are valid)
 - Outgoing configuration:** ok
 - TEST** button.

To test outgoing mail settings:

1. Navigate to the Config>System Profiles>System Settings page and scroll down to locate the Test Outgoing Mail Settings area.
2. Enter an email address (or series of email addresses, separated by commas) to which the test email will be sent by the Juniper ATP Appliance .
3. Click the Test button to test your email notification configuration. An email will be sent by the Juniper ATP Appliance to the email address(es) entered, based on the configuration settings.

NOTE This test verifies the ability to send email, not whether the email addresses are valid.

Managing Certificates

Use the Config>System Profiles>Certificate Management page to create a self-signed certificate or secure socket layer (SSL) certificate signing request (CSR), or, to import and install a user-provided certificate.

Note that a Common name (fully-qualified domain name (FQDN) of the server is required when creating new certificates.

NOTE The Juniper ATP Appliance allows enhances whitelisting functionality by allowing users to whitelist based on a signing certificate. Refer to [Configuring Whitelist Rules on page 168](#) for more information.

Creating a Self-Signed Certificate/CSR

Users may create certificates using two available options:

- Create a new self-signed certificate

- Create a certificate signing request (CSR)

The first option - Create a new private key and self-signed certificate- creates a new private key, and then generates a new self-signed certificate, as is done today whenever the appliance hostname is changed.

The second option - Create a certificate signing request using an existing private key - prompts the user for the certificate details and uses those details with the current private key to generate a CSR, which the user can then download to be signed by a trusted certificate authority (CA).

Alternatively, it is possible to create a certificate signing request using a new private key - this option invalidates any outstanding CSRs because a new private key is created. This allows the user to change the private key if the previous private key was compromised. If the user chooses to proceed, the system then prompts the user for certificate details and uses those details, and the new private key, to generate a CSR, which the user can then download to be signed by a trusted CA.

To create a self-signed certificate:

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>System Profiles>Certificate Management page.
2. Click Create Self Signed Certificate.

3. In the Create Self Signed Certificate window, enter the details for each field prompt:

NOTE Some fields are optional but used during certificate signing request creation if provided.

Common Name (Server FQDN)	Fully qualified domain name of the Server.
Organization (Optional)	Organization for which the certificate is to be created.
Organization Unit (Optional)	Organization Unit or department, network, etc.

Email Address (Optional)	Email address of the administrator creating the certificate.
Locality (Optional)	Locality of the enterprise.
State or Province (Optional)	State or province in which the Server using the certificate is located.
Country Code (Optional)	Country in which the Server using the certificate is located.
Key Length	Choose either 2048-bit keys or 4096-bit keys. Typically, 2048 bits are used for extremely valuable keys like root key pairs used by a certifying authority. Note that a longer key length is harder to brute force, but using a longer key length also requires more computational resources on the server and client.

4. After entering the self signed certificate details, click Create and the certificate will be created and applied to the running configuration.

To create a Certificate Signing Request CSR:

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>System Profiles>Certificate Management page.
2. Click Create CSR.
3. In the Create CSR window, enter the details for each field prompt:

NOTE By clicking the Create New Private Key option will invalidate any previously created CSR.

Common Name (Server FQDN)	Fully qualified domain name of the Server.
Organization (Optional)	Organization for which the certificate is to be created.
Organization Unit (Optional)	Organization Unit or department, network, etc.
Email Address (Optional)	Email address of the administrator creating the certificate.
Locality (Optional)	Locality of the enterprise.
State or Province (Optional)	State or province in which the Server using the certificate is located.
Country Code (Optional)	Country in which the Server using the certificate is located.
Create New Private Key	Click to create a new private key as part of the certificate signing request. Note that by clicking this option, previously created CSRs will be invalidated. Do not select this option if you prefer to use an existing private key.

4. Download the CSR file and send it to the trusted CA. The trusted CA will send the user a certificate file and CA bundle. Navigate to Config> System Profiles > Certificate Management and click Upload and Install Certificate to upload the certificate and CA bundle PEM files.

The appliance validates and installs the certificates provided.

Uploading and Installing a User-Provided Certificate

To install a user-provided certificate from a trusted Certificate Authority (CA), the following is to be provided by the administrator:

- Private key (optional) - uploaded
- Client certificate - uploaded
- CA bundle (optional) - uploaded

This information may be provided in one of two ways:

- Import the private key, client certificate, and CA bundle as separate PEM files. PEM encoding is a private key format that stores an RSA private key for use with cryptographic systems such as SSL.
 - Import the data as a PKCS#12 bundle with an optional passphrase for decrypting the contents. PKCS#12 is a archive file format for storing multiple cryptography objects as a single file; it is used to bundle a private key with its X.509 certificate or to bundle all members of a chain of trust. Select the Certificate Format. Let's start with PEM. Click PEM.
5. Click Choose File to upload a Private Key (this step is optional).
 6. Click Choose File to upload a Certificate File.
 7. Click Choose File to upload a CA Bundle File (this step is optional).
 8. Click Upload and Install Certificate.

Alternatively, you can choose the PKCS#12 format.

NOTE The PKCS#12 format allows an admin to create a backup of current certificates, from which a restore backup operation could be performed using the PKCS#12 import. So be careful to only upload the PKCS#12 files created by the Juniper ATP Appliance, not any PKCS#12 file created independently.

1. Click to select PKCS#12 as your preferred Certificate Format. Enter a PKCS#12 Passphrase (this is an optional step).

NOTE The PKCS#12 passphrase should match the passphrase defined when the user created the PKCS#12 file. Otherwise, the file cannot be decrypted.

2. Or click Choose File to upload a PKCS#12 Bundle File.
3. Click Upload and Install Certificate. This action will replace existing SSL certificates.

Downloading a Certificate or PKCS#12 Bundle

Download a PKCS#12 bundle in order to backup a current certificate.

1. Navigate to Config>System Profiles >Certificate Management and scroll down to the Download Certificate area of the page.
2. Enter the certificate PKCS#12 Passphrase (optionally) and click Download Certificate to download and save the PKCS#12 bundle. The download will contain the server's private key. Although the PKCS#12 passphrase is optional when the user downloads the file, it is recommended to set the passphrase so that if the file is lost, the private key is not exposed.

NOTE To load certificates from backup, click the Upload & Install Certificate button from the Upload and Install Certificate area of the Config>System Profiles>Certificate Management page. Certificate", and uploads the PKCS#12 bundle.

TIP An SSL certificate browser message may display after uploading an SSL certificate and applying an auto refresh of the page. The browser's certificate information states "Connection to the website is not fully secured because it contains unencrypted elements (such has images)....." This is not a Juniper ATP Appliance Web UI issue and the message represents standard cautionary browser behavior.

Configuring GSS Settings

Use the Config>System Profiles>GSS Settings configuration window to configure and/or view Global Security Services settings or to perform a detection data update to GSS for global malware aggregation and reporting.

NOTE Be sure to whitelist the Juniper ATP Appliance to avoid being SSL intercepted.

The screenshot displays the Juniper ATP Appliance web interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various system settings, with 'GSS Settings' highlighted. The main content area shows the 'GSS (Global Security Services) enabled:' checkbox checked. Below it, 'GSS Documents Upload enabled:' is unchecked. A 'GSS run now:' button is present, followed by a 'Submit' button. The 'Remote Support' section shows 'Enable Remote Support:' as unchecked and a 'Duration:' field with a '(hrs)' label, also followed by a 'Submit' button.

To configure GSS Settings:

1. Navigate to the Config>System Profiles>GSS Settings page.
2. Enter or select GSS settings [options and fields are described below].

- Click Submit to apply the configuration.

Table 3-3 GSS Settings Options

GSS (Global Security Services) Enabled	Click the checkbox to disable [enabled by default].
One-Way Update Option	To enable One-Way GSS communication, ensure that the GSS Enabled checkbox is unchecked. Note that there is an additional license cost to enable one way (from Juniper ATP Appliance GSS to the Core) GSS communication.
Two-Way Update Option	To enable Two-Way GSS communication: A) The Core pulls software and content from GSS and is controlled by Config> System Profile>SystemSettings> Software/Content Update Enabled. B) The Core also pushes logs, malware, and health data to GSS and is controlled by selecting Config>GSS Settings>GSS enabled.
GSS Documents Upload Enabled	Click the checkbox to enable upload of detection data to the GSS [disabled by default]. Checking this box enables uploads of suspected bad Microsoft Office documents and pdf files to GSS when GSS is enabled.
GSS Run Now	Click the Run button to perform an ad hoc update of detection and detonation data to the GSS. Enter Duration in hours for the period of time for which remote access to the Juniper ATP Appliance at the customer site is to be enabled, then click Submit to apply. Note: Maximum duration for enabled Remote Support is 999 hours.

A GSS connection is required in order for the Juniper ATP Appliance to run regular licensing checks.

Remote Support

Remote support allows Juniper Technical Support to SSH into a Juniper ATP Appliance at the customer site to perform troubleshooting activities. To enable Remote Support:

- On the Config>System Profiles>GSS Settings page, click Enable Remote Support.
- Enter Duration in hours for the period of time for which remote access to the Juniper ATP Appliance at the customer site is to be enabled, then click Submit to apply.

Configuring Web Collectors

Use the Web Collectors configuration window to identify, edit, re-configure and/or view settings and status for connected Juniper ATP Appliance Web Collectors.

NOTE Although Web Collectors can be disabled from the Central Manager Web UI, or its settings modified, additional Web Collectors are not “added” via the Central Manager Config>System Profiles>Web Collectors Web UI page. To add a new Web Collector to the distributed defense system, use the instructions in the Juniper ATP Appliance Traffic Collector Quick Start Guide to install the Traffic Collector and then configure it to connect to the Central Manager by setting the CM IP address using Collector CLI commands/configuration wizard. Be sure to also refer to the Juniper ATP Appliance CLI Command Reference for more information.

You must expand rows in the Web Collectors table by clicking on the row arrow to see detailed information. Additional information in expanded rows includes: Collector Name, IP Address, configured interfaces, the date traffic was last seen from this Collector, and Internal Networks and subnets to which the Collector is associated.

Use the Search field to search for Collector details.

Figure 4 Web Collector Configuration Options

The screenshot shows the Juniper ATP Appliance Central Manager Web UI. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar contains various system settings like 'Password Reset', 'Roles', 'Zones', 'Users', 'SAML Settings', 'RADIUS Settings', 'System Settings', 'Certificate Management', 'GSS Settings', 'Web Collectors', 'Email Collectors', 'Secondary Cores', 'Golden Image VMs', and 'Licensing'. The main content area displays a table of Web Collectors. The first row is expanded, showing details for 'PartnerDemo-New-Collector'.

Collector	Hardware	IP address	Description	Zone	Software	Threat Protection	Enable
PartnerDemo-New-Collector	8 CPUs	192.168.1.131	PartnerDemo-New-Collector	Default Zone	4.1.1.13	4.1.1.8	✓
<p>Details for Collector PartnerDemo-New-Collector</p> <p>Name: PartnerDemo-New-Collector Description: PartnerDemo-New-Collector</p> <p>IP Address: 192.168.1.131 Enabled: Yes</p> <p>Interfaces: eth0, eth1 Netmask: 255.255.0.0</p> <p>Last Seen: Oct 18 14:18:26 Eastern Standard Time Install Date: 08/19/15</p> <p>Proxy Inside Addresses: Proxy Outside Addresses:</p> <p>Zone: Default Zone</p> <p>Edit Delete</p>							
PartnerDemo-New-Collector	8 CPUs	192.168.1.170	PartnerDemo-New-Collector	Default Zone	5.0.1.10	5.0.1.6	✓
vcoll149	8 CPUs	10.2.10.149	vcoll149	Default Zone	4.0.1.19	4.0.1.3	✓
demo-next2-core	16 CPUs	192.168.1.122	webcollector	Default Zone	4.1.0.780	4.1.0.156	✓
demonext-xcollector	8 CPUs	192.168.1.164	demo next x collector	Default Zone	4.1.1.13	4.1.1.8	✓
Partner-Collector-Demo-Next	8 CPUs	192.168.1.131	Partner-Collector-Demo-Next	Default Zone	4.0.1.31	4.0.1.8	✓

To view, edit disable/enable, or delete Web Collector and Zone configurations:

1. Navigate to the Config>System Profiles>Web Collectors page.
2. Click the arrow icon for the Collector or Zone configuration to be modified in order to expand the row and display Collector details.

Rows must be expanded to edit configuration information.

3. Click the Delete button to remove a Web Collector configuration from the distributed defense system.
4. Click the Edit button to modify the configuration. For example, to modify a Zone configuration, click the Edit button, then modify the Zone setting by selecting another Zone from the Zone dropdown menu, as shown below.

NOTE To configure zones per MSSP tenant for selection here, refer to [Configuring MSSP Multi-Tenancy Zones on page 107](#).

To configure MSSP tenant-specific Zones:

1. Configure tenants per MSSP and assign Zones.
2. At the Juniper ATP Appliance Central Manager Web UI Config>System Profiles>Zones page, name and describe the MSSP Zones.

3. At the Juniper ATP Appliance Central Manager Web UI Config>System Profiles>Web Collectors page, assign Collectors to a defined Zone.
4. View Zone data from the Juniper ATP Appliance Central Manager Web UI Incidents page.

NOTE To view tenant-specific Zone data and correlation analytics, navigate to the Juniper ATP Appliance Web UI Operations Dashboard and Research Dashboard displays. Generate Reports that include Zone analytics from the Juniper ATP Appliance Web UI Reports tab.

5. Modify other settings in the Edit window as well, as needed (descriptions are provided below, then click Save to apply the revised configuration settings.

NOTE When deleting a Collector using the Web UI, that same Collector cannot be added back because the configuration is disabled in the Central Manager database.

The editable Web Collector fields are defined as follows:

Table 3-1 Editable Web Collector Configuration Options

Name	Juniper ATP Appliance traffic Collector name.
Description	Description of the configured collector, such as Location; for example: San Francisco building - 2nd floor.
IP Address	IP Address of the Collector.
Enabled	Click to checkmark for enabling; remove checkmark to disable the Collector.
Interfaces	The configured interfaces on the Collector for traffic inspection and management network.
Netmask	Collector's IP Address Subnet Netmask.
Last Seen	Date of last seen activity on the Collector.
Install Date	Date Collector was installed.
Proxy Inside Addresses	<p>IP Address of proxy server inside the enterprise network or network segment; configured with the Juniper ATP Appliance CLI collector mode command: JuniperATPHost (collector)# "set proxy inside add <proxy ip> <proxy_port>"</p> <p>Refer to Span-Traffic Proxy Data Path Support on page 70 and the Juniper ATP Appliance CLI Command Reference for more information.</p>
Proxy Outside Addresses	<p>IP Address of proxy server outside the enterprise network or network segment; configured with the Juniper ATP Appliance CLI collector mode command: JATPHost (collector)# set proxy outside add <proxy ip></p> <p>Refer to Span-Traffic Proxy Data Path Support on page 70 and the Juniper ATP Appliance CLI Command Reference for more information</p>
Internal Addresses	IP Address(es) of the internal enterprise subnet(s) to which the Collector is associated.
Zone	Tenant-specific Zone defined per MSSP.

Status of Proxy and deployed Collector: online | off line

Note that the Web Collector page displays the status of the Collector and whether it is operational and online. Use this page to check Web Collector status and Proxy status.

Configuring Email Collectors

Use the Config>System Profiles>Email Collectors configuration window to add, edit, re-configure and/or view settings for Email Servers from which Juniper ATP Appliance Email Collectors will collect email traffic.

NOTE Phishing Correlation requires an Active Directory configuration; see [Configuring Active Directory on page 184](#) for more information. Juniper ATP Appliance Email Collector components are part of the Juniper ATP Appliance Core software service; no physical appliance installation or configuration is required.

Figure 4 Email Collector BCC Settings

The screenshot displays the 'Config' section of the Juniper ATP Appliance interface, specifically the 'Email Collectors' configuration page. The left sidebar contains navigation links: Dashboard, Incidents, File Uploads, Mitigation, Reports, Custom Rules, Config, Notifications, System Profiles, Password Reset, Roles, Zones, Users, SAML Settings, RADIUS Settings, System Settings, Certificate Management, GSS Settings, Web Collectors, Email Collectors, Secondary Cores, Golden Image VMs, and Licensing. The main configuration area is titled 'Email Collectors' and includes a 'Capture Method' section with radio buttons for BCC, JATP MTA Receiver, and Collect from Juniper Cloud. The BCC method is selected. Below this are fields for 'Email Server', 'Protocol' (with options: auto, IMAP, POP3, POP2), 'SSL' (with options: Enabled, Disabled), 'Recipient Email Address' (set to 'juniperdoc'), 'Password' (masked with dots), 'Mail Interval (min)' (set to 5), 'Keep Mail on Server' (with options: Keep, Delete), and 'Enabled' (with options: Enabled, Disabled). A 'Cancel' button is located below these fields. The 'Current Email Collectors' table lists three collectors:

Capture Method	Details	Enabled	Actions
JATP MTA Receiver	MTA Receiver IP: 10.2.118.35 Recipient Email: journal@67.91.204.16 Receive from my Email Servers only: Yes	Yes	Delete Edit
BCC	Email Server: imap.zoho.com Recipient Email Address: email_user2 Protocol: IMAP SSL: Enabled Keep Mail on Server: Delete Poll Interval (min): 1	No	Delete Edit
BCC	Email Server: mail.cyphort.com Recipient Email Address: journal@cyphort.com	No	Delete Edit

At the bottom of the interface, it states 'Powered by Juniper Version 5.0.1.10 Content Version 5.0.1.6' and provides links for 'Support', 'Resources', and 'Contact Us'.

Figure 5 Email Collector Settings - Juniper ATP Appliance MTA Receiver

Current Email Collectors

Capture Method	Details	Enabled	Actions
JATP MTA Receiver	MTA Receiver IP: 10.2.118.35 Recipient Email: journal@67.91.204.16 Receive from my Email Servers only: Yes	Yes	Delete Edit
BCC	Email Server: imap.zoho.com Recipient Email Address: email_user2 Protocol: IMAP SSL: Enabled Keep Mail on Server: Delete Poll Interval (min): 1	No	Delete Edit
BCC	Email Server: mail.cyphort.com Recipient Email Address: journal@cyphort.com Protocol: AUTO SSL: Enabled Keep Mail on Server: Delete	No	Delete Edit

NOTE Juniper ATP Appliance-MTA-Cloud Collectors communicate with the Internet directly and appropriate firewall rules should be created.

Adding a New Email Server

To add a new Email Collector Server to the distributed defense system:

1. Navigate to the Config>System Profiles>Email Collectors page.
2. Click the Add New Email Collector button.

NOTE Advanced Juniper ATP Appliance-MTA Email Collector features require an enabled Juniper ATP Appliance Advanced license. Refer to [Setting the Juniper ATP Appliance License Key on page 142](#) for more information.

3. Enter required information and make configuration selections (descriptions are provided below), then click Save to apply new configuration settings.

Table 3-1 Email Server Settings

Capture Method	BCC, Juniper ATP Appliance MTA Receiver or Collect from Juniper ATP Appliance Cloud.
Email Server	Enter the IP Address or hostname of the Email server from which the Juniper ATP Appliance Core Email Collector will receive journaled or BCC email traffic.
Protocol	Select an email protocol: Auto IMAP POP3 POP2
SSL	Select either Enable or Disable.

Table 3-1 Email Server Settings

Capture Method	BCC, Juniper ATP Appliance MTA Receiver or Collect from Juniper ATP Appliance Cloud.
Email Server	Enter the IP Address or hostname of the Email server from which the Juniper ATP Appliance Core Email Collector will receive journaled or BCC email traffic.
MTA Receiver IP	IP address of the Message Transfer Agent (MTA) Receiver Option: "Receive from my Email Servers Only" [Yes No] If your response is 'Yes', provide the email gateways you are using: Gmail Office365 Local Email Gateway In each case, enter an additional On-Premise Email Gateway Subnet (Comma Separated); providing the subnet is optional for Gmail or Office 365. Note: If you are using both Cloud (i.e Office 365 or Gmail) and on-premise email servers in a hybrid email deployment, then please enter an on-premise email server subnet.
Collector IP	IP address of the Juniper ATP Appliance Collector that is collecting from the Juniper ATP Appliance Cloud. This IP address can be the Core-CM IP address, or a separate standalone MTA Receiver Server IP address.
Recipient Email Address	Enter the Recipient Email Address.
Password	Enter the Email Server mailbox password.
Poll Interval	Enter the polling interval (in minutes); this is the frequency by which the Email Collector polls for email traffic; the default is 5 minutes.
Keep Mail on Server	Select an email retention setting: Keep Delete
Enabled	Choose setting to Enable or Disable the Email Server.

Editing or Deleting Email Server Settings

To edit or delete Email Server settings:

1. Navigate to the Config>System Profiles>Email Collectors page.
2. Click the Edit or Delete button in the Current Email Collectors list.
3. To edit, modify settings and configuration selections (descriptions are provided above), then click Save to apply new configuration settings.

Configuring Mac OSX or Windows Secondary Cores

Use the Secondary Core detection engine configuration window to identify, edit, re-configure and/or view settings and status for connected Juniper ATP Appliance Mac OSX or Windows (Core+CM) Secondary Cores.

NOTE Although a Secondary Core can be disabled from the Central Manager Web UI, or its settings modified, additional Mac OSX or Windows (Core+CM) Cores are not "added" via the Central Manager Config>System Profiles>Secondary Cores Web UI page.

NOTE To cluster or add a new Mac OS X or Windows Secondary Core to the Juniper ATP Appliance distributed defense system, use the instructions in the Juniper ATP Appliance Mac OSX Detection Engine Quick Start Guide or the Juniper ATP Appliance Core/CM Quick Start Guide to install the Mac Mini or Core+CM as a Secondary Core and then configure it to connect to the Central Manager by setting the CM IP

address using CLI commands/configuration wizard.

Be sure to also refer to the Juniper ATP Appliance CLI Command Reference for more information.

NOTE For information about configuring Secondary Cores for Juniper ATP Appliance vCore installations as Amazon Web Services (AWS) AMIs, refer to the Juniper ATP Appliance Virtual Core for AWS Quick Start Guide.

You must expand rows in the Secondary Cores table by clicking on the row arrow to see detailed information. Additional information in expanded rows includes: Mac OSX or Core+CM (Windows) Core Name, IP Address, configured interfaces, and the date traffic was last seen on this Secondary Core Engine.

Use the Search field to search for Secondary Core details.

Table 3-2 Secondary Core Configuration Details

Name	Juniper ATP Appliance Secondary Core name
Description	Description of the configured Secondary Core.
IP Address	IP Address of the Secondary Core.
Enabled	Click to checkmark for enabling; remove checkmark to disable the Secondary Core.
Interfaces	The configured interfaces on the Secondary Core.
Netmask	Secondary Core IP Address Subnet Netmask.
Last Seen	Date of last seen activity on the Secondary Core.
Install Date	Date the Secondary Core was installed.
Internal Addresses	IP Address(es) of the internal enterprise subnet(s) to which the Collector is associated.

The Clustered Core feature allows multiple Core detection engines to run in tandem to support larger networks. Juniper ATP Appliance supports Windows Core+CM device Secondary Cores (in addition to the Mac-Mini Secondary Cores from previous releases).

The installation procedures for clustering are the same installation procedures set for non-clustered devices.

- The first install (perhaps an existing device currently deployed) will be automatically registered as the Primary whenever a second install takes place.
- A second (or additional) Core+CM or Mac-Mini device, when installed, automatically becomes a(nother) Secondary Core.

NOTE Do not change any configuration on the existing Primary device already in use. If all devices are new installations, any device can be the Primary device, and any of the additional devices can be the Secondary Cores. Juniper ATP Appliance supports up to 6 clustered Secondary per Primary installation.

After the installation steps are performed (the steps are provided in the Juniper ATP Appliance Core-CM Quick Start Guide), it will take approximately 10 minutes for the Central Manager services to detect the new Secondary Core(s) and instantiate detection engine processes on those Secondary Core(s). The Central Manager Web UI will then display the new Secondary Core(s) in the Config>System Profiles>Secondary Cores table from which additional clustered Secondary Core management options can take place, as described below.

Refer to the Juniper ATP Appliance Core-CM Quick Start Guide for Juniper ATP Appliance Virtual Core for AWS Quick Start Guide for installation information.

Using the Secondary Core Web UI Config Options

To view, edit disable/enable, or delete Secondary Core configurations:

1. Navigate to the Config>System Profiles>SecondaryCores page.
2. Click the arrow icon for the Mac OSX or Windows (Core+CM) Secondary Core to be modified in order to expand the row and display configuration details.

Rows must be expanded to edit configuration information.

3. Click the Delete button to remove a Secondary Core configuration from the distributed defense system.
4. Click the Edit button to modify the configuration.
5. In the edit window, modify the settings (descriptions are provided below, then click Save to apply the revised configuration settings.

The editable Secondary Core fields are defined as follows:

Table 3-3 Editable Mac OS X Core Configuration Options

Name	Juniper ATP Appliance Mac OSX or Core+CM (Windows) Secondary Core Engine name.
Description	Description of the configured Secondary Core Engine
IP Address & Net Mask	IP Address of the internal enterprise subnets to which the Secondary Core is associated.
Enabled	Click to checkmark for enabling; remove checkmark to disable the Secondary Core.

Status of the deployed Secondary Core: online | off line

Note that the Secondary Core page displays the status of the Collector and whether it is operational and online. Use this page to check Mac OS X or Core+CM (Windows) Secondary Core status.

Figure 4 A Mac OS X Secondary Core Status Display

Secondary Core	Hardware	IP address	Description	Enabled
mac-mini-suba	4 CPUs, Mac OSX	10.2.128.25	swdwd	<input checked="" type="checkbox"/>
Details for Secondary Core "mac-mini-suba":				
Name	mac-mini-suba	Description	swdwd	
IP Address	10.2.128.25	Enabled	Yes	
Interfaces	eth0, eth1	Netmask	255.255.0.0	
Last Seen	2015-10-08 13:41:53.667-07	Install Date	05/09/14	
Edit	Delete			
demo-esx-core1	8 CPUs	192.168.1.100	ESX Cortex	<input checked="" type="checkbox"/>
Details for Secondary Core "demo-esx-core1":		Details for Slave Core		
Name	demo-esx-core1	Description	ESX Cortex	

Configuring Golden Image VMs

Configure a custom VM "Golden Image" to refine threat relevance that is explicitly tuned to your enterprise OS environment. This feature, available from the Central Manager Config>System Profiles>Golden Image VMs page, allows users to define and add their own custom Windows 7 OS images against which malware is analyzed in Juniper ATP Appliance detonation chambers.

Figure 5 Config Tab Golden Image VMs Configuration Page

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules **Config**

Notifications +

System Profiles -

Password Reset

Roles

Zones

Users

SAML Settings

RADIUS Settings

System Settings

Certificate Management

SS Settings

Web Collectors

Email Collectors

Secondary Cores

Golden Image VMs

Licensing

Image Name: Description: VNC ID: Architecture: 32-bit VM Size (GB): 20 Web Protection: YES NO

Network Segment: default

Cancel

Current VM Images

Description	Enabled	Status	Actions
GI - Demo	No	Running, VNC Id: 1	Controls Delete Edit

Juniper ATP Appliance uses its own Windows images in detonation chambers by default, but these default OS images do not always match every enterprise OS environment. Support for a custom VM image (Win7 32-bit and 64-bit) provides every customer with the ability to match detonation against their actual deployed enterprise Win 7 OS environment. Juniper ATP Appliance first runs malware against its detection engine OS images during analysis, and then, in sequence, the potential malware is passed to the Custom Golden Image VM for further analysis and detonation.

NOTE For Virtual Core, the 64-bit Windows 7 Golden Image is available only when the ESXi server and the guest VM (where the Virtual Core is operating) are configured to enable the virtualized hardware-assisted virtualization (VHV). This allows the guest VM (i.e. the virtual core) to be capable of running KVM, which is required for the 64-bit Golden Image). For more information about configuring the ESXi Server and the Golden Image to enable virtualized HV for the outer guest VM, see [Configuring the ESXi Server to Enable Virtualized HV on page 141](#).

With regard to Threat Relevance, if Juniper ATP Appliance's OS images find an object to be malicious, but the custom OS image does not, then relevance is decreased and the risk is reduced for that environment during threat severity calculations.

The customer-defined Golden Image VM can also be used to test confirmed-malicious objects.

CAVEAT Golden Images are limited to .EXE format at this time.

Golden Image VM Config Process

To configure, create a Windows 7 custom image and then interact with that "golden image" using VNC during configuration. Once configured, Juniper ATP Appliance automatically instruments and deploys the custom image for malware analysis and detection.

NOTE Do not use a cloned Windows 7 image during Golden Image installation; a clone image will not work. Required work flow is to insert the correct ISO, open a VNC connection, then follow the Windows 7 OS Image installation prompts.

The Custom Golden Image VM configuration process steps are as follows:

Step 1: Mount the Custom OS ISO location and Boot the VM.

Step 2: Connect to the Custom Golden Image VM via VNC and Install Windows OS.

NOTE During the Windows 7 installation process, Windows performs a required reboot and the VNC connection is dropped. This is expected. Manually restart the VM and reconnect to VNC immediately after losing the VNC during Windows installation.

Step 3: Reboot the VM*

Step 4: Finalize and Enable the custom Golden Image VM.

Step 5: Reconnect to VNC and install Adobe Acrobat, if necessary.

Step 6: Install Preferred AV Software to Golden Image

TIP *TIP: RealVNC cannot connect to the Juniper ATP Appliance Golden Image without first modifying the RealVNC configuration as follows: (1) Navigate to RealVNC "Options"; (2) Disable "Adapt to Network Speed"; (3) Set the Compression Slider to "Best Quality" - "All Available Colors, Minimum Compression".

Step 1: Mount the Custom OS ISO and Boot the VM

1. Navigate to the Config>System Profiles>Golden Image VM page in the Central Manager Web UI.
2. Click the New VM Image button.
3. Enter the settings for the new Windows 7 custom Golden Image VM.

The input fields are described below.

Custom VM Image Configuration Fields	Description
Image Name	Enter the name of the custom VM image you are creating.
Descriptions	Enter a description for the new golden image.
VNC ID	Enter your VNC ID; the ID must be a unique integer.
Architecture	Select 32-bit or 64-bit
Disk Size (GB)	Enter the size of the disk to be used for the custom image. The default is 20 GB.
Risk Reduction	Select a risk reduction setting: yes or no, where "yes" represents a value of 0.3 and "no" indicates a risk reduction value of 0, respectively. The default is No (0). Risk Reduction is factored into the threat relevance metric. If the Golden Image determines that a potential malware object is benign, then the risk reduction is applied as a reduced relevance value

Custom VM Image Configuration Fields	Description
Network Segment	<p>Enter the network segment that is running the OS for which this custom VM Image is being created.</p> <p>Relevance is not calculated if the analyzed malware does not match the network segment configured here.'</p>

4. After entering the custom Golden Image VM settings, click Add to create the image.
5. When the image is displayed in the Current Golden Images VM table, click the Controls link to prepare to install and mount the new custom image.
6. [Optional: To edit the original settings for this new VM Image, click Edit and re-enter the custom image settings information.]
7. Mounting
When mounting the install media for the OS from a file share:
 - › Enter the mount path in the ISO NFS/SMB Mount Path field in the Controls window (be sure you are mounting from an open file share):

SMB Syntax: //<IP Address>/<dir>/<file>

NFS Syntax: i<IP Address>:<dir>/<file>

NOTE Be sure your permission settings allow access to the open file share.

- › Click to checkmark Mount CD ISO at Boot

Click the Boot VM: boot button.

Step 2: Connect to the VM via VNC & Install Windows OS

8. Using your VNC client, connect to the Golden Image VM and perform a typical installation of your enterprise's Windows OS to be used by Juniper ATP Appliance for malware analysis.

NOTE During the Windows installation process, Windows performs a required reboot and the VNC connection is dropped. This is expected. Manually restart the VM and reconnect to VNC immediately after losing the VNC during Windows installation.

Step 3: Reboot the Golden Image VM

9. Return to the Central Manager Web UI Config>System Profiles>Golden Image VM page, select the Controls link for the relevant VM from the Current VM Images table, and then click on Boot VM: boot button again.

Step 4: Finalize and Enable the Custom Golden Image VM

With this next step, Juniper ATP Appliance adapts the configured custom image to the Juniper ATP Appliance analysis and detection architecture, then automatically adjusts the new OS to established firewall settings and installs required drivers, and so on. As part of this process, Juniper ATP Appliance shuts down the VM, so in order to complete the VM image configuration, you must enable the VM in step 12.

10. From the Controls window, and click Finalize Image: finalize.
After you click Finalize, you will be asked to login to the Custom Image VM via VNC and carefully follow the prompts as the Juniper ATP Appliance finalize script runs on the Golden VM Image. The final step of the script will be that the Golden Image VM will be shut down.
11. To complete the configuration of the custom VM image, click Enable Image: enable.

Step 5: Reconnect to VNC to install Adobe Acrobat, if necessary

12. Connect once more to the VNC port and install Adobe Acrobat to the custom OS environment, if necessary.

NOTE The PDF Reader and Adobe Acrobat exe must be mountable.

Step 6: Installing Preferred AV Software to Golden Image

NOTE This step is optional.

Install any preferred AV software by connecting once more to the VNC port for the custom OS Golden Image environment (if not already connected).

In order to ensure that your Golden Image is using the latest AV updates: (1) boot up the Golden Image, (2) VNC to it, and (3) manually trigger the Windows and AV updates. Finalize the Golden Image so that all the changes are saved. This process is essential for installing any software to the Golden Image OS.

IMPORTANT: After installing the AV software, be sure to click the Finalize button in the Controls window one more time to allow the AV software to "whitelist" the Juniper ATP Appliance software. At the end the finalize process, a pop-up query requests that you confirm you do want to whitelist the Juniper ATP Appliance software. Do allow whitelisting of the Juniper ATP Appliance software to prevent it from being blocked.

NOTE If a Golden Image is modified or edited, it must be re-enabled and re-finalized.

TIP MOUNTING A DIRECTORY INTO A GOLDEN IMAGE VM

For Samba drive users, mount from within the Golden Image VM by right-clicking on "Computer" Window, and selecting "Map Network Drive" or "Add a Network Location". No 3rd party software needs to be installed in this case. Thereafter, enter the IP address of the Samba server and share name to run the share and download software for installation into the Golden Image.

For NFS drive users, first enable the "Client for NFS" option in order to mount a drive. This feature is only available on the Windows 7 Ultimate Edition and Enterprise Edition.

NOTE You cannot mount a CD while the Golden Image VM is running. To mount a CD, do this only when booting the VM.

NOTE To connect to a remote Samba server from inside a running VM, you must first whitelist the Samba server's IP address using the CLI command:

```
set firewall whitelist add <samba_server_ip_address>
```

Viewing Custom Image Results

A new row in the Incidents tab Summary table displays Custom VM Image results as "Golden Image."

If three Golden Image VMs have been configured, then three golden image results will show in the Operations Dashboard as well as the Incidents page, as shown below.

Configuring the ESXi Server to Enable Virtualized HV

Configuring an ESXi Server in order to enable Virtualized HV is only suggested for VMWare ESXi version 5.1 and later.

NOTE Be sure that the ESXi is on hardware version 9 or above.

To configure an ESXi Server to enable Virtualized HV:

1. SSH to the ESXi host.
2. In /etc/vmware, edit the 'config' file and add the following setting

```
vhv.enable = "TRUE"
```

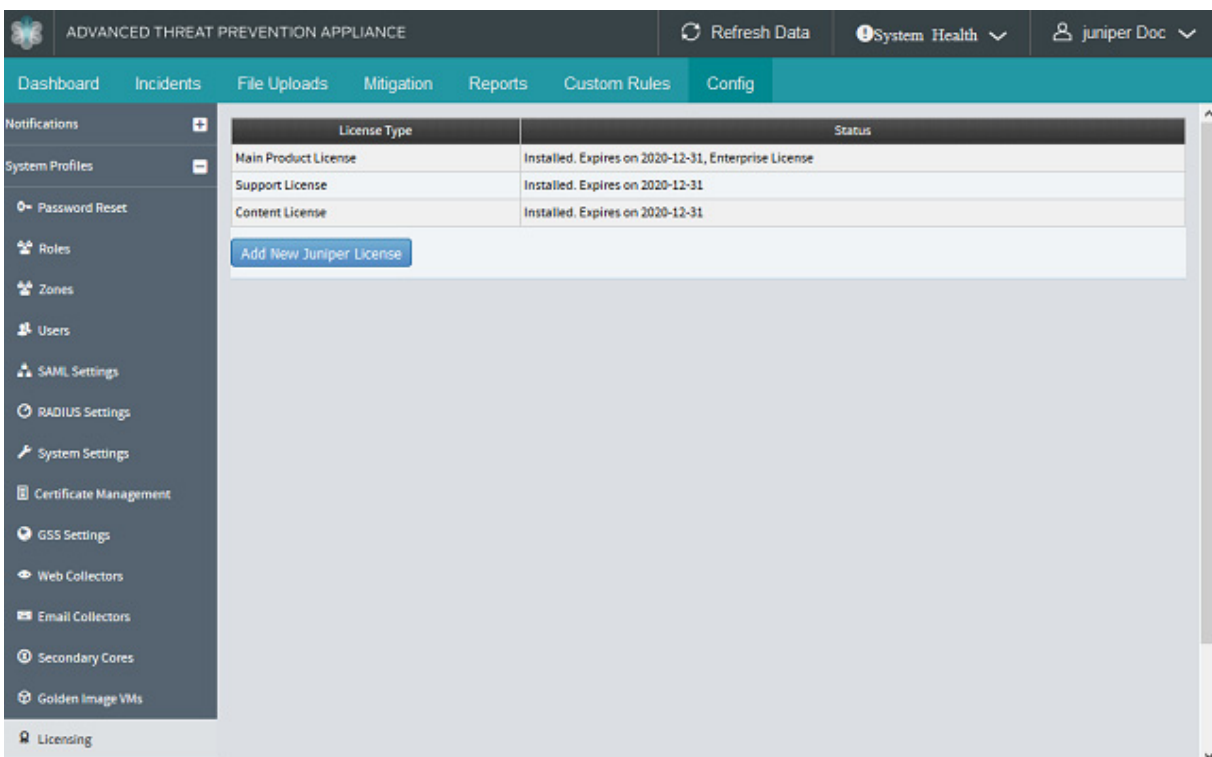
3. Use the vSphere Web Client to configure the guest VM by editing the VM settings via VM settings > Options > CPU/MMU Virtualization.
4. Select the Intel EPT option to complete the configuration.

Setting the Juniper ATP Appliance License Key

Without a valid product license key, the Juniper ATP Appliance system will not work. Likewise, an expired product key, or an expired support or content license, prevents full operations and disables content or software updates.

Use the Config>System Profiles>Licensing configuration window to upload a License key to the Juniper ATP Appliance or software service. To license your system, you will need to upload the license using this configuration window and also use the CLI to get the system UUID.

NOTE License Keys are obtained from Juniper Customer Support.



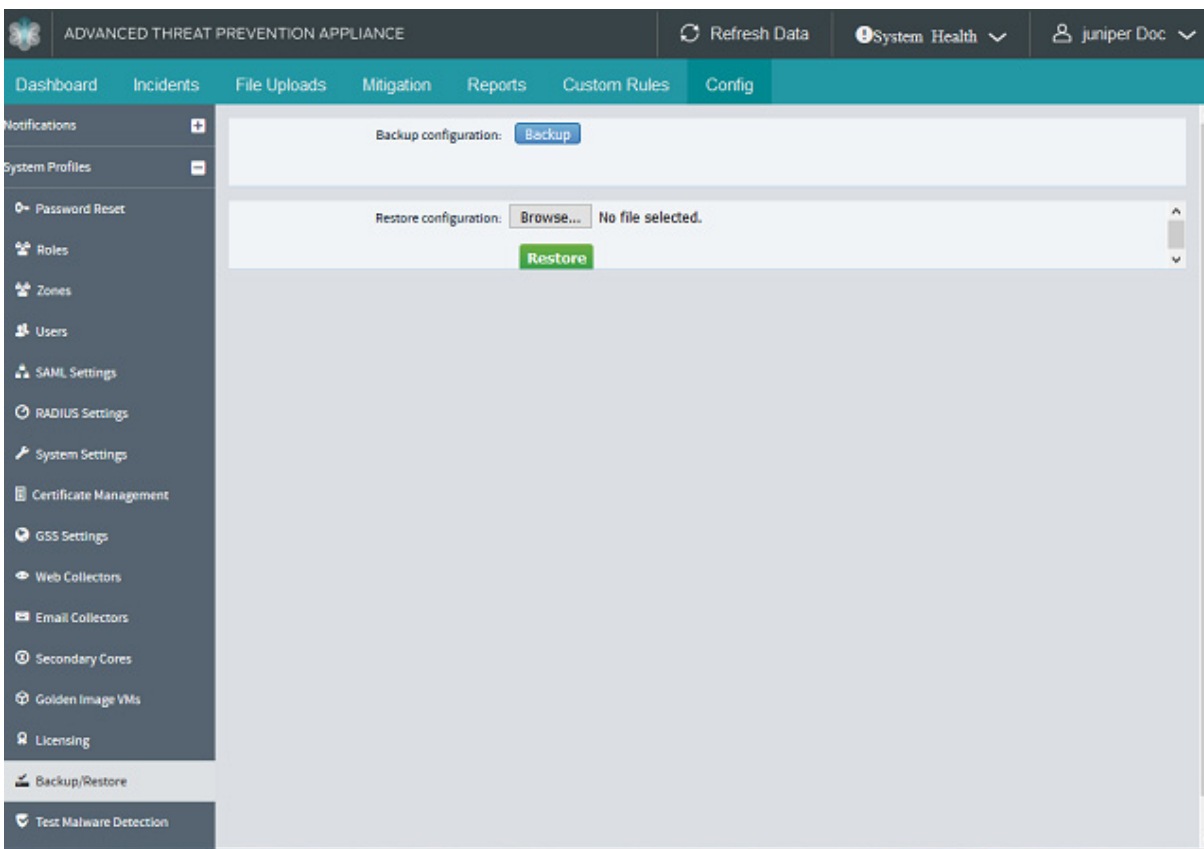
To upload a product license key:

1. Navigate to the Config>System Profiles>Licensing page.
2. Click Add New Juniper ATP Appliance License button to upload a new license key file.
3. Click the Choose File button to select the license key for upload, then click Submit to apply the configuration.

NOTE A GSS connection is required in order for Juniper ATP Appliance to run regular licensing checks. Adding a license manually does not enable JATPSupport.

Configuring Backup and Restore Options

Use the Backup/Restore configuration window to perform a backup of the Juniper ATP Appliance configuration, or restore the system configuration settings from a saved configuration file.



Backing up the current configuration

To backup the current system configuration:

1. Navigate to the Config>System Profiles>Backup/Restore page.
2. Click the Backup button to backup the appliance or software service database.

Restoring a saved configuration

To restore a saved configuration file as the current running config:

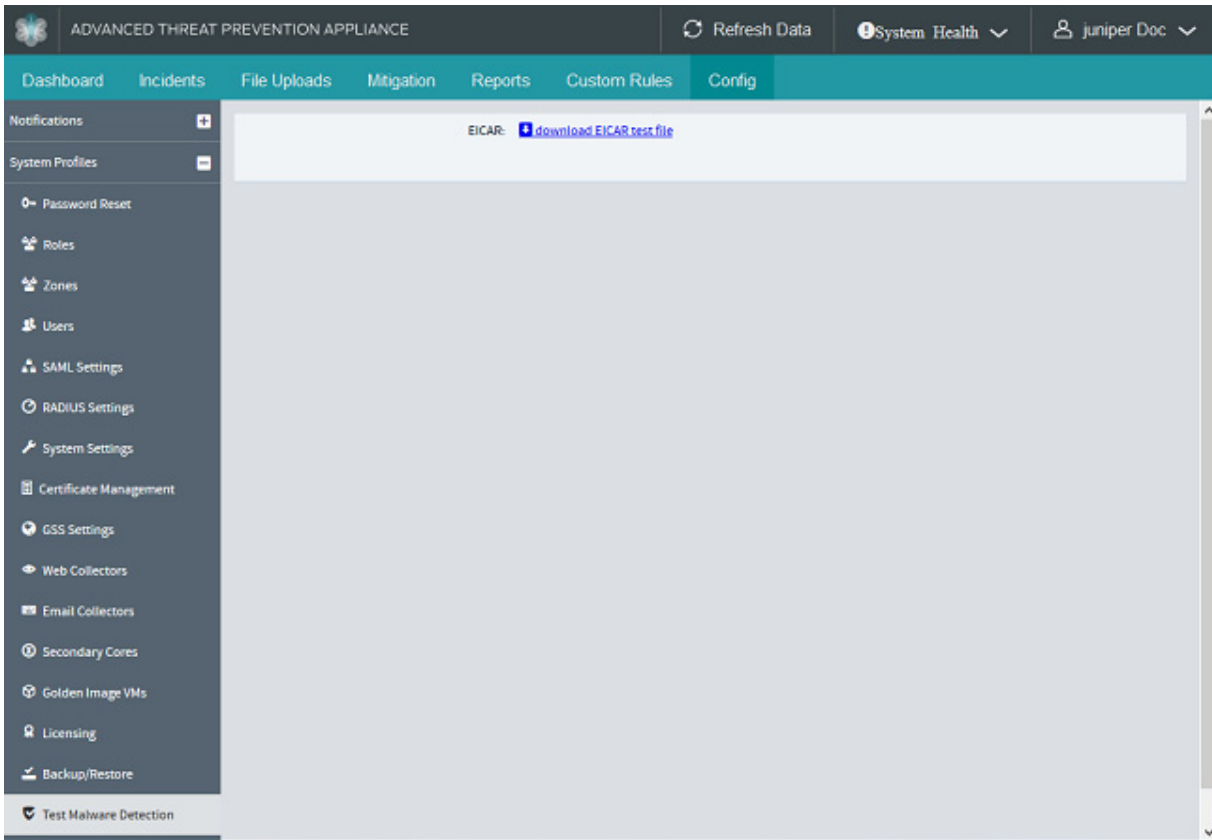
1. Navigate to the Config>System Profiles>Backup/Restore page.
2. Click the Choose File button to select and upload a previously saved configuration file, then click Restore to apply the configuration settings to the appliance or service.

NOTE The backup and restore feature cannot be performed on a CM/Core installation for different major releases. For example, do not restore a previously backup file (generated from a Release 3.2.0 appliance) to a appliance running Release 3.2.0.

Testing Malware Detection Capabilities

Use the Config>System Profiles>Test Malware Detection configuration window to perform a test of the appliance detection and detonation capabilities.

Figure 6 Download Eicar Test Link



To run the EICAR anti-malware test package:

1. Navigate to the Config>System Profiles>Test Malware Detection page.
2. Click the Download EICAR Test File button to download the signature-based EICAR anti-malware test package.
3. Run the EICAR test to confirm Juniper ATP Appliance Core detection capabilities.

Configuring Environmental Settings

Use the Config>Environmental Settings page to configure integration with existing security infrastructure and other security vendors and services.

The following configurations are supported:

- “Configuring Email Mitigation Settings” in the next section.
- Configuring Firewall Auto-Mitigation on page 147
- Configuring Enterprise Network Asset Values on page 163
- Configuring Anti-Virus Integration on page 164
- Configuring Endpoint Integration: CrowdStrike and Carbon Black Response on page 166
- Configuring BlueCoat ProxySG Integration on page 167
- Configuring Whitelist Rules on page 168
- Configuring YARA Rules on page 172
- Configuring Active Directory on page 184

- [Configuring Custom SNORT Rules on page 192](#)

Configuring Email Mitigation Settings

Use the [Config>Environmental Settings>Email Mitigation Settings](#) page to configure Gmail or Exchange Server mitigation quarantine options. These settings allow you to quarantine emails that are detected as malicious by using Office 365 APIs or Gmail APIs:

- ["To configure Gmail Quarantine mitigation settings:" in the next section.](#)
- [To configure Exchange Online Quarantine mitigation settings: on page 146](#)

NOTE All content on the Juniper ATP Appliance email cloud is encrypted; email quarantine options require encryption of email attachments saved on the disk using a Mitigation Key provided by the user. The Juniper ATP Appliance Central Manager includes a form for user-input of the required mitigation encryption key.

To configure Gmail Quarantine mitigation settings:

1. Navigate to Central Manager Web UI [Config>Environmental Settings>Email Mitigation Settings](#) page and select the Gmail as the Email Type.
2. Enter the established Quarantine Label name.
3. Enter an Email Address (for testing the configuration).
4. Enter your full Gmail JSON Key.
5. Click Add to complete the configuration.
6. To edit the quarantine settings, click Edit in the Current Email Mitigations Configured table.
7. To delete a quarantine setting, click Delete in the desired row of the Current Email Mitigations Configured table.

Figure 7 Gmail Quarantine Settings Page

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications System Profiles Environmental Settings

Email Mitigation Settings

Firewall Mitigation Settings Asset Value Anti-Virus Configuration Endpoint Integration Settings BlueCoast Configuration Whitelist Rules YARA Rule Upload SNORT Rule Upload Identity Configuration Splunk Configuration External Event Collectors

Email Type: ☒ Gmail ☐ Exchange Online

Quarantine Label: QuarantinedByJATP

Email Address (for testing):

Email AZURE Key File:

Generate:

Cancel

Current Email Mitigations Configured

Description	Actions
Gmail	Disable Delete Edit Test

To configure Exchange Online Quarantine mitigation settings:

1. Navigate to Central Manager Web UI Config>Environmental Settings>Email Mitigation Settings page and select Exchange Online as the Email Type.
2. Enter the established Authority Host URL.
3. Enter the Office Resource URI.
4. Enter the Tenant ID.
5. Enter the Client ID.
6. Enter the name of the Quarantine Folder.
7. To Generate New Azure Key Credentials, click the Check box.
8. Enter Key Bits; default is 4096.
9. Enter Certificate Lifetime number of days.
10. Enter Azure Manifest Key Credentials.
11. Click Add to complete the configuration.
12. To edit the quarantine settings, click Edit in the Current Email Mitigations Configured table.
13. To delete a quarantine setting, click Delete in the desired row of the Current Email Mitigations Configured table.

Configuring Firewall Auto-Mitigation

Use the Config>Environmental Settings>Firewall Mitigation Settings page to configure auto-mitigation of Juniper ATP Appliance-detected malware at a Palo Alto Network (PAN) Firewall, a Juniper SRX Firewall, a Cisco ASA Firewall, Fortinet Firewall and/or a Check Point Firewall.

Figure 8 Juniper ATP Appliance Auto-Mitigation Configuration Page

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications

System Profiles

Environmental Settings

Email Mitigation Settings

Firewall Mitigation Settings

Asset Value

Anti-Virus Configuration

Endpoint Integration Settings

BlueCoat Configuration

Whitelist Rules

YARA Rule Upload

SNORT Rule Upload

Identity Configuration

Splunk Configuration

External Event Collectors

Mitigation Type:

ASA

Check Point

Fortinet

PAN

SRX

Hostname/IP:

NEXGEN Port Number:

830

SRX Public Key:

juniperdoc

SRX Address/Zone Mode:

Zone Attached

Zone Defined

Address Book or Zone:

Address Set:

Cancel

Current Auto Mitigation Rules

Description	Actions
SRX: 192.168.1.113:830	Disable Delete Edit Test

NOTE This is the Firewall Auto-Mitigation configuration page. Use the Mitigation tab Firewall blocking options to apply configured Auto-Mitigation Rules.

This section has six distinct configuration options:

- Configuring a PAN Firewall - Refer to [Configuring a PAN Firewall on page 148](#).
- Configuring a centralized PANORAMA PAN Firewall management device - Refer to [Configuring a PANORAMA Device for Centralized PAN FW Mitigation Management on page 150](#)
- Configuring a Cisco ASA Firewall - Refer to [Configuring a Cisco ASA Firewall on page 158](#).
- Configuring a Check Point Firewall - Refer to [Configuring a Check Point Firewall on page 162](#).

The PAN firewall will enforce a firewall policy using the PAN OS Dynamic Address Group (DAG) and associated Tag. The DAG is not tied to a fixed IP Address.

Juniper ATP Appliance does not push rules out to PAN; instead, you add or remove addresses from the PAN DAG. From there, you can also instruct PAN to block addresses in the DAG, or perform other actions. The API that provides access to the DAG is available on PAN OS from which users can configure networks of PAN devices.

The Juniper ATP Appliance/Juniper SRX Firewall integration relies on Junos address sets. The Juniper ATP Appliance platform automatically pushes a malicious IP address to an SRX by adding the malicious IP address to one or more configured Junos address sets on the SRX.

Refer to the respective sections for Cisco ASA, Fortinet and Check Point configuration overviews.

About Auto-Mitigation

The Juniper provides comprehensive automatic mitigation at integrated enterprise blocking devices. In previous releases, mitigation intelligence was manually pushed to integrated partner devices to perform threat blocking (except for those partner devices that polled Juniper ATP Appliance, such as Bluecoat, for example). In this release, users configure whether they want mitigation intelligence pushed automatically to blocking devices without user interaction, or whether they prefer to use the manual push option for each mitigation rule distributed to the blocking infrastructure.

Refer to [Configuring Auto-Mitigation on page 122](#) for information about setting and enabling auto-mitigation. When enabling Auto-Mitigation, Juniper ATP Appliance ATA is enabled at the same time.

Configuring a PAN Firewall

Configuration of Juniper ATP Appliance-PAN Firewall integration for auto-mitigation is a two-step process:

1. Configure the Dynamic Address Group and Juniper ATP Appliance-Tag using the PAN Firewall Web UI.
2. Complete the configuration at this [Config>Environmental Settings>Firewall Mitigation Settings](#) page.

Configuring a PAN Firewall Tag

1. From the PAN OS 6.0 Web UI, navigate to the Objects tab and select the Tags page from the left panel menu. Enter a Juniper ATP Appliance-Tag and click OK; example: JATP-tag
2. From the Objects tab, select Address Group from the left panel menu, then click Add to create a new Dynamic Address Group. In the fields provided, enter criteria shown below and click OK.
 - › Name (example: JATP-dag)
 - › Description (example: Juniper ATP Appliance Dynamic Address Group)
 - › Type (example: Dynamic)
 - › Match (example: 'JATP-tag')
3. Navigate to the Policies tab and select the Security from the left panel menu options, then click Add to add a Security Policy Rule.
4. From the Source sub-tab, under Source Address, add the previously created Dynamic Address Group (checkmark JATP-dag, per our example); click OK, then click Commit in the upper right corner of the window.

Configuring a New Auto-Mitigation Rule at the Juniper ATP Appliance CM Web UI

1. Navigate to the [Config>Environmental Settings>Firewall Mitigation Settings](#) page.
2. Click Add New Auto-Mitigation Rule.

NOTE Definitions for each FW Mitigation Setting field are provided further below.

3. Select PAN from the Mitigation Type category and PAN-OS Firewall from the Device Type options.
4. Enter a Hostname/IP, a Host Protocol and a Port Number for the PAN FW device integration.
5. Enter a Username and Password.
6. Enter the Mitigation URL Category and TAG.

TIP If a user wants to change the URL and DAG category, the revised rules does not get triggered into automatic rule pushing. To push into a new category, delete the existing configuration and add a new one.

- Enter the Expire Days and click Add.

Table 3-1 Auto-Mitigation Settings Defined

Mitigate Type	Select PAN-OS to configure an individual PAN FW.
Host IP/URL	IP address or the or FQDN/hostname of the PAN Firewall.
Host Protocol	Select HTTPS or HTTP.
Port Number	Enter the port number of the PAN OS administrative console.
User Name	Enter the admin account username.
Password	The admin account password.
TAG	The Tag that is associated with the configured DAG ("JATP-tag" in our example above).
Mitigation URL Category	Enter URL. This option provides blocking based on URLs to Palo Alto Networks firewalls. URL-based blocking allows more precise blocking control.
Expire Days	Enter the number of days before the rule expires. Expiry days default to 0, which means the rule will not expire.

Implementing an Auto-Mitigation Rule

Apply the configured Auto-Mitigation Rule from the Juniper ATP Appliance Central Manager Mitigation page.

- Select a threat row (or multiple rows) in the Mitigation table and click Apply.
- After clicking Apply, all rules are pushed to the PAN Firewall and will be visible in the PAN Firewall CLI within 10-20 seconds. Multiple rules can be pushed at the same time and all will be reflected in the PAN CLI at the same time.

This is an asynchronous operation so you may continue to push other rules and use other CM Web UI pages as necessary.

Refresh the page after 60 seconds to see a push SUCCESSFUL message for the rows selected.

- A Remove button is available per row pushed for auto-mitigation in the event you need to remove the auto-mitigation rule.

To enable or disable an auto-mitigation blocking rule:

- From the Config>Environmental Settings>Firewall Mitigation Settings page.
- Click Enable or Disable from the Current Auto Mitigation Rules table to enable or (disable) stop forwarding of auto-blocking.

Current Auto Mitigation Rules				
Description	Actions			
ASA : 10.2.128.51; Group: system-test	Enable	Delete	Edit	Test
PAN-OS : https://10.2.10.32:443 Tag: cyph-tag	Disable	Delete	Edit	Test
Panorama : https://10.2.128.75:443 Address Group: cyph-dag	Pending...	Delete	Edit	Test

To delete a PAN FW rule(s) and/or configuration:

1. From the Config>Environmental Settings>Firewall Mitigation Settings page.
2. If there are no rules currently being pushed to the Pan FW, click the Delete option.
3. If rules are currently being pushed, then the Delete option is disabled; click Remove all IP Addresses.

Current Auto Mitigation Rules				
Description	Actions			
ASA : 10.2.128.51; Group: system-test	Enable	Delete	Edit	Test
PAN-OS : https://10.2.10.32:443 Tag: cyph-tag	Disable	Delete	Edit	Test
Panorama : https://10.2.128.75:443 Address Group: cyph-dag	Pending...	Delete	Edit	Test

NOTE In order to delete the PAN FW config, first 'Remove all IP addresses' and then select 'Delete.'

Verifying Auto-Mitigation Rule Operations

1. From the PAN-OS CLI, enter:

show object dynamic-address-group all

Configuring a PANORAMA Device for Centralized PAN FW Mitigation Management

The Juniper ATP Appliance platform monitors and detects malicious IP addresses and the URLs that link to malware. In previous releases, Juniper ATP Appliance's integration with Palo Alto Networks (PAN) firewalls allowed Juniper ATP Appliance to block malicious URLs and IPs by pushing those IP addresses and URLs to individual PAN FW devices. But some enterprises utilize an array of PAN firewalls deployed in various locations. For this reason, Juniper ATP Appliance offers integration with Palo Alto Network's Panorama, a network security management device that controls the distributed network of PAN firewalls from a central location. The Juniper ATP provides the flexibility to either configure integration with individual PAN-OS FWs as usual, or configure integration with a centralized Panorama device as part of Juniper ATP Appliance's Firewall and Secure Gateway auto mitigation options. See [Configuring a PAN Firewall on page 148](#) for individual FW integrations.

The Juniper ATP Appliance/Panorama integration pushes IP address(es) to a firewall Address Group, and it pushes URL(s) to a custom URL category for each configured firewall Device Group. Multiple Device Groups can also be configured.

NOTE Refer to the Palo Alto Networks Panorama documentation for information about configuring centralized Device Groups, Address Groups and associated policies.

Configuring Centralized Panorama Integration

2. Navigate to the Config>Environmental Settings>Firewall Mitigation Settings page.
3. Click Add New Auto-Mitigation Rule.

NOTE Definitions for each FW Mitigation Setting field are provided further below.

4. Select PAN from the Mitigation Type category and Panorama from the Device Type options.
5. Enter a Hostname/IP.
6. Enter a configured Device Group. If there are multiple Device Groups, enter each device group name separated by a space.
7. Enter a Host Protocol and a Port Number for the centralized PANORAMA FW device.

8. Enter a Username and Password.
9. Enter the Mitigation URL Category.
10. Enter an Address Group.
11. Enter the Expire Days and click Add.

Table 3-2 PANORAMA Auto-Mitigation Settings Defined

Mitigate Type	Select Panorama to configure a centralized Panorama management server device.
Host IP/URL	IP address or the or FQDN/hostname of the Panorama device.
Device Group	Enter the Device Group name(s). Multiple device groups can be specified (separated by a character space). Setup Device Group(s) at the Panorama Console from the Manage Devive Groups page; this is where all firewalls in a Panorama firewall network are grouped.
Host Protocol	Select HTTPS or HTTP.
Port Number	Enter the port number of the PAN OS administrative console.
User Name	Enter the admin account username.
Password	The admin account password.
Mitigation URL Category	Enter the URL. This option provides blocking based on URLs to Palo Alto Networks firewalls. URL-based blocking allows more precise blocking control. Juniper ATP Appliance/Panorama pushes URL(s) to a custom URL category for each configured firewall Device Group. Pushes are via the mitigation secure web gateway from Juniper ATP Appliance to the distributed PAN FWs.
Address Group	The group location to which Juniper ATP Appliance pushes IP addresses for PAN blocking. Enter an existing Address group you've created at the Panorama console that is specific to Juniper ATP Appliance. If an Address Group is not specified, PAN will create a new Address Group when the push is executed.
Expire Days	Enter the number of days before the rule expires. Expiry days default to 0, which means the rule will not expire.

Implementing the Auto-Mitigation Rule

Apply the configured Auto-Mitigation Rule from the Juniper ATP Appliance Central Manager Mitigation page.

1. Select a threat row (or multiple rows) in the Mitigation table and click Apply.

NOTE The Apply action pushes the Auto-Mitigation Rule to the Panorama device from which policies are executed on distributed PAN-OS firewalls in a given Device Group.

2. After clicking Apply, all rules are pushed to the PAN Firewalls via Panorama and will be visible in the PAN Firewall CLI within 10-20 seconds. Multiple rules can be pushed at the same time and all will be reflected in the PAN CLI at the same time.

This is an asynchronous operation so you may continue to push other rules and use other CM Web UI pages as necessary.

Refresh the page after 60 seconds to see a push SUCCESSFUL message for the rows selected.

3. A Remove button is available per row pushed for auto-mitigation in the event you need to remove the auto-mitigation rule.

To delete a Panorama rule(s) and/or configuration:

1. From the Config>Environmental Settings>Firewall Mitigation Settings page.
2. If there are no rules currently being pushed to the Panorama device, click the Delete option.
3. If rules are currently being pushed, then the Delete option is disabled; click Remove all IP/URL Addresses.

Current Auto Mitigation Rules				
Description	Actions			
ASA : 10.2.128.51; Group: system-test	Enable	Delete	Edit	Test
PAN-OS : https://10.2.10.32:443 Tag: cyph-tag	Disable	Delete	Edit	Test
Panorama : https://10.2.128.75:443 Address Group: cyph-dag	Pending...	Delete	Edit	Test

NOTE In order to delete the Panorama config, first 'Remove all IP/URL addresses' and then select 'Delete.'

Verifying Auto-Mitigation Rule Operations

1. From the CLI of each individual PAN-OS firewall in the Panorama Device Group, enter the following command to verify operations:

```
show object dynamic-address-group all
```

Configuring Juniper SRX Firewall Mitigation

Juniper provides mitigation integration with the Juniper SRX Firewall. When the Juniper ATP Appliance platform pushes a malicious IP address to an SRX, that IP address is added to one or more configured Junos address sets on the SRX. This section describes that configuration.

An SRX network administrator configures Junos policies on the SRX that deny access or monitor traffic involving specific address sets; these address sets, either zone-defined or zone-attached, will contain all malicious IP addresses detected by Juniper ATP Appliance.

An SRX administrator configures standard Junos address sets and policies to contain malicious IP addresses reported by Juniper ATP Appliance for mitigation; anything from the mitigated address is to be blocked (moved from trusted to untrusted per policy). The administrator must configure policies that will appropriately handle traffic on the configured mitigation address sets. The next section describes how to configure the Juniper ATP Appliance platform to identify the SRX mitigation address set(s).

TIP JUNOS SRX ADDRESS BOOKS & ADDRESS SETS

In Junos, address sets are nested inside an address book. Detailed descriptions of address sets and books can be found in the Junos documentation. In general, an address book is the set of all possible addresses and host names that might appear within a security zone. An address set is a user-configurable subset of an address book. An address book can contain multiple address sets, and an address set can contain multiple addresses.

An address set can be configured as either Zone-Attached (Global) or Zone-Defined.

- Zone-Defined address sets (also sometimes referred to as Zone-Specific) are configured on SRX systems running version 11.2 or earlier for a specific zone. A Zone-Defined address set uses 1 default address book per zone; in zone-defined configuration mode, each security zone has a single unnamed address book. Address sets are defined within this zone-specific address book. The SRX uses the name "address book" as the default name for Zone-Defined address sets. A trusted zone is user-configured, and an untrusted zone is typically represented by the internet and unknown servers.

- Global or Zone-Attached or Zone-Defined address sets can be configured for SRX systems running version 11.2 or later; in addition to the newer zone-attached configuration mode, Junos versions 11.2 and later also support the legacy zone-defined configuration mode. For Zone-Attached address set configurations, the admin must specify both the address book or zone as well as the address set. The syntax for global zone-attached address sets differs from zone-defined. See TIP examples below.

TIP When choosing an SRX address book mode as Zone Attached, specify the address book name in the “Address Book or Zone” input field in the CM Web UI, and the Address Set in the “Address Set” input field. The address-set containing a dummy IP address must be created under the address-book at the SRX CLI. For example:

```
1. Address-book book1 with address-set asset
Address Book or Zone : book1
Address-set : asset

2. Address-book global with address-set asset
Address Book or Zone : global
Address-set : asset
```

If choosing an SRX address book mode as Zone Defined, specify the zone name in the “Address Book or Zone” input field, and the address set in the “Address Set” input field. The address-set containing a dummy IP address must be created under the address-book for that zone at the SRX CLI.

You can create multiple entries (one for each zone) by separating the zones and address-sets with a space. For example: If you want to push several IP addresses to zone “untrust1” with address-set “asset1” and zone “untrust2” with address-set “asset2”, be sure to configure:

```
Address Book or Zone : untrust1 untrust2
Address-set : aset1 aset2
```

Configuring Security Policy Address Sets at the SRX CLI

The tasks to be completed at the SRX before configuration of SRX integration from the Juniper ATP Appliance Web UI are listed below:

1. Configure Zone based address book and address set security policies, as needed:

Zone-Defined Example with Syntax descriptions:

```
set security zones security-zone <JATP-Zone-name> address-book address
Customer_addr 0.0.0.0/32

set security zones security-zone <JATP-Zone-name> address-book address-set
<JATP-addressSet> address Customer_addr
```

2. Configure Zone attached address book and address set security policies, as needed:

Zone-attached Global Example:

```
set security address-book global address-set <JATP-addressSet> address
Customer_addr

set security address-book global address Customer_addr 0.0.0.0/32

set security address-book global address-set Customer_addressSet address
Customer_addr
```

Zone-attached User Defined Example:

```
set security address-book <JATP-book> address-set <JATP-addressSet> address
```

Customer_addr

...where <JATP-book> is the address-book (configured in “Address Book or Zone” in the Juniper ATP Appliance Web UI, and <JATP-addressSet> is the address-set configured in the “Address Set” field.

```
set security address-book <JATP-book> address Customer_addr 0.0.0.0/32
```

```
set security address-book <JATP-book> address-set <JATP-aset> address Customer_addr
```

NOTE Juniper ATP Appliance only pushes malicious IP addresses to the address-sets configured at the SRX CLI. An admin must configure the policies on the SRX to block connections going to the those malicious IP addresses. For example:

```
set security policies from-zone Internal to-zone Internet policy Customer_deny
match source-address any
set security policies from-zone Internal to-zone Internet policy Customer_deny
match destination-address <JATP-addressSet>
set security policies from-zone Internal to-zone Internet policy Customer_deny
match application junos-http
set security policies from-zone Internal to-zone Internet policy Customer_deny then
deny
```

3. Move to the Juniper ATP Appliance Web UI to configure SRX integration.

- › For instructions on setting a zone-defined address book configuration, see [Defining a Zone-Defined SRX Configuration at the Juniper ATP Appliance Web UI on page 154](#) in the next section.
- › For instructions on setting a zone-attached address book configuration, see [Defining a Zone-Attached SRX Configuration at the Juniper ATP Appliance Web UI on page 157](#).
- › For information about generating an SSH Key Pair, see [Generating an SRX SSH public/private key pair on page 156](#).
- › For information about monitoring SRX firewall activity, see [Viewing SRX Activity from the Juniper ATP Appliance Mitigation Tab on page 156](#).

Defining a Zone-Defined SRX Configuration at the Juniper ATP Appliance Web UI

Configuring Zone-Defined SRX mitigation is a two part process:

- Use the SRX CLI to specify the security zone and address set(s).
- Use the Juniper ATP Appliance Web UI to configure SRX mitigation integration.

To configure a Zone-Defined SRX integration:

1. Configure security policies as either zone-defined or global zone-attached by defining address book/address sets at the SRX CLI; for example:

Figure 4 Sample SRX CLI Configuration Example

```

set security policies from-zone Internal to-zone Internet policy Customer_deny then deny
insert security policies from-zone Internal to-zone Internet policy Customer_deny before policy All_Internal_!
4. Config => Env settings => SRX
5. Ready to push IP => show tat packet is allowed
6. Push , then refresh
7. Goto srx => show security address-book
8. Goto client and get page again
9. remove ip
10. show in srx that removed
clear security policies hit-count
show security policies hit-count

2. Workflow
1. load base config
2.
SSH-key:
set system login user admin class super-user
set system login user admin authentication ssh-rsa "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCSsHajm5L/kZxP3gPDDGY1/aVzQVhhU110oE06Uo+6501tLAYdI2hNTJ/JAa5JJJKpGga80x8UzY4U/
k9fkikF19CVEXg0DkEP+OdUY38g9BJDno2bgIfrh3dmsJ8zn/yo319i+e6+
c2klk8NA9Q2i8B0EbaueScSkaQuRQ5x5ii8IoK7wm5P39I6UNXFTHeQ7vyjXA/
uH182qVhcnkohlA15bXPTW4qNV859jElmY5UHLpQ6EzWle5Qj1BOIF0glyyHv2gR2QAmEaJ2H2eg1KEu6NDbJyh9OQNOI13KOAIF1QfKmk
xaQVebaQwJH69b5idjTDNR Auto-generated by Cyphort for SRX integration. ID: 71801C38-C22E-438C-88EA-2922AF1F6A

set security zones security-zone Internet address-book address Customer_addr 0.0.0.0/32
set security zones security-zone Internet address-book address-set Customer_asset address Customer_addr
3.
set security policies from-zone Internal to-zone Internet policy Customer_deny match source-address any
set security policies from-zone Internal to-zone Internet policy Customer_deny match destination-address Cust
set security policies from-zone Internal to-zone Internet policy Customer_deny match application junos-http
set security policies from-zone Internal to-zone Internet policy Customer_deny then deny
insert security policies from-zone Internal to-zone Internet policy Customer_deny before policy All_Internal_!
4. Configure SRX
5. Push rule
6. show security zones

```

2. Navigate to the Config>Environmental Settings>Firewall Mitigation Settings page in the Juniper ATP Appliance Central Manager Web UI and select SRX.
3. Enter the SRX Host name or IP address. at the Host name/IP field.
4. Enter the NETCONF Port Number to allow login to the SRX: 830.

NOTE The NETCONF port number is configured on the SRX and the defined port number is entered at the Juniper ATP Appliance Web UI Config NETCONF Port Number field.

5. Enter the username and password for SRX login at the User Name and Password fields.

NOTE There are two modes available for logging into the SRX: username and password configuration, or SSH Key and secret passphrase (the SSH secret passphrase is the password defined in the Password field in column 2). To configure an SSH public/private key pair, refer to the section [Generating an SRX SSH public/private key pair](#) below.

6. Enter the number of days before automatic deletion of mitigated IP addresses [0 days indicate addresses should never be deleted] in the Expire Days field.
After the number of days set for expire, the IP address will be removed automatically from the SRX.
7. Select Zone Defined for address set configuration in the SRX Address Book Mode area. The sample configuration mode shown below is Zone Defined.
8. Define the zone in the Address Book or Zone field (address book is for Zone-Attached sets, and Zone is for Zone-Defines sets); in the example above, the Zones are set as “trusted” and “untrusted” for our Zone-Defined configuration.
9. Define the address set(s) at the Address Set field; in our example, we have defined “asset1” and “asset2” per our SRX policy.
10. Click Save. Or, if you want to generate an SSH Key, follow the steps immediately below.
11. In the Current Auto-Mitigation Rules table, locate the SRX configuration you just saved and click the Test link to verify SRX integration.
12. Click Edit to modify the configuration settings, or Delete to remove the configuration.

13. The following is an example of the information Juniper ATP Appliance pushes to the SRX for Zone-Defined firewall mitigations:

Sample Syntax for a Zone Defined Mitigation named "trust":

Example : Pushing IP address 31.170.165.131 to SRX

```
set security zones security-zone trust address-book address JATP-AUTO-GENERATED-ADDRESS-31.170.165.131 31.170.165.131/32
```

```
set security zones security-zone trust address-book address-set asset1 address JATP-AUTO-GENERATED-ADDRESS-31.170.165.131
```

Viewing SRX Activity from the Juniper ATP Appliance Mitigation Tab

To monitor SRX mitigation operations at the Juniper ATP Appliance Web UI, navigate to the Mitigation tab to view firewall mitigation activity:

ADVANCED THREAT PREVENTION APPLIANCE										
Refresh Data System Health juniper Doc										
Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config										
IP Filtering URL Filtering IPS Signatures Endpoint Infection Verification Emails										
Search										
	Push to Device	Severity	Confidence	Owner	Threat	Threat Source	Malware IP	Threat Target	Detection Date	Status
<input type="checkbox"/>	Enabled	Medium	Max	cyadmin	malvertising	Juniper Labs	23.254.165.61		Sep 2 20:11:54 Eastern Standard Time	
<input type="checkbox"/>	Disabled	Medium	Max	JATP	malvertising	Juniper Labs	89.44.47.210		Sep 2 20:11:54 Eastern Standard Time	
<input type="checkbox"/>	Enabled	Medium	High	cyadmin	VIRUS:WIN32_SALITY_AU.CY	Local	108.179.219.135	10.1.7.197	Sep 9 13:13:55 Eastern Standard Time	
<input type="checkbox"/>	Enabled	Max	High	gsuzuki	TROJAN_Fareit.CY	Local	115.47.49.181	10.1.0.33	Apr 21 03:55:46 Eastern Standard Time	
<input type="checkbox"/>	Disabled	Medium	High	JATP	VIRUS:WIN32_SALITY_AU.CY	Local	122.155.168.149	10.1.7.197	Sep 9 13:13:55 Eastern Standard Time	
<input type="checkbox"/>	Enabled	Medium	High	cyadmin	TROJAN_ZeroAccess.CY	Local	173.193.250.103	10.1.7.132	Sep 8 01:13:57 Eastern Standard Time	
<input type="checkbox"/>	Disabled	Medium	High	JATP	TROJAN_ASKTOOLBAR.CY	Local	18.23.92.114	ny_demo_175	Mar 7 13:12:40 Eastern Standard Time	
<input type="checkbox"/>	Enabled	Medium	High	USER	TROJAN_ASKTOOLBAR.CY	Local	183.44.23.12	sample_61	Feb 10 18:55:12 Eastern Standard Time	
TROJAN_Trojan.CY										Mar 15 16:54:36 Eastern Standard Time

When a policy is in the process of being applied, an administrator may note that the message in the Mitigation page for that operation states "Pending Apply":

To remove a blocking rule, click Delete in the Config to remove a blocking configuration.

Generating an SRX SSH public/private key pair

- To generate an SSH public/private key pair, create or edit the SRX configuration.
- Check Enabled as well as the Generate New SSH Key Pair checkboxes.

3. Click Save.
4. Click Edit in the Current Auto-Mitigation Rules table to open that same SRX configuration; the new SSH public key is displayed in the window:
5. Copy the generated SSH public key and paste at SRX CLI to configure the SRX accordingly; for example:

```
set system login user admin authentication ssh-rsa "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQAC8gjrdWo5dpOHT+PtliV1N6rV4nBTdTE12zQdZSqqbBo
OBWe....."
```

NOTE The SSH secret passphrase used by the Key is the password defined in the Password field in column 2.

Defining a Zone-Attached SRX Configuration at the Juniper ATP Appliance Web UI

Similar to setting Zone-Defined SRX mitigation, Zone-Attached SRX integration is a two part process:

- Define a custom address book and attach the address book to one or more zones using the SRX CLI.
- Use the Juniper ATP Appliance Web UI to configure SRX mitigation integration.

To configure a Zone-attached policy from the SRX (to be performed by the SRX administrator):

1. Using the SRX CLI, create an address book "Customer_addressbook" and address-set "Customer_addressSet" with an IP that will not be removed.
2. Attach the address-book to one or more zones.
3. Move to the Juniper ATP Appliance Central Manager Web UI to integrate with the SRX zone-attached address book and address sets.

To configure Zone-Attached SRX integration from the Juniper ATP Appliance Central Manager Web UI:

4. Navigate to the Config>Environmental Settings>Firewall Mitigation Settings page in the Juniper ATP Appliance Central Manager Web UI and select SRX.

NOTE In SRX Firewalls running Junos version 11.2 or later, zone attached methods use a "global" address book that is always defined and is always (implicitly) attached to every security zone. If an admin chooses to specify an address set in this global address book, they can just type the word "global" in the address book name field. (this is the default address book's actual name). The "global" address book is a special address book named "global" and should be referenced as such in the Juniper ATP Appliance Web UI for zone-attached configurations if that book is the one to be used in the configuration. In our example, we use an address book named "trust."

5. Enter the SRX Host name or IP address. at the Host name/IP field.
6. Enter the NETCONF Port Number to allow login to the SRX: for example, 830.

NOTE The NETCONF port number is configured on the SRX and the defined port number is entered at the Juniper ATP Appliance Web UI Config NETCONF Port Number field.

7. Enter the username and password for SRX login at the User Name and Password fields.

NOTE There are two modes available for logging into the SRX: username and password configuration, or SSH Key and secret passphrase (the SSH secret passphrase is the password defined in the Password field in column 2). To configure an SSH Key, refer to the section [Generating an SRX SSH public/private key pair](#).

8. Enter the number of days before automatic deletion of mitigated IP addresses [0 days indicate addresses should never be deleted] in the Expire Days field.
9. Select Zone Attached for address set mitigation configuration in the SRX Address Book Mode area. The sample configuration mode shown below is Zone Attached.

10. Define the Address Book Name in the Address Book or Zone field (address book is for Zone-Attached sets, and Zone is for Zone-Defined sets); in the example above, the Address Book is set as “trust” for our Zone-Attached configuration example.
11. Define the address set(s) at the Address Set field; in our example, we have defined “asset2” per our SRX policy.
12. Click Save. Or, if you want to generate an SSH Key, follow the steps in the section [Generating an SRX SSH public/private key pair on page 156](#).
13. In the Current Auto-Mitigation Rules table at the bottom of the Config>Environmental Settings>Firewall Mitigation Settings page, locate the SRX configuration you just saved and click the Test link to verify SRX integration.
14. Click Edit to modify the configuration settings, or Delete to remove the configuration.
15. The following is an example of the information Juniper ATP Appliance pushes to the SRX for Zone-Attached firewall mitigations:

Example :

Pushing IP address 31.170.165.131 to SRX

Sample Syntax for “Global” Address Book and Address Set Zone Attached Mitigation:

```
set security address-book global address JATP-AUTO-GENERATED-ADDRESS-31.170.165.131 31.170.165.131/32

set security address-book global address-set asset2 address JATP-AUTO-GENERATED-ADDRESS-31.170.165.131
```

Sample Syntax for User Defined Address Book and Address Set Zone Attached Mitigation:

```
set security address-book book1 address JATP-AUTO-GENERATED-ADDRESS-31.170.165.131 31.170.165.131/32

set security address-book book1 address-set asset2 address JATP-AUTO-GENERATED-ADDRESS-31.170.165.131
```

Configuring a Cisco ASA Firewall

With integrated Cisco ASA Firewall support, enterprises with deployed ASA Firewalls are able to push IP addresses from Juniper ATP Appliance products to the Cisco ASA Firewall platform for malware blocking. Juniper ATP Appliance uses a REST interface to communicate with the ASA Firewall.

TIP To perform Cisco ASA Firewall integration, an ASA Administrator must download and enable the REST API Agent from <http://www.cisco.com> --note that downloading requires a valid Cisco service contract. The “Cisco ASA REST API Quick Start Guide” is available online. Be sure to review the “ASA REST API Compatibility” section of the “Cisco ASA Compatibility” document to determine if the REST API is supported on a particular ASA hardware platform.

Cisco ASA Firewall Configuration

A Cisco ASA administrator must configure a “network object group” on the ASA. Note that multiple network object groups are a “hidden” feature on the ASA Firewall.

Cisco ASA Firewall Configuration Example:

Here is a sample ASA configuration:

```
(config)# object-group network JATP-BLOCK
(config-network)# network object host 1.1.1.1

(config)# access-list 101 extended deny ip object-group JATP-BLOCK any
```

NOTE This configuration requires a “dummy” IP address to allow for configuration of the network object group. An identical requirement is required for the SRX integration strategy.

Juniper ATP Appliance ASA Firewall Configuration

Navigate to the Config>Environmental Settings>Firewall Mitigation Settings page to configure auto-mitigation of Juniper ATP Appliance-detected malware at a Cisco ASA Firewall.

To configure the ASA Firewall, use the following procedure:

1. Select ASA from the Mitigation Type column.
2. Enter the firewall hostname or IP address in the Hostname/IP field.
3. Enter the firewall Port Number if different than the default 443.
4. Enter the administrator User Name and Password.
5. Enter the Network Object Group as configured on the ASA firewall.
6. Enter the Expiry number of days for the connection; the default is 60 days.

Configurations at the FortiManager Console

Begin by applying this required configuration on FortiManager before configuring the Juniper ATP Appliance device:

```
Enable rpc_permit read/write:

# config system admin user
(user)# edit admin

(admin)# show
config system admin user
  edit "admin"
    set profileid "Super_User"
    set adom "all_adoms"
    set policy-package "all_policy_packages"
    config meta-data
      edit "Contact Email"
      next
      edit "Contact Phone"
      next
    end
    set rpc-permit read-write
    config dashboard
      edit 1
        set name "System Information"
      end
  end

config system admin user
edit <user>          <-- replace <user> with the account name
set rpc-permit read-write
next
end
```

At the FortiManager console, create the following:

- An ADOM (Administrative Domain) that also needs to be enabled. Once an ADOM is created the ADOM name is needed for JSON RPC requests
- An Address Group must be created with at least one IP address (dummy) even before the Juniper ATP Appliance adds any additional IP addresses.

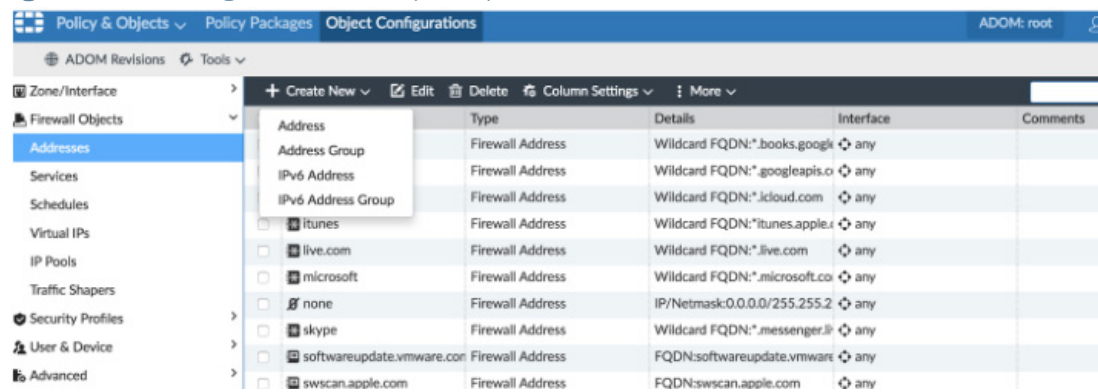
- Webfilter Profile (optional) needs to be created, and URL filtering needs to be enabled as shown in the sections immediately below.

NOTE An Address Group name (if specified) is used to push blocking information for IP addresses. The Webfilter Profile name (if specified) is used to push blocking information for URLs. While these two parameters are optional, at least one --an Address Group or Webfilter name-- must be specified. An error message is displayed if neither is specified.

- Create a Policy package (optional). If specified, policies are installed (pushed) to all the FortiGates listed as Installation Targets in the policy package. If the policy package name is not configured on the Juniper ATP Appliance, it will not push or install these policies to FortiGates and such an install would then need to be done manually or via other means (for instance, by running custom scripts according to a schedule).

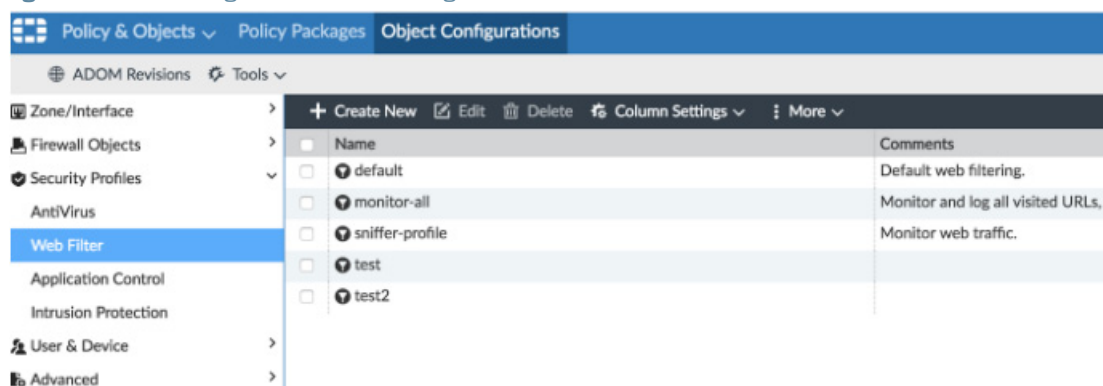
FortiManager requires that IP addresses be added to a common pool of 'Addresses' and these addresses can be added to an address group. When creating an address group at the FortiManager console, be sure you specify at least one IP address in that group. See menu below.

Figure 5 FortiManager Address Group Setup



You also need to create a Web/Filter Profile at the FortiManager console, under which its possible to add URLs for blocking.

Figure 6 FortiManager Web Filter Configuration



In the FortiManager webfilter profile, the URL filter must be enabled. All URLs to be blocked will be pushed to this URL filter from the Juniper ATP Appliance.

Figure 7 Enabling the URL filter at the FortiManager

Edit Webfilter Profile

Name: test

Comments: Write a comment (0/255)

Advanced Options

Inspection Mode: ☒ Proxy ☐ Flow Based ☐ DNS

☐ Log all URLs

☐ FortiGuard Categories

☐ Allow Blocked Override

Search Engines

☐ Search Engine Safe Search - Google, Yahoo!, Bing, Yandex

☐ YouTube Education Filter

☐ Log all search keywords

Static URL Filter

☐ Block Invalid URLs

☒ Enable URL Filter

Create Delete

URL	Type	Action	Referrer Host	St

Also required for Fortinet FW and FortiManager integration is a Policy Package with policies that reference the address group and webfilter name created for integration. Specify the installation targets (fortigate devices) to which this policy package is to be installed.

Figure 8 Setting a FortiManager Policy Package

Policy Packages

Policy Package Install ADOM Revisions Tools

default

- IPv4 Policy
- IPv4 Interface Policy
- Installation Targets

trial1

- IPv4 Policy
- IPv4 Interface Policy
- Installation Targets

Create New Edit Delete Section Column Settings Section View Global View

Seq.#	Name	From	To	Source	Destination
1	policy_test1	any	any	Detected_BLOCK_IPs	all
2	Implicit Deny	any	any	all	all

Configurations at the Juniper ATP Appliance Central Manager

To configure the Fortinet Firewall and management platform, use the following procedure:

1. Select Fortinet from the Mitigation Type column.
2. Enter the firewall hostname or IP address in the Hostname/IP field.
3. Enter the administrator User Name and Password.
4. Enter the Address Group as configured on the Fortinet firewall.
5. Enter the Web/Filter Profile name as configured on the Fortinet firewall.

NOTE An Address Group name (if specified) is used to push blocking information for IP addresses. The Webfilter Profile name (if specified) is used to push blocking information for URLs. While these two parameters are optional, at least one --an Address Group or Webfilter name-- must be specified. An error message is displayed if neither is specified.

6. If configuring the FortiManager platform, click FortiManager and additional fields are displayed.

NOTE Juniper ATP Appliance Fortinet integration supports FortiManager version 5.4 or later.

7. Enter the Administrative Domain name (ADOM) configured for the FortiManager.
8. Enter the Policy package name, also configured at the FortiManager.
9. Click Add to finalize the configuration.

FortiManager is the manager of FortiGate devices and offers JSON-RPC API based access for configuration. The Juniper ATP Appliance uses these APIs.

Configuring a Check Point Firewall

Configured Check Point Firewall integration allows Juniper ATP Appliance products to communicate and perform threat mitigation in concert with Check Point firewalls. A Juniper ATP Appliance administrator can choose to block a particular threat or remove a previously propagated mitigation via Check Point Firewall integration. Communication takes place via the SSH interface through which Check Point users may also access the CLI of the Check Point device.

Blocking information is submitted using Check Point APIs. By pushing malicious IP addresses to integrated Check Point appliances, similar to Juniper ATP Appliance's established PAN and Juniper integration support, an administrator identifies threats at the Firewall or Secure Web Gateway, and submits the selected objects to the configured Check Point Firewall from the Central Manager Web UI.

NOTE Check Point Firewall integration requires Check Point GAiA operating system release R76, R77, or later. Check Point IPSO and Secure Platform (SPLAT), which are predecessors of GAiA, are not supported.

Configuring and Deploying the Check Point Firewall

A Juniper ATP Appliance product propagates malicious IP addresses to Check Point appliances using the Check Point Suspicious Activity Monitor (SAM) feature. SAM status and commands are available under the "SmartView Monitor" app in the Check Point "Smart Console" family of Web UI applications.

Deploying Check Point GAiA appliances involves configuration of Security Management Servers and Security Gateways. In standalone configurations, the Security Management Server and the Security Gateway are installed on the same machine. In distributed configurations, a single Security Management Server can manage a number of subordinate Security Gateways.

Juniper ATP Appliance supports both standalone and distributed Check Point deployments. In either case, the Juniper ATP Appliance must be configured with the IP address of the Check Point Security Management Server.

Unlike other integrations, no address group or similar object need be configured. With Check Point, an administrator can choose to drop or reject connections to the mitigated IP, and either close or maintain existing connections. These choices are selected during Juniper ATP Appliance configuration of Check Point integration.

Juniper ATP Appliance firewall blocking corresponds to Check Point CLI SAM commands, as follows:

```
fw sam -J any <blocked_address>
# Drop and close

fw sam -C -i any <blocked_address>
fw sam -C -j any <blocked_address>

fw sam -s <sam_server> -S <SIC_name> -f
<fw_host> -[ i | j | I | J ] any
<blocked_address>
```

```
fw_host can be All, localhost, Gateways, or a group or object name
fw sam -s <sam_server> -S <SIC_name> -f
      <fw_host> -C -i any <blocked_address>
fw sam -s <sam_server> -S <SIC_name> -f
      <fw_host> -C -j any <blocked_address>
```

The Check Point “FW SAM CLI Reference” guide is available online.

Configuring Juniper ATP Appliance Integration with Check Point

To configure Check Point Firewall integration:

Navigate to the Config>Environmental Settings>Firewall Mitigation Settings page to configure auto-mitigation of Juniper ATP Appliance-detected malware at a Check Point Firewall.

1. Select Check Point from the Mitigation Type column.
2. Enter the firewall hostname or IP address in the Hostname/IP field.
3. Enter the administrator User Name and Password.

NOTE Check Point login credentials configured on Juniper ATP Appliance must correspond to a Check Point account with /bin/bash as its shell - this corresponds to “expert” mode in the Check Point CLI. Note that this is not the default shell; the default is clish.

4. Enter the Expiry number of days for the connection; the default is 60 days.
5. Select an Inhibit Mode option:
 - › Drop and Close - drop the packet and close the connection when blocking request is received at the firewall
 - › Reject and Close - reject the packet and close the connection
 - › Drop - drop the packet. With drop (block), the packet is dropped and nothing is sent back to the sending program/system. So an attacker cannot know if they ever reached their destination or a firewall. It looks to the attacker as if the IP address has nothing there at all.
 - › Reject - reject the packet. With reject, a TCP RST or ICMP port unreachable for UDP is returned to the sender.
6. Enter the Secure Internal Communications SIC Name of the security management server for the Check Point firewall.
7. Select an Enforcement Host option:
 - › All - all enforcement hosts and groups or object
 - › Gateways - secure gateways as preferred enforcement hosts
 - › Group or Object - a configured security policy group or object

Objects represent the hosts, gateways, networks, and hosts managed by the Check Point firewall. A Group might show each Network Object group as a branch. The Security Gateways enforce an enterprise's security policies and act as a security enforcement point.

Configuring Enterprise Network Asset Values

Use the Asset Value configuration window to define network segment risk values. By qualifying the asset values of your own enterprise network segments, you are adding additional focus to the in-context threat metrics assessed by the Juniper ATP Appliance detection system. Asset Value context helps to filter out the overwhelming noise associated with non-context-driven threat reporting.

For example, the security of the finance department or engineering department in your enterprise may represent high risk assets or critical intellectual property, so you may want to enter the IP address of those network segments in the Asset Value configuration window. The Juniper ATP Appliance detection and chain heuristics engines use configured asset values to ascertain threat metrics for detected incidents.

The screenshot shows the configuration interface of the Juniper Advanced Threat Prevention Appliance. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various configuration sections, with 'Asset Value' selected. The main content area displays the 'Asset Value' configuration form, which includes fields for 'Network Segment', 'Network Value' (with radio buttons for Max, High, Med, Low), and 'Description'. Below the form is a 'Current Networks' table listing network segments and their assigned values.

Current Networks

Network	Value	Actions
192.168.1.0/24 - PCI	Med	Delete Edit
10.2.1.0 - Dev OPS	Max	Delete Edit
10.1.1.0/24 - Guest Wireless	Low	Delete Edit
10.1.1.0/24 - IT Management Network	Max	Delete Edit
10.1.0.0/24 - Onsite Contractor Network	Max	Delete Edit

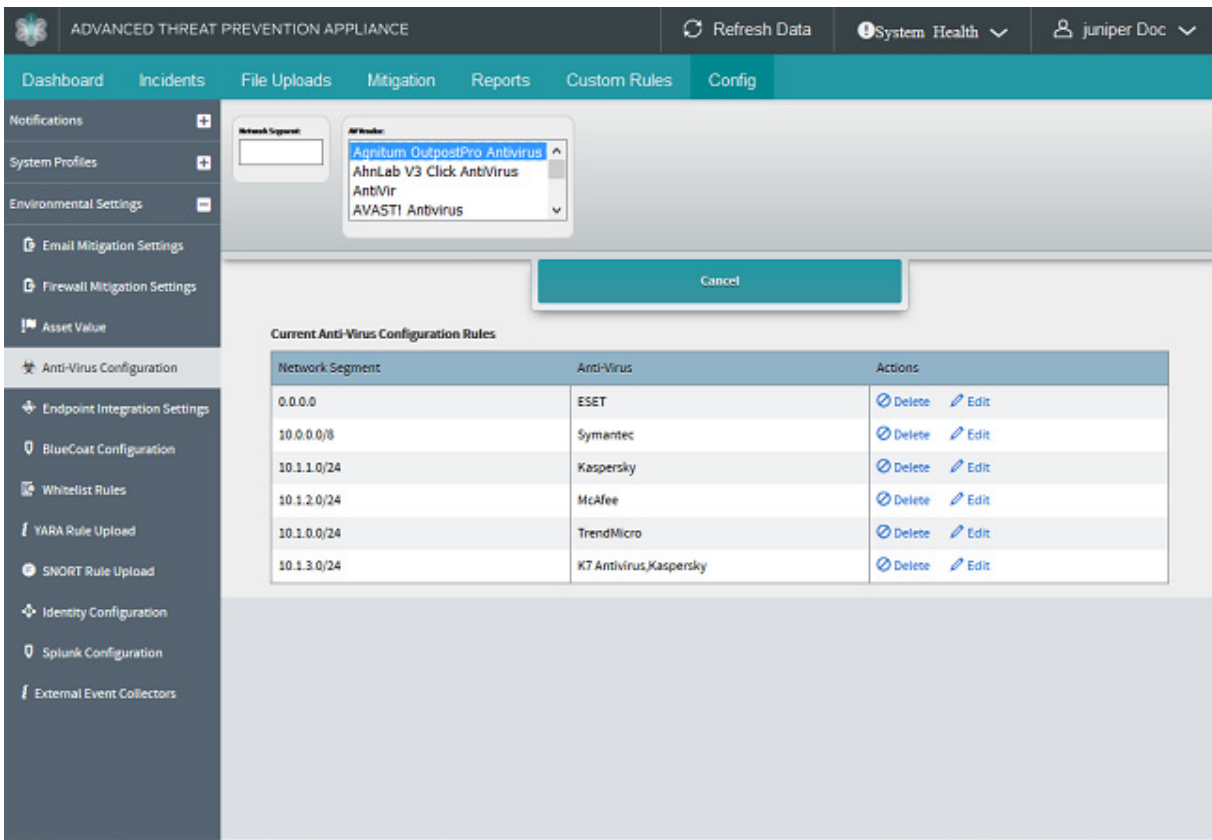
To assign Asset Value to a network segment:

1. Navigate to the Config>Environmental Settings>Asset Value page.
2. Enter the IP Address of the high asset-value network segment in the Network Segment field, or enter "default" to set the default=high risk setting.
3. Enter a network Value: Max | High | Med | Low
4. Enter a description for the Asset; for example: CEO Office.
5. Click Submit.

Configuring Anti-Virus Integration

Use the Config>Environmental Settings>Anti-Virus Configuration page to set anti-virus tool integration per enterprise network segment.

Figure 9 Anti-Virus Configuration Settings

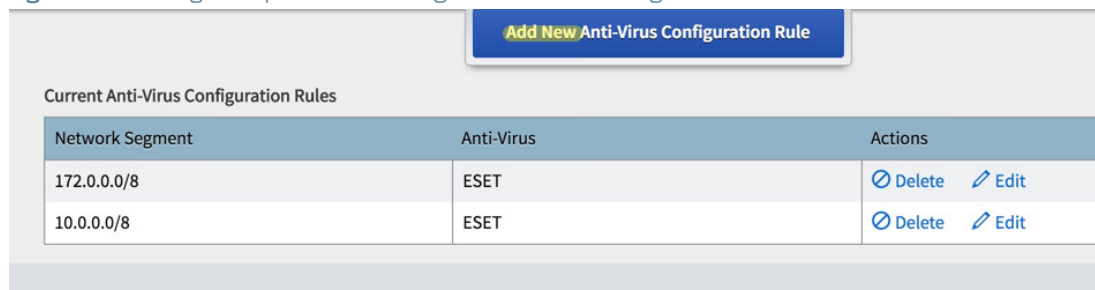


To perform anti-virus configuration:

1. Navigate to the Config>Environmental Settings>Anti-Virus Configuration page.
2. Enter the IP Address of a network segment.
3. Select the configured Anti-Virus package for that segment from the AV Vendor list and click Add.

NOTE Add multiple network segments as necessary: for example, you might add one network segment as 100.0.0.0/8 and the other one as 3.0.0.0/8 to cover all your segments, as shown in the following figure.

Figure 10 Adding Multiple Network Segments to AV Configuration



Configuring Endpoint Integration: CrowdStrike and Carbon Black Response

Use the Juniper ATP Appliance Central manager Web UI Config>Environmental Settings>Endpoint Integration Settings configuration page to configure Carbon Black Response and/or CrowdStrike endpoint integration.

- [Configuring Carbon Black Response Endpoint Integration on page 166](#)
- [Configuring CrowdStrike Endpoint Integration on page 167](#)

Configuring Carbon Black Response Endpoint Integration

Carbon Black Response is providing one source of information in calculating the risk score of a malware - Is the malware run on the end-point? The question is asked to a Carbon Black Response server based on three criteria: the malware md5, the end-point IP address, and the malware download timestamp.

Configuration of Carbon Black Response for endpoint monitoring and mitigation is a two-step process:

1. Obtain the Carbon Black Response Account API key from the Carbon Black Response Web UI. See Also: [Obtaining the Carbon Black Response API Key on page 166](#) below.
2. Enter the Key and other device configuration information to the Juniper ATP Appliance Web UI Carbon Black page shown below.

Figure 11 Central Manager Carbon Black Response Configuration Page

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications System Profiles Environmental Settings

Email Mitigation Settings Firewall Mitigation Settings Asset Value Anti-Virus Configuration Endpoint Integration Settings

BlueCoat Configuration Whitelist Rules YARA Rule Upload SNORT Rule Upload Identity Configuration Splunk Configuration External Event Collectors

Endpoint Type: ☒ CarbonBlack ☐ CrowdStrike

Hostname/IP:

Host Protocol: ☒ https ☐ http

Port Number:

API Key:

Cancel

Current Endpoint Integration

Description	Actions
-------------	---------

Obtaining the Carbon Black Response API Key

1. From the Carbon Black Response Web UI, click the top right admin user dropdown and select Profile info.
2. From the left panel Profile info menu, select API Token.
3. Copy the API Token from Your API Token box.
4. Obtain the hostname of the Carbon Black Response server (example: <https://JATP.cloud.carbonblack.com>)

Configuring the Carbon Black Response Integration at the Juniper ATP Appliance CM

1. Navigate to the Config>Environmental Settings>Endpoint Integration Settings page.
2. Select CarbonBlack as the Endpoint Type.
3. Enter the device Hostname or IP address.
4. Enter the Host Protocol: HTTPS or HTTP.
5. Enter the device Port Number.
6. Enter the Carbon Black Response API Key and click Submit.

Configuring CrowdStrike Endpoint Integration

Before configuring CrowdStrike Endpoint Integration, obtain the following data:

- CrowdStrike Falcon API server hostname
- CrowdStrike Falcon API user
- CrowdStrike Falcon API key

NOTE AD integration must be enabled as a prerequisite for CrowdStrike Endpoint Integration.

1. Navigate to the Config>Environmental Settings>Endpoint Integration Settings page.
2. Select CrowdStrike as the Endpoint Type.
3. Enter the device Hostname or IP address.
4. Enter the CrowdStrike API User.
5. Enter the CrowdStrike API Key.
6. Click Add.
7. Click Test in the Current Endpoint Integration table row to verify the CrowdStrike integration. This link tests whether the CrowdStrike server is reachable and the API user and key is working.

At the Central Manager Web UI Incidents, if an endpoint has executed malware, an EX flag is displayed.

Configuring BlueCoat ProxySG Integration

Juniper ATP Appliance publishes a "web page" with a list of URLs to which the BlueCoat proxy device is directed for network forensics integration. BlueCoat ProxySG polls the malicious URL list periodically to collect blocking details.

Bluecoat can be configured to apply various rules to the Juniper ATP Appliance list, including blocking, as desired.

Be sure to whitelist the Juniper ATP Appliance to avoid being SSL intercepted. On the BlueCoat sie, this is accomplished by adding a policy rule in the SSL Intercept layer and setting the Juniper ATP Appliance GSS hostname as the destination in the policy rule; set the action to "Disable SSL Interception".

See Also: [Configuring a Bluecoat Secure Web Gateway Log Collector on page 219](#) and [Configuring Bluecoat Secure Web Gateway Splunk Ingestion on page 224](#) for External Event Collection Bluecoat options.

To configure BlueCoat integration from the Juniper ATP Appliance side:

1. Navigate to the Central Manager Web UI Config>Environmental Settings>BlueCoat Configuration page.
2. Check Availability.
3. Enter BlueCoat Exception Page value; the default is content_filter_denied.

NOTE If there is a need to change the default to a user-defined value, create the exception first on BlueCoat. Note that the exception format must be followed: it cannot include spaces or an exclamation mark (!).

4. Enter the Cache Age; the default is 10 minutes (0 for no cache).
5. Enter the Allowed IPs (or leave the field empty to allow all IPs).
6. Enter URL, or click Refresh URL or Get PEM File buttons.
7. Click Submit.

To configure BlueCoat integration from the BlueCoat side:

1. Create and import a CA Certificate by navigating to the BlueCoat ProxySG Management Console Configuration>SSL>CA Certificates page.
2. On the Import CA Certificate page, click Apply (at the bottom).
3. From the SSL>CA Certificates page, select CA Certificate Lists from the left panel menu tab.
4. Highlight browser-trusted from the list, then click Edit.
5. In the Edit CA Certificate window, select the Juniper ATP Appliance intended certificate and click Add to move the newly created CA Certificate entry from left to right.=, then click Apply.
6. Set up polling by navigating to the Policy>Policy Files page.
7. Check the box for Automatically Install New Policy When Central File Changes.
8. Click the Install button for the Install Central File from: REMOTE FILE option.
9. In the Install Central File window, paste the URL from Juniper ATP Appliance (Config>Environmental Settings>BlueCoat Configuration>URL) into the Installation URL field and click Install.
10. In the File Installed window, a message displays “The file was successfully downloaded and installed;” click OK.
11. Next, configure how often BlueCoat is going to poll by setting the following from the CLI; refer to the following example:

```
# ssh admin@10.2.121.10
10.2.121.100 - Blue Coat SGVA Series> enable
Enable Password:
10.2.121.100 - Blue Coat SGVA Series#(config)policy poll-interval 5
```

This example sets a 5 minute interval between polls.

Configuring Whitelist Rules

An enhanced Whitelist feature now includes the addition of distinct attributes (also referred to as selectors) with which whitelisting can be filtered.

Filtering attributes (selectors) are based on:

- Threat Source IP
- Threat Target IP
- Threat Source Domain
- Threat Source Host
- Threat Target Host
- Source Email Id
- Destination Email Id
- Threat Source URI
- Threat SHA1 Hash
- Certificate Signer

Supported selectors vary by event type. The support matrix for various event types includes:

Exploit	src_ip, dst_ip, host, domain, uri, sha1sum
Cooking (Analysis)	src_ip, dst_ip, host, domain, uri, sha1sum
Infection	src_ip, dst_ip
Analysis via File Submission (File Upload)	sha1sum

TIP Adding an unsupported selector to a rule may prevent the event from matching the rule, and may thereby result in it not filtering out.

NOTE Whitelisted events are suppressed in the Incidents tables, and alert generation is also suppressed, but this does not affect malware analysis. However, Whitelist selectors can be removed and the corresponding incidents that were suppressed will be regenerated.

TIP Be aware that the different selectors in a whitelist rule are AND'ed. To perform an OR operation, create separate rules using the selectors that need to be ORed.

Configure Whitelist filtering rules from the Configuration tab Whitelist Rules page; administer whitelists and filtering criteria using the Incidents page Add to Whitelist link.

Figure 12 Whitelist Rules Configuration Page

Name	Threat Source IP	Threat Target	Threat Source Domain	Threat Source Host	Threat Target Host	Source Email Id	Destination Email Id	Threat Source URI	Threat SHA1
cyphort-whitelist	199.226.104.50	192.168.1.31		tyctpr.huvvqxqv.com	sfo_demo_31			http://tyctpr.huvvqxqv.com/smnMbFXwg/skpcvSJcid.html	2a1eb8eeca584c7fef429f
Email Whitelist						cloudmta4@gmail.com	admin@cydevel.com, cyphort-it@cyphort.onmicosoft.com		
Not_A_Worm_Whitelist	172.16.0.1	10.2.1.135							
OSX-Whitelist				niria-coperta.com	sj_demo_101			http://niria-coperta.com/malware_vault/malware/newton_qa/file_samples/malware_osx/b321c30a764a909853d413d8f3088e2b374c6e14a43c14c16c5c484d66f2ad9f	1d9c79c4db14e47d4ac8ff
OSX-Whitelist02	167.116.3.229	167.116.3.227		Infographiste.com				http://infographiste.com/malware_vault/malware/newton_qa/file_samples/malware_osx/e403b7a0db0fc3533678f8e17f35de30a472a04d3fd7b8c14bb7120	7c52e250af316ab5094ac

NOTE Be sure to whitelist the Juniper ATP Appliance to avoid being SSL intercepted.

To configure Whitelist filtering rules:

1. Navigate to the Config>Whitelist Rules page in the Central Manager Web UI.
2. Click Add to configure criteria for a new whitelist rule.

Figure 13 Create New Whitelist Rule Window

3. In the Create New Whitelist Rule window, enter the criteria for the new rule and checkmark for inclusion at this time (can be disabled and re-enabled later, as needed).

TIP Use all selectors shown to match a specific event or uncheck some selectors to broaden the scope of whitelisting.

NOTE When you select multiple attributes for the whitelist, it is an AND condition.

The fields are defined as follows.

Rule Criteria	Description
Name	Enter a name for the rule.
Threat Source IP	Enter the IP Address of the Threat Source.
Threat Target IP	Enter the IP Address of the targeted endpoint.
Threat Source Domain	Enter the domain name of the Threat Source.
Threat Source Host	Enter the HTTP protocol (server) host for the Threat Source.
Threat Target Host	Enter the HTTP protocol (server) host for the Threat Target.
Source Email Id	Enter the Source Email ID.
Destination Email Id	Enter the Destination Email ID.
Threat Source URI	Enter the URI for the Threat Source.
Threat SHA1 Hash	Enter the SHA1 hash.

Rule Criteria	Description
Certificate Signer	<p>Enter the full name as it appears on the digital certificate. So if the signer is Google, Inc, you cannot enter just Google because the whitelist rule will not match the files signed by Google, Inc.</p> <p>This is an optional entry; if there is no signer, then leave the Certificate Signer field blank.</p>

- Click Submit to complete the Whitelist Rule configuration.

NOTE The Juniper ATP Appliance Release allows enhances whitelisting functionality by allowing users to whitelist based on a signing certificate.

Updating and Redefining Whitelist Filters from the Incidents Page

On the Incident tab, when an Incident includes the option to Add to Whitelist, as shown below, these same criteria can be again edited and applied as part of the incident whitelisting process.

The screenshot displays the Juniper ATP Appliance interface. At the top, there's a navigation bar with 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. Below this, a table lists incidents. The incident with ID 648219 is highlighted, showing a 'MED' risk level and a 'TROJAN_DROP_D (Dropper)' threat. Below the table, the 'Details for TROJAN_FAKEAV' are shown, including source information and file type. On the right side of the details, a list of actions is available: 'Download Sample', 'Download Behavior Log', 'Add to Whitelist' (which is circled in red), 'Report False Positive', and 'Screenshot'.

- To edit Whitelist Filter criteria while adding the incident to the whitelist, click the Add to Whitelist link.
- In the Update Whitelist Rule window, you may add additional whitelist rule criteria, deselect (uncheck) currently established criteria, or update the rule set as is.
- Click Submit and the incident is added to the whitelist according to the criteria defined and checked in the Update Whitelist Rule window.

Figure 14 Update Whitelist Rule Window

CAUTION: It is important to proceed slowly when adding/removing/updating (making any changes) to a whitelist rule. Wait for few minutes after making any changes so that the whitelisting can take effect. If it seems that the rules are not updating, perform a dummy rule update to rectify the situation, using the following test-run strategy:

1. Navigate to the Config>Whitelist Rules page and click Add Rule.
2. Provide a rule name for the test rule such as DummyRule.
3. Provide the hash value as :abcd
4. click on Submit.
5. Wait a few minutes and then remove this rule.

NOTE Whitelist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the whitelist state as rules cannot be saved in that case.

Configuring YARA Rules

Configure and enable YARA rules to analyze object and traffic files for relevant malware matches. When a malware byte-pattern match is identified, analysts can specify that byte-pattern as a YARA rule and upload to the Juniper ATP Appliance Central Manager to be used to detect related malicious files during Juniper ATP Appliance malware detonation and analysis cycles.

YARA rules can be defined as malware families based on textual or binary patterns obtained from samples of identified families. Rule descriptions consist of a set of strings and a Boolean expression that establishes the rule's logic. In addition, YARA integration results are displayed on the Incidents page and indicate whether an object can be classified as malicious. YARA rules are also used to classify malware samples.

To Create a YARA Rule

Write a text file that contains one or more YARA rules that specify a pattern, condition or string to match. A few examples follow:

```
rule match_test
{
  strings:
    $a = {6B 41 18 22 32 11 88 7C 16 5F 94}
    $b = {8D 4G B0 2S C1 83 S0 24 99 6A 4T 59 F4 K9}
    $c = "FDHJBVFSGHLKHGFFDDFDGKJKJFD"
  condition:
    $a or $b or $c
}
```

```
rule excel_test
{
  strings:
    $excel = "Excel"
  condition:
    $excel
}
```

NOTE Administrators can define YARA rules for a particular file type (for example: 'pdf', 'exe', 'docx') or apply the rule to all file types (for example: 'common'). Multiple rules can be contained within one YARA Rule file.

To upload and enable a YARA Rule:

Navigate to Config>Environmental Settings>YARA Rule Upload.

The screenshot shows the Juniper ATP web interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings categories, with 'YARA Rule Upload' selected under 'Environmental Settings'. The main content area is titled 'YARA Rule Upload' and contains a 'File Types' section with checkboxes for exe, dll, pdf, doc, xls, ppt, java, and apk. The 'exe' checkbox is checked. Below this is a 'Choose Your File' section with a 'Browse...' button and the text 'No file selected.'. To the right is a 'Description' text input field. Further right are 'Enabled' and 'Disabled' radio buttons, with 'Enabled' selected, and an 'Add' button. A 'Cancel' button is located below the 'Add' button. At the bottom, there is a table titled 'Current YARA Rules' with columns for 'File Suffix', 'Description', and 'Actions'.

1. Select a File Type: exe | dll | pdf | doc | xls | ppt | java | apk
2. Click Choose File to browse and upload the YARA file.
3. Enter a Description.
4. Click the radio button to Enable or Disable.
5. If enabling, the Add button will display; click Add to initiate the YARA rule compiling and syntax validation. If there are no syntax errors, the YARA rule is added to the detection system.

NOTE Upload one rule at a time. However, one rule file may contain multiple rules.

Once a YARA rule is compiled and added to the system, network objects are scanned for any rule matches. Rule matches contribute to threat detection and are recognized as malware on the Web UI Incidents page.

Reviewing YARA Rule Malware Detection

There are several locations on the Incidents page where YARA rule matching is displayed as malware.

Figure 15 Yara Rule Match Reporting also Displays in Incidents Downloads Details

SUMMARY

EXPLOITS

DOWNLOADS

EXTERNAL SOURCES

Severity	Threat Name	File Type
Count of system calls to num-traced-calls		
null		
VM Network Callbacks:	newcard.dyndns.biz	port 53 DNS
	sqm.microsoft.com	port 53 DNS
Anti-Debugging: None		
Processes Spawned: None		
Mutexes: None		
Registry Modifications: None		
Files Opened: None		
YARA Information		
Rule Name	Severity	File Name
mz_executable	null	yara-exe-1.yara

Configuring Identity

Identity configuration options allow for the import of Active Directory identity information sent to Juniper ATP Appliance via Splunk ingestion. This feature supplements Juniper ATP Appliance's existing support of direct log ingestion to a Juniper ATP Appliance Core, adding the Splunk forwarding options for enterprises that use Splunk deployments for log and event handling.

[See Also: Configuring Identity on page 174.](#)

In previous releases, Identity information was available directly from Active Directory.

You will need to perform several configurations:

- Configure Splunk from the Juniper ATP Appliance Web UI Juniper ATP Appliance Config>Environmental Settings>Splunk Integration.
- Configure Carbon Black Response from the Juniper ATP Appliance Config>Environmental Settings>External Event Collectors.
- Configure Identity for AD and Splunk from the Juniper ATP Appliance Config>Environmental Settings>Identity Configurations page in the next section, below:
 - ["Setting Identity Configuration for Splunk" in the next section](#)
 - [Setting Identity Configuration for Active Directory on page 194](#)
 - [Active Directory Log Ingestion on page 194](#)

Setting Identity Configuration for Splunk

To configure Anti-SIEM Splunk Ingestion, perform the following steps.

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>Splunk Configuration page; click Add New Identity Source.

Figure 16 Identity Configuration Page

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Notifications System Profiles Environmental Settings

Email Mitigation Settings Firewall Mitigation Settings Asset Value Anti-Virus Configuration Endpoint Integration Settings BlueCoat Configuration Whitelist Rules YARA Rule Upload SNORT Rule Upload Identity Configuration Splunk Configuration External Event Collectors

Source Type: ☐ Active Directory ☒ Splunk

Identity Sources: ☐ Audit Logs ☐ LDAP Add-on

Event Log Collection Method: ☒ WMI ☐ Universal Forwarder

Optional Splunk Index:

Use Reverse DNS: ☒ Enabled ☐ Disabled

Exclude Hostnames (comma-separated):

Note: Identity mappings for these hosts are ignored.

Cancel

Current Identity Sources

Identity Source Type	Details	Actions
Active Directory	Domain Controller Hostname: 192.168.1.111 Domain Component Name: demo-ed.cyphort.com Search Type: Global Catalog Search LDAP Port Number: 3268	Delete Edit Test

2. Select Splunk as the Source Type.
3. Select an Identity Source: Audit Logs or LDAP Add-on.
4. Select an Event Log Collection Method: WMI or Universal Forwarder.
5. Enter an Optional Splunk Index.
6. Select Enable or Disable for the Use Reverse DNS setting.
7. Enter Exclude Hostnames, separated by commas. Identity mappings for these hosts are ignored and not included in event handling and displays.
8. Click Submit to complete the configuration.

Setting Identity Configuration for Active Directory

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>Splunk Configuration page; click Add New Identity Source.
2. Select Active Directory as the Source Type.
3. Enter a Hostname/IP Address.
4. Enter a Username and Password.
5. Enter a Search Type: Global Catalog Search or Local Search.
6. Select Enable or Disable for the Use Reverse DNS setting.
7. Enter a Domain Component Name.
8. Select an SSL setting: Enabled or Disabled.
9. Enter an LDAP Port Number.

NOTE Typically used port numbers: Global Catalog Search [SSL Enabled - 3289; SSL Disabled - 3268]; Local Search [SSL Enabled - 636; SSL Disabled - 389]

10. Choose to Enable or Disable the Use Reverse DNS setting.
11. Enter Exclude Hostnames, separated by commas. Identity mappings for these hosts are ignored and not included in event handling and displays.
12. Click Submit to complete the configuration.

Active Directory Log Ingestion

The Juniper ATP Appliance supports AD log ingestion via Splunk using either its Universal Forwarder on DC or the WMI method.

- [“Splunk Universal Forwarder of Active Directory Logs” in the next section](#)
- [Splunk WMI Forwarding of Active Directory Logs on page 202](#)

IMPORTANT: A few notices before you begin:

- Active Directory, Splunk and Juniper ATP Appliance all need to be NTP-synced.
- AD log ingestion can only be either Direct or via Splunk at a time.
- In AD logs via Splunk, the “Exclude hostname” configuration in the UI should be set to indeed exclude the hostname.
- If your enterprise environment has not previously employed AD-Splunk integration, and this is a first-time deployment, Juniper ATP Appliance supports both the WMI method and the Universal Forwarder method, and does not recommend one over the other. However, Splunk documentation recommends the Universal Forwarder for Domain Controllers because there have been performance issues reported for the WMI method.

Splunk Universal Forwarder of Active Directory Logs

To configure Splunk for AD using the Splunk App on DC, use the following procedure:

1. Install an Add-On for receiving security audit logs;

Review this link to determine which infrastructure Add-On to install:

<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/HowtodeploytheSplunkAppforWindowsInfrastructure>

Review this link to learn more about Splunk deployment options:

<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/WhataSplunkAppforWindowsInfrastructuredeploymentlooklike>

Deployment Options:

- › Splunk App for Windows Infrastructure (for receiving Security Audit logs) on Search Head
 - › Splunk Add On for Active Directory (for ldap search) on Search Head
 - › Splunk Add On for Windows on Search Head, Indexer and Universal Forwarder
2. Configure Active Directory Add On from the Splunk Web Console, as shown below:

Figure 17 Splunk Add-on Configuration for Receiving & Forwarding AD Security Audit Logs

splunk App: Splunk Supporting Add-on for Active Directory Administrator

Search Welcome Configuration Reference

Configuration

default

Domain name * default

Alternate domain name * id1.eng.cyphort.com

Base DN * dc=id1,dc=eng,dc=cyphort,dc=com

LDAP Server

Hostname * 10.2.14.3

Port 3269

SSL ☒

Credentials

Bind DN administrator@id1.eng.cyphort.com

Password *****

Connection status ! Untested Test connection

* Indicates a required field Save

- Configure the Splunk Indexer to receive Windows Data by navigating to Settings>Forward And Receiving (Data)->Configure Receiving->New

Figure 18 Splunk Add New Forwarding & Receiving Data Configuration Window

Add new

Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

9997

For example, 9997 will receive data on TCP port 9997.

Cancel

- Deploy Splunk App for Windows Infrastructure; use the following linked instructions:

<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/WhataSplunkAppforWindowsInfrastructuredeploymentlooklike>
<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/InstallSplunkIndexer>

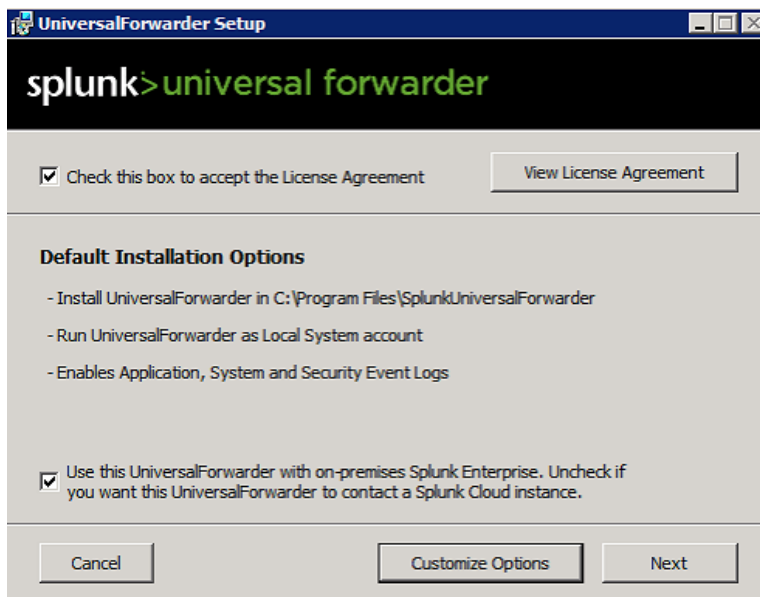
NOTE Download and install the Universal Forwarder on the Domain Controller with information from the following links.

The Universal Forwarder is one method for sending event logs to Splunk Indexer; the other method is Agentless forwarding using the WMI method, shown in the next section [Splunk WMI Forwarding of Active Directory Logs on page 202](#)).

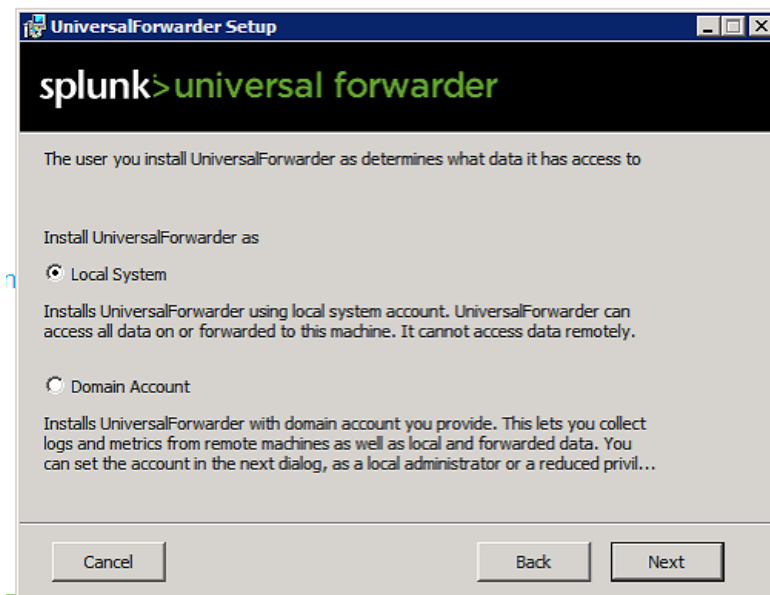
- Download the Universal Forwarder: https://www.splunk.com/en_us/download/universal-forwarder.html
- Download the MSI and start the installation. Configure the Universal Forwarder with instructions from this link:

http://docs.splunk.com/Documentation/Forwarder/6.5.3/Forwarder/InstallWindowsuniversalforwarderfromaninstaller#Install_the_universal_forwarder_for_use_with_on-premises_Splunk_instances

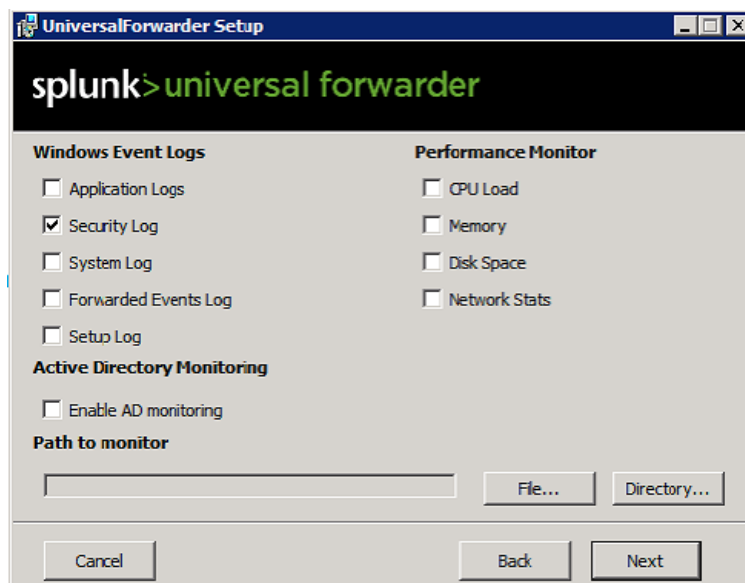
- Click on the Customize option after selecting the appropriate checkboxes as shown in the image below:



- Click Next and then choose Local Account unless you want to poll other domain controllers using WMI. Click Next again.



- In the next configuration window, shown below, select the Security Log forwarding option. Click Next.



- Enter the Deployment Server Hostname and Port (default is 8089), then click Next.

The screenshot shows the 'UniversalForwarder Setup' window. At the top, it says 'splunk>universal forwarder'. Below that, a message states: 'If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.' The 'Deployment Server' section has a 'Hostname or IP' label and two input fields separated by a colon. The first field is empty, and the second field contains '8089'. Below the fields, a note says 'Enter the hostname or IP of your deployment server, e.g. ds.splunk.com' and 'default is 8089'. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.

- Enter the Receiver Index and Port (default is 9997), as in the example shown below, and then click Next..

The screenshot shows the 'UniversalForwarder Setup' window. At the top, it says 'splunk>universal forwarder'. Below that, a message states: 'If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.' The 'Receiving Indexer' section has a 'Hostname or IP' label and two input fields separated by a colon. The first field contains '10.2.20.76' and the second field contains '9997'. Below the fields, a note says 'Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com' and 'default is 9997'. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.

- Follow instructions to Get Active Directory Data from this link:
<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/DownloadandconfiguretheSplunkAdd-onsforActiveDirectory>
 - Configure GPO's for AD and Powershell.
 - Download Splunk Add On For Microsoft Active Directory.
 - Download Splunk Add On for Microsoft Powershell.
 - Un-TAR both downloaded TAR files using 7zip or another archive utility.
 - Copy the resulting SA-ModularInput-PowerShell and Splunk_TA_microsoft_ad to the Universal Forwarder installed path:

C:\Program Files\SplunkUniversalForwarder\etc\apps

- Restart Universal Forwarder components:
 - › services.msc
 - › Find SplunkForwarder Service and restart it.
 - Verify Splunk Search Head is receiving data by performing one of the following procedures:
 - › Search the UI at App & Reporting > Data Summary to verify that the Domain Controller Host is configured.
 - › Or search using "source="wineventlog:security" AND EventCode=4769 AND Service_Name != krbtgt | table _time Account_Name Client_Address Service_Name | rename _time as Logon_Time Account_Name as UserName Client_Address as IPAddress Service_Name as HostName"
6. Configure Splunk App for Windows Infrastructure on the Splunk Web Indexer; note the prerequisites:

The screenshot shows the 'Prerequisites' step of the 'App: Splunk App for Windows Infrastructure' setup wizard. The progress bar indicates the current step is 'Prerequisites', with previous steps being 'Introduction', 'Check Data', 'Customize Features', and 'Finish'. A 'Redetect' button is available. Below the progress bar, there is a section titled 'Check prerequisites to be installed on the search head'. A yellow warning box contains the text: 'Bypass pre-requisite checks. Note: bypassing prerequisites might result in reduced or limited app functionality'. The prerequisites list includes:

- Splunk v6.2.0+**: Status is 'OK'. Sub-points: 'OK: Splunk v6.5.3 detected' and 'OK: Key value store is enabled. Learn more.'
- Splunk Add-on for Microsoft Windows v4.7.2+**: Status is 'X' (failed). Message: 'Could not determine the version for Splunk Add-on for Microsoft Windows. Check if the feature is installed. Download here.'
- Splunk Supporting Add-on for Microsoft Windows Active Directory v2.0.1+**: Status is 'OK'. Sub-point: 'OK: Splunk Supporting Add-on for Microsoft Windows Active Directory v2.1.4 detected'
- Users and/or groups configured with the winfra-admin user role:**: Status is 'X' (failed). Message: 'No users or groups with winfra-admin user role detected. Assign the winfra-admin user role via Splunk Settings >> Access Controls'

- Give winfra-admin role to admin user by modifying the roles for admin user as shown below:

Full name

Email address

Time zone

Set a time zone for this user.

Default app

Set a default app for this user. Setting this here overrides the default app inherited from the user's role(s).

Assign to roles

Assign this user to one or more roles. The user will inherit all the settings and capabilities from these roles.

Available roles

[add all »](#)

Selected roles

[« clear all](#)

☐ admin
☒ can_delete
☒ power
☒ splunk-system-role
☒ user
☐ winfra-admin

☒ admin
☒ winfra-admin

Set password

Password

Confirm password

Splunk WMI Forwarding of Active Directory Logs

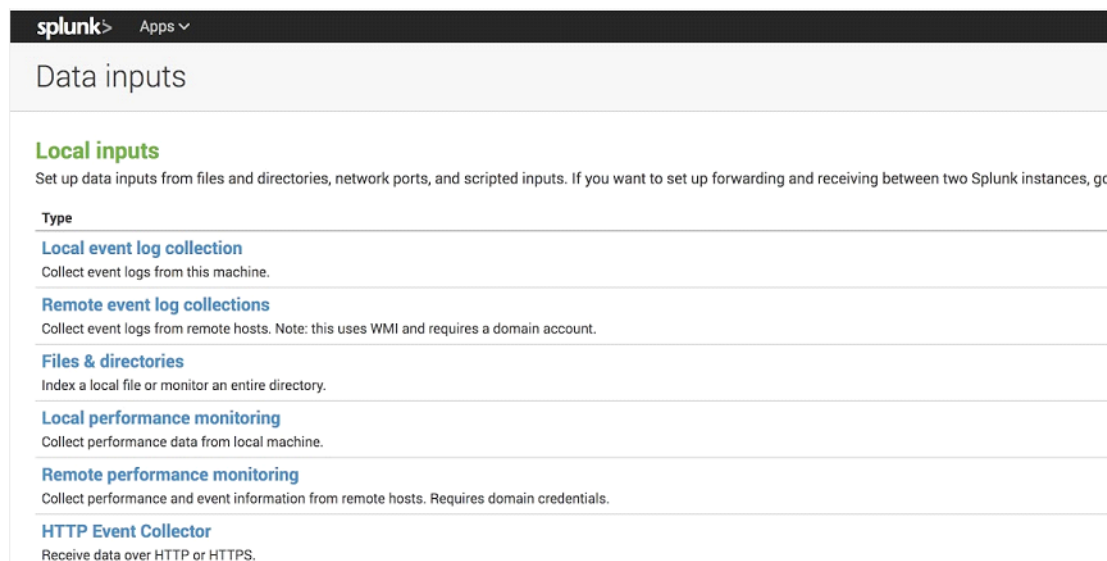
Use the following procedure to setup AD Integration with Splunk using the WMI method.

NOTE Setup requirements for the Splunk Server are also available from this link:
<http://docs.splunk.com/Documentation/Splunk/6.6.0/Data/MonitorWMIdata>

1. Both Splunk Enterprise and your Windows network must be correctly configured for WMI data access. Review the following prerequisites before attempting to use Splunk Enterprise to get WMI data.

Before Splunk Enterprise can get WMI-based data:

- Splunk Enterprise must be installed with a user that has permissions to perform remote network connections. While installing Splunk it would ask for local account or domain account. Choose domain account.
 - The user Splunk Enterprise runs as must be a member of an Active Directory (AD) domain or forest and must have appropriate privileges to query WMI providers.
 - The Splunk user must also be a member of the local Administrators group on the computer that runs Splunk Enterprise.
 - The computer that runs Splunk Enterprise must be able to connect to the remote machine(AD) and must have permissions to get the desired data from the remote machine once it has connected.
2. After installing Splunk, logon to Splunk and navigate to Settings -> Data Inputs:
 3. Click on the second option - Remote Event Log Collection, then click on New.



4. Choose a name for the log collection and enter the AD server IP address.
5. If Splunk can perform a WMI query to the AD server, then the Select Event Logs option is displayed, as shown below; Choose Security and click Next.

Add Data | Select Source | Input Settings | Review | Done | < | Next >

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Configure this instance to monitor Event Log channels of remote Windows machines u Management Instrumentation (WMI) framework. Splunk must run as an Active Director access to the remote machine. Both Splunk and the remote machine must reside in the forest. [Learn More](#)

Event Log collection name?

Choose logs from this host?

Select Event Logs

Available item(s)	add all »	Selected item
Application		
Security		
System		
DFS Replication		
DNS Server		

Select the Windows Event Logs you want to index from the list

Collect the same set of logs from additional hosts?

6. Enter the host details on the next page. If you want to choose an indexer, choose it or leave the default.

Review configurations and Submit.

7. From the Splunk Server, navigate to C:\Program Files\Splunk\etc\system\local and add the following configuration:

```
[WinEventLog://Security]
disabled = 0
start_from = oldest
current_only = 0
evt_resolve_ad_obj = 1
checkpointInterval = 5
```

Restart Splunk and verify that all Active Directory Security Logs are available in Splunk.

Configuring Active Directory

Endpoint Identity integration supports Email and HTTP incident correlations. In turn, Email Correlation is integrated with Juniper ATP Appliance's east-west enterprise-wide lateral detection framework. The Juniper ATP Appliance supports remote authentication to Active Directory (AD) servers in customer networks. With AD and endpoint identity integration, lateral spread detections display the endpoint hostname as the node name (instead of host IP address) if it's available.

NOTE Active Directory configuration is required for the Identity feature to work.

See Also: [Configuring Identity on page 174](#).

See also [AD Domain Controller Configuration Requirements and Tips on page 191](#) and [Troubleshooting Active Directory on page 192](#).

Active Directory configuration is described in the following consecutive sections:

- [Part 1 - Obtaining a Domain Component Name for a Domain Controller on page 185](#)
- [Part 2 - Configuring an Active Directory Domain Controller from the Web UI on page 190](#)

Part 1 - Obtaining a Domain Component Name for a Domain Controller

This Part1 section describes how to obtain the domain component name required to configure AD from an Active Directory Domain Controller. Perform these steps before configuring the AD Domain Controller integration from the Juniper ATP Appliance Central Manager Web UI described in Part 2.

Prerequisites for Active Directory Integration

Adhere to the following requirements before configuring AD integration:

- A configured user for AD must have Administrator privileges because both Windows Management Instrumentation (WMI) and LDAP searches require Admin credentials. The AD user can be a "read only" Admin user, but does need to have following permissions:
 - The user account must belong to the "Distributed COM Users" Active Directory group.
 - The user account must have permission to access WMI namespaces (CIMV2 namespace) on the Domain Controller machine.
 - The user account must have permission to read the security event log on the domain controller machine.
- Active Directory Domain Controller and the Juniper ATP Appliance Core/CM must be synced to an NTP server, because Juniper ATP Appliance queries the AD based within a specified time period (ranging from the current time to 5 minutes).
- If the AD Domain Controller is behind a firewall then be sure to open up the firewall to allow the Juniper ATP Appliance Core/CM device to reach the AD.
 - Open the firewall for the port numbers required for LDAP Search and WMI query.
 - LDAP Search default port number
 - › For Local Search:Port 389 (non SSL), Port 636 (SSL).
 - › For Global Catalog Search:Port 3268 (non SSL), Port 3269 (SSL).

NOTE For SSL mode Customer should install Active Directory Certificate Services and install a certificate. Domain Controller Server should be restarted after this as LDAPS doesn't work without restart.

- WMI uses TCP port 135 for initial connection. If the core is behind a firewall then customer needs to open up the firewall for port 135 and must also:
 - › Either tie WMI to a fixed port and open up the firewall for the fixed port as well. This fixed port will be used for WMI data exchange.

NOTE You can find instructions for tying WMI to a fixed port at this URL:
[https://msdn.microsoft.com/en-us/library/bb219447\(VS.85\).aspx](https://msdn.microsoft.com/en-us/library/bb219447(VS.85).aspx)

Also check if windows firewall is opened up for fixed port.

- › Or On the firewall, open up the port range 49152 - 65535 because DCOM might use any of the ports within this range.
- Ensure that the Audit policy on AD allows successful logons to generate the necessary events, specifically a Kerberos event type with the event code 4769.
- Be sure to configure the Windows Security Log Property "Overwrite events as needed (oldest event first)" option, for the maximum log file size, because Juniper ATP Appliance scrapes these logs for Identity (security logs must be running logs in order for Juniper ATP Appliance to obtain Identity information).

Also setup a non-Admin user in order to query the Domain Controller Event Log for Windows 2008 and Windows 2012.

The Juniper ATP Appliance Core queries the Domain Controller event log to obtain the host-to-IP mapping. Be sure to configure the Juniper ATP Appliance Core/CM to query the Domain Controller with a user who is part of the Domain Administrator group. This may be restrictive and potentially risky to administrators.

An AD Agent running on the Juniper ATP Appliance Core does not need an Admin user because it uses WMI to query the Active Directory Domain Controllers for the Security Event logs. Juniper ATP Appliance also uses

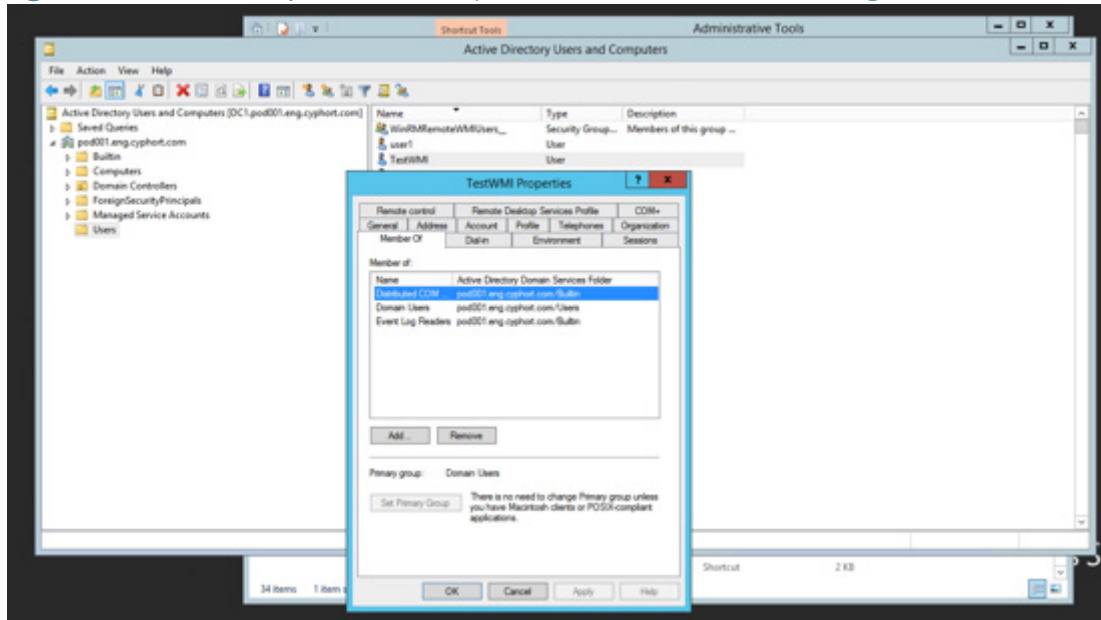
Distributed COM (DCOM) technology to handle its remote calls to the domain controller. For a non-admin user, be sure to set the following permissions in order to allow querying the DC:

- DCOM permission (this should belong to the Distributed COM Users AD group).
- WMI permission to access WMI namespaces (CIMV2 namespace) on the domain controller device.
- Permission to read the security event log on the domain controller device.

Creating a Domain User or Group

To create a Domain User or Group, add the new user/group to a domain Built-in Group: "Distributed COM Users" and "Event Log Readers" using the Active Directory Users and Computers window options, as shown below.

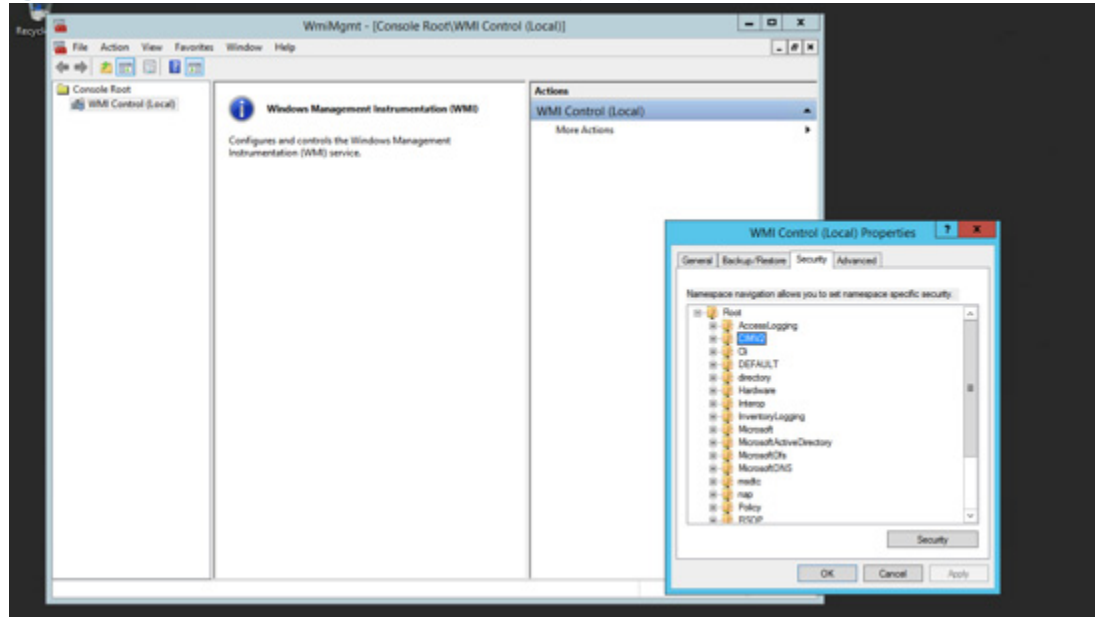
Figure 19 Active Directory Users and Computers Window "Member Of" Settings



Next, set the User/Group WMI permissions.

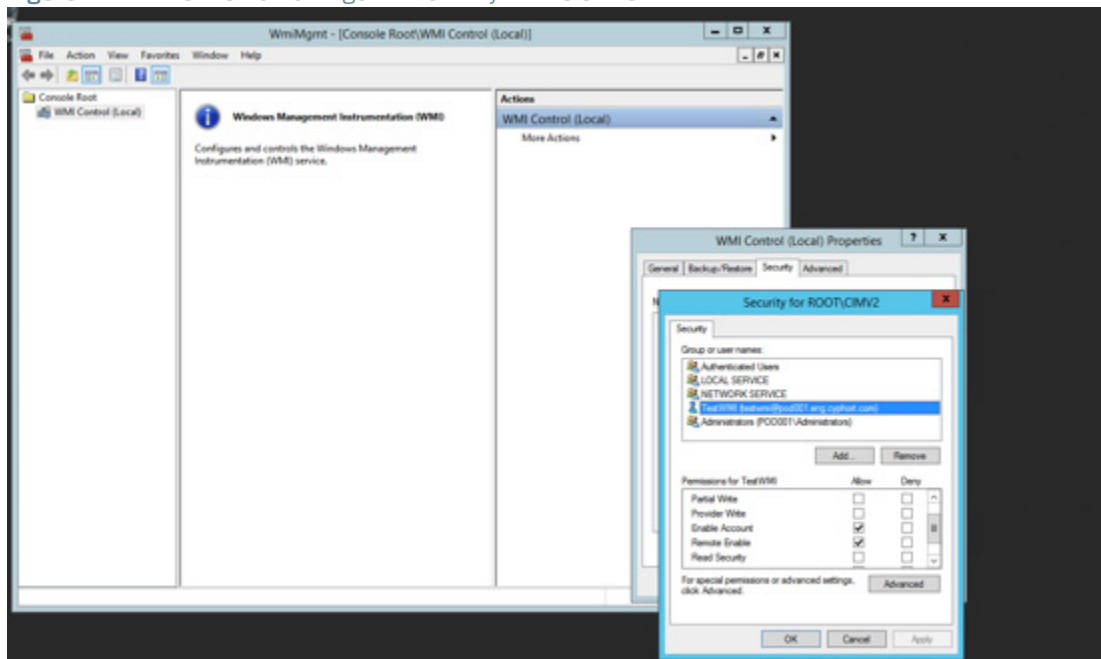
1. Run the Windows Management Instrumentation (WMI) console.
2. Select Start, click Run, and then type: `wmicmgmt.msc`
3. Click OK and press Enter.
4. Right-click "WMI Control" and select "Properties".
5. Select the Security tab, and then expand "Root".
6. Select "CIMV2" and then click "Security".

Figure 20 Windows Management Instrumentation (WMI) Console Settings



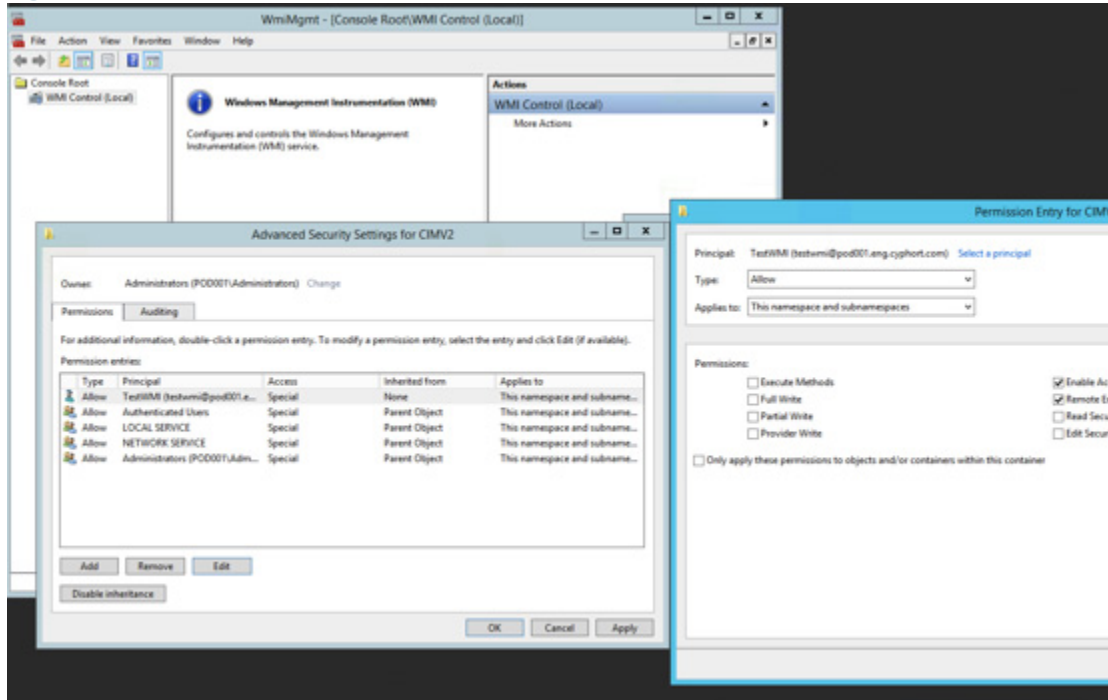
7. Add the domain user that you've created to work with the AD Domain Controller. Set the "Enable Account" and "Remote Enable" permissions to the user.

Figure 21 WMI Console Settings for Security for ROOT\CIMV2



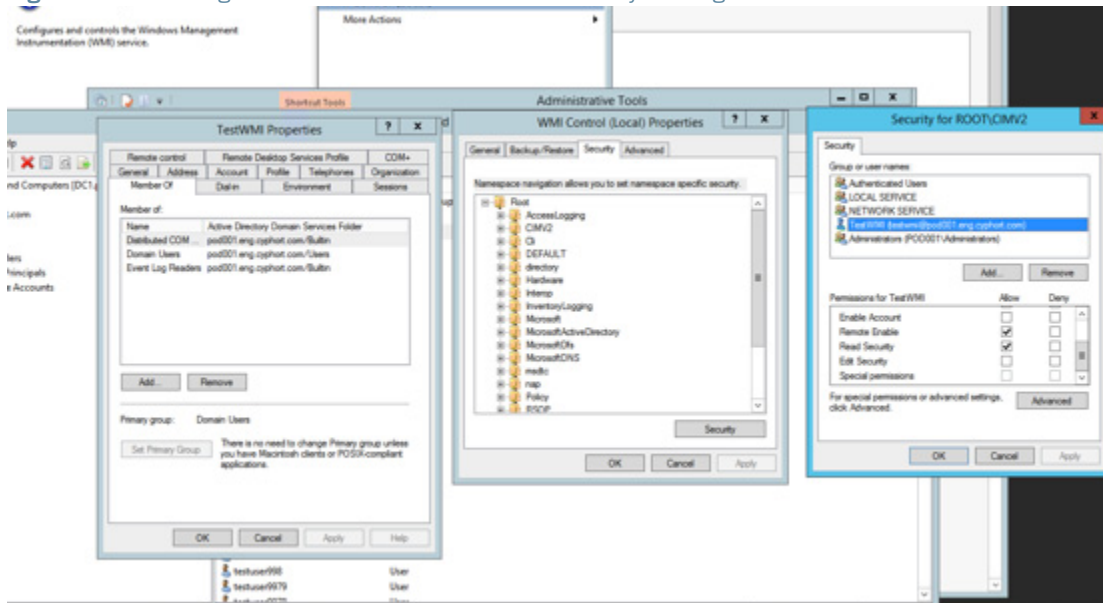
8. Click "Advanced". Select the domain user and check that "Apply to" is set to "this namespace and subnamespaces".

Figure 22 WMI Console Advanced Security Settings for CIMV2



9. Select OK to save changes.

Figure 23 Finalizing the WMI Console Advanced Security Settings

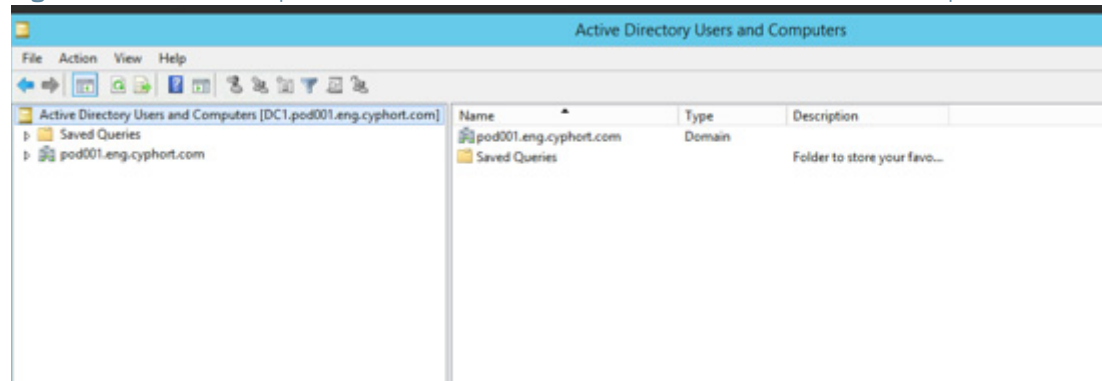


Next, obtain the Domain Component Name for the Domain Controller.

1. Navigate to the AD Server.
2. Run "Administrative Tools."

3. Run "Active Directory Users and Computers"
4. Click on "Active Directory Users and Computers" and on the right side locate the Name (for example: pod001.eng.JATP.com is displayed as the Domain Component Name in the sample screenshot below).
5. You will use this exact same domain component name from Step 4; take note so that you can add it to the Domain Component field on Juniper ATP Appliance's Active Directory Configuration Page (described in Part 2 below [Part 2 - Configuring an Active Directory Domain Controller from the Web UI on page 190](#)).

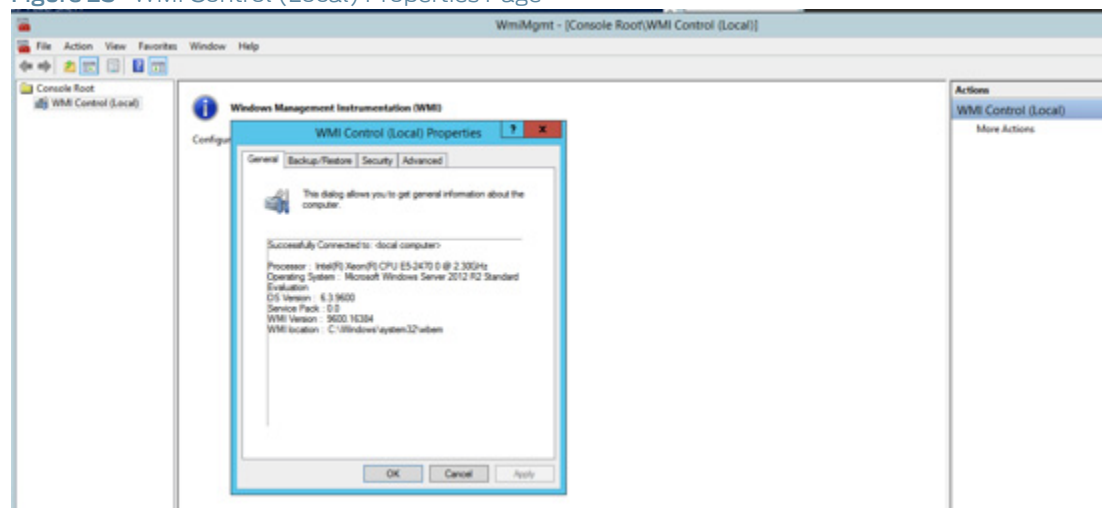
Figure 24 Domain Component Name in the Name Column of the AD Users and Computers Window



Next, test the Local WMI services.

1. Click Start, click Run, type `wmicmgmt.msc`, and then click OK.
2. Right-click WMI Control (Local), and then click Properties.
3. If the WMI service is configured correctly, the WMI Control will connect to WMI and display the Properties dialog box. On the General tab, you should see information about the operating system and the version of WMI.

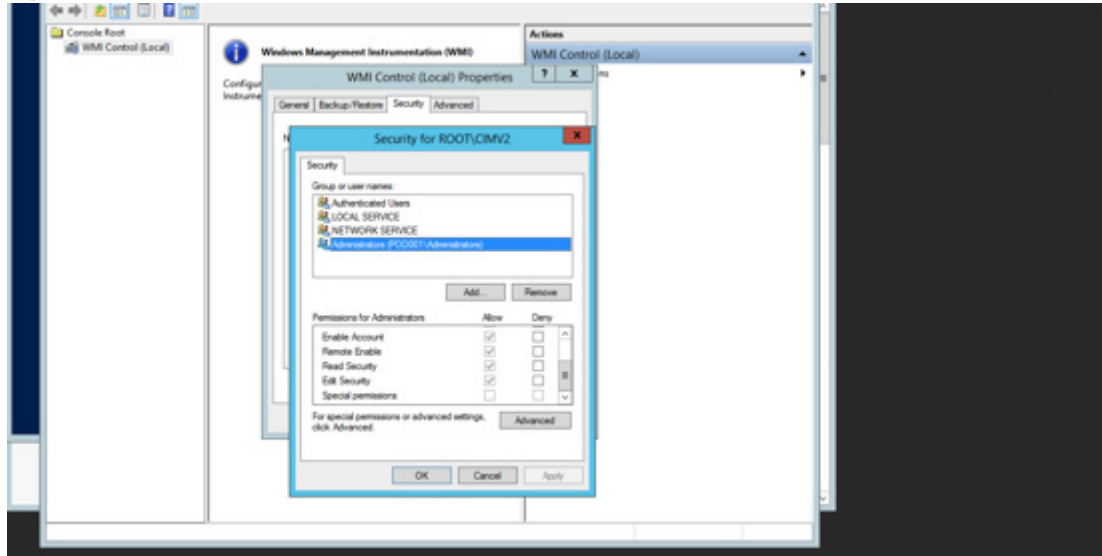
Figure 25 WMI Control (Local) Properties Page



Now, verify WMI permissions:

1. On the AD computer, click Start, click Run, type `wmicmgmt.msc`, and then click OK.
2. Right-click WMI Control, and then click Properties.
3. On the Security tab, expand Root, and then click WMI.
4. Click Security in the results pane to see the permissions. If the user does not have permission, then set permissions.

Figure 26 WMI Console Security Settings



Next, verify the LDAP SSL connection. After a certificate is installed, follow these steps to verify that LDAP is enabled:

1. Start the Active Directory Administration Tool (Ldp.exe).

NOTE The Active Directory Administration Tool program is installed in the Windows 2000 Support Tools area.

2. On the Connection menu, click Connect.
3. Type the name of the domain controller to which you want to connect.
4. Type 636 as the port number.
5. Click OK.
6. Proceed to [“Part 2 - Configuring an Active Directory Domain Controller from the Web UI”](#) in the next section.

Part 2 - Configuring an Active Directory Domain Controller from the Web UI

To configure an Active Directory Domain Controller, perform the following steps.

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>Active Directory Configuration page.
2. Click the Add New AD Domain Controller button. See [AD Domain Controller Configuration Requirements and Tips on page 191](#).
3. Enter the AD Domain Controller Hostname/IP.
4. Enter the AD Server User's User Name and Password.
5. Choose a Search Type option: Global Catalog Search or Local Search. Global search is a search of the entire AD database. Local Search is a search configured to be specific to a certain domain component, such as the finance department, for example,
6. Enter the AD Domain Controller Domain Component Name if the Local Search option is selected. For Local Search, the component name is required (not optional).
7. Choose an SSL status: Enabled or Disabled.
8. Enter an LDAP Port Number.
9. Click Submit. The Current AD Domain Controller table lists the new AD Controller.

10. To edit the AD Controller settings, click Edit in the Current AD Domain Controller table.
11. To delete the AD Controller settings, click Delete in the Current AD Domain Controller table.

NOTE The typically used AD Domain Controller LDAP Port Numbers for Global Catalog Search are SSL Enabled 3269; SSL Disabled 3268. The typically used AD Domain Controller LDAP Port Numbers for Local Search are SSL Enabled 636; SSL Disabled 389.

To test the connection, click the Test link in the Current AD Domain Controller table:

A system message will display the results of the WMI and LDAP connection to the AD Domain Controller.

AD Domain Controller Configuration Requirements and Tips

Juniper ATP Appliance polls the AD Domain Controller every 5 minutes to get the Identity data from AD. Identity data is retrieved from AD's Security event logs using WMI by querying logs for the event code 4769 and AD Datastore using LDAP search. Identity data includes mapping each authentication event, endpoint host name, endpoint IP address, username used to login into the endpoint and user's email address. Multiple AD domain controllers can be configured and polled in 5 minute intervals.

Configuration Requirements and Tips

Review the following list of AD Domain Controller requirements and suggested configuration settings:

- A configured AD user must have administrator privileges. The AD account admin must (1) belong to the Distributed COM Users AD group, (2) the account must have permission to access WMI namespaces (CIMV2 namespace) on the domain controller device, (3) the account must have permission to read the security event log on the domain controller device.
- The Active Directory Domain Controller and the Juniper ATP Appliance Core+CM must both be synced to an NTP server in order to optimize AD polling in 5 minute intervals.
- If the Active Directory Domain Controller is behind a firewall, then the administrator must open up the firewall to allow the Juniper ATP Appliance Core+CM to reach the AD controller. Open the firewall for port numbers that are required for LDAP searches and WMI queries.

LDAP Search default port numbers:

- › For local search (of a specified domain component), use port numbers 389 for non-SSL and 636 for SSL.
- › For a global search (of a specified domain component), use port numbers 3268 for non-SSL and 3269 for SSL.

NOTE For SSL mode, be sure to install "Active Directory Certificate Services" and install a certificate. The AD Domain Controller Server should be restarted after installing the certificate because LDAP will not work without the restart.

- WMI uses TCP port 135 for the initial connection. If the Core+CM is behind a firewall, then the administrator must open up the firewall for port 135 and then also:
 - EITHER, tie the WMI to a fixed port and open up the firewall to the fixed port as well. Port 135 is used for the initial connection handshake. The fixed port is used for WMI data exchange.
 - › Instructions to tie WMI to a fixed port are available at:
[https://msdn.microsoft.com/en-us/library/bb219447\(VS.85\).aspx](https://msdn.microsoft.com/en-us/library/bb219447(VS.85).aspx)
 - › Also check to be sure the windows firewall is opened up for the fixed port.
 - OR, On the firewall, open up the port range 49152 - 65535 (because DCOM might use any of the port from this range).
- Ensure that the Audit Policy on the AD domain controller allows successful logons, particularly Kerberos event types with the event code 4769.
- Configure the Windows Security Log Property setting: "Overwrite events as Needed (oldest event first)"; select the maximize file size for full identity polling coverage.

Refer also to [Prerequisites for Active Directory Integration on page 185](#) for information about setting up a non-admin user to query the Domain Controller Event Log for Windows 2008 and Windows 2012.

Troubleshooting Active Directory

This section provides information about determining whether the Active Directory Domain Controller integration is working.

- Run the “setupcheck all” command from the Juniper ATP Appliance CLI or click Test button option in the Current AD Domain Controller window located in the Config>Environmental Settings>Active Directory Configuration page to check if Active Directory integration is working.
- If the Active Directory Domain Controller integration is not working:
 - › The AD Agent will still send a Health Alert every 1 hour.
 - › The AD Agent will also send GSS an Alert if the AD is unreachable for some reason.

An AD Agent may not be able to get Identity information for the following reasons:

- Active Directory Domain Controller not reachable (connectivity issue or it's down)
- A Query on the Active Domain Controller takes a longer time to finish (the controller may be slow due to memory or CPU issues).
- Network Latency may be too high.

Configuring Custom SNORT Rules

Juniper ATP Appliance users can upload SNORT Rules from the Central Manager Web UI Config Tab to be matched against network traffic monitored by Juniper ATP Appliance Collectors, with match results displayed in the Central Manager Custom Rules Tab. Juniper ATP Appliance correlates triggered rules with incidents that were active at the time of the trigger and the results are displayed on the Incidents Tab.

Sample Snort Rules

```
alert tcp !172.16.254.0/24 any -> 172.16.45.100 !80 ( \
  msg:"Access Alert - NON Web traffic to Host 45.100 from unauthorized source.
  Only mgmt net 172.1.45.0 allowed."; \
  flags:S; \
  classtype: policy-violation; \
  sid:5100001; \
  rev:1; \
)

alert tcp !172.16.254.0/24 any -> 172.16.45.100 80 ( \
  msg:"Web Alert - NON GET request found Host 45.100 Methods other than GET from
  non-mgmt net not allowed."; \
  content:"GET"; \
  http_method; \
  classtype: web-application-activity; \
  sid:5500001; \
  rev:1; \
)

alert tcp any any -> 172.16.45.100 80 ( \
  msg:"Web Alert - php request on Host 45.100. No php files on server."; \
  content:"GET"; \
  pcre:"/GET.*\.php/i"; \
  classtype: web-application-activity; \
  sid:5500002; \
  rev:1; \
)

alert tcp 172.16.254.0/24 any -> 172.16.45.100 80 ( \
  msg:"Web Alert - MGMT POST to NON form_posting uri. "; \
  content:"POST"; \
  pcre:"/POST.*\form_posting/i"; \
  classtype: web-application-activity; \
  sid:5500003; \
)
```



```

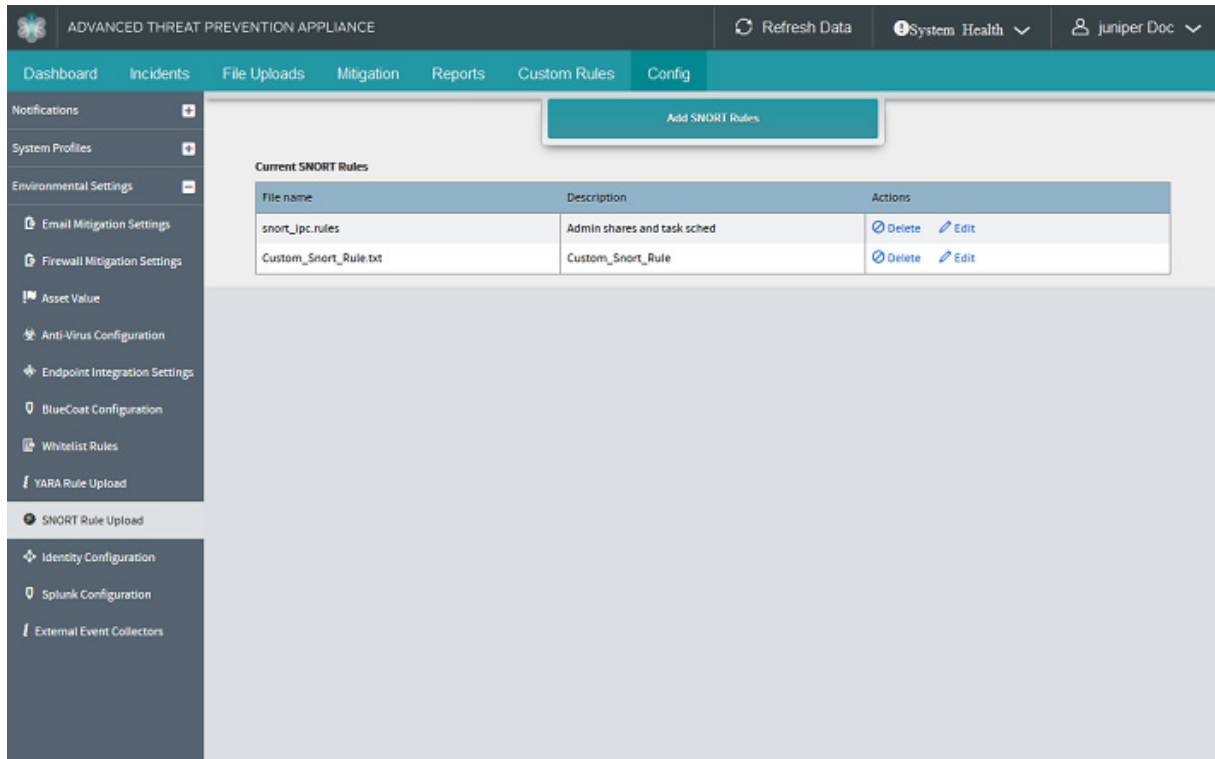
    rev:1; \
)

```

To upload a SNORT Rule file:

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>Snort Rule Upload page.

Figure 27 Juniper ATP Appliance Central Manager SNORT Rules Upload Page



2. Click the Add SNORT Rules button.
3. Click Choose File and browse to select your custom SNORT file for upload to the Juniper ATP Appliance system.
4. Enter a description for the SNORT rule in the Description field, then click Add.
5. To edit or delete a custom SNORT Rule, click the Delete or Edit link in the Current SNORT Rules table Actions column:

Setting Anti-SIEM Identity Configurations

Identity configuration options allow for the import of Active Directory identity information sent to Juniper ATP Appliance via Splunk ingestion. This feature supplements Juniper ATP Appliance's existing support of direct log ingestion to a Juniper ATP Appliance Core, adding the Splunk forwarding options for enterprises that use Splunk deployments for log and event handling.

You will need to perform several configurations:

- Configure Splunk from the Juniper ATP Appliance Web UI Juniper ATP Appliance Config>Environmental Settings>Splunk Integration.

- Configure Carbon Black Response from the Juniper ATP Appliance Config>Environmental Settings>External Event Collectors.
- Configure Identity for AD and Splunk from the Juniper ATP Appliance Config>Environmental Settings>Identity Configurations page in the next section, below:
 - [“Setting Identity Configuration for Splunk” in the next section](#)
 - [Setting Identity Configuration for Active Directory on page 194](#)
 - [Active Directory Log Ingestion on page 194](#)

Setting Identity Configuration for Splunk

To configure Anti-SIEM Splunk Ingestion, perform the following steps.

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>Splunk Configuration page; click Add New Identity Source.
2. Select Splunk as the Source Type.
3. Select an Identity Source: Audit Logs or LDAP Add-on.
4. Select an Event Log Collection Method: WMI or Universal Forwarder.
5. Enter an Optional Splunk Index.
6. Select Enable or Disable for the Use Reverse DNS setting.
7. Enter Exclude Hostnames, separated by commas. Identity mappings for these hosts are ignored and not included in event handling and displays.
8. Click Submit to complete the configuration.

Setting Identity Configuration for Active Directory

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>Splunk Configuration page; click Add New Identity Source.
2. Select Active Directory as the Source Type.
3. Enter a Hostname/IP Address.
4. Enter a Username and Password.
5. Enter a Search Type: Global Catalog Search or Local Search.
6. Select Enable or Disable for the Use Reverse DNS setting.
7. Enter a Domain Component Name.
8. Select an SSL setting: Enabled or Disabled.
9. Enter an LDAP Port Number.

NOTE Typically used port numbers: Global Catalog Search [SSL Enabled - 3289; SSL Disabled - 3268]; Local Search [SSL Enabled - 636; SSL Disabled - 389]

10. Choose to Enable or Disable the Use Reverse DNS setting.
11. Enter Exclude Hostnames, separated by commas. Identity mappings for these hosts are ignored and not included in event handling and displays.
12. Click Submit to complete the configuration.

Active Directory Log Ingestion

Juniper ATP Appliance’s support of Direct Ingestion of Active Directory (AD) Logs is not a new feature and has been available for many Juniper ATP Appliance product release versions. The Juniper ATP Appliance also supports AD log ingestion as via Splunk using either its Universal Forwarder on DC or the WMI method.

- [“Splunk Universal Forwarder of Active Directory Logs” in the next section](#)

- [Splunk WMI Forwarding of Active Directory Logs on page 202](#)

IMPORTANT: A few notices before you begin:

- Active Directory, Splunk and Juniper ATP Appliance all need to be NTP-synced.
- AD log ingestion can only be either Direct or via Splunk at a time.
- In AD logs via Splunk, the “Exclude hostname” configuration in the UI should be set to exclude the hostname of AD.
- If your enterprise environment has not previously employed AD-Splunk integration, and this is a first-time deployment, Juniper ATP Appliance supports both the WMI method and the Universal Forwarder method, and does not recommend one over the other. However, Splunk documentation recommends the Universal Forwarder for Domain Controllers because there have been performance issues reported for the WMI method.

Splunk Universal Forwarder of Active Directory Logs

To configure Splunk for AD using the Splunk App on DC, use the following procedure:

1. Install an Add-On for receiving security audit logs;

Review this link to determine which infrastructure Add-On to install:

<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/HowtodeploytheSplunkAppforWindowsInfrastructure>

Review this link to learn more about Splunk deployment options:

<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/WhataSplunkAppforWindowsInfrastructuredeploymentlookslike>

Deployment Options:

- › Splunk App for Windows Infrastructure (for receiving Security Audit logs) on Search Head
 - › Splunk Add On for Active Directory (for ldap search) on Search Head
 - › Splunk Add On for Windows on Search Head, Indexer and Universal Forwarder
2. Configure Active Directory Add On from the Splunk Web Console, as shown below:

Figure 28 Splunk Add-on Configuration for Receiving & Forwarding AD Security Audit Logs

splunk App: Splunk Supporting Add-on for Active Directory Administrator

Search Welcome Configuration Reference

Configuration

default

Domain name * default

Alternate domain name * id1.eng.cyphort.com

Base DN * dc=id1,dc=eng,dc=cyphort,dc=com

LDAP Server

Hostname * 10.2.14.3

Port 3269

SSL ☒

Credentials

Bind DN administrator@id1.eng.cyphort.com

Password *****

Connection status ! Untested Test connection

* Indicates a required field

Save

- Configure the Splunk Indexer to receive Windows Data by navigating to Settings>Forward And Receiving (Data)->Configure Receiving->New

Figure 29 Splunk Add New Forwarding & Receiving Data Configuration Window

Add new

Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

9997

For example, 9997 will receive data on TCP port 9997.

Cancel

- Deploy Splunk App for Windows Infrastructure; use the following linked instructions:

<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/WhataSplunkAppforWindowsInfrastructuredeploymentlookslike>
<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/InstallSplunkIndexer>

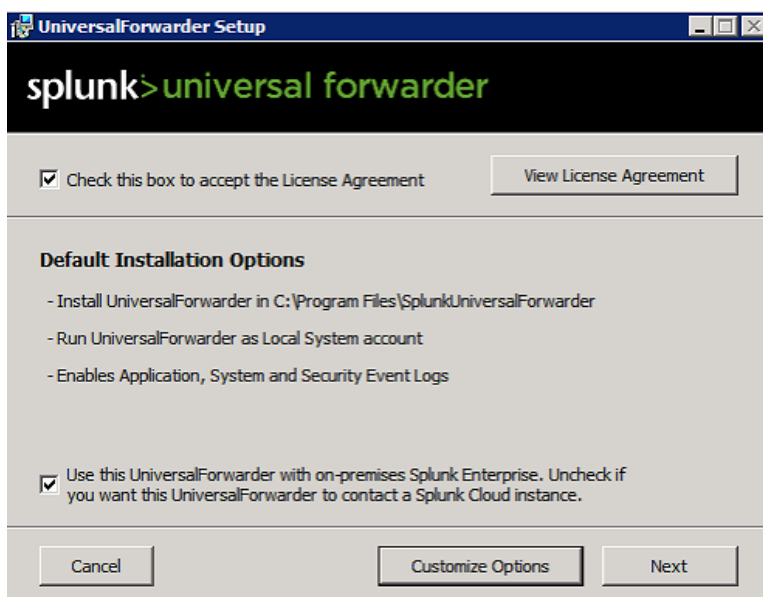
NOTE Download and install the Universal Forwarder on the Domain Controller with information from the following links.

The Universal Forwarder is one method for sending event logs to Splunk Indexer; the other method is Agentless forwarding using the WMI method, shown in the next section [Splunk WMI Forwarding of Active Directory Logs on page 202](#)).

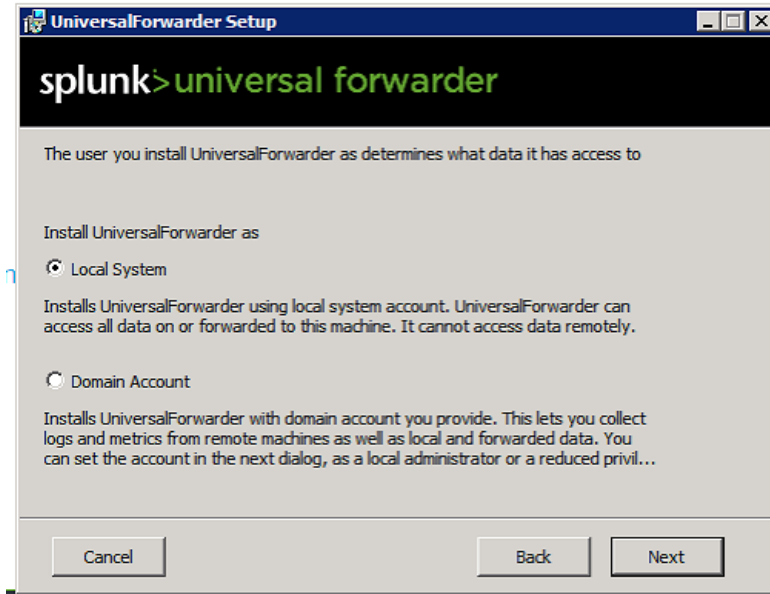
- Download the Universal Forwarder: https://www.splunk.com/en_us/download/universal-forwarder.html
- Download the MSI and start the installation. Configure the Universal Forwarder with instructions from this link:

http://docs.splunk.com/Documentation/Forwarder/6.5.3/Forwarder/InstallWindowsuniversalforwarderfromaninstaller#Install_the_universal_forwarder_for_use_with_on-premises_Splunk_instances

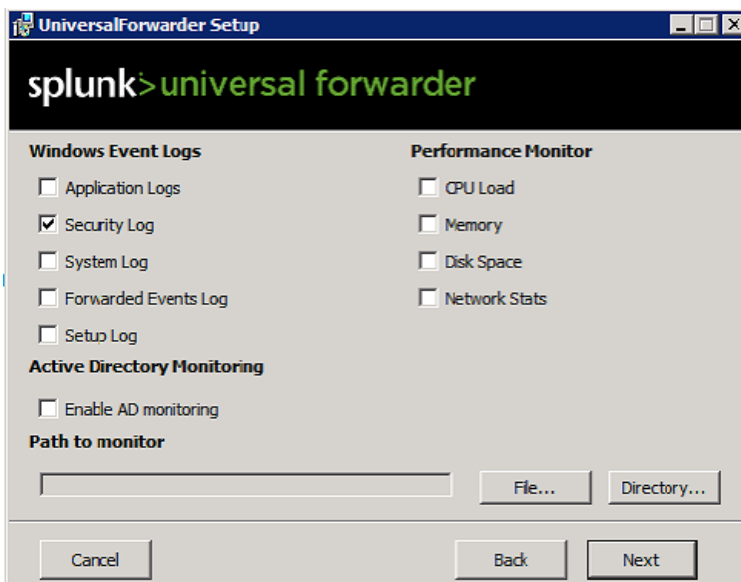
- Click on the Customize option after selecting the appropriate checkboxes as shown in the image below:



- Click Next and then choose Local Account unless you want to poll other domain controllers using WMI. Click Next again.

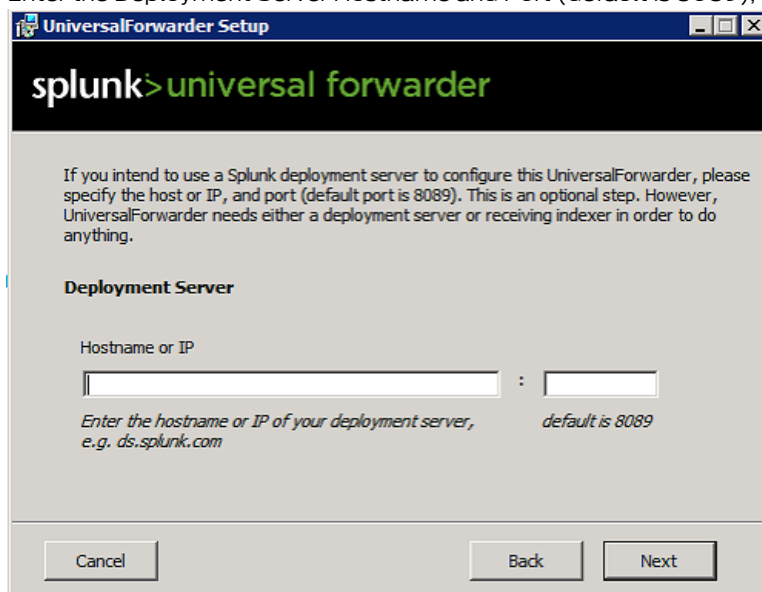


- In the next configuration window, shown below, select the Security Log forwarding option. Click Next.



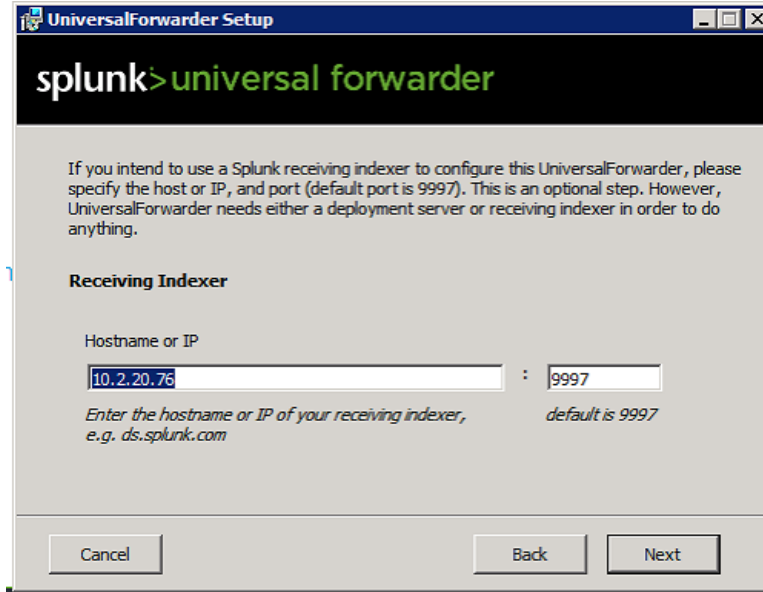
The screenshot shows the 'UniversalForwarder Setup' window. At the top, it says 'splunk>universal forwarder'. Below this, there are two columns of checkboxes. The left column is titled 'Windows Event Logs' and includes 'Application Logs', 'Security Log' (which is checked), 'System Log', 'Forwarded Events Log', and 'Setup Log'. The right column is titled 'Performance Monitor' and includes 'CPU Load', 'Memory', 'Disk Space', and 'Network Stats'. Below these columns is a section for 'Active Directory Monitoring' with a checkbox for 'Enable AD monitoring'. Underneath is a 'Path to monitor' label followed by a text input field and 'File...' and 'Directory...' buttons. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

- Enter the Deployment Server Hostname and Port (default is 8089), then click Next.



The screenshot shows the 'UniversalForwarder Setup' window. At the top, it says 'splunk>universal forwarder'. Below this is a paragraph of text: 'If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.' Below this text is a section titled 'Deployment Server'. It contains a label 'Hostname or IP' followed by a text input field, a colon, and another text input field for the port. Below the input fields is a note: 'Enter the hostname or IP of your deployment server, e.g. ds.splunk.com' and 'default is 8089'. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

- Enter the Receiver Index and Port (default is 9997), as in the example shown below, and then click Next..



5. Follow instructions to Get Active Directory Data from this link:
<http://docs.splunk.com/Documentation/MSApp/1.4.1/MSInfra/DownloadandconfiguretheSplunkAdd-onsforActiveDirectory>
 - Configure GPO's for AD and Powershell.
 - Download Splunk Add On For Microsoft Active Directory.
 - Download Splunk Add On for Microsoft Powershell.
 - Un-TAR both downloaded TAR files using 7zip or another archive utility.
 - Copy the resulting SA-ModularInput-PowerShell and Splunk_TA_microsoft_ad to the Universal Forwarder installed path:
`C:\Program Files\SplunkUniversalForwarder\etc\apps`
 - Restart Universal Forwarder components:
 - › services.msc
 - › Find SplunkForwarder Service and restart it.
 - Verify Splunk Search Head is receiving data by performing one of the following procedures:
 - › Search the UI at App & Reporting > Data Summary to verify that the Domain Controller Host is configured.
 - › Or search using "source="wineventlog:security" AND EventCode=4769 AND Service_Name != krbtgt | table _time Account_Name Client_Address Service_Name | rename _time as Logon_Time Account_Name as UserName Client_Address as IPAddress Service_Name as HostName"

6. Configure Splunk App for Windows Infrastructure on the Splunk Web Indexer; note the prerequisites:

The screenshot shows the Splunk Web interface for the 'App: Splunk App for Windows Infrastructure'. The 'Setup' progress bar is at the 'Prerequisites' step. Below the progress bar, the 'Prerequisites' section is displayed with a 'Redetect' button. A yellow warning box contains the text: 'Bypass pre-requisite checks' and 'Note: bypassing prerequisites might result in reduced or limited app functionality'. The prerequisites list includes: 'Splunk v6.2.0+' (OK: Splunk v6.5.3 detected, OK: Key value store is enabled. Learn more.), 'Splunk Add-on for Microsoft Windows v4.7.2+' (Could not determine the version for Splunk Add-on for Microsoft Windows. Check if the feature is installed. Download here.), 'Splunk Supporting Add-on for Microsoft Windows Active Directory v2.0.1+' (OK: Splunk Supporting Add-on for Microsoft Windows Active Directory v2.1.4 detected), and 'Users and/or groups configured with the winfra-admin user role:' (No users or groups with winfra-admin user role detected. Assign the winfra-admin user role via Splunk Settings >> Access Controls).

Prerequisites [Redetect](#)

Check prerequisites to be installed on the search head

☐ **Bypass pre-requisite checks**
Note: bypassing prerequisites might result in reduced or limited app functionality

✓ **Splunk v6.2.0+**
OK: Splunk v6.5.3 detected
OK: Key value store is enabled. [Learn more.](#)

✗ **Splunk Add-on for Microsoft Windows v4.7.2+**
Could not determine the version for Splunk Add-on for Microsoft Windows. Check if the feature is installed. [Download here.](#)

✓ **Splunk Supporting Add-on for Microsoft Windows Active Directory v2.0.1+**
OK: Splunk Supporting Add-on for Microsoft Windows Active Directory v2.1.4 detected

✗ **Users and/or groups configured with the winfra-admin user role:**
No users or groups with winfra-admin user role detected.
Assign the winfra-admin user role via Splunk Settings >> [Access Controls](#)

- Give winfra-admin role to admin user by modifying the roles for admin user as shown below:

Full name

Email address

Time zone

Set a time zone for this user.

Default app

Set a default app for this user. Setting this here overrides the default app inherited from the user's role(s).

Assign to roles

Assign this user to one or more roles. The user will inherit all the settings and capabilities from these roles.

Available roles

[add all »](#)

Selected roles

[« clear all](#)

- ☐ admin
- ☒ can_delete
- ☒ power
- ☒ splunk-system-role
- ☒ user
- ☐ winfra-admin

- ☒ admin
- ☒ winfra-admin

Set password

Password

Confirm password

Splunk WMI Forwarding of Active Directory Logs

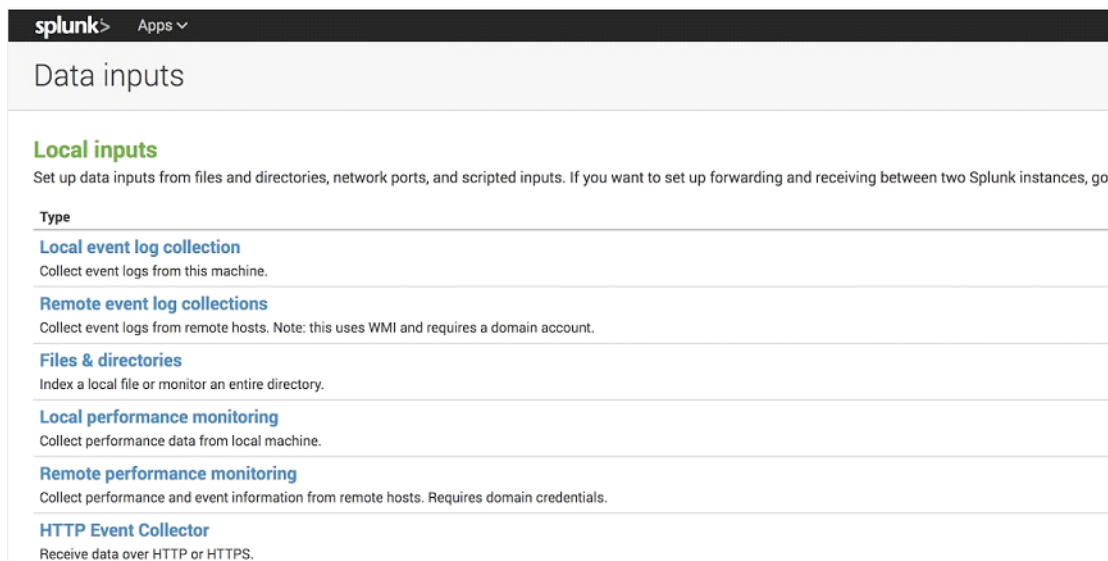
Use the following procedure to setup AD Integration with Splunk using the WMI method.

NOTE Setup requirements for the Splunk Server are also available from this link:
<http://docs.splunk.com/Documentation/Splunk/6.6.0/Data/MonitorWMIdata>

1. Both Splunk Enterprise and your Windows network must be correctly configured for WMI data access. Review the following prerequisites before attempting to use Splunk Enterprise to get WMI data.

Before Splunk Enterprise can get WMI-based data:

- Splunk Enterprise must be installed with a user that has permissions to perform remote network connections. While installing Splunk it would ask for local account or domain account. Choose domain account.
 - The user Splunk Enterprise runs as must be a member of an Active Directory (AD) domain or forest and must have appropriate privileges to query WMI providers.
 - The Splunk user must also be a member of the local Administrators group on the computer that runs Splunk Enterprise.
 - The computer that runs Splunk Enterprise must be able to connect to the remote machine(AD) and must have permissions to get the desired data from the remote machine once it has connected.
2. After installing Splunk, logon to Splunk and navigate to Settings -> Data Inputs:
 3. Click on the second option - Remote Event Log Collection, then click on New.



4. Choose a name for the log collection and enter the AD server IP address.
5. If Splunk can perform a WMI query to the AD server, then the Select Event Logs option is displayed, as shown below; Choose Security and click Next.

splunk Apps ▾

Add Data

Select Source Input Settings Review Done

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Configure this instance to monitor Event Log channels of remote Windows machines u Management Instrumentation (WMI) framework. Splunk must run as an Active Director access to the remote machine. Both Splunk and the remote machine must reside in the forest. [Learn More](#)

Event Log collection name? AD

Choose logs from this host? 10.2.14.3

Select Event Logs

Available item(s)	add all »	Selected ite
Application		
Security		
System		
DFS Replication		
DNS Server		

Select the Windows Event Logs you want to index from the list

Collect the same set of logs from additional hosts? optional

6. Enter the host details on the next page. If you want to choose an indexer, choose it or leave the default.

Review configurations and Submit.

7. From the Splunk Server, navigate to C:\Program Files\Splunk\etc\system\local and add the following configuration:

```
[WinEventLog://Security]
disabled = 0
start_from = oldest
current_only = 0
evt_resolve_ad_obj = 1
checkpointInterval = 5
```

8. Restart Splunk and verify that all Active Directory Security Logs are available in Splunk.

Carbon Black Response - Splunk Integration

Use the following information to perform Carbon Black Response and Splunk integration using either:

- [“Carbon Black Response Direct Log Ingestion: Event Forwarder of JSON Logs” in the next section](#)
- [Carbon Black Response Integration via Splunk Forwarder on page 206](#)
- [Carbon Black Response Ingestion Reporting at Juniper ATP Appliance on page 209](#)

NOTE See also [Configuring Carbon Black Response Log Events via Splunk on page 229](#); [Splunk Side Configuration for Carbon Black Response on page 229](#); [Configuring Carbon Black Response via Direct Log Ingestion on page 229](#).

IMPORTANT: A few notices about Carbon Black Response and Splunk integration:

- Juniper ATP Appliance requires Active Directory (AD) data for correlation with Carbon Black logs.
- AD, Splunk and Juniper ATP Appliance must be NTP-synced.
- Currently, from Carbon Black, only watchlist alert events are consumed by Juniper ATP Appliance:
 - › alert.watchlist.hit.ingress.host
 - › alert.watchlist.hit.ingress.binary
 - › alert.watchlist.hit.ingress.process
 - › alert.watchlist.hit.query.binary
 - › alert.watchlist.hit.query.process
- Correlation between Juniper ATP Appliance and Carbon Black Response is within 5 minutes.
- The endpoint hostname is the only match for correlating Carbon Black Response and Juniper ATP Appliance events.
- With Carbon Black Response Event Forwarder, there is an option to forward logs in JSON or LEEF format; Juniper ATP Appliance supports JSON format only at this time for both Splunk and Direct Log ingestion.
- For Direct Log Ingestion, logs can be sent to any random Juniper ATP Appliance port.
- The difference between Carbon Black Response integration and Carbon Black Direct Log Ingestion:
 - › During Carbon Black Response integration, Juniper ATP Appliance queries for only those events detected by Juniper ATP Appliance to obtain confirmation about the endpoint execution.
 - › In CB Log Ingestion, all events irrespective of whether Juniper ATP Appliance has seen it or not is pulled.
 - › If a CB event is correlated in CB log ingestion, then we don't mark the EX Progression.

Carbon Black Response Direct Log Ingestion: Event Forwarder of JSON Logs

1. Install the Carbon Black Response Event Forwarder :
<https://developer.carbonblack.com/reference/enterprise-response/event-forwarder/>
2. To send the Carbon Black Response event logs to any server via TCP or UDP, edit the Event Forwarder CONF file as in the example shown below:

```
In /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf
```

```
rabbitmq_username=cb
rabbitmq_password=<password>
cb_server_hostname=127.0.0.1
```

Take the username & password for the above from /etc/cb/cb.conf, search for RabbitMQUser & RabbitMQPassword and copy the value from the above file.

```
In /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf
```

Search for and enter the values shown below:

```
output_type=tcp or udp
output_format=json
```

If the TCP option is selected, configure the tap server and the listening port. Currently, you can select any random port to listen to.

```
tcpout=10.2.9.35:10516
```

If udp option is selected above, then configure the tap server & the listening port. Currently you can select any random port to listen to:

```
udpout=10.2.9.35:10516
```

Next, run the below command to receive output indicating which server the event forwarder has connected to.

```
[root@scb ~]# /usr/share/cb/integrations/event-forwarder/cb-event-forwarder -check
2017/05/08 03:42:38 Connected to tcp:10.2.9.35:10516 at 2017-05-08 03:42:38.068386476 -0700 PDT.
2017/05/08 03:42:38 Initialized output: tcp:10.2.9.35:10516
```

Start the event-forwarder:

```
[root@cb]# initctl start cb-event-forwarder
```

Carbon Black Response Integration via Splunk Forwarder

1. From the Carbon Black Response Server, install the Carbon Black Response Event Forwarder:
<https://developer.carbonblack.com/reference/enterprise-response/event-forwarder/>
2. Download the relevant binaries from this link:
https://www.splunk.com/en_us/download/universal-forwarder.html
3. Install Splunk Add on for Bit9 Carbon Black to your Splunk instance. Set the Splunk Common Information Model.
<https://splunkbase.splunk.com/app/2790/>
4. Configure the Carbon Black Response Event Forwarder; this is required to save the Carbon Black Response event logs to a file using the contents to forward data to Splunk.

```
In /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf
```

```
rabbitmq_username=cb
rabbitmq_password=<password>
cb_server_hostname=127.0.0.1
```

Apply the username and password shown above from /etc/cb/cb.conf, search for RabbitMQUser and RabbitMQPassword, and copy the value to the above CONF file.

```
In /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf
```

Search & enter the values below:

```
output_type=file
output_format=json
outfile=/var/cb/data/event-forwarder/data.json
```

The above outfile can be anything; in this example, the link stores the event logs.

Run the command below to get the output shown below.

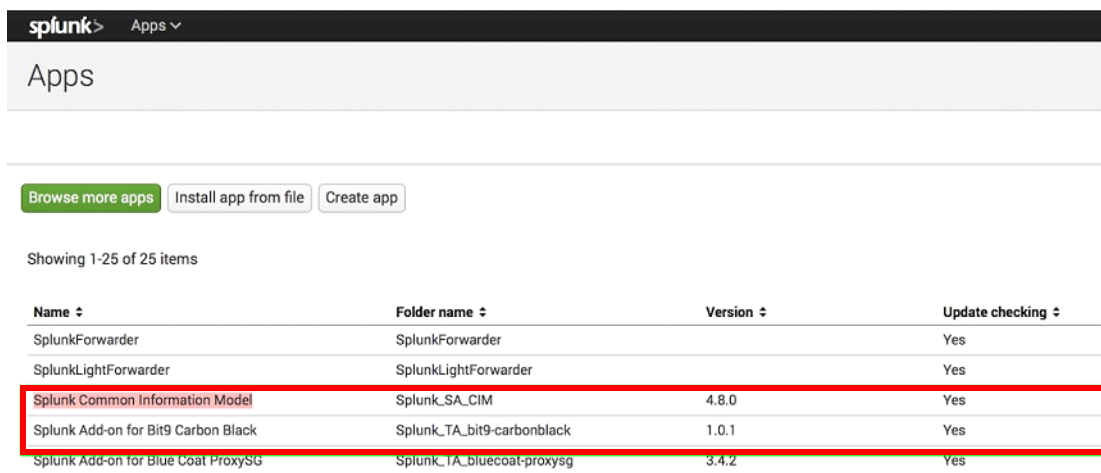
```
[root@cb]# /usr/share/cb/integrations/event-forwarder/cb-event-forwarder -check
2017/04/20 02:42:58 Initialized output: File /var/cb/data/event-forwarder/data.json
```

Start the event-forwarder:

```
[root@cb]# initctl start cb-event-forwarder
```

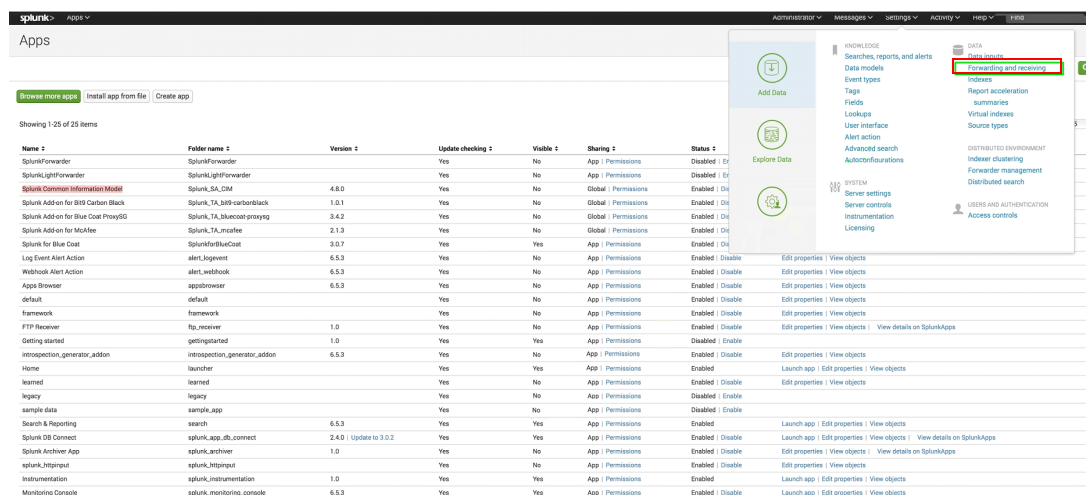
5. Configure the Splunk Add on for Bit 9 Carbon Black Response.

6. Set the Splunk Common Information Model as shown below:



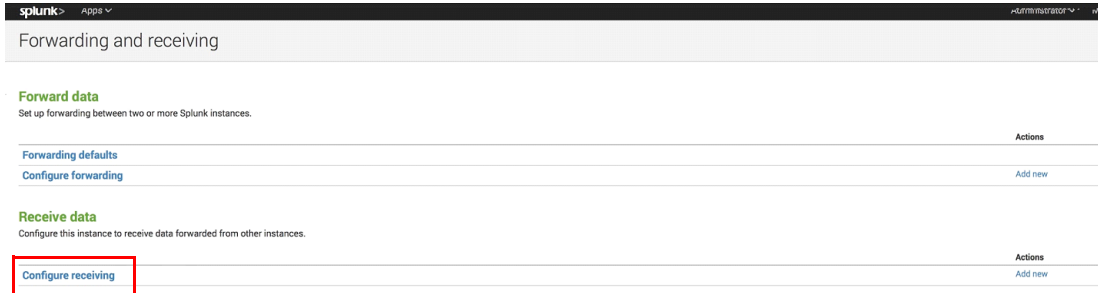
Name	Folder name	Version	Update checking
SplunkForwarder	SplunkForwarder		Yes
SplunkLightForwarder	SplunkLightForwarder		Yes
Splunk Common Information Model	Splunk_SA_CIM	4.8.0	Yes
Splunk Add-on for Bit9 Carbon Black	Splunk_TA_bit9-carbonblack	1.0.1	Yes
Splunk Add-on for Blue Coat ProxySG	Splunk_TA_bluecoat-proxysg	3.4.2	Yes

7. Configure the Receiver for your Splunk Instance to set the Splunk Forwarder to forward data; Navigate to Splunk > Settings > Forwarding & Receiving.

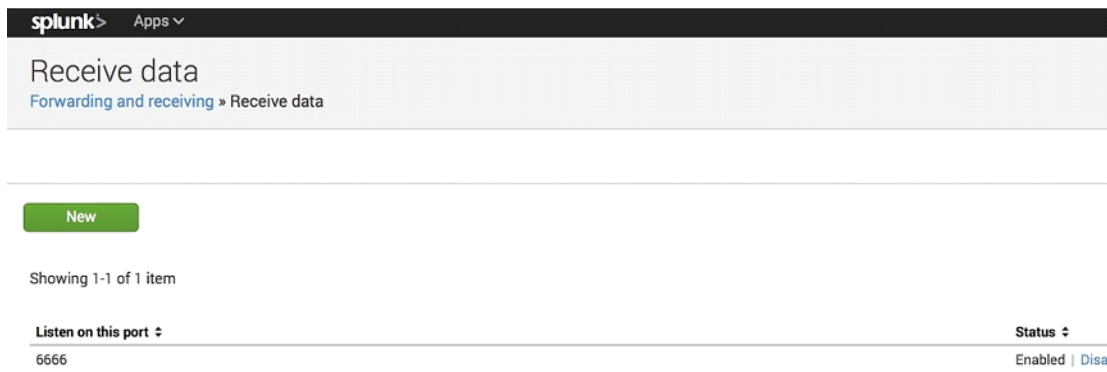


Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		No	App	Permissions	Disabled	Enable
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App	Permissions	Disabled
Splunk Common Information Model	Splunk_SA_CIM	4.8.0	Yes	No	Global	Permissions	Enabled
Splunk Add-on for Bit9 Carbon Black	Splunk_TA_bit9-carbonblack	1.0.1	Yes	No	Global	Permissions	Enabled
Splunk Add-on for Blue Coat ProxySG	Splunk_TA_bluecoat-proxysg	3.4.2	Yes	No	Global	Permissions	Enabled
Splunk Add-on for McAfee	Splunk_TA_mcafee	2.1.3	Yes	No	Global	Permissions	Enabled
Splunk for Blue Coat	SplunkForBlueCoat	3.0.7	Yes	Yes	App	Permissions	Enabled
Log Event Alert Action	alert_logevent	6.5.3	Yes	No	App	Permissions	Enabled
Webhook Alert Action	alert_webhook	6.5.3	Yes	No	App	Permissions	Enabled
App Browser	appbrowser	6.5.3	Yes	No	App	Permissions	Enabled
default	default		Yes	No	App	Permissions	Enabled
framework	framework		Yes	No	App	Permissions	Enabled
FTP Receiver	ftp_receiver	1.0	Yes	No	App	Permissions	Enabled
Getting started	gettingstarted	1.0	Yes	Yes	App	Permissions	Disabled
Introspection generator_addon	introspection_generator_addon	6.5.3	Yes	No	App	Permissions	Enabled
Home	launcher		Yes	Yes	App	Permissions	Enabled
learned	learned		Yes	No	App	Permissions	Enabled
legacy	legacy		Yes	No	App	Permissions	Disabled
sample data	sample_app		Yes	No	App	Permissions	Disabled
Search & Reporting	search	6.5.3	Yes	Yes	App	Permissions	Enabled
Splunk DB Connect	splunk_app_db_connect	2.4.0 / Update to 3.0.2	Yes	Yes	App	Permissions	Enabled
Splunk Archive App	splunk_archiver	1.0	Yes	No	App	Permissions	Disabled
splunk_httpinput	splunk_httpinput		Yes	No	App	Permissions	Enabled
Instrumentation	splunk_instrumentation	1.0	Yes	Yes	App	Permissions	Enabled
Monitoring Console	splunk_monitoring_console	6.5.3	Yes	Yes	App	Permissions	Enabled

8. Click on Configure Receiving.



9. Configure a port to listen on. In this example: port 6666.



10. Set up the Splunk Universal Forwarder to forward Carbon Black Response data to Splunk by downloading and installing the Universal Forwarder RPM on the Carbon Black Response server:
https://www.splunk.com/en_us/download/universal-forwarder.html

```
rpm -ivh splunkforwarder-6.5.3-36937ad027d4.i386.rpm

[root@cb]# cd /opt/splunkforwarder/bin

[root@cb]# ./splunk
Data forwarding configuration management tools.
Commands:
  enable local-index [-parameter <value>] ...
  disable local-index [-parameter <value>] ...
  display local-index
  add forward-server server
  remove forward-server server
  list forward-server
Objects:
  forward-server      a Splunk forwarder to forward data to be indexed
  local-index         a local search index on the Splunk server

[root@cb bin]# ./splunk add forward-server 10.2.14.219:6666
```

In the above command 10.2.14.219 is the splunk server & 6666 is the port we have configured in Step 3 on which Splunk is receiving.

```
[root@cb local]# pwd
/opt/splunkforwarder/etc/system/local

[root@cb local]# cat inputs.conf
[default]
```



```
host = cbtest

[monitor:///var/cb/data/event-forwarder]
sourcetype = bit9:carbonblack:json

[root@cb local]
```

11. Add an input host file. In this example, cbtest is used, which can be searched for in Splunk.

The monitor is the directory of data.json, which is configured in Step 1.

The sourcetype shows which data needs to be sent, which is from Carbon Black Response.

```
[root@cb bin]# cd /opt/splunkforwarder/bin
[root@cb bin]# ./splunk start
```

12. Start Splunk.

13. Check the forward-server.

```
[root@cb bin]# ./splunk list forward-server
Splunk username: admin
Password:
Active forwards:
10.2.14.219:6666
Configured but inactive forwards:
None
[root@cb bin]#
```

Carbon Black Response Ingestion Reporting at Juniper ATP Appliance

Carbon Black Response log ingestion can be viewed from the Juniper ATP Appliance Central Manager Web UI Incidents page and Events Timeline Dashboard:

Configuring Anti-SIEM Splunk Ingestion

Configure Splunk integration from the Juniper ATP Appliance Web UI as well as from the Splunk UI.

- [Juniper ATP Appliance Side - Splunk Integration Configuration on page 209](#)
- [Splunk Side - Splunk Configuration on page 210](#)

Juniper ATP Appliance Side - Splunk Integration Configuration

To configure Anti-SIEM Splunk Ingestion, perform the following steps.

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>Splunk Configuration page.

Figure 30 Anti-SIEM Splunk Ingestion Configuration Page

The screenshot shows the 'Config' tab of the Juniper ATP Appliance interface. The left sidebar contains various configuration categories, with 'Splunk Configuration' selected. The main panel displays the 'Splunk Ingestion Settings' form. The 'Enabled' checkbox is checked. The 'Splunk host' field is empty. The 'Splunk management port' is set to '8089'. The 'Splunk login' is 'juniperdoc' and the 'Splunk password' is masked with asterisks. A green 'Submit' button is at the bottom of the form. Below the form is a 'Test Splunk Ingestion Settings' section with a green 'Test' button.

2. Enter the Splunk Host IP address and Splunk Management Port number.

NOTE Be sure to enter the Splunk port number 8089, not 8080.

3. Enter your Splunk Login and Password.
4. Click Enable to make the configuration active; deselect to disable the configuration.
5. Click Submit to activate an enabled Splunk configuration.
6. Test the Splunk Configuration Ingestion Settings by clicking the Test button.

NOTE Splunk environments allow for implementation of multiple ports that are all user-configurable; be sure to configure the Splunk management port on this page if you are having trouble connecting to Splunk. Check your Splunk site for your settings if your admin is not using the defaults.

Splunk Side - Splunk Configuration

At the Splunk console, include the following settings for integration with Juniper ATP Appliance; in this example, the PAN Add-on is configured:

Figure 31 Palo Alto Networks Add-on for Splunk

Browse more apps Install app from file Create app

Showing 1-1 of 1 item

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Palo Alto Networks Add-on for Splunk	Splunk_TA_paloalto	3.8.0	Yes	No	Global Permissions	Enabled Disable	Set up E

Figure 32 Splunk Common Information Model Settings

Showing 1-1 of 1 item

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Splunk Common Information Model	Splunk_SA_CIM	4.8.0	Yes	No	Global Permissions	Enabled Disable	Set up Edit

NOTE At the Splunk console, be sure PAN-Add-ons and Splunk Common Information Model is configured for Juniper ATP Appliance to talk to Splunk.

Integrating Anti-Siem External Event Collectors

To setup Anti-SIEM External Event Collectors, perform the following configurations per vendor option:

- Firewall
[PAN Next Gen Firewall: Log Collector | Splunk Ingestion] [page 211](#)
- Web Gateway
[Bluecoat Secure Web Gateway: Log Collector | Splunk Ingestion] [page 219](#)
- Endpoint AV
[ESET | McAfee ePO | Symantec: Log Collector | Splunk Ingestion] [page 225](#)
- Endpoint Response
[Carbon Black Response: Log Collector | Splunk Ingestion] [page 229](#)

Anti-SIEM Firewall [PAN: Log Collector | Splunk Ingestion]

To configure Anti-SIEM External Event Collector settings for PAN Next Gen Firewalls, perform the following configurations for direct Log Collection or Splunk ingestion options:

PAN Log Collector Configuration - Juniper ATP Appliance Side

Use the following procedure to configure direct ingestion of event data from PAN, where Juniper ATP Appliance essentially acts as a syslog server but one that identifies only relevant malware events.

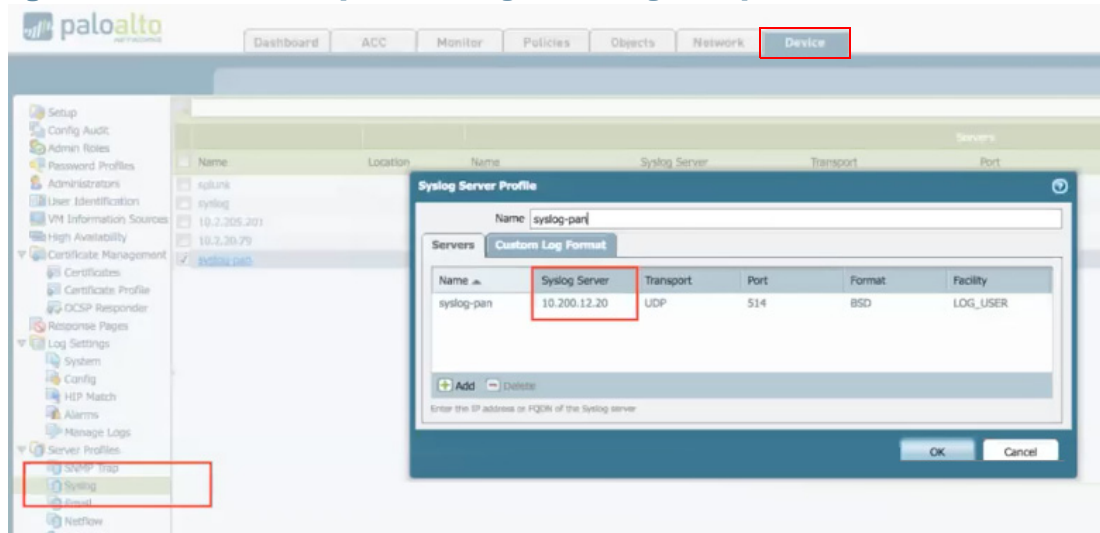
1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page.
2. Select Firewall as the Source Type, and PAN Next Gen Firewall as the Vendor Name.
3. For Transport, select the Log Collector option.
4. Enter the Log Source Identifier; for example: PA-200. This is the host name portion of the syslog message that Juniper ATP Appliance uses to identify which vendor is incoming, and how Juniper ATP Appliance will parse its logged events. [On the PAN UI in the following screenshot, notice that the configured Device Name is the same as the Juniper ATP Appliance Log Source Identifier.]
5. Choose SSL Enabled | Disabled.
6. Select a Default Severity setting: Max | High | Med | Low | Benign
7. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from PAN direct ingestion will be created according to the severity setting selected in step 6. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
8. Click Add to perform the Log Collector configuration.

PAN-Side Direct Ingestion Settings

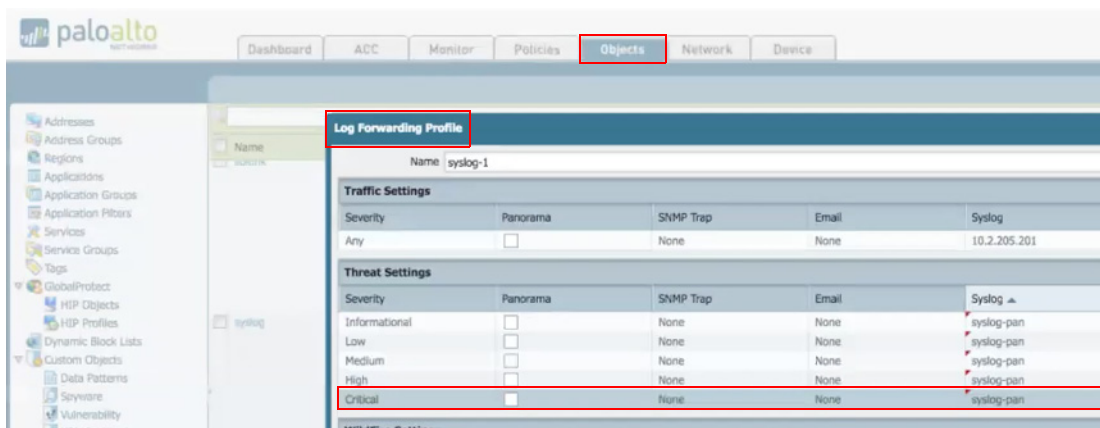
At the PAN UI, configure your Juniper ATP Appliance Core as a syslog server. If your PAN device is exporting to your own syslog server, just add Juniper ATP Appliance as another syslog server because PAN can export to multiple syslog destinations simultaneously.

1. Navigate to the PAN console Device>Syslog>+Add configuration page:

Figure 33 Anti-SIEM Firewall [PAN: Direct Ingestion Configuration]

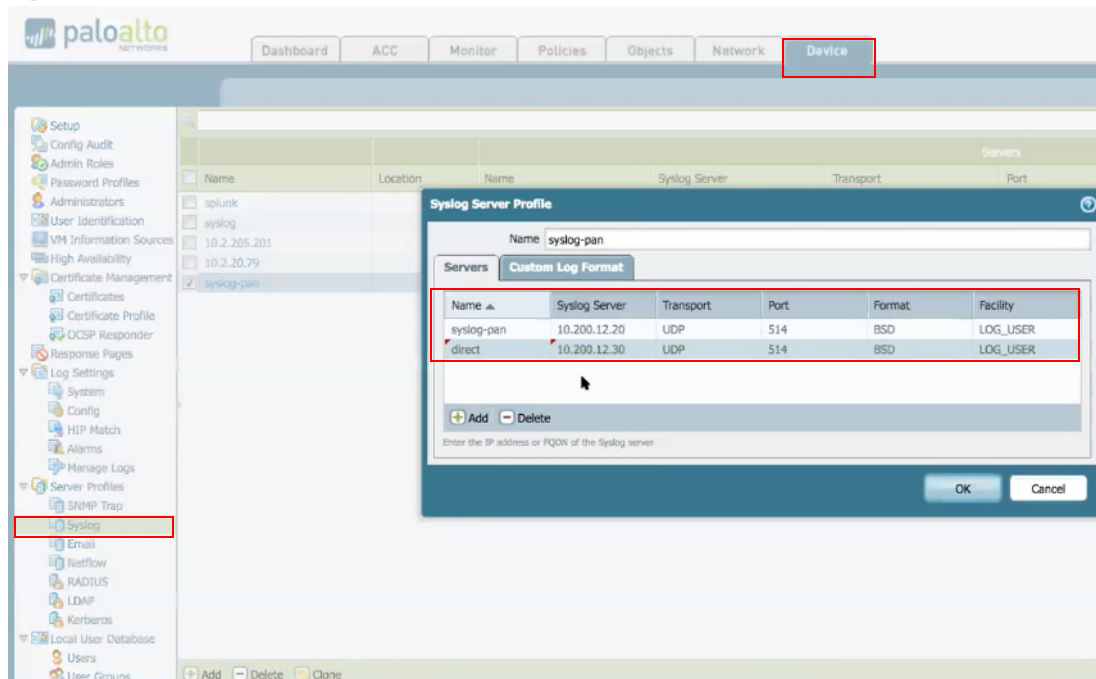


2. Select the same syslog server for log forwarding on the Objects>Log Forwarding>+Add page from the syslog dropdown:



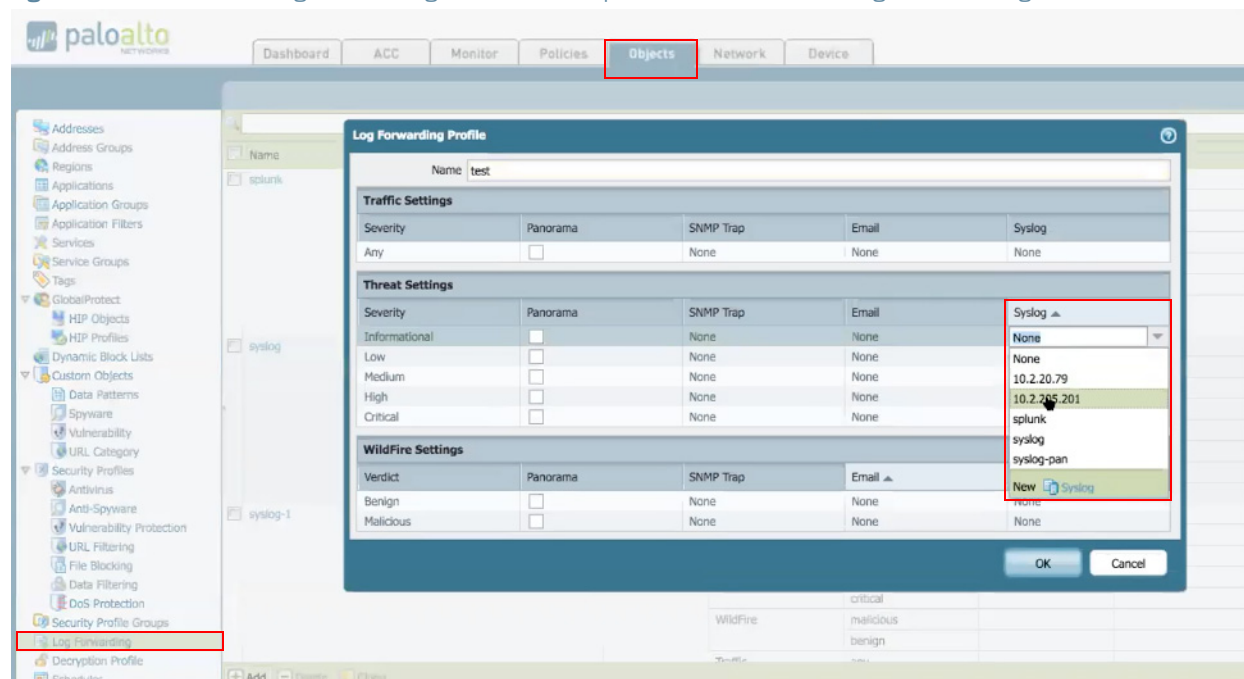
During forwarding of syslogs from PAN, when events exceed the 1500 supported limit, Juniper ATP Appliance recommends limiting export from PAN to critical events only by adjusting settings on the PAN console Log Forwarding Profile page.

Figure 34 Sample Direct Ingestion Configuration from PAN Side



Be sure to navigate to the Syslog Log forwarding Profile, select where to send the logs (either to the Juniper ATP Appliance Core via direct ingestion, or to Splunk, or to both, and then Commit.

Figure 35 Commit the Log Forwarding Profile to Complete PAN-Side Direct Ingestion Configuration



Direct Ingestion PAN Event Filtering

The number generated syslogs/sec during direct ingestion is 1500; the number of syslogs/day (average of 10 hours) is 54 million. For this reason, Juniper ATP Appliance uses event filtering for efficient ingestion, handling and reporting of events and does not store any events that are informational or benign.

PAN events created via direct ingestion for display in the Juniper ATP Appliance Events Timeline Dashboard use the following filters:

- › Ignore informational events
- › Ignore events with the action “wildfire-upload-success”, “wildfire-upload-skip” and “forward” because these logs are not indicative of malware events.

Figure 36 Sample Direct Ingestion Log

Check `tail -f /var/log/cyos/logcollector/cyos-log-collector.log`

```
2017-06-23 15:38:21,153 [INFO/MainThread/pid:24421] default/default: Starting submission
2017-06-23 15:38:22,924 [INFO/MainThread/pid:25189] default/default: Connecting to ps
2017-06-23 15:38:22,924 [INFO/MainThread/pid:25189] default/default: Connecting to cc

2017-06-23 15:40:47,777 [INFO/MainThread/pid:25189] default/default: Submitting:
{'can_correlate_bidirectionally': False, 'endpoint_ip': '172.16.2.101', 'event_type': 'third_party', 'detection_method': 'trust-untrust', 'vendor_product': 'pan', 'can_create_incident': True, 'action_is_blocked': True, 'collector_uuid': '00000000-0000-0000-0000-000000000003', 'event_id': 1498257645.0, 'force_correlate': True, 'event_action': 'Download', 'third_party_severity': 0.0, 'LOG': 'LOG', 'action_response': 'deny', 'third_party_info': {'file_name': '7e8e1d0ab5db517cdcdddbafd54bbb4ac6651bc3eada369d2eb34428a9f6f3c', 'severity': 1, '2017/06/23 15:40:45,001606020919,THREAT,virus,1,2017/06/23 15:40:45,74.0.0.10,172.16.2.101,0.0.0.0,0.0.0.0,trust-untrust,,,web-browsing,vsys1,untrust,trust1/1,syslog-1,2017/06/23 15:40:45,3000,1,80,25577,0,0,0x30000,tcp,deny,\"7e8e1d0ab5db517cdcdddbafd54bbb4ac6651bc3eada369d2eb34428a9f6f3c\",Trojan/Win32.swisyn.fxgg(2151712),any,medium,server-to-client,8038,0.1.255.255,0,,0,,,1,,,,,,0\\x00}', 'can_correlate': True}
```

PAN and Splunk Integration Configuration

Use the following procedure to configure Splunk integration for the PAN Next Gen Firewall on the Juniper ATP Appliance side. Refer to for information about configuring integration from the Splunk side.

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:

Figure 37 Anti-SIEM Firewall [PAN: Splunk Ingestion Configuration]

The screenshot shows the configuration page for the Anti-SIEM Firewall. The left sidebar lists various configuration categories. The main configuration area includes the following settings:

- Source Type:** Firewall (selected)
- Vendor Name:** PAN Next Gen Firewall (selected)
- Transport:** Splunk (selected)
- Optional Splunk Index:** pan
- Default Severity:** Low (selected)
- Create Incident:** Enabled (selected)

An 'Add' button is located to the right of the Default Severity options. Below the configuration fields is a 'Cancel' button. At the bottom, there is a table titled 'Current Third Party Sources' with the following structure:

Category	Vendor	Transport	Actions

2. Select Firewall as the Source Type, and PAN Next Gen Firewall as the Vendor Name.
3. For Transport, select the Splunk option.
4. Enter the Optional Splunk Index; enter the index used for PAN logging into Splunk. For example: pan
5. Select a Default Severity setting: Max | High | Med | Low | Benign
6. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from Splunk ingestion will be created according to the severity setting selected in step 5. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
7. Click Add to perform the Splunk integration.

NOTE For more information about Splunk integration, refer to [Configuring Anti-SIEM Splunk Ingestion on page 209](#). For guidelines specific to Splunk configurations from the Splunk console, see the next section.

Splunk Side Configuration for PAN

This section does not cover Splunk configuration. However, when configuring Splunk from the Splunk console for integration with Juniper ATP Appliance, there are a few items you'll need to be sure are set for PAN:

1. Navigate to Splunk>Apps>Manage Apps, then confirm configuration is established for Palo Alto Add-on for Splunk., and that Status shows as Enabled.

Browse more apps Install app from file Create app

Showing 1-1 of 1 item

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Palo Alto Networks Add-on for Splunk	Splunk_TA_paloalto	3.8.0	Yes	No	Global Permissions	Enabled Disable	Set up Edit

2. At Splunk>Apps>Manage Apps, check for and confirm setup is complete and Enabled for Common Information Model.

Browse more apps Install app from file Create app

Showing 1-1 of 1 item

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
Splunk Common Information Model	Splunk_SA_CIM	4.8.0	Yes	No	Global Permissions	Enabled Disable	Set up Edit

3. At Settings>Data>Data Inputs>UDP/TCP, click the link to review the Index. You can click this link to check the Index configured for PAN. Be sure to do the same on the Juniper ATP Appliance Configuration page for [Anti-SIEM Firewall \[PAN: Log Collector | Splunk Ingestion\] on page 211](#) for the Splunk configuration.

New

Showing 1-1 of 1 item Results per page 25

UDP port	Source type	Status	Actions
514	pan:log	Enabled Disable	Clone Delete

4. From the Splunk>Settings>Data Inputs>Port>PortNumber page, under “More Settings” (check the checkbox to expand), confirm that the Source type is “pan:log,” and check the index that is currently configured so you could use it in the Juniper ATP Appliance Configuration for Anti-SIEM Firewall [PAN: Splunk Ingestion Configuration] on [page 211](#) for the Splunk configuration.

Settings | Splunk

If set, overrides the default source value for your UDP entry (host:port).

Source type
Set sourcetype field for all events from this source.

Set sourcetype
Manual

Source type *
pan:log

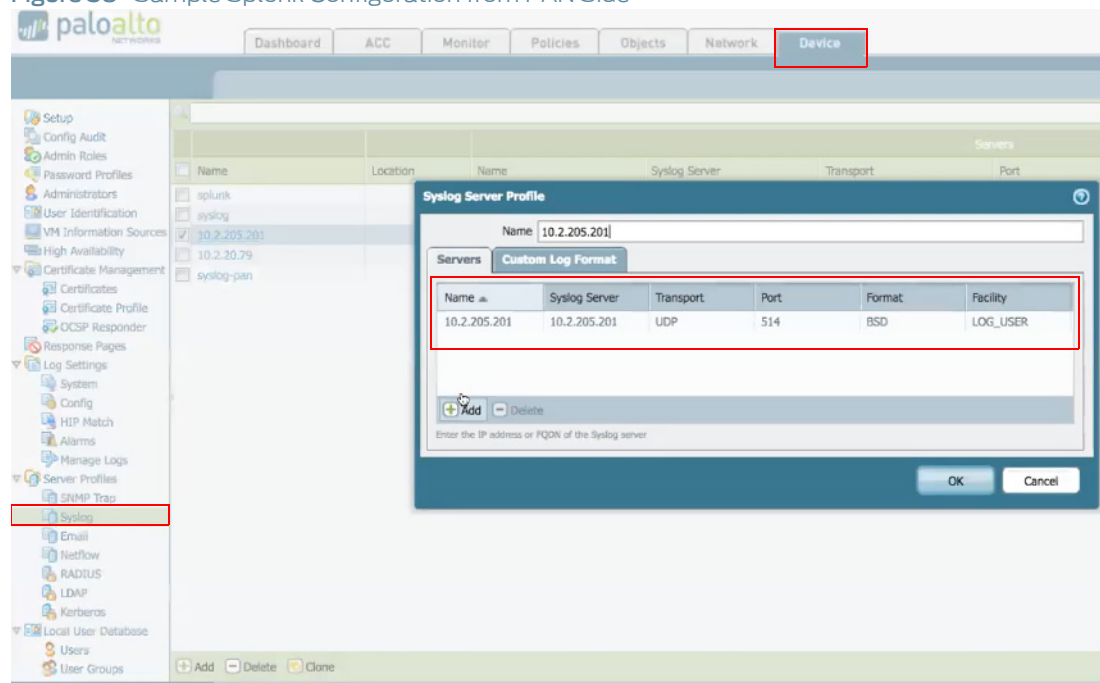
☒ More settings

Host
Set host
☐ IP ☒ DNS ☐ Custom
"DNS" sets the host to the DNS entry of the remote server.

Index
Set the destination index for this source.
Index
pan

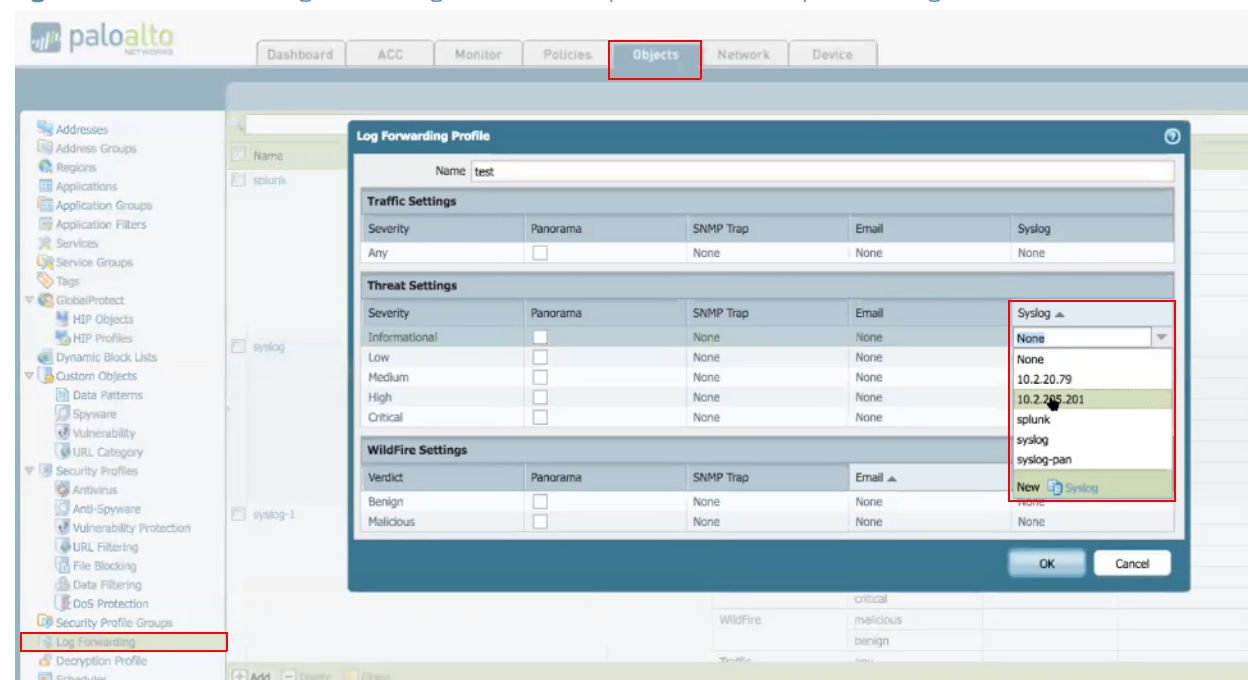
NOTE The Source type must be configured as “pan:log” and Index as “pan” for integration with Juniper ATP Appliance.

Figure 38 Sample Splunk Configuration from PAN Side



Be sure to navigate to the Syslog Log forwarding Profile, select where to send the logs (either to the Juniper ATP Appliance Core via direct ingestion, or to Splunk, or to both and then Commit.

Figure 39 Commit the Log Forwarding Profile to Complete PAN-Side Splunk Configuration



Splunk Integration Event Filtering

PAN events created via Splunk integration classify events according to the following Splunk “Common Information Models” (CIM) via the Splunk PAN Add-on:

- › Web
- › Intrusion Detection
- › Malware Attacks

NOTE To display relevant information in the Juniper ATP Appliance Event Timeline Dashboard, Juniper ATP Appliance ignores informational events; benign and allowed events are also ignored by Juniper ATP Appliance.

Figure 40 Splunk Ingestion Log

Check `/var/log/cyos/logingestion/cyos-splunk-poller-service.log`

```
2017-06-22 11:09:19,176 [INFO/10.2.129.6:8089/pid:32043] default/default: Using Web query:
| datamodel Web Web search
| eval cy_epoch_time=_time
| search Web.action=blocked AND ((sourcetype=pan:threat AND severity!=informational index=pan))
| fields Web.* src_ip src_host dest_ip dest_host
_raw cy_epoch_time host sourcetype
vendor_action

2017-06-22 11:09:19,177 [INFO/10.2.129.6:8089/pid:32043] default/default: Using IDS query:
| datamodel Intrusion_Detection search
| eval cy_epoch_time=_time
| search (sourcetype=pan:threat AND IDS_Attacks.action!=allowed index=pan)
| fields IDS_Attacks.* src_ip src_host dest_ip dest_host
```

Figure 41 Sample Splunk Log via PAN

Check `/var/log/cyos/logingestion/cyos-splunk-poller-service.log`

```
INFO:cy_logger_stdout:default/default: Get events indexed between '2017-06-23 11:08:01.689746
11:09:02.242997'
2017-06-23 11:09:02,373 [INFO/10.2.205.201:8089/pid:24746] default/default: web: 0 logs, made 0 e
INFO:cy_logger_stdout:default/default: web: 0 logs, made 0 events, 0 seconds
2017-06-23 11:09:02,504 [INFO/10.2.205.201:8089/pid:24746] default/default: ids: 0 logs, made 0 eve
INFO:cy_logger_stdout:default/default: ids: 0 logs, made 0 events, 0 seconds
2017-06-23 11:09:02,653 [INFO/10.2.205.201:8089/pid:24746] default/default: malware: 0 logs, made
INFO:cy_logger_stdout:default/default: malware: 0 logs, made 0 events, 0 seconds
2017-06-23 11:10:02,653 [INFO/10.2.205.201:8089/pid:24746] default/default: Get events indexed be
11:09:02.242997' - '2017-06-23 11:10:02.653717'
INFO:cy_logger_stdout:default/default: Get events indexed between '2017-06-23 11:09:02.242997'
11:10:02.653717'
2017-06-23 11:10:02,794 [INFO/10.2.205.201:8089/pid:24746] default/default: web: 0 logs, made 0 e
INFO:cy_logger_stdout:default/default: web: 0 logs, made 0 events, 0 seconds
2017-06-23 11:10:03,187 [INFO/10.2.205.201:8089/pid:24746] default/default: ids: 1 logs, made 1 ev
INFO:cy_logger_stdout:default/default: ids: 1 logs, made 1 events, 0 seconds
2017-06-23 11:10:03,338 [INFO/10.2.205.201:8089/pid:24746] default/default: malware: 0 logs, made
INFO:cy_logger_stdout:default/default: malware: 0 logs, made 0 events, 0 seconds
```

Incident Reporting for PAN Syslog Ingestion

Refer to the following sample Incident display to view Juniper ATP Appliance detection and reporting of PAN syslog ingestion.

In this example, PAN allowed a download to pass through, and Juniper ATP Appliance detected the event.

Note that Juniper ATP Appliance detected the Download and external source log collection also marked it as a malicious event:

This same incident is reported on the Juniper ATP Appliance Events Timeline host view as follows; note that both the PAN Download Event and the Juniper ATP Appliance Malware Detection Event are reported:

In another, different example, we can see in the Events Timeline Dashboard that Juniper ATP Appliance detected a malicious event, and PAN performed a DENY:

TIP Be sure to expand the Timeline view to see how and when the enduser enacted the malicious download:

Anti-SIEM Web Gateway [Bluecoat: Log Collector | Splunk Ingestion]

Juniper ATP Appliance integrates with Bluecoat Proxy Secure Gateway to facilitate mitigation. Bluecoat periodically retrieves bad Web URLs from Juniper ATP Appliance and blocks them. (The list of bad URLs are the same as those delineated on the Juniper ATP Appliance's Mitigation tab > Secure Web Gateways, which lists the URLs to be mitigated. Essentially, Bluecoat has the capability of pulling the malicious URLs list from Juniper ATP Appliance through HTTP/HTTPS. Hence, Juniper provides the malicious URLs list for Bluecoat to poll.

Juniper ATP Appliance leverages existing third party security devices such as Bluecoat to automatically block malicious Web URLs. This is extremely significant because other vendors do not block malicious Web downloads; they only block infections.

Use the following procedures to configure Bluecoat Secure Web Gateway Log Collector Ingestion or Splunk Ingestion.

- [“Configuring a Bluecoat Secure Web Gateway Log Collector” in the next section](#)
- [Configuring Splunk to Bluecoat Integration on page 220](#)
- [Configuring Bluecoat to Juniper ATP Appliance Integration on page 221](#)
- [Configuring Bluecoat Secure Web Gateway Splunk Ingestion on page 224](#)

Configuring a Bluecoat Secure Web Gateway Log Collector

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:

Figure 42 Anti-SIEM Web Gateway [Bluecoat: Log Collector Configuration]

The screenshot shows the 'Config' tab of the Juniper ATP Appliance interface. The left sidebar contains a navigation menu with options like Notifications, System Profiles, Environmental Settings, and various configuration sections. The main content area is titled 'ADVANCED THREAT PREVENTION APPLIANCE' and includes a 'Refresh Data' button and user information 'juniper Doc'. Below the navigation menu, there are four configuration sections: 'Source Type' (with radio buttons for Firewall, Web Gateway, Endpoint AV, and Endpoint Response; 'Web Gateway' is selected), 'Vendor Name' (with a dropdown menu showing 'Bluecoat Secure Web Gateway' selected), 'Transport' (with radio buttons for Log Collector and Splunk; 'Log Collector' is selected), and 'Default Severity' (with radio buttons for Max, High, Med, Low, and Benign; 'Low' is selected). There is also a 'Create Incident' section with radio buttons for Enabled and Disabled; 'Disabled' is selected. A 'Cancel' button is located below these sections. At the bottom, there is a table titled 'Current Third Party Sources' with columns for Category, Vendor, Transport, and Actions.

2. Select Web Gateway as the Source Type.
3. Select Bluecoat Secure Web Gateway as the Vendor Name.
4. For Transport, select the Log Collector option.
5. Enter the Input Port.
6. Select a Default Severity setting: Max | High | Med | Low | Benign
7. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from Splunk ingestion will be created according to the severity setting selected in step 6. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
8. Click Add to perform the Bluecoat Secure Web Gateway Log Collector configuration.

Configuring Splunk to Bluecoat Integration

Before configuring Splunk for Bluecoat integration with Juniper ATP Appliance, consider the following prerequisites:

- Have the Splunk enterprise version installed and running
- Have the Splunk for Bluecoat app installed and running
- Have the Splunk Add-on for Blue Coat ProxySG running
- Have Bluecoat CLI access, with access to Enable Mode and Configure Mode
- Note that Juniper ATP Appliance only supports the bcreportermain_v1 log type currently, so no other log type will work
- Be sure to use NTP service on the Splunk server so that Splunk and Bluecoat time are in sync
- After integration, observe the Splunk logs under "bcoat_logs" and confirm the time matches Splunk's time. For example, if Splunk is in PST, the data coming from Bluecoat under "bcoat_logs" index should also be set for PST. If there is no time match, integration might not work properly

Juniper ATP Appliance Side Configuration

1. Navigate to Config > Environmental Settings > Splunk Configuration at the Juniper ATP Appliance Central Manager console.
2. Add the Splunk configuration Username, Password and Port, then set as Enabled and click Test Configuration to verify. If the connection is established successfully, a success message is displayed.
3. Add Bluecoat as an External Event Collector; refer to [Anti-SIEM Web Gateway \[Bluecoat: Log Collector | Splunk Ingestion\] on page 219](#).
Be sure to select transport "log collector / Splunk. Provide a port number if selecting log collector and an optional index if selecting the splunk option, then add the settings.

Bluecoat Side Configuration

1. Login to the Bluecoat CLI and enter Enable mode, then enter Configure mode.
2. Enter access-log settings: enter the command "edit log main."
3. Select client type as custom client.
4. Select access log enable.
5. Select upload type text.
6. Select custom client primary <Juniper ATP Appliance Core IP or Splunk Server IP> <any port number you want to use for integration > and click Enter.
7. Enable continuous upload and the integration is done on Juniper ATP Appliance side

Splunk Side Configuration

1. At the Splunk console, navigate to Settings -> Data Inputs.
2. In the Local Input menu, click Add New in the TCP Port menu. A new page will open with 4 fields:
3. In the Port field input the port number (the port number configured in the Bluecoat custom client), then click Next. Make sure the type remains as TCP.
4. In the next window, select the source type as "bluecoat:proxysg:access:syslog".
5. On the same page, select the index type as "bcoat_logs," and click Review.
6. Review the data and click Next. The bluecoat configuration is now complete.

Within a few minutes the Bluecoat logs will start appearing on the Splunk side. Be sure to use index="bcoat_logs" for filtering the logs.

Configuring Bluecoat to Juniper ATP Appliance Integration

In order to allow Bluecoat to connect to Juniper ATP Appliance's self signed SSL apache server with HTTPS, the PEM file from the Juniper ATP Appliance server must be accessed. Then, you import the PEM file to the Bluecoat SSL certificate list.

NOTE The common name (CN) in the PEM has to be matched with the hostname in the URL Bluecoat is using to poll. This is the reason why PEM regeneration is tied to parsing of the common name obtained from the PEM file to add it to the generated URL.

Juniper ATP Appliance Side Setup

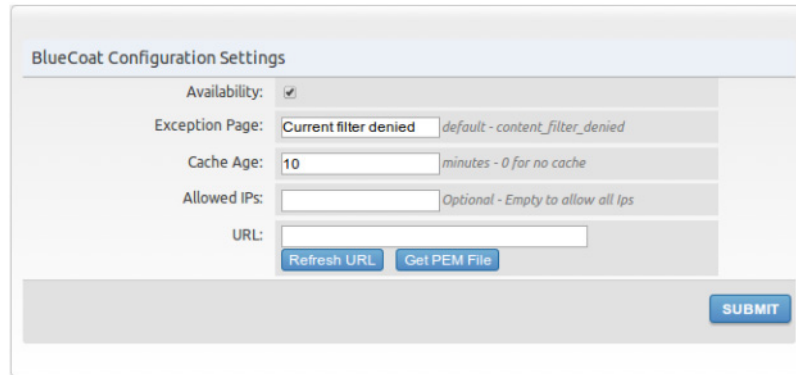
1. Navigate to Config > System Settings > System Settings.
2. Change the "Server fully qualified domain name" appropriately. This is going to be the common name in the PEM, and also the host name that Bluecoat is sending the request to. Therefore, you need to make sure Bluecoat can access this host by using the name specified.
3. Click the Submit button. The new PEM file is generated on the server, and the Apache requires a restart to apply the change. Refresh the UI by pressing F5 until you see a new warning "The site's security certificate is not trusted!" (via Chrome, for example). This warning indicates that the PEM is changed.

4. Navigate to the Bluecoat configuration console.

Bluecoat Side Setup

1. Enter the information required as described below:

Figure 43 Bluecoat Configuration Settings

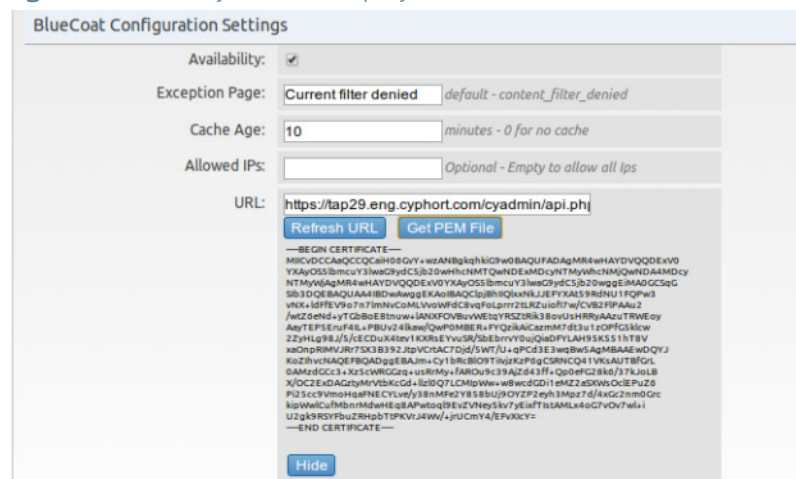


The image shows a web form titled "BlueCoat Configuration Settings". It contains the following fields and controls:

- Availability:** A checkbox that is checked.
- Exception Page:** A text input field containing "Current filter denied" with a hint "default - content_filter_denied".
- Cache Age:** A text input field containing "10" with a hint "minutes - 0 for no cache".
- Allowed IPs:** A text input field that is empty, with a hint "Optional - Empty to allow all Ips".
- URL:** A text input field that is empty.
- Below the URL field are two buttons: "Refresh URL" and "Get PEM File".
- At the bottom right of the form is a large "SUBMIT" button.

- **Availability:** This setting controls whether the Juniper ATP Appliance URL is available to be polled by Bluecoat.
 - **Exception Page:** This is a string to be included in the URL list, allowing Bluecoat to display a predefined exception page if a malicious URL is requested.
 - **Cache Age:** This value is used to determine how long the malicious URLs list is cached to avoid a repetitive attack and also to help reduce the Juniper ATP Appliance server load.
 - **Allowed IPs:** If leaving it blank, Juniper ATP Appliance is not checking who polls the list. Otherwise, only the IPs specified is allowed to poll.
2. **Get PEM File** button. Clicking this button will display the server PEM key content; copy and paste this key into Bluecoat in order to let Bluecoat to accept Juniper ATP Appliance's self-signed certificate.

Figure 44 PEM Key Content Display

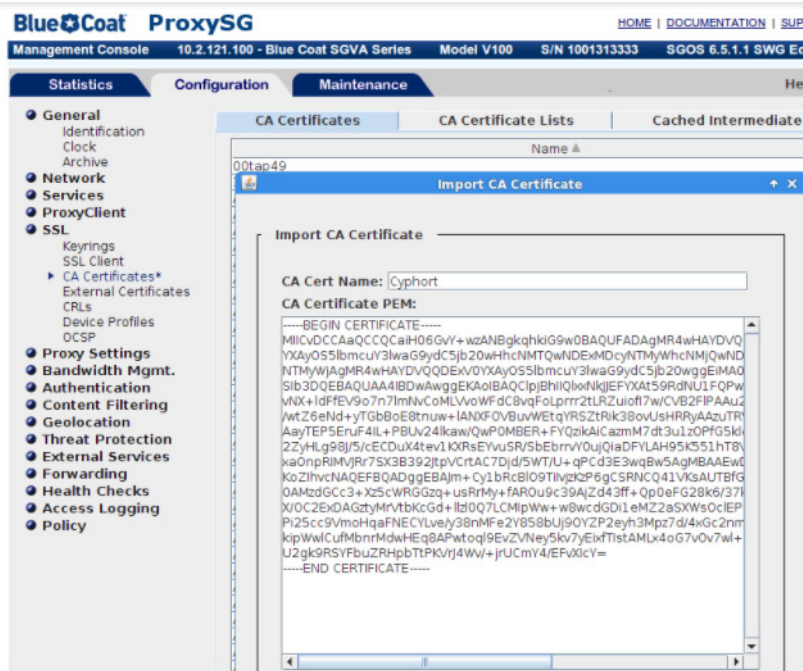


The image shows the same "BlueCoat Configuration Settings" form as in Figure 43, but with the "URL" field populated with the value "https://tap29.eng.cyphort.com/cyadmin/api.php". Below the "URL" field, the "Refresh URL" button is highlighted in blue. The "Get PEM File" button is also visible. Below the "Get PEM File" button, the PEM key content is displayed, starting with "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----". A "Hide" button is located at the bottom of the PEM key content.

3. **Refresh URL** button: Clicking this button will (re-)generate the polling URL.
4. To import a CA Certificate from the Bluecoat side: navigate to the Configuration tab SSL > CA Certificates section and click the Import button.

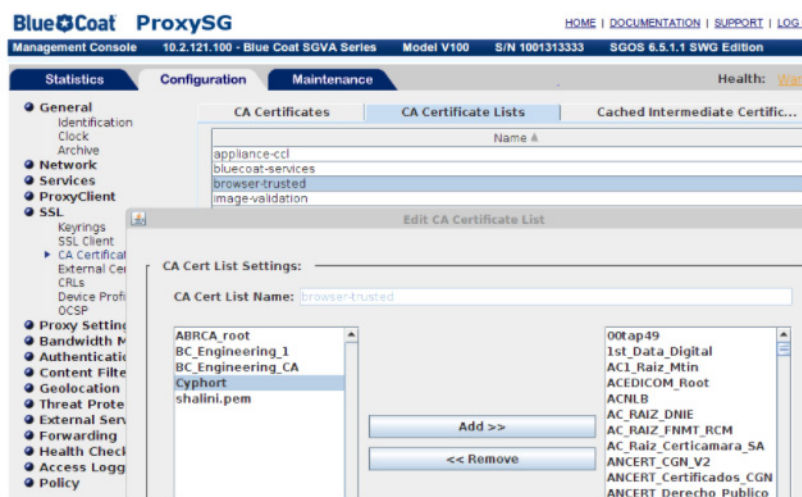
- Enter a unique name, and copy and paste the PEM key from system settings to here.

Figure 45 PEM Copied to Bluecoat



- Click Apply.
- Under SSL > CA Certificates, switch the tab to CA Certificate Lists.
- Highlight "browser-trusted" and click Edit.
- Add the newly created CA Certificate entry from left to right, then click Apply.

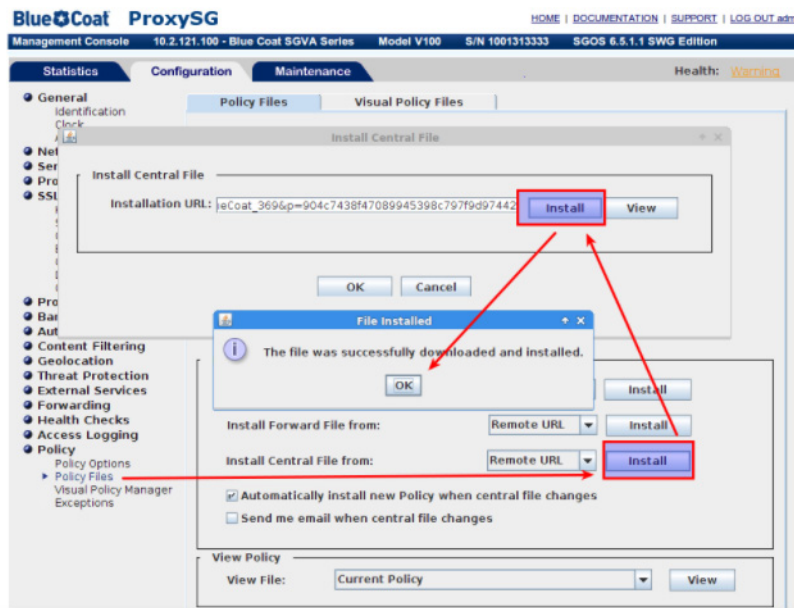
Figure 46 Adding the CA Certificate to the Bluecoat Configuration



- To set up the polling, navigate to Policy > Policy Files.

11. Click Install for the “Install Central File from:” section.
12. Paste the URL from the Juniper ATP Appliance server to here:

Figure 47 Adding the Juniper ATP Appliance URL to the Bluecoat Configuration



13. You will see the “The file was successfully downloaded and installed” message. Check the box “Automatically install new Policy when central file changes”.
14. The final step is to configure how often Bluecoat should poll:


```
# ssh admin@10.2.121.10
10.2.121.100 - Blue Coat SGVA Series>enable
Enable Password:
10.2.121.100 - Blue Coat SGVA Series#(config)policy poll-interval 5
ok
```

This sets a 5 minute interval between polls.

Configuring Bluecoat Secure Web Gateway Splunk Ingestion

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:
2. Select Web Gateway as the Source Type.
3. Select Bluecoat Secure Web Gateway as the Vendor Name.
4. For Transport, select the Splunk option.
5. Enter the Optional Splunk Index; for example: pan
6. Select a Default Severity setting: Max | High | Med | Low | Benign
7. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from Splunk ingestion will be created according to the severity setting selected in step 6. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
8. Click Add to perform the Splunk integration

Anti-SIEM Endpoint AV [ESET | McAfee ePO | Symantec: Log Collector | Splunk Ingestion]

Use the following procedures to configure Log Collection or Splunk Ingestion for Endpoint AV vendors ESET, McAfee ePO and/or Symantec AV.

- [“Configuring ESET Endpoint AV Log Collection”](#) in the next section
- [Click Add to perform the McAfee ePO Log Collector configuration.](#)
- [Configuring Symantec EP Endpoint AV Log Collection](#)
- [Configuring McAfee ePO Endpoint AV Splunk Ingestion](#)
- [Configuring Symantec EP Endpoint AV Log Collection](#)

Configuring ESET Endpoint AV Log Collection

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:

Figure 48 Anti-SIEM Endpoint AV [ESET:Log Collector Configuration]

The screenshot shows the Juniper ATP Appliance Central Manager Web UI. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar lists various settings categories, with 'External Event Collectors' selected. The main content area displays configuration options for an external event collector. Under 'Source Type', 'Endpoint AV' is selected. Under 'Vendor Name', 'ESET' is selected. Under 'Transport', 'Log Collector' is selected. Under 'Default Severity', 'Low' is selected. A 'Cancel' button is located below these settings. Below the settings, there is a section for 'Current Third Party Sources' with a table header: Category, Vendor, Transport, and Actions.

2. Select Endpoint AV as the Source Type.
3. Select ESET as the Vendor Name.
4. For Transport, select the Log Collector option.
5. Enter the Log Source Identifier.
6. Choose an SSL setting: Enabled or Disabled; “enabled” is recommended.
7. Select a Default Severity setting: Max | High | Med | Low | Benign

8. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from Splunk ingestion will be created according to the severity setting selected in step 5. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.

Click Add to perform the ESET Log Collector configuration.

Configuring McAfee ePO Endpoint AV Log Collection

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:
2. Select Endpoint AV as the Source Type.
3. Select McAfee ePO as the Vendor Name.
4. For Transport, select the Log Collector option.
5. Enter the Log Source Identifier; for example: MCAFEE-EPO.
6. Choose an SSL setting: Enabled or Disabled; "enabled" is recommended.
7. Select a Default Severity setting: Max | High | Med | Low | Benign
8. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from Splunk ingestion will be created according to the severity setting selected in step 5. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
9. Click Add to perform the McAfee ePO Log Collector configuration.

Configuring Symantec EP Endpoint AV Log Collection

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:
2. Select Endpoint AV as the Source Type.
3. Select Symantec EP as the Vendor Name.
4. For Transport, select the Log Collector option.
5. Enter the Log Source Identifier.
6. Choose an SSL setting: Enabled or Disabled.
7. Select a Default Severity setting: Max | High | Med | Low | Benign
8. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from Splunk ingestion will be created according to the severity setting selected in step 5. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
9. Click Add to perform the Symantec EP Log Collector configuration.

Configuring McAfee ePO Endpoint AV Splunk Ingestion

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:
2. Select Endpoint AV as the Source Type.
3. Select McAfee ePO as the Vendor Name.
4. For Transport, select the Splunk option.
5. Enter the Optional Splunk Index; for example: pan
6. Select a Default Severity setting: Max | High | Med | Low | Benign

7. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from Splunk ingestion will be created according to the severity setting selected in step 5. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
8. Click Add to perform the Splunk integration.

McAfee ePO Splunk integration: Splunk-Side Configuration

1. Install McAfee ePO version 5.2 with latest patch.
2. Install latest Splunk enterprise version
3. Install Splunk Add-on for McAfee . <https://splunkbase.splunk.com/app/1819/>
4. Install and configure DB Connect for Splunk:
 - › Download and install DB Connect Version 2.4.0 Add-on. This is required to connect to the McAfee ePO database to pull ePO events from the McAfee ePO server database. <https://splunkbase.splunk.com/app/2686/>

NOTE This app works on JAVA 1.8 version; be sure to update the ubuntu/windows version to run Splunk with JAVA 1.8

Steps:

```
sudo add-apt-repository ppa:webupd8team/java
sudo apt-get update
sudo apt-get install oracle-java8-installer
sudo apt-get install oracle-java8-set-default
```

- › Install a JDBC driver for your database. Refer to the section: Microsoft SQL Server. <http://docs.splunk.com/Documentation/DBX/2.4.0/DeployDBX/Installdatabasedrivers>

NOTE Copy the jdbc driver(sqljdbc4.jar) under path:
/opt/splunk/etc/apps/splunk_app_db_connect/bin/lib

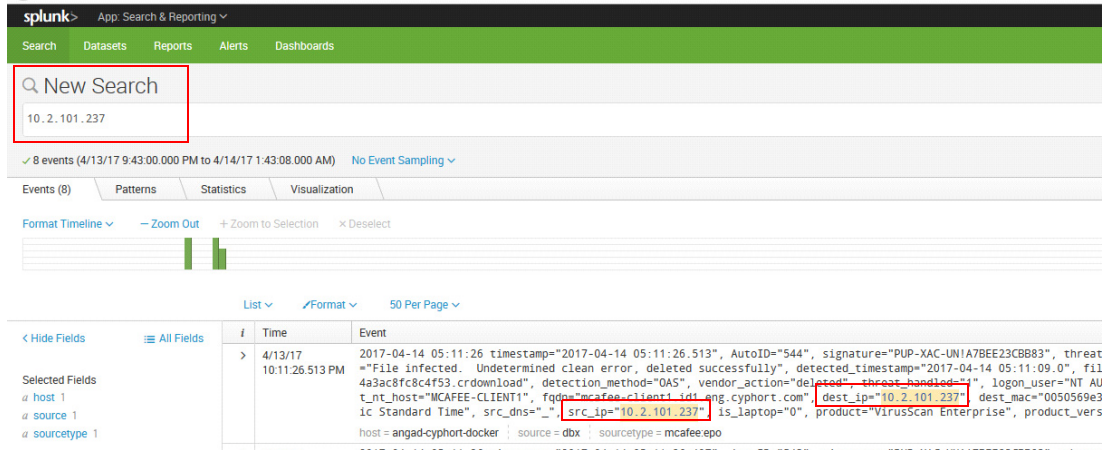
- › After installing DB Connect and restarting Splunk Enterprise, launch DB Connect and complete the initial setup <http://docs.splunk.com/Documentation/DBX/2.4.0/DeployDBX/Singleserverdeployment#Set up Splunk DB Connect>
- › Create a database identity, set up a database connection, and create a new database input for Splunk Add-on for McAfee .

NOTE

1) Use the Splunk DB Connect GUI method to create a database connection instead of modifying db_connections.conf file to create a connection.

2) Under the Execution Frequency setting, change from 3600 sec to 1 sec so that it pulls the data from the epo db every second. <http://docs.splunk.com/Documentation/AddOns/released/McAfeeEPO/ConfigureDBConnectv2inputs>

5. Generate a threat event on the ePO server and search through that event log to find the endpoint IP address that was attacked, or the malware name; as shown on in the following example:



6. Login to the Juniper ATP Appliance Web UI and navigate to Config>Environmental Settings>External Event Collectors and ADD a new external collector using the Splunk option; refer to the Juniper ATP Appliance-Side [Configuring McAfee ePO Endpoint AV Splunk Ingestion on page 226](#) for more information.
7. View the McAfee ePO threat events on the Juniper ATP Appliance Events Timeline Dashboard by filtering the timeline by "IP Address" of the endpoint.

McAfee ePO Direct Log Ingestion: McAfee ePO Side Configuration

1. Confirm you have installed McAfee ePO version 5.2 version with the latest patch (hotpatch ePolicy Orchestrator (EPO) 5.3.2 HF1185471).
2. Login to the ePO 5.2 UI and create a syslog-registered server via tabs Configuration>Registered Servers:



3. Create a new server by entering all required details as shown in the figure above. Enter the Juniper ATP Appliance Core hostname/IP as the Server Name, and enter 10514 for the TCP port number.
4. Click the Test connection button to confirm that the settings are correct and ePO is ready to send syslog events to Juniper ATP Appliance. The message "Syslog connection success" indicates that the ePO is ready to push threat events to the Juniper ATP Appliance Core and the Juniper ATP Appliance Core is ready to accept the events.
5. View the McAfee ePO threat events on the Juniper ATP Appliance Events Timeline Dashboard by filtering the timeline by the IP Address of the endpoint, as show in the screenshot below.

Anti-SIEM Endpoint Response [Carbon Black Response: Log Collector | Splunk Ingestion]

To configure Carbon Black Response for endpoint alert event handling via direct log ingestion or Splunk ingestion, use the following procedures.

- [“Configuring Carbon Black Response Log Events via Splunk” in the next section](#)
- [Splunk Side Configuration for Carbon Black Response on page 229](#)
- [Configuring Carbon Black Response via Direct Log Ingestion on page 229](#)
- [Carbon Black Response - Splunk Integration on page 230](#)
- [Carbon Black Response Ingestion Reporting at Juniper ATP Appliance on page 235](#)

Configuring Carbon Black Response Log Events via Splunk

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:
2. Select Carbon Black Response as the Vendor Name.
3. For Transport, select the Splunk option.
4. Enter the Optional Splunk Index; for example: pan
5. Select a Default Severity setting: Max | High | Med | Low | Benign
6. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from Splunk ingestion will be created according to the severity setting selected in step 5. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
7. Click Add to perform the Splunk integration.

NOTE For more information about Splunk integration, refer to [Configuring Anti-SIEM Splunk Ingestion on page 209](#).

Splunk Side Configuration for Carbon Black Response

This section does not cover Splunk configuration. However, when configuring Splunk from the Splunk console for integration with Juniper ATP Appliance, there are a few items you'll need to be sure are set for PAN:

Navigate to Splunk.

Configuring Carbon Black Response via Direct Log Ingestion

1. Navigate to the Juniper ATP Appliance Central Manager Web UI Config>Environmental Settings>External Event Collectors configuration page:

Figure 49 Anti-SIEM Endpoint Response [Carbon Black Response:Log Collector Configuration]

The screenshot shows the 'Config' tab of the Juniper ATP Appliance interface. The left sidebar contains a navigation menu with options like Notifications, System Profiles, Environmental Settings, Email Mitigation Settings, Firewall Mitigation Settings, Asset Value, Anti-Virus Configuration, Endpoint Integration Settings, BlueCoat Configuration, Whitelist Rules, YARA Rule Upload, SNORT Rule Upload, Identity Configuration, Splunk Configuration, and External Event Collectors. The main configuration area is divided into several sections:

- Source Type:** Radio buttons for Firewall, Web Gateway, Endpoint AV, and Endpoint Response (selected).
- Vendor Name:** Radio buttons for Carbon Black Response (selected) and Splunk.
- Transport:** Radio buttons for Log Collector (selected) and Splunk. Below this is an 'Input Port' dropdown menu.
- Default Severity:** Radio buttons for Max, High, Med, Low (selected), and Benign.
- Create Incident:** Radio buttons for Enabled and Disabled (selected).

A 'Cancel' button is located below the configuration options. Below the configuration area is a table titled 'Current Third Party Sources' with columns for Category, Vendor, Transport, and Actions.

2. Select Carbon Black Response as the Vendor Name.
3. For Transport, select the Log Collector option.
4. Enter the Input Port.
5. Select a Default Severity setting: Max | High | Med | Low | Benign
6. Configure Create Incident by selecting the Enable or Disable option. All incidents created by Juniper ATP Appliance from log ingestion will be created according to the severity setting selected in step 5. The Create Incident setting, when enabled, creates incidents for third party events directly and sends email alert notifications, even if there are no correlates with Juniper ATP Appliance-detected events.
7. Click Add to save the Log Collector configuration.

Carbon Black Response - Splunk Integration

Use the following information to perform Carbon Black Response and Splunk integration using either:

- [“Carbon Black Response Direct Log Ingestion: Event Forwarder of JSON Logs” in the next section](#)
- [Carbon Black Response Integration via Splunk Forwarder on page 206](#)
- [Carbon Black Response Ingestion Reporting at Juniper ATP Appliance on page 209](#)

NOTE See also [Configuring Carbon Black Response Log Events via Splunk on page 229](#); [Splunk Side Configuration for Carbon Black Response on page 229](#); [Configuring Carbon Black Response via Direct Log Ingestion on page 229](#).

IMPORTANT: A few notices about Carbon Black Response and Splunk integration:

- Juniper ATP Appliance requires Active Directory (AD) data for correlation with Carbon Black logs.
- AD, Splunk and Juniper ATP Appliance must be NTP-synced.
- Currently, from Carbon Black, only watchlist alert events are consumed by Juniper ATP Appliance:
 - › alert.watchlist.hit.ingress.host
 - › alert.watchlist.hit.ingress.binary
 - › alert.watchlist.hit.ingress.process
 - › alert.watchlist.hit.query.binary
 - › alert.watchlist.hit.query.process
- Correlation between Juniper ATP Appliance and Carbon Black Response is within 5 minutes.
- The endpoint hostname is the only match for correlating Carbon Black Response and Juniper ATP Appliance events.
- With Carbon Black Response Event Forwarder, there is an option to forward logs in JSON or LEEF format; Juniper ATP Appliance supports JSON format only at this time for both Splunk and Direct Log ingestion.
- For Direct Log Ingestion, logs can be sent to any random Juniper ATP Appliance port.
- The difference between Carbon Black Response integration and Carbon Black Direct Log Ingestion:
 - › During Carbon Black Response integration, Juniper ATP Appliance queries for only those events detected by Juniper ATP Appliance to obtain confirmation about the endpoint execution.
 - › In CB Log Ingestion, all events irrespective of whether Juniper ATP Appliance has seen it or not is pulled.
 - › If a CB event is correlated in CB log ingestion, then we don't mark the EX Progression.

Carbon Black Response Direct Log Ingestion: Event Forwarder of JSON Logs

1. Install the Carbon Black Response Event Forwarder :
<https://developer.carbonblack.com/reference/enterprise-response/event-forwarder/>
2. To send the Carbon Black Response event logs to any server via TCP or UDP, edit the Event Forwarder CONF file as in the example shown below:

```
In /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf
```

```
rabbitmq_username=cb
rabbitmq_password=<password>
cb_server_hostname=127.0.0.1
```

Take the username & password for the above from /etc/cb/cb.conf, search for RabbitMQUser & RabbitMQPassword and copy the value from the above file.

```
In /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf
```

Search for and enter the values shown below:

```
output_type=tcp or udp
output_format=json
```

If the TCP option is selected, configure the tap server and the listening port. Currently, you can select any random port to listen to.

```
tcpout=10.2.9.35:10516
```

If udp option is selected above, then configure the tap server & the listening port. Currently you can select any random port to listen to:

```
udpout=10.2.9.35:10516
```

Next, run the below command to receive output indicating which server the event forwarder has connected to.

```
[root@scb ~]# /usr/share/cb/integrations/event-forwarder/cb-event-forwarder -check
2017/05/08 03:42:38 Connected to tcp:10.2.9.35:10516 at 2017-05-08 03:42:38.068386476 -0700 PDT.
2017/05/08 03:42:38 Initialized output: tcp:10.2.9.35:10516
```

Start the event-forwarder:

```
[root@cb]# initctl start cb-event-forwarder
```

Carbon Black Response Integration via Splunk Forwarder

1. From the Carbon Black Response Server, install the Carbon Black Response Event Forwarder:
<https://developer.carbonblack.com/reference/enterprise-response/event-forwarder/>
2. Download the relevant binaries from this link:
https://www.splunk.com/en_us/download/universal-forwarder.html
3. Install Splunk Add on for Bit9 Carbon Black to your Splunk instance. Set the Splunk Common Information Model.
<https://splunkbase.splunk.com/app/2790/>
4. Configure the Carbon Black Response Event Forwarder; this is required to save the Carbon Black Response event logs to a file using the contents to forward data to Splunk.

```
In /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf
```

```
rabbitmq_username=cb
rabbitmq_password=<password>
cb_server_hostname=127.0.0.1
```

Apply the username and password shown above from /etc/cb/cb.conf, search for RabbitMQUser and RabbitMQPassword, and copy the value to the above CONF file.

```
In /etc/cb/integrations/event-forwarder/cb-event-forwarder.conf
```

Search & enter the values below:

```
output_type=file
output_format=json
outfile=/var/cb/data/event-forwarder/data.json
```


The above outfile can be anything; in this example, the link stores the event logs.
Run the command below to get the output shown below.

```
[root@cb]# /usr/share/cb/integrations/event-forwarder/cb-event-forwarder -check
2017/04/20 02:42:58 Initialized output: File /var/cb/data/event-forwarder/data.json
```

Start the event-forwarder:

```
[root@cb]# initctl start cb-event-forwarder
```

5. Configure the Splunk Add on for Bit 9 Carbon Black Response.
6. Set the Splunk Common Information Model as shown below:

The screenshot shows the Splunk Apps page. At the top, there are buttons for 'Browse more apps', 'Install app from file', and 'Create app'. Below this, it says 'Showing 1-25 of 25 items'. A table lists various apps. The 'Splunk Common Information Model' is highlighted with a red box. The table has columns for Name, Folder name, Version, and Update checking.

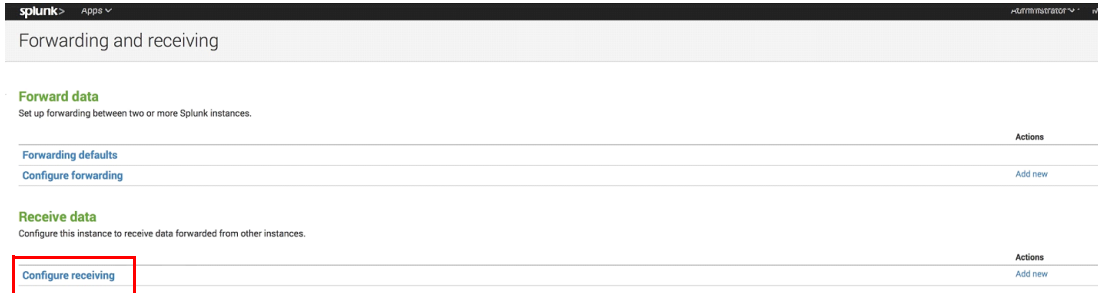
Name	Folder name	Version	Update checking
SplunkForwarder	SplunkForwarder		Yes
SplunkLightForwarder	SplunkLightForwarder		Yes
Splunk Common Information Model	Splunk_SA_CIM	4.8.0	Yes
Splunk Add-on for Bit9 Carbon Black	Splunk_TA_bit9-carbonblack	1.0.1	Yes
Splunk Add-on for Blue Coat ProxySG	Splunk_TA_bluecoat-proxysg	3.4.2	Yes

7. Configure the Receiver for your Splunk Instance to set the Splunk Forwarder to forward data; Navigate to Splunk > Settings > Forwarding & Receiving.

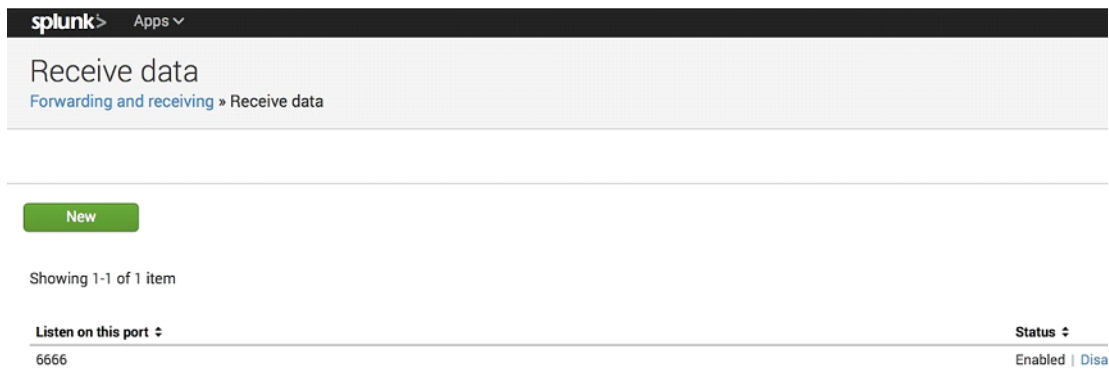
The screenshot shows the Splunk Settings page. On the right side, there is a sidebar with various settings categories. The 'Forwarding and receiving' link is highlighted with a red box. The main content area shows a list of settings for the 'Forwarding and receiving' section.

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	Edit properties View objects
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	Edit properties View objects
Splunk Common Information Model	Splunk_SA_CIM	4.8.0	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for Bit9 Carbon Black	Splunk_TA_bit9-carbonblack	1.0.1	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for Blue Coat ProxySG	Splunk_TA_bluecoat-proxysg	3.4.2	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects
Splunk Add-on for McAfee	Splunk_TA_mcafee	2.1.3	Yes	No	Global Permissions	Enabled Disable	Edit properties View objects
Splunk for Blue Coat	SplunkforBlueCoat	3.0.7	Yes	Yes	App Permissions	Enabled Disable	Edit properties View objects
Log Event Alert Action	alert_logevent	6.5.3	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	6.5.3	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	6.5.3	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
default	default		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
framework	framework		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
FTP Receiver	ftp_receiver	1.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects View details on SplunkApps
Getting started	gettingstarted	1.0	Yes	Yes	App Permissions	Disabled Enable	Edit properties View objects
introspection_generator_addon	introspection_generator_addon	6.5.3	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	Edit properties View objects
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	Edit properties View objects
Search & Reporting	search	6.5.3	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Splunk DB Connect	splunk_app_db_connect	2.4.0 Update to 3.0.2	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects View details on SplunkApps
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App Permissions	Disabled Enable	Edit properties View objects View details on SplunkApps
splunk_intelinput	splunk_intelinput		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Instrumentation	splunk_instrumentation	1.0	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
Monitoring Console	splunk_monitoring_console	6.5.3	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects

8. Click on Configure Receiving.



9. Configure a port to listen on. In this example: port 6666.



10. Set up the Splunk Universal Forwarder to forward Carbon Black Response data to Splunk by downloading and installing the Universal Forwarder RPM on the Carbon Black Response server:
https://www.splunk.com/en_us/download/universal-forwarder.html

```
rpm -ivh splunkforwarder-6.5.3-36937ad027d4.i386.rpm

[root@cb]# cd /opt/splunkforwarder/bin

[root@cb]# ./splunk
Data forwarding configuration management tools.
Commands:
  enable local-index [-parameter <value>] ...
  disable local-index [-parameter <value>] ...
  display local-index
  add forward-server server
  remove forward-server server
  list forward-server
Objects:
  forward-server      a Splunk forwarder to forward data to be indexed
  local-index         a local search index on the Splunk server

[root@cb bin]# ./splunk add forward-server 10.2.14.219:6666
```

In the above command 10.2.14.219 is the splunk server & 6666 is the port we have configured in Step 3 on which Splunk is receiving.

```
[root@cb local]# pwd
/opt/splunkforwarder/etc/system/local

[root@cb local]# cat inputs.conf
[default]
```

```
host = cbtest

[monitor:///var/cb/data/event-forwarder]
sourcetype = bit9:carbonblack:json

[root@cb local]
```

11. Add an input host file. In this example, cbtest is used, which can be searched for in Splunk.

The monitor is the directory of data.json, which is configured in Step 1.

The sourcetype shows which data needs to be sent, which is from Carbon Black Response.

```
[root@cb bin]# cd /opt/splunkforwarder/bin
[root@cb bin]# ./splunk start
```

12. Start Splunk.

13. Check the forward-server.

```
[root@cb bin]# ./splunk list forward-server
Splunk username: admin
Password:
Active forwards:
10.2.14.219:6666
Configured but inactive forwards:
None
[root@cb bin]#
```

Carbon Black Response Ingestion Reporting at Juniper ATP Appliance

Carbon Black Response log ingestion can be viewed from the Juniper ATP Appliance Central Manager Web UI Incidents page and Events Timeline Dashboard.

CHAPTER 4

Managing Incidents

The following topics are in this chapter:

- [Understanding Threats and Incidents](#)
- [Threats and the Attack Life Cycle](#)
- [Understanding Severity](#)
- [Interpreting Context-Aware Incident Details](#)
- [Navigating the Incidents Page](#)
- [Malware Download Naming Conventions](#)

Understanding Threats and Incidents

Detailed incidents are generated by the Juniper ATP Appliance analysis and detection engines for related malware events.

For example, during an enterprise user's web browsing session, a link from a compromised website might load an advertisement that redirects the user's browser to an exploit site. From the exploit site, the browser might then download malicious mobile code to the user's endpoint. The malicious code might be armored, designed to evade discovery while allowing the attacker to take control of the user's device. This command and control (CnC) of the enterprise endpoint might download data theft software, or it may gain direct access to intellectual property and proprietary information or documents. The CnC code might involve obfuscated callbacks to the command and control server for data exfiltration, and the malware might then also compromise other assets in the enterprise network such as a share or dropbox where it will be inadvertently downloaded again by other corporate users.

All of the web-based malware events described above are detected by Juniper ATP Appliance as a combined incident. The results of Juniper ATP Appliance's context-aware detonation engines are displayed on the Incidents page with sub-tab displays that contain malware results specific to Kill Chain progression and incident summaries.

The Incidents table is an important mechanism for filtering, sorting, and searching detection results for analysts and enterprise response teams.

Figure 4-1 Central Manager Incidents Tab - Max Severity Risk

ADVANCED THREAT PREVENTION APPLIANCE											
<div> Refresh Data System Health juniper Doc </div>											
Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config											
All Incidents (53 shown, 53 total)											
Search: Show Threat All Zones Last Week											
Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	646210	MAX	DNVY	DL	Web	greatfilesarey.asi	sj_test_20	Default Zone	Windows 1	w-Collector	Jan 17 10:51 am
Acknowledged	6270	MAX	TROJAN_WALDEK.DC	DL	Web LOG	greatfilesarey.asi	JOSH-DESKTOP	Default Zone	unknown	2 Collectors	Jan 17 10:51 am
New	646214	MED	TROJAN_FAKEAV	DL	Web	greatfilesarey.asi	sj_demo_119	Default Zone	unknown	PartnerDemo-New-Collector	Jan 17 10:51 am
New	646211	MED	WORM_CONFICKER_Z	DL	Web	greatfilesarey.asi	test_215	Default Zone	unknown	PartnerDemo-New-Collector	Jan 17 10:51 am

Details for TROJAN_WALDEK.DC	
SUMMARY	EXTERNAL SOURCES
Destination Email ID:	-
Risk:	Max
Threat Category:	Trojan_Generic
Asset Value:	Max
Target OS:	unknown
Relevance:	Medium
Progression:	Download
Protocol:	HTTP:LOG
OS Matched:	No
Virus Scanner Recognised:	Recognized by Selected AntiVirus

The Incidents page is integrated with the Juniper ATP Appliance CM Dashboard. The Dashboard also displays incident detection results for all related malware events. Double-clicking a bubble in the Dashboard Threat View opens the Incident page in-focus for that host's incident and related events.

Below the Incidents table, the left panel Details and Summary sections include sub-tabs for each Kill Chain result specific to the incident row selected in the table above. Sub-tabs include Exploits | Downloads | User Uploads | Infections | Execution | Data Theft.

Context-Aware Kill Chain Stage and Progression per Incident

Exploit	XP	Activity that could expose users to malicious objects.
Download	DL	Download of an object identified as malicious.
User Upload	UP	A data upload performed at an endpoint.
Execution	EX	Execution of malicious code on the enterprise endpoint [identified through Bit9/Carbon Black API integration]
Infection	IN	Identified evidence of infection (CnC).
Data Theft	DT	Analysis of data exfiltration from the endpoint.

Threats and the Attack Life Cycle

The incidents detected by Juniper ATP Appliance reveal a variety of related events as they correlate to specific phases of the malware infection life cycle and Kill Chain. For example, when exploit content is delivered by a browser, the inspection and analysis components of the Juniper ATP Appliance Collectors and Cores perform in-depth object analysis. Juniper ATP Appliance sends the full view of the web page and associated network objects, including the exploit, to the engines for dynamic behavioral analysis in virtualization, then emulation engines.

The consecutive virtualization and emulation environments are exploited as the malicious code executes, initiating a download of a "malware binary, another stage of the Kill Chain progression that Juniper ATP Appliance is actively tracking. When the malware binary is loaded into the Juniper ATP Appliance detonation engines, the binary instructs the system to transmit a network callback to the CnC center, for remote control by the attacker. Internal to the appliance, Juniper ATP Appliance captures and analyzes the network traffic generated by the malware and generates a dynamic network rule in order to identify this same callback traffic across the monitored, integrated network infrastructure. Juniper ATP Appliance's mitigation rules block the callback traffic, capture and record all files created or modified during detonation, and generate an Incident representing all the events that took place in the virtualization and emulation engines, sending notification(s) to GSS and the administrator so that the infection detected by the Juniper ATP Appliance Cores can be remediated on the infected host in real time in the enterprise network. All of this data is represented in the Juniper ATP Appliance CM Incidents tables and sub-tabs.

Understanding Severity

Juniper ATP Appliance Threat Severity determinations are shown in the Incidents table as Risk levels. The colors do not relate to whether an infection is confirmed or not; they are based on the Threat Metric Risk Score.

Severity Risk Colors

- › Red-**Max** = Critical / Maximum risk events
- › Red-**High** = High risk events
- › Orange -**Med** = Medium risk events
- › Yellow -**Low** = low risk events
- › Green -**Benign** = clean events; benign (clean) events are displayed under the Show Benign option.

Severity Range

Severity is defined as a value (including decimals) between 0 and 1.

Severity Calculations				
Max	High	Med	Low	Benign

Severity Calculations				
1	1	1	0.75	0
1	1	0.75	0.5	0
1	0.75	0.5	0.25	0
0.75	0.5	0.25	0	0

To search for all clean/benign events, specify a minimum severity of 0 and maximum severity of 0.

Severity and the Kill Chain

Kill Chain	Recommended Mitigation Action
EX, IN, DL+IN, DT	Immediate response required; <ul style="list-style-type: none"> • wipe infected endpoint hosts • block malware IP addresses (download server or CnC server)
DL	Immediate response required <ul style="list-style-type: none"> • Deploy IVP or Bit9 integration (if configured) to confirm if the endpoint has executed the malware and is infected.
XP, UP	Not an urgent action. <ul style="list-style-type: none"> • Use IVP to confirm if machine is infected

Severity and Risk Calculations

Risk calculation is context-specific and takes the following criteria into account:

- The Relevance of the threat:
 - Antivirus configuration of the endpoint
If you have configured which of your network segments are using which antivirus software (see Config Tab options), then, if the AV software for this endpoint can catch the malware download, then the risk calculation is lowered.
 - OS Match
If the operating system of the endpoint and the OS for which the malware was designed are a match, then risk calculation is higher. For example, OSX malware on a Windows machine (an OS Mismatch) represents a lower risk than Windows malware on a Windows machine.
- Asset Value of the enterprise network segment
 - Asset Value for the network segment or endpoint
The Juniper ATP Appliance system allows network segments to be configured with an asset value (Low, Medium, High, Critical) indicating the importance of this endpoint. This value is used in risk calculations.
- Severity of the malware event
 - Malware severity
Different types of malware download are assigned different severities as part of risk calculation determinations.

When a malicious event is detected, the Juniper ATP Appliance detection and analysis engines determine severity as part of their Threat Metric determinations. As indicated, an infected host can undergo a combination of events—an initial infection, a secondary binary drop, as well as a callback—coupled with asset value assessments and chain heuristics— that together contribute to determining the severity of the attack.

All malware callback events are considered high severity events, which are displayed as "High" in the Central Manager Web UI. A callback event allows Juniper ATP Appliance to determine whether the endpoint has been infected. Binary downloads are assigned severity according to the threat category from the Core detonation and analysis engines; a callback could be Low, Medium, High or Critical.

Severity is closely linked to the infection life cycle and Juniper provides unprecedented visibility into the details of every stage of the infection life cycle.

Interpreting Context-Aware Incident Details

The details provided on the Juniper ATP Appliance Incidents page include information about each malware attack and infection as well information that may be useful to analysts.

In the case of a Web Infection, an analyst would want to know how the source IP was initially infected.

From the Incident table, an analyst can determine that an infection came from a browser exploit attack or download, for example, and whether this event included another dropper binary. The particular malware family and any callbacks from the same malware family can also be determined. In every case, when a callback is matched to an actual Asset in the enterprise, the asset is determined to be compromised.

TIP TIP: Analysts can drill down further to understand how the malware is working. Open the left panel sub-tabs on the Incidents page (Downloads and Infections) to review attack details.

Sometimes, a low severity, when combined with other threat-level events, it may be listed as a high severity incident.

In the case of a browser exploit, several events may appear to be malicious, but it might be difficult to tell. In order to know if an exploit is truly malicious, analysts can run the Juniper ATP Appliance Infection Verification Package (IVP) at the targeted endpoint, or configure CarbonBlack integration, to verify infection.

From an analyst's perspective, it is important to determine if an end asset was actually compromised. IVP helps determine if the incident is an attempted attack or a full exploit.

IVP also recognizes whether affected hosts downloaded multiple different binaries but a callback was generated on only one of them. It is sometimes possible that the other delivered binaries did not actually exploit an endpoint asset, but Juniper ATP Appliance reveals that there has been an exploit (EX) because of one callback from one host in the enterprise. In order to determine if this is truly an APT, an analyst must review the information provided about how the malware behaved and operated in the OS.

Juniper ATP Appliance allows analysts to see when an executable file was delivered; if it corrupted a root file system (a major red flag), then it may have ultimately loaded a DLL. The executable might register a new Windows service, which is another red flag. It is important to note that properly signed binaries are whitelisted, which is one way that legitimate installers are filtered out.

In some callback and DT instances, there may be a simple DNS match. But it is impossible to tell if an asset was compromised based only on the DNS. It is likely, but in order to confirm it, analysts must compare when the DNS record was first added to the database relative to when the asset first generated the DNS request.

Navigating the Incidents Page

Review the entries in the Incidents table.

- To drill down into more information about a particular incident, select a row in the table. The Details area below the Incidents table adjusts to display details for the selected row/incident.
- Click the Upload File button on the upper right of the Incidents tab, and in the "Submit file for analysis" window that displays, select the file to upload for analysis and click the Submit file button. The Upload File feature calls the "file_submit" API and then, following analysis, displays the results returned from the API in a pop-up page in the Central Manager Web UI. The results are also displayed in the Incidents page table with the Kill Chain designation: DL (in this example) along with the incident sha1sum and filename.
- Click the Mitigate Incident link to the right of the Details area to view mitigation options for the selected threat.

- Click the “New” link in the Status column to change the status from a drop down menu, which allows administrators with access privileges to tag individual incidents as either:
New | Acknowledged | In Progress | Resolved

Setting Incident Status and Entering User Comments

All users who have access to incident details can mark an incident they’ve triaged or resolved so that other Juniper ATP Appliance users can monitor progress. There are four states available:

New | Acknowledged | In Progress | Resolved

All users with access can also add Comments to incidents; when the Status link (for example, “New” in the screenshot below) is clicked on the Incidents page Status column, it opens a window in which the status can be updated and user comments and progress reports can be entered, as shown below:

The following table describes the columns and displays in the Incidents table.

Table 4 Main Incident Table Column Definitions

Column	Description
Status	User-defined description of the resolution state of the Incident. Available options include: New Acknowledged In Progress Resolved. Click the Status descriptor per row to open the Status and User Commenting window for a given incident.
Risk	Threat Metric and Severity Rating
Threat	Name used to identify the detected download or infection.
Kill Chain	The Kill chain attack phase or progression determined by the detection engine: XP (exploit) DL (download) UP (upload) EX (execution) IN (infection) DT (data theft)
Threat Source	The IP address or domain name of the malware source.
Threat Target	The IP address of the targeted host.
Target OS	The Operating system targeted by the malware.
Collector	Name of the Juniper ATP Appliance traffic inspection Collector that performed the initial object analysis and sent the malware object to the Core engines for behavioral analysis.
Date & Time	The timestamp for the malware download or infection as the current local time in the UTC standard format.

NOTE Click the up or down arrow in the column header to reorder the column contents.

Use the Details tables and sub-tab displays to review detailed information about any threat row selected from the Incidents table. The Details table is specific to the row selected in the Incidents table above, and it updates every time a new row is selected in the Incidents table.

Details Summary

The following table describes the categories in the Details Summary window.

Table 4-1 Details Summary window

Category	Description
Time	The date and time of the detected threat.

Table 4-1 Details Summary window

Category	Description
Target	Targeted host or device.
Summary	A summary description of the risk and threat name.
Severity	The severity rating.
Source IP	IP address or domain name of the malware source
Progression	Single or combined Kill Chain stages; example: DL+IN
Relevance	Threat Metric context determination; example: OS Mismatch
Asset Value	User-defined network segment asset value.
Triggers	Static analysis, behavioral analysis, reputation and network engines that were triggered by the events related to this incident.

Viewing Golden Image Results in Incidents Summary

A row in the Incidents tab Summary table displays Custom VM Image detection results for infection (IN) and exploit (XP) events as "Golden Image," as shown below.

If three custom VM images have been configured, then three golden image results will show in the Summary.

Configure a custom VM golden image(s) specific to your enterprise OS environment(s) from the Config>Custom VM Image page of the Central Manager Web UI.

NOTE There are several circumstances in which the Golden Images results field on the Summary tab (outlined in the figure above) might be empty. For example, the malware may have been blocked by the AV (and hence would not undergone malware analysis in the detection engine) so no analysis results would be generated, or the malware was perhaps detected by the signature engine but not by the regular detection engine (and hence would not have been re-cooked by the golden image analysis engine).

Object Rescans History Timestamps on Incidents Page

Juniper ATP Appliance automatically rescans objects in order to ensure that the static and reputation detection results are up-to-date, and to protect against false positives and false negatives. In addition, when new machine learning models are available, any recaptured objects are analyzed to produce a new set of static, behavioral and reputation detection results

NOTE Juniper ATP Appliance sends an HTML email alert when correcting false negative events (when the appliance rescans and there is a detection). Alerts are not sent for false positive events.

The Juniper ATP Appliance Web Central Manager Incidents page displays the detection history of each scanned and analyzed object to show detection changes over time. The timestamps for each object rescan are shown in the History section of the Details area on the Incidents page; shown below.

In addition, this improved detection functionality includes alerts for each malware event detected during rescanning and re-analysis. An alert after rescanning may change a false positive result to a corrected benign event.

When an HTML email alert is generated following an object rescan event, the alert message states:

"Alert generated due to new analysis of sample" (this message differentiates a normal alert from a rescan alert):

Custom Time Range Filtering

Use the Custom Time Frame option to query for a slice of the detection database by time. The Custom Time Frame filter is available from the same pulldown menu from which to select filtering for the Last 24 hours, Last Week, and so on.

From the Incidents page, select Custom Time Frame from the dropdown menu shown in the following Web UI figure in order to display all incidents (including benign) for the time period you designate; you can then use the search to query a specific MD5 for example.

NOTE Benign objects are automatically cleared from the detection database after 30 days.

Several Use Cases for Custom Time Range filtering of the detection database:

- To find an event that a Third Party detected but not displayed in the Benign listings.
 - A. Select Custom Time Range
 - B. Search by a text string found in the Incident columns.
- To find all events seen from a particular Traffic Collector
 - C. Select Custom Time Range
 - D. Sort by Collector name or Search by text string found in Incident columns.

Malware Download Naming Conventions

The general naming scheme for malware downloads is as follows:

`Category[_Family].Suffix`

“Category” would be malware of the type Adware, Suspicious, Trojan, Virus, Worm or Exploit.

The “Family” name applies to Trojan categorizations, and is obtained either from VirusTotal or the Juniper ATP Appliance Detection Engine’s behavioral classifier.

The “Suffix” meanings are:

- › .DC = Deep Cooker
- › .CY = Reputation engine + Static detection
- › .Rep = Reputation Engine Only (Reputation Engine detection)
- › .Static = (3rd party static detection scanner)

Uppercase names, such as TROJAN_NAME.DC indicates that there is a match on the VirusTotal database and chances are that this is a high confidence detection. For example: TROJAN_BROWSERFOX.DC.

A mixed-case naming means that other detection triggers were observed. There are 2 types of classifications: `Category[_Family].Static` and `Category[_Family].DC`

`Category[_Family].Static` is higher confidence because it is based on third party static detection.

The `Category[_Family].DC` format indicates that the detection occurred in the Detection Engine. If the Detection Engine was the only trigger, this may be a false positive, but it might also indicate a zero-day attack.

CHAPTER 5

Mitigation and Reporting

The following topics are in this chapter:

- [Network Mitigation Options](#)
- [Mitigation Options from the Incidents Tab](#)
- [Generating Reports](#)
- [Sample Executive Report Segments](#)

Network Mitigation Options

Use the Mitigation tab to block specific threats on integrated security devices in the enterprise network. Additionally, use this Mitigation page to view a list of threats you previously whitelisted via the Incidents page mitigation options.

Figure 5-1 Juniper ATP Appliance Mitigation using existing security infrastructure

Search:	Push to Device	Severity	Confidence	Owner	Threat	Threat Source	Malware IP	Threat Target	Detection Date	Status
<input type="checkbox"/>	Enabled	Medium	Max	cyadmin	malvertising	Juniper Labs	23.254.165.61		Sep 2 20:11:54 Eastern Standard Time	[+] Successful
<input type="checkbox"/>	Disabled	Medium	Max	JATP	malvertising	Juniper Labs	89.44.47.210		Sep 2 20:11:54 Eastern Standard Time	
<input type="checkbox"/>	Enabled	Medium	High	cyadmin	VIRUS:WIN32_SALITY_AU.CY	Local	108.179.219.135	10.1.7.197	Sep 9 13:13:55 Eastern Standard Time	[+] Successful 192.168.1.113: Success
<input type="checkbox"/>	Enabled	Max	High	gsuzuki	TROJAN_Fareit.CY	Local	115.47.49.101	10.1.0.33	Apr 21 03:55:46 Eastern Standard Time	[+] Successful
<input type="checkbox"/>	Disabled	Medium	High	JATP	VIRUS:WIN32_SALITY_AU.CY	Local	122.155.168.149	10.1.7.197	Sep 9 13:13:55 Eastern Standard Time	
<input type="checkbox"/>	Enabled	Medium	High	cyadmin	TROJAN_ZeroAccess.CY	Local	173.193.250.103	10.1.7.132	Sep 9 01:13:57 Eastern Standard Time	[+] Successful
<input type="checkbox"/>	Disabled	Medium	High	JATP	TROJAN_ASKTOOLBAR.CY	Local	18.23.92.114	ny_demo_175	Mar 7 13:12:40 Eastern Standard Time	
<input type="checkbox"/>	Enabled	Medium	High	USER	TROJAN_ASKTOOLBAR.CY	Local	183.44.23.12	sample_61	Feb 10 18:55:12 Eastern Standard Time	[+] Successful
<input type="checkbox"/>	Enabled	High	High	cyadmin	TROJAN_Trojan.CY	Local	193.106.172.140	10.1.1.29	Mar 15 16:54:36 Eastern Standard Time	[+] Successful
<input type="checkbox"/>	Disabled	Medium	High	JATP	VIRUS:WIN32_SALITY_AU.CY	Local	195.22.26.231	10.1.7.197	Sep 9 13:13:55 Eastern Standard Time	
<input type="checkbox"/>	Disabled	Medium	High	JATP	VIRUS:WIN32_SALITY_AU.CY	Local	195.22.26.253	10.1.7.197	Sep 9 13:13:55 Eastern Standard Time	
<input type="checkbox"/>	Enabled	High	High	USER	TROJAN_Stealth.CY	Local	188.48.763.106	10.1.7.31	May 10 18:22:45 Eastern Standard Time	[+]

The Juniper ATP Appliance Central Manager Web UI Mitigation Tab provides five different mitigation option views:

- Use the Search option on each page to search incident and threat criteria.

Review each blocking strategy in the following sections.

Blocking Threats at Firewalls

1. Click the Firewalls button on the Mitigation page to view a list of detected threats that Juniper ATP Appliance recommends you block on enterprise firewall(s).
2. Click the left-most checkbox(es) to select one or multiple threats for blocking at the Firewall(s), then click the Apply button.
3. [Alternatively, click the Remove button to remove the selected threat row from the Mitigation list.]

Note: If a mitigation rule is removed and its removal fails, it moves into a failed-remove state. You must repair the issue that caused the remove to fail and then click Remove again to finalize the removal. Some errors that might require a fix before the rule can be removed include (1) Juniper ATP Appliance not being able to obtain the config lock because there were uncommitted changes on the SRX, or perhaps (2) invalid credentials. Be aware, however, that when Juniper ATP Appliance attempts to remove a rule and the removal fails, a detail error message is displayed in the in the Web UI. It is not possible to have a failed-remove state but then try to re-Apply the mitigation rule; do repair the condition causing the removal failure please.

The threats to be blocked (potentially) are detailed as follows:

- › Malware IP - The IP Address associated with the threat to be blocked
- › Threat Target- Name of the targeted host.
- › Threat - Name of the incident by malware name.
- › Detection Date - Date and time of the malware detection.
- › Auto-Mitigation - Indicator of pre-configured auto-mitigation

Use the Search field to quickly locate a specific threat.

Caveat: Whitelist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the whitelist state because whitelist rules cannot be saved.

The mitigation IP address of a CNC server is not be available for Inside proxy deployments. When a Juniper ATP Appliance is deployed behind a proxy, the Mitigation-> Firewall page in the Juniper ATP Appliance Central Manager Web UI (which typically displays the CNC server IP address to mitigate) will be empty. The destination IP address of any callback is made to the proxy server ip address, so it is not relevant to display the proxy server IP address on the Mitigation->Firewall page.

Refer to the Juniper ATP Appliance CLI Command Reference for more information about setting data path proxies from collector mode, or management network proxy IP addresses from server mode.

Blocking Threats at Secure Web Gateways

1. Click the Secure Web Gateway button on the Mitigation page to view a list of detected threats identified for blocking on an enterprise secure web gateway(s).
2. View the malicious URLs identified for blocking at the SWG(s).

The threats to be blocked (potentially) are categorized as follows:

- › Domain/URL - The domain or URL associated with the threat to be blocked
- › Threat - Name of the detected threat
- › Threat Target - IP address of the targeted host.
- › Detection Date - Date and time of the Juniper ATP Appliance threat detection.

Use the Search field to quickly locate a specific threat.

Blocking Threats at the IPS/NextGen Firewall

1. Click the IPS/Next Gen Firewalls button on the Mitigation page to view a list of detected threats that Juniper ATP Appliance recommends you block on enterprise IPS/NextGen Firewall(s).
2. Click the left-most checkbox(es) to select one (or click Select All) to download signature files for API file submission or other forensics.

The threats to be blocked (potentially) are categorized as follows:

- › Threat - Name of the detected threat
- › Detection Date - Date of the Juniper ATP Appliance threat detection
- › Detection Location - Collector or Core Engine Detection Device

Use the Search field to quickly locate a specific threat.

Verifying Threats on the Endpoint

The Endpoint display lists infections to be verified by downloading the IVP tool and directly validating infections at your enterprise endpoint(s). In addition, at the bottom of the page, a second table lists Endpoint Infection results status information.

1. Click the Endpoints button on the Mitigation page to view a list of detected threats that Juniper ATP Appliance recommends you verify as active infections on enterprise endpoint(s).

2. Click the Download IVP link in the Action column to begin the IVP verification process.

The Infections to be Verified table columns are defined as follows:

- › Severity - The severity of the threat to be verified
- › Target - The IP Address of the enterprise host associated with the malware download (DL)
- › Threat - Name of the detected threat
- › Exposure Date - Date of the Juniper ATP Appliance threat detection at the endpoint
- › Action - The Download IVP link that generates and downloads a custom IVP package for the selected threat.

Use the Search field to quickly locate a specific threat.

IVP is customized for each malware incident and packaged for delivery to endpoints where it is run specifically to verify whether an infection took place at the endpoint(s) as a result of the currently selected malware download (DL) detected by the Juniper ATP Appliance analysis engines as listed in the Incidents table.

Use a thumb drive to install the package at the enterprise endpoints and then run the custom IVP verification test. The IVP package for a given malware event is not re-usable for a different malware download event; the IVP package is created in real time specifically for each detected malware event.

This IVP process will be automated in an upcoming release. In an upcoming Juniper ATP Appliance release, an alternate delivery option will push the IVP verification package to all enterprise endpoints from the Juniper ATP Appliance Central Manager using a configured domain controller group policy.

Run the IVP script and IVP installer on a targeted (or all) endpoints in the network to determine if the download caused an actual infection.

Using Whitelists

Use the Add to Whitelist option to perform ad hoc incident whitelisting.

1. Click Add to Whitelist button from the Incidents page sub-tab displays to whitelist a detected Download or Data Theft threat.

Figure 5-2 Add to Whitelist Option

The screenshot shows the 'ADVANCED THREAT PREVENTION APPLIANCE' interface. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The 'Incidents' tab is active, showing a list of incidents. Below the incident list, the 'Details for TROJAN_FAKEAV' section is expanded, showing the 'DOWNLOADS' sub-tab. In the 'DOWNLOADS' section, the 'Add to Whitelist' button is highlighted with a red circle.

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector
New	648222	MED	TROJAN_FAKEAV	DL	Web	greatfilesarey.asia	sj_demo_129	Default Zone	unknown	Partnerfw-Colec
New	648221	MED	TROJAN_FAKEAV	DL	Web	greatfilesarey.asia	sj_demo_128	Default Zone	unknown	Partnerfw-Colec
New	648220	HIGH	WORM_CRIDEX.CY	DL	Web	greatfilesarey.asia	sample_122	Default Zone	unknown	Partnerfw-Colec
New	648219	MED	TROJAN_DROP_D (DRIFF)	DL	Web	greatfilesarey.asia	test_127	Default Zone	unknown	Partnerfw-Colec

Details for TROJAN_FAKEAV

SUMMARY DOWNLOADS

Search:

Severity	Threat Name	File Type	Collector
Captured From:	HTTP Traffic		
Source:	172.16.0.1		
Source Address:	greatfilesarey.asia (172.16.0.1)		
Source URL:	http://greatfilesarey.asia/malware_vault/malware/newton_qa/file_samples/malware_exe/WL-fb2396747652ae592a894d9473280f1-3-0, Alexa Rank: -1		
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows		

Download Sample
Download Behavior Log
Add to Whitelist
Report False Positive
Screenshot

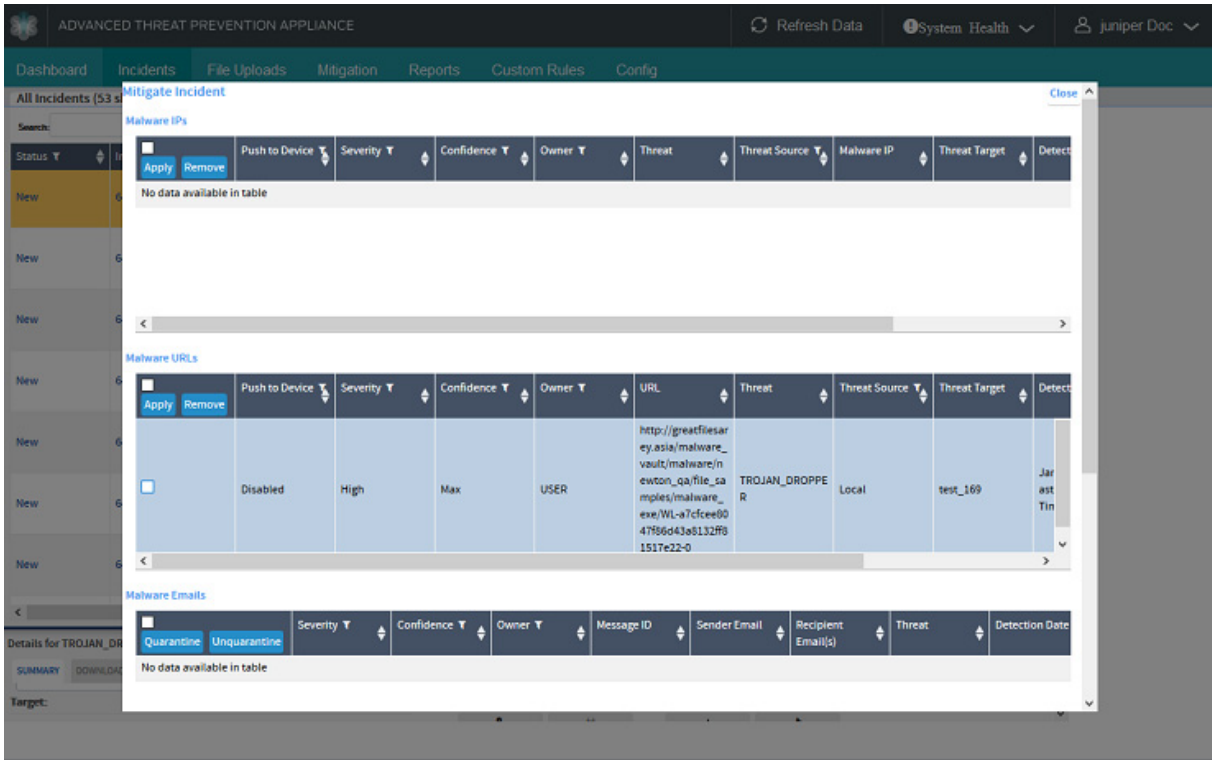
NOTE After whitelisting a DL, all instances of it are removed from the Incidents tab

After selecting Add to Whitelist, update the existing whitelist rules as necessary, as shown in the following figure.

Mitigation Options from the Incidents Tab

Mitigation options are also available from the Central Manager Incidents page.

Figure 5-3 Incidents Page Mitigation Options



The Details Summary area below the Incidents table displays a Mitigate Incident link.

1. Click the Mitigate Incident link to open the Mitigate Incident window for Malware IPs and Malware URLs.
2. Click to checkmark a threat row, and click Apply to submit the threat for blocking.

Updating Whitelist Filtering Rules

Configure Whitelist filtering rules from the Configuration>Whitelist Rules page. Additionally, you can re-configure and refine rule settings while administering whitelists from the Incidents page by using the Add to Whitelist link.

Update configured Whitelist Rules whenever an Incident includes the option to Add to Whitelist, as shown below, the filtering rules criteria can be edited and applied as part of the incident whitelisting process.

1. To edit Whitelist Filter criteria while adding the incident to the whitelist, click the Add to Whitelist link.
2. In the Update Whitelist Rule window, you may add additional whitelist rule criteria, deselect (uncheck) currently established criteria, or update the rule set as is.
3. Click Submit and the incident is added to the whitelist according to the criteria defined and checked in the Update Whitelist Rule window.

Generating Reports

Use the Reports tab to select one of the three on-demand Threat Report templates (defined below), and then click either Display, Delete or Edit to modify the report presentation.

- Select the Executive Report option to generate an Executive summary of all threats categorized by malware severity for all detection times.

- Select the Technical Report option to generate a Technical summary of all threats for all detection times [in HTML format by default], named Recent Malware Report. Reports for System Audit and System Health are also available.

Report Types and Options

Each report type displays a set of custom options, as shown below.

Figure 5-4 Juniper ATP Appliance Executive Report Options

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Report Category: ☒ Executive Report ☐ Technical Report

Report Name: ☒ Malware by Severity

Zone: ☒ Default ☐ ABC Corp ☐ Acme Corp

Date Range: ☐ Last Day ☒ Last Week ☐ Last Month ☐ Last Year

Max. Rows Displayed: 25

Format: ☒ HTML ☐ PDF

Generate On: ☒ On Demand ☐ By Schedule

Shareable: ☒ Public ☐ Private

Save

Cancel

Report Templates

Description	Creator	Delivery	Actions
Executive Report: Malware by Severity, Last Week, HTML, Zone: Default Zone	cyadmin	On Demand	Display Delete Edit
Executive Report: Malware by Severity, Last Week, PDF, Zone: Default Zone	gsuzuki	On Demand	Display Delete Edit

Figure 5-5 Juniper ATP Appliance Technical Report Options

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules Config

Report Category: ☐ Executive Report ☒ Technical Report

Report Name: ☐ Events ☒ Hosts infected by CnC ☐ Who Downloaded Malware ☐ System Audit ☐ System Health

Zone: ☒ Default ☐ ABC Corp ☐ Acme Corp

Date Range: ☐ Last Day ☒ Last Week ☐ Last Month ☐ Last Year

Max. Items Results: 25

Format: ☒ HTML ☐ PDF

Malware Severity: ☒ All malware ☐ Critical, High or Med ☐ Critical or High

Generate On: ☒ On Demand ☐ By Schedule

Distribution: ☐ Public ☐ Private

Cancel

Report Templates

Description	Creator	Delivery	Actions
Executive Report: Malware by Severity, Last Week, HTML, Zone: Default Zone	cyadmin	On Demand	Display Delete Edit
Executive Report: Malware by Severity, Last Week, PDF, Zone: Default Zone	gsuzuki	On Demand	Display Delete Edit

Click Display to display the report in a browser window.

Click Delete to delete a report template from the list.

Click Edit to modify a report template; the "Edit" and "Customize" options are identical [see Customize Reports options below].

Customizing Reports

- To customize report(s), click the blue Create a Custom Report Template button, make selections, and click Save to preserve modified or customized template settings.

Custom template options are described below:

Executive Report

Refer to the section [Sample Executive Report Segments on page 254](#) for an overview of the main segments published to Executive Reports.

Options for creating a custom Executive Report:

Table 5-1 Executive Report Settings

Report Name	Malware by Severity
Date Range	Options: Last Day Last Week Last Month Last Year.
Maximum Number of Results	Enter the number of results to display in the report [the default is 25].
Format	Options: HTML or PDF.
Generate	Options: On Demand By Schedule.

Table 5-1 Executive Report Settings

Days	Options: Mon Tues Wed Thurs Fri Sat Sun
Time	Enter time in format 00:00 am or pm
Recipient(s) email	Enter email address(es), separated by commas.

Technical Report

Options for creating a custom Technical Report:

Table 5-2 Technical Report Settings

Report Name	Events Hosts Infected by CnC Who Downloaded Malware System Audit System Health
Date Range	Options: Last Day Last Week Last Month Last Year.
Maximum Number of Results	Enter the number of results to display in the report [the default is 25].
Format	Options: HTML or PDF.
Malware Severity	Options: All Malware Critical, High or Med Critical or High
Generate	Options: On Demand By Schedule.
Days	Options: Mon Tues Wed Thurs Fri Sat Sun
Time	Enter time in format 00:00 am or pm
Recipient(s) email	Enter email address(es), separated by commas.

System Audit Report

Options for creating a custom System Audit Report:

Table 5-3 System Audit Report Settings

Report Name	System Audit
Event Type	Select the event type(s) to include in the alert notification: Login/Logout Failed logins Add/Update Users System Settings Restarts System Health
Users	Select All Users or Current User for the notification report.
Date Range	To filter the report notification by time period, select one: Last Day Last Week Last Month Last Year
Max Num Results	Enter the number of rows of results to include in the alert notification [default is 25].
Format	Select HTML or PDF as the notification output format.
Generate	Options: On Demand By Schedule.
Days	Options: Mon Tues Wed Thurs Fri Sat Sun
Time	Enter time in format 00:00 am or pm

Table 5-3 System Audit Report Settings

Recipient(s) email	Enter email address(es), separated by commas.
--------------------	---

System Health Report

Options for creating a custom System Health Report:

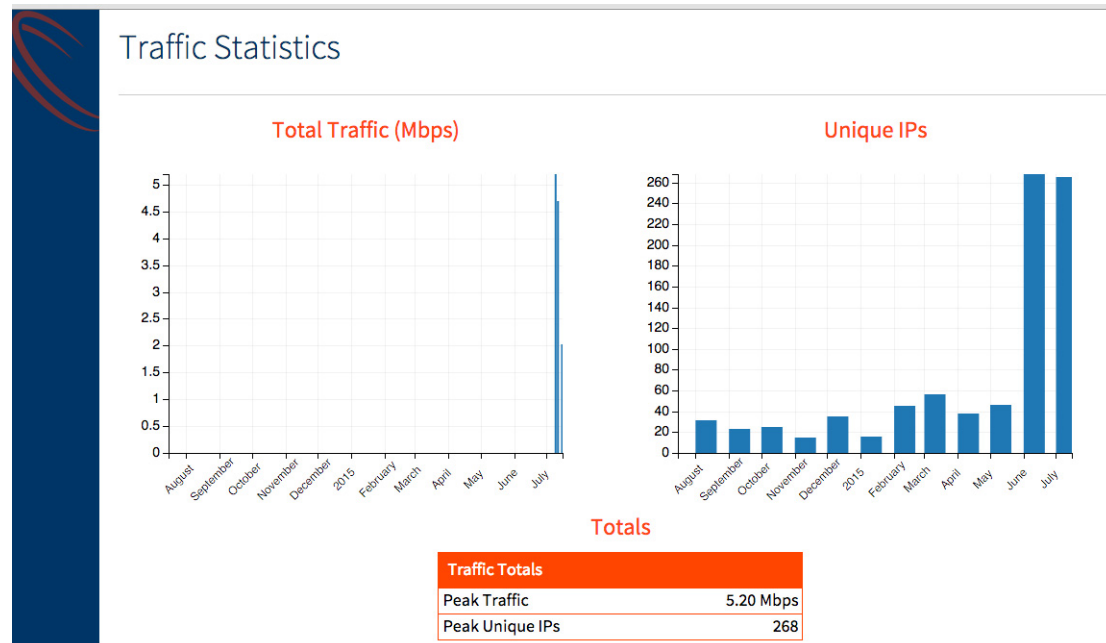
Table 5-4 System Health Report Settings

Report Name	System Audite
Health	Select Overall Health or Processing Delay for the health report.
Format	Select HTML or PDF as the notification output format.
Generate	Options: On Demand By Schedule
Days	Options: Mon Tues Wed Thurs Fri Sat Sun
Time	Enter time in format 00:00 am or pm
Recipient(s) email	Enter email address(es), separated by commas.

Sample Executive Report Segments

Some of the main categories of information and statistics provided in a Juniper ATP Appliance Executive Report are shown in the series of samples below:

Traffic Statistics

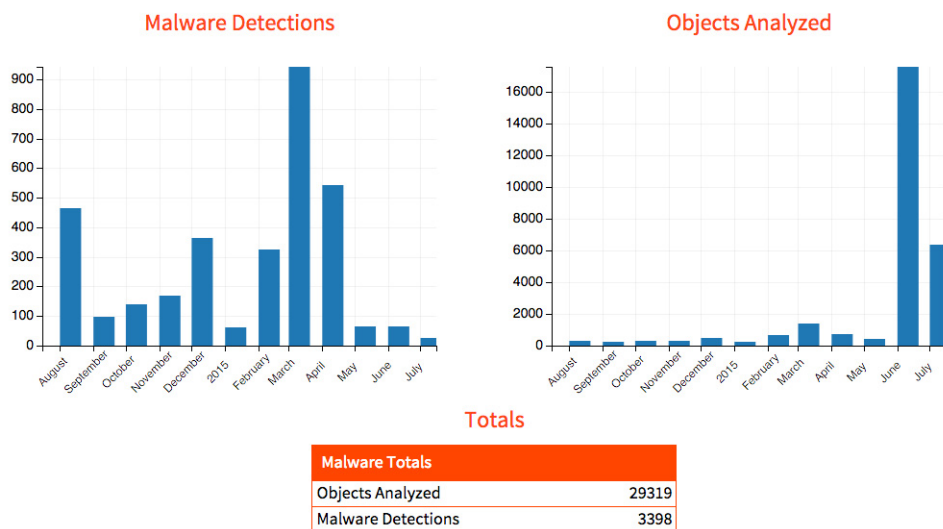


Total Traffic(Mbps): The total traffic seen by the Core.

Unique IPs: The count of unique Internal or destination IPs seen by the Core.

Malware Statistics

Malware Statistics

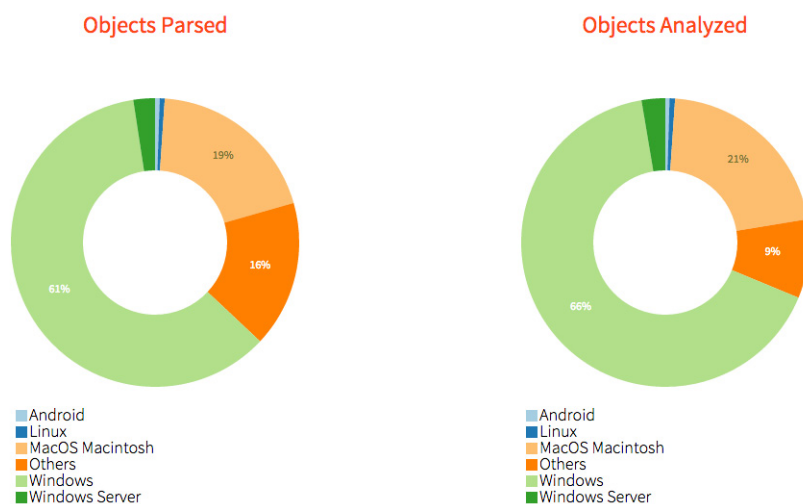


Objects Analyzed: The number of downloadable files detected by the Core and analyzed.

Malware Detections: Total number of threats identified by the Core in the network.

File Statistics by Operating System

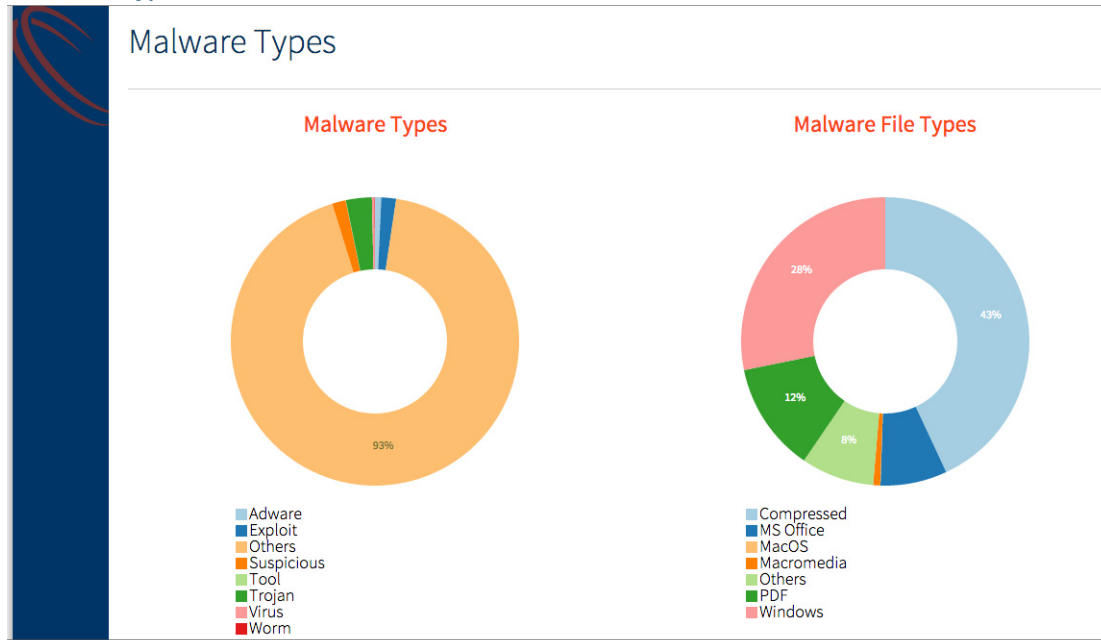
File Statistics by Operating System



Objects Parsed: Percentage of the different files seen by the Core in the network.

Objects Analyzed: Percentage of the different files analyzed by the Core in the network. This is always a subset of objects parsed. A few of the files such as jpeg, gif, txt etc. that are parsed are not analyzed in the Core.

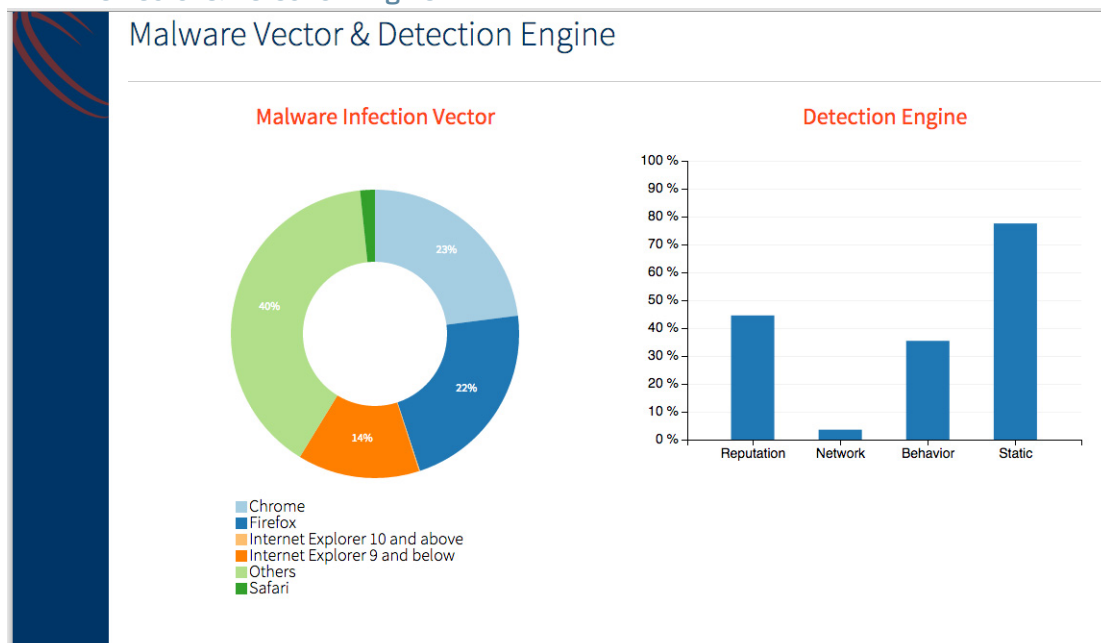
Malware Types



Malware Types: The categories of the malware as seen by the Core.

Malware File Types: Percentage of the different file types that were detected as malware by the Core.

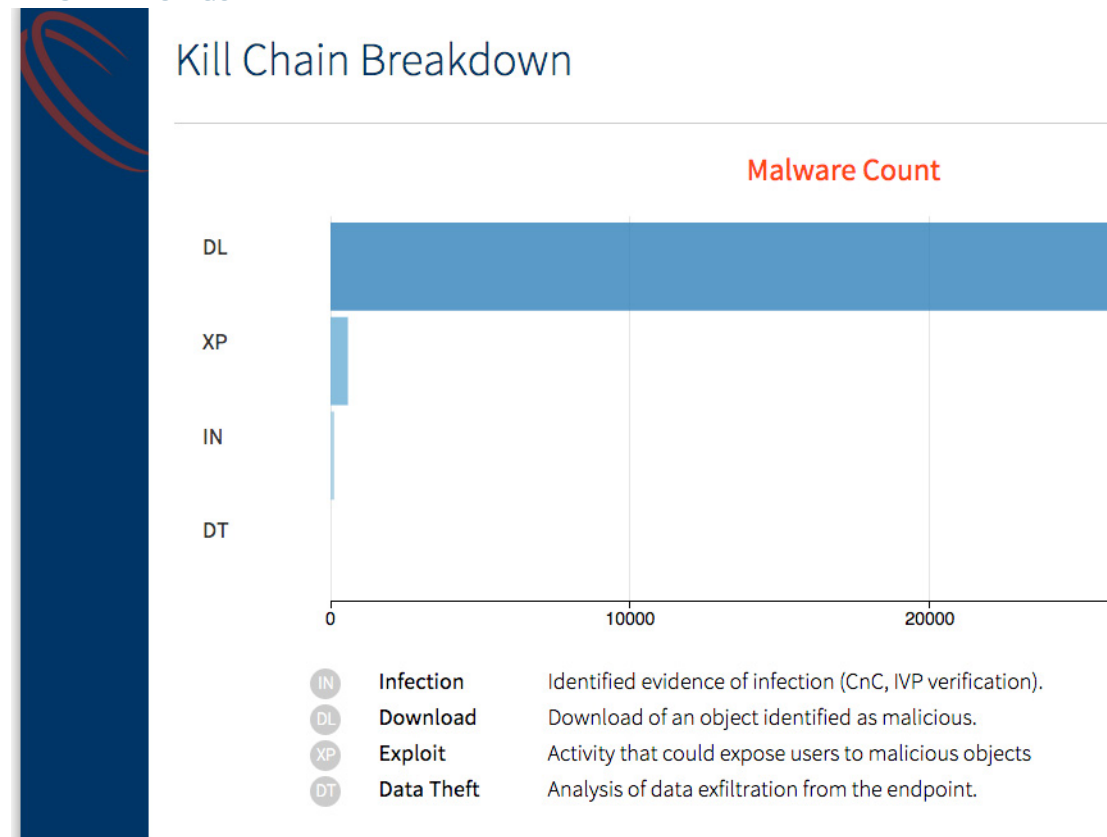
Malware Vector & Detection Engine



Malware Infection Vector: Percentage of Malware per Browser type

Detection Engine: Percentage of Malware detected by the Core by various detection engines.

Kill Chain Breakdown



Kill Chain Breakdown: Total count of Malware detected by various kill chains.

Top Malware Serving Countries

Top Malware Serving Countries

Top countries serving malware infecting your organization

Country	Detections
US	3211
DE	79
VG	19
RU	17
IL	15
CN	14
LV	12
FR	8
BR	6
AU	5

Malware Detections Breakdown (Part 1)

Malware Detections Breakdown (Part 1 of 48)

Malware Name	# Detections	1st Detection Date
High Severity		
EXPL_PDFJSC.DC	100	02/23/2015
EXPL_PDFJSC.CY	93	12/18/2014
TROJAN_ZBOT.CY	50	01/13/2015
EXPL_CVE-2013-0074.CY	44	03/18/2015
TROJAN_FAREIT.CY	37	03/18/2015
EXPL_PDFKA.DC	30	12/18/2014
Trojan.DC	30	12/17/2014
EXPL_PIDIEF.DC	27	02/23/2015
Exploit.Static	26	03/17/2015
TROJAN_CEEINJECT.CY	26	03/18/2015
TROJAN_SWRORT.DC	24	02/18/2015
TROJAN_VAWTRAK.CY	15	03/18/2015
EXPL_FIEXP.Rep	13	01/01/2015
TROJAN_CARBERP.CY	12	03/18/2015
WORM_AINSLOT.CY	11	12/18/2014
SUSP_GENERIC.Rep	10	03/18/2015

Malware Targets (Part 1)

Malware Targets (Part 1 of 13)

Target	# Detections	1st Detection Date
10.3.1.231	388	03/18/2015
67.161.7.243	377	04/07/2015
10.3.1.38	284	03/20/2015
10.1.10.89	173	12/30/2014
208.74.183.152	127	12/18/2014
10.3.1.175	79	07/16/2014
10.1.9.106	64	12/03/2014
198.233.198.200	64	02/20/2015
10.3.1.237	50	07/18/2014
10.3.1.189	48	10/14/2014
tap59.local	43	07/31/2014
67.91.205.130	35	07/17/2014
67.91.205.174	35	11/25/2014
10.3.1.252	34	04/02/2015
10.1.9.25	33	07/18/2014
98.189.185.26	32	12/15/2014

CHAPTER 6

System Information and Updates

The following topics are in this chapter:

- [CHECKING APPLIANCE HEALTH](#)
- [UPGRADING JUNIPER ATP APPLIANCE SOFTWARE AND SECURITY CONTENT](#)
- [CEF LOGGING SUPPORT FOR SIEM](#)

Checking Appliance Health

Click the System Health dropdown to view real-time operational status for the Juniper ATP Appliance inspection and detection engines.

Internet	Internet connection status
Behavior Engine	Core behavior analysis engine status
Static Engine	Static analysis engine status
Correlation	Hierarchical Reasoning Engine (HRE) machine learning component status
Web Collectors	Web collectors status is displayed if there are distributed Web Collector devices enabled. Note: If the current system is an All-in-One and no additional Collector device is configured, then the Web Collectors item in the dropdown menu will be absent.
Secondary Cores	Secondary Cores status is displayed if there are distributed Mac Mini Secondary or Windows Secondary Core devices enabled.

System Dashboard

The System Dashboard is also available from the Dashboard tab as well for monitoring system inspection and detection metrics:

The System Dashboard includes metrics for the following:

- Scanned Traffic Objects/Offered Traffic Objects
- Core Utilization (Windows and Mac OSX)
- Objects Processed
- Average Analysis Time (in Minutes) (Windows and Mac OSX)
- Malware Objects

System Charts can be displayed for:

Last 24 Hours | Last Week | Last Month | Last 3 Months | Last Year

Collectors Dashboard

The Collectors Dashboard is another dashboard available from the Dashboard tab:

The Collectors Dashboard includes metrics for the following collector inspection and analysis Trend displays (options are select from the Trend dropdown menu):

- Total Traffic (Mbps)
- CPU Usage
- Memory Usage
- Found Objects
- Malware Objects

System Charts can be displayed for:

Last 24 Hours | Last Week | Last Month | Last 3 Months | Last Year

The Collectors Dashboard Summary table provides configured and statistical information in the following columns:

Table 6-5 Collectors Dashboard Summary

Summary Column	Description
Plot	Click to display [multiple] plots for comparisons in the graph above; colors are displayed for each selected graphical plot line
Collector Name	Name of the installed Traffic Collector
IP Address	IP Address of the Collector
Memory	Memory Usage statistics
CPU	CPU usage statistics
Disk	Disk Usage
Total Traffic	Total Traffic Scanned in Kbps or Mbps
Objects	Objects analyzed
Malware Objects	Malware Objects detected
Last Malware Seen	Last malware incident detected and analyzed
Status	Last status check on the Collector (example: "83 seconds ago")
Enabled	Green checkmark indicates that the Collector is currently enabled; a red X indicates that the Collector is disabled or offline.

Upgrading Juniper ATP Appliance Software and Security Content

Upgrading of software and security content is automatic when configured from the Central Manager Web UI Config>System Settings>System Settings page.

- To enable automatic upgrades, check the "Software Update Enabled" and/or "Content Update Enabled" options on the System Settings page.

Ongoing updates take place on a regular schedule:

- The software and content update (if enabled) checks for available updates every 30 minutes.
- The Core detonation engine image upgrade check occurs daily at midnight.

CEF Logging Support for SIEM

Juniper ATP Appliance's detection of malicious events generates incident and alert details that can be sent to connected SIEM platforms in CEF format via UDP.

NOTE Refer to the [Juniper ATP Appliance CEF Logging Support for SIEM document](#), which focuses on CEF outputs for SIEM mapping and integration. Juniper ATP Appliance also provides JSON-based HTTP API results and ASCII TEXT notifications that are not discussed in this guide.

The Juniper ATP Appliance Central Manager WebUI Config>Notifications>SIEM Settings page provides the option to configure event and system audit notifications for SYSLOG or CEF-based SIEM servers. The servers, in turn, must be configured to receive the Juniper ATP Appliance notifications in CEF format.

syslog Trap Sink Server

When configuring the Juniper ATP Appliance to generate alert notifications in Syslog format, an administrator must confirm that the syslog trap-sink SIEM server support. The Syslog output is accessible for parsing only on the syslog server and cannot be viewed from the Juniper ATP Appliance CLI or Web UI.

CEF Format

Common Event Format (CEF) is an open standard syslog format for log management and interoperability of security related information from different devices, network appliances and applications. This open log format is adopted by Juniper ATP Appliance for sending Juniper ATP Appliance malware event notifications to the configured channel.

The standard CEF format is:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity|Extension
```

The Juniper ATP Appliance CEF format is as follows:

```
CEF:0|Juniper ATP Appliance|Cortex|<Juniper ATP Appliance version x.x.x.x>|<event
type: http,email,datatheft...>|<malware name>|<incident risk mapping to 0-
10>|externalId=<Juniper ATP Appliance Incident ID> eventId=<Juniper ATP Appliance
event ID> <ExtensionField=value...>...
```

The CEF format contains the most relevant malware event information, making it available for event consumers to parse and use the data interoperably. To integrate events, the syslog message format is used as a transport mechanism. This mechanism is structured to include a common prefix applied to each message, and contains the date and hostname as shown below:

```
<timestamp in UTC> host <message>
where message=<header>|<extension>
```

Here is the common prefix as shown in Splunk:

```
<Timestamp in UTC> <server-fully-qualified domain name of the Juniper ATP
Appliance box> <CEF format>
```

Definitions for the primary CEF fields as well as the CEF Extensions are provided and detailed in the [Juniper ATP Appliance CEF and Syslog Support for SIEM guide](#).

NOTE The Username field is included in the SIEM logs while sending audit logs.
