

Juniper Advanced Threat Prevention Appliance

Email Collector Quick Start 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 Email Collector Quick Start 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.

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>

Inside This Guide

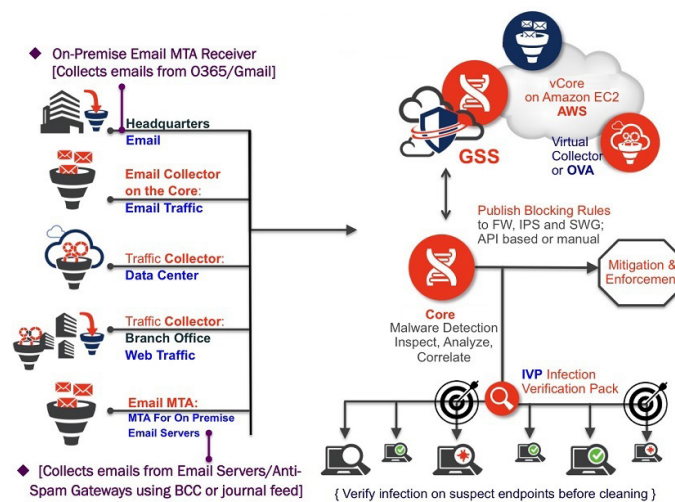
- ON-PREMISE JUNIPER ATP APPLIANCE-MTA-RECEIVER DEPLOYMENTS
- ON-PREMISE BCC EMAIL COLLECTOR DEPLOYMENTS
- CONFIGURING COLLECTOR EMAIL JOURNALING
- CORE/CM AND ALL-IN-ONE EMAIL COLLECTOR INSTALLATION OPTIONS
- INSTALLING THE JUNIPER ATP APPLIANCE COLLECTOR OPEN VIRTUAL APPLIANCE (OVA)
- INSTALLING AND CONFIGURING THE AWS VCORE AMI
- VERIFYING AWS CONFIGURATIONS
- CONFIGURING JUNIPER ATP APPLIANCE EMAIL TRAFFIC COLLECTION
- SETTING THE SAME DEVICE KEY PASSPHRASE ON ALL JUNIPER ATP APPLIANCE DEVICES
- VERIFYING CONFIGURATIONS AND TRAFFIC FROM THE CLI
- ACCESSING THE JUNIPER ATP APPLIANCE CENTRAL MANAGER WEB UI
- WHAT TO DO NEXT?

Welcome to the Juniper ATP Appliance Email Collector Quick Start Guide.

Juniper ATP Appliance's Email Collector detects malicious URLs and attachments delivered via email and correlates these detections with web downloads and lateral spread events. There are three Juniper ATP Appliance email options:

- An On-Premise Email MTA-Receiver
- A BCC or Journal Email Server Account

Figure 1 Juniper ATP Appliance Email Collection and Detection Options



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

On-Premise Juniper ATP Appliance-MTA-Receiver Deployments

Juniper ATP Appliance MTA Receiver deployments collect emails from different servers including Office 365, Gmail and MS Exchange. It also supports any other email servers/anti-spam gateway that supports additional SMTP receivers for sending emails to the Juniper ATP

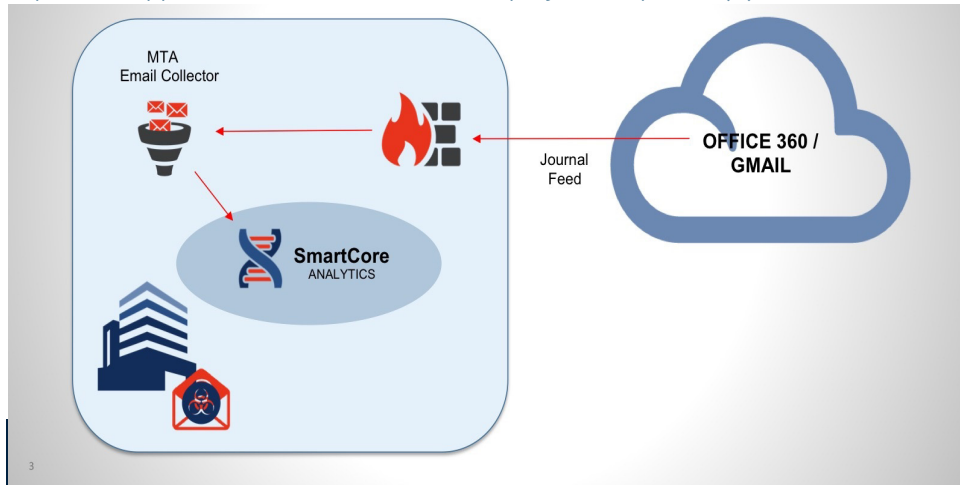
Appliance MTA Receiver (without adding any SMTP envelop headers to make the original email an attachment). The Juniper ATP Appliance admin must configure the supported servers (to direct the email stream to the Juniper ATP Appliance MTA Receiver) using the email address setup on the MTA Receiver (for example: CustomerX@MTA-IP or CustomerX@DomainName).

Juniper ATP Appliance's On-Premise MTA Receiver extracts objects/URL links and submits them to the Juniper ATP Appliance Core for analysis. With multi-vector threat detection, if existing security infrastructure fails to detect a phishing link, Juniper ATP Appliance monitors the download from that link, detects the CnC callbacks caused by the download, correlates any lateral spread that the download can trigger, and blocks the threat with mitigation. Benefits include:

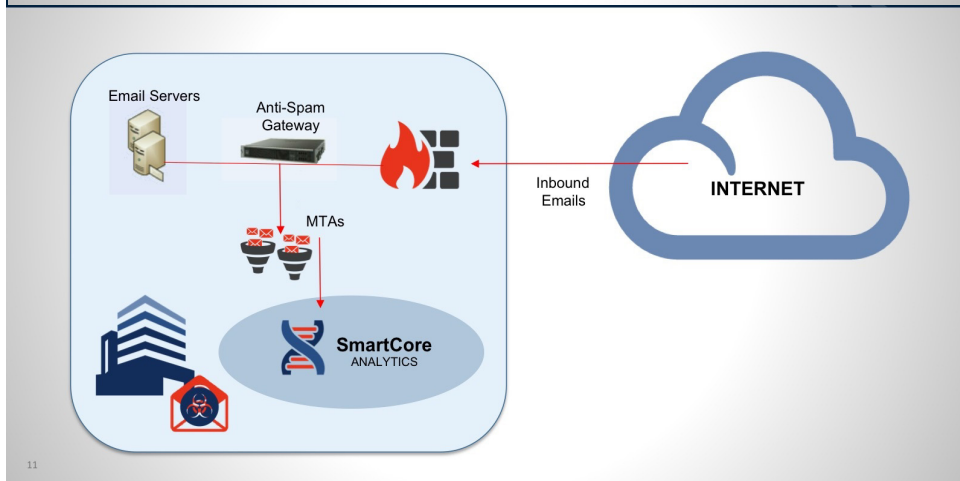
- Visibility into email borne threats at high scale (2.4 Million emails/day)
- Detection of Malicious Email Attachments and URL Links
- Ability to quarantine malicious emails

Figure 2 Juniper ATP Appliance Email MTA-Receiver Deployment Options: (a) for Office 365 and Gmail Analysis

(a)



(b)



Generalized Administrator Tasks for Juniper ATP Appliance On-Premise MTA Deployments

After installing a Juniper ATP Appliance Core or All-in-One system, both of which contain an Email Traffic Collector in the Core component, an admin will need to perform the following tasks:

- open a firewall rule to allow emails from office 365/gmail to the mta (from *.protection.outlook.com to JuniperATPmta_external_ip:25)
- use the external ip address or fqdn of the mta to create a journal rule in office 365 (user@1.1.1.1 or user@customer.com)
- configure mailbox name and mta ip from the Juniper ATP Appliance web interface in:
 - › System Profiles > Email Collector > Add New Email Collector > Juniper ATP Appliance MTA Receiver
 - › Configure Mitigation information To Auto-Mitigate: Environmental Settings > Email Mitigation Settings
- ports used:
 - › (Collection) Office 365 / Gmail / Exchange Connects To MTA using TCP:25 (Inbound) (TLS Can Be Enabled)
 - › (Submission) MTA Connects To Core/CM Using TCP:443
 - › (Mitigation) Core/cm Connects To Office 365/ Gmail Using TCP:443 (Outbound)

On-Premise BCC Email Collector Deployments

This method of email collection relies on a BCC or Journal mailbox which receives copies of emails to be inspected. The Juniper ATP Appliance BCC email collector periodically pulls these emails to examine them for threats.

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 urls and email attachments are sent from the Email Collector to the Juniper ATP Appliance Core for detonation in the Juniper ATP Appliance SmartCore. 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, refer to the next section.

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.

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, use the following procedures:

Create a Journaling Mailbox on the Exchange Server

NOTE See also “Configuring Microsoft Exchange Server 2013 Journaling.”

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

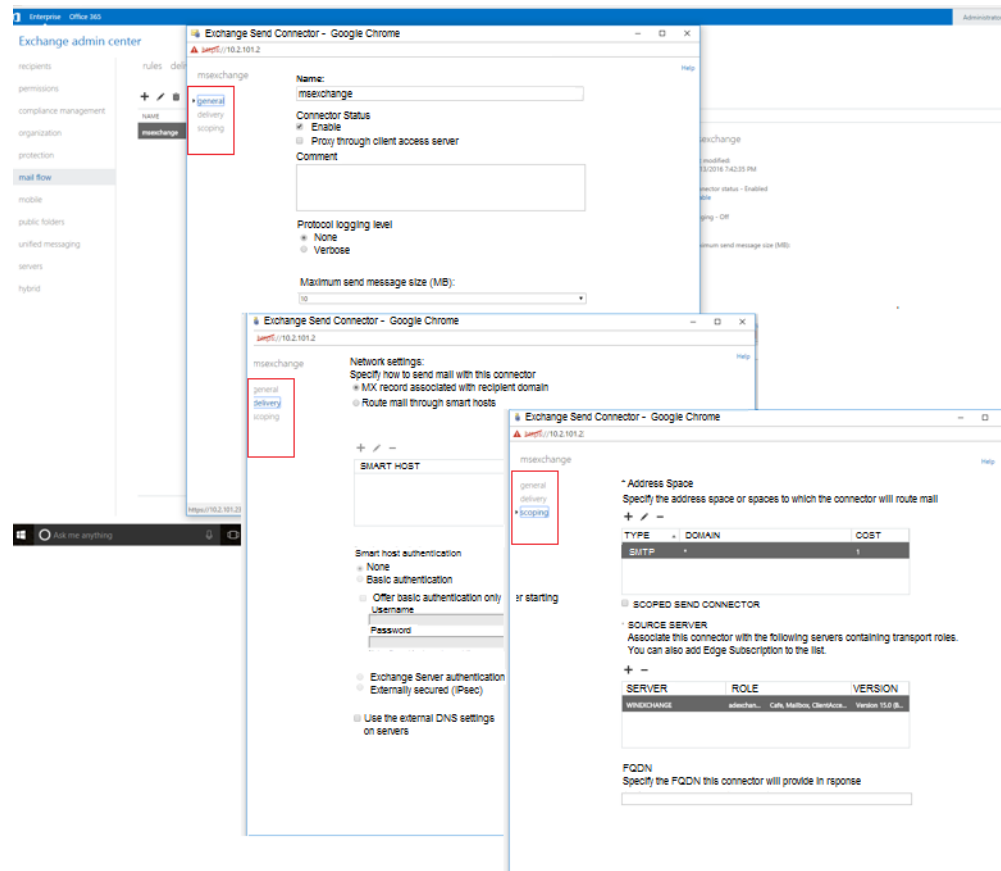
[See also Configuring Microsoft Exchange Server 2010 Journaling in the next section.]

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

Step 2 Select the Send Connectors tab.

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

Figure 3 Send Connector Settings

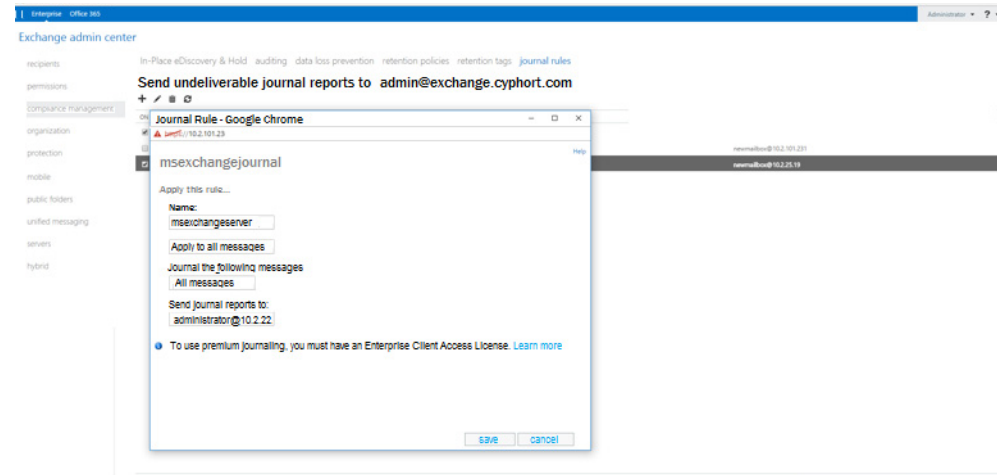


Step 4 Save the connector settings.

Step 5 Navigate to Compliance Management>>Journal Rules to configure Journal rules.

Step 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 4 Setting Journal Rules



Configuring Microsoft Exchange Server 2010 Journaling

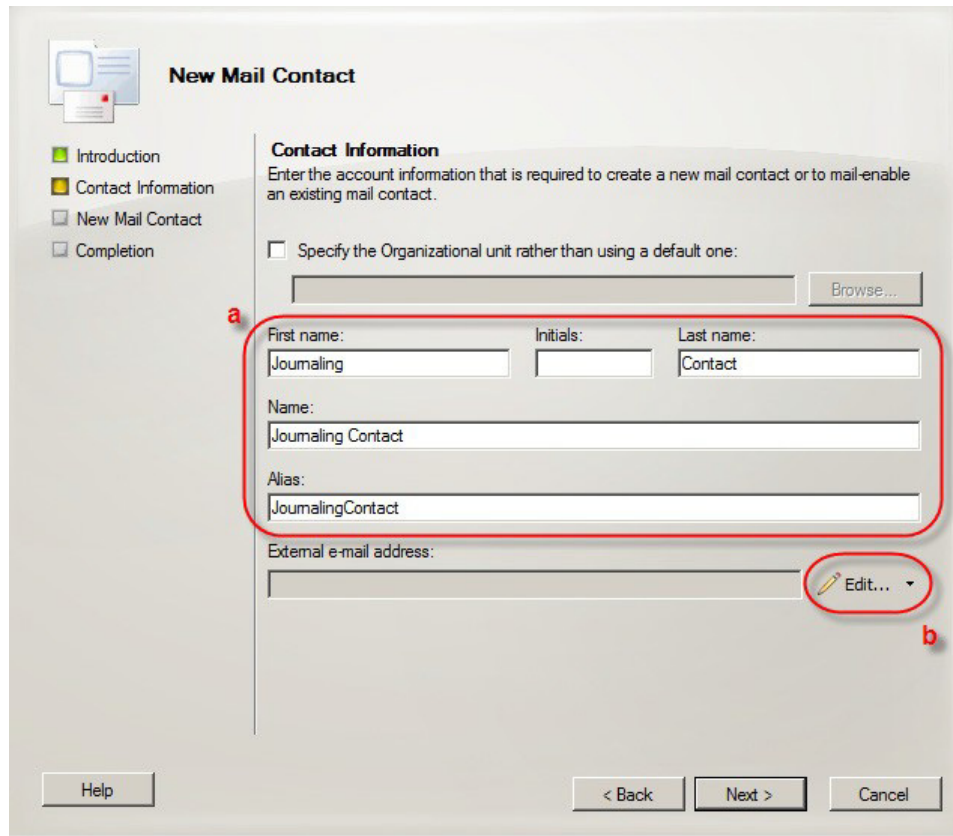
To configure Journaling on your Exchange 2010 server, follow these steps:

- Set up a journaling contact
- Configure an SMTP send connector
- Activate journaling
- Implement journal rules (select users only)

[See also Configuring Microsoft Exchange Server 2013 Journaling in the previous section.]

Create a journaling contact

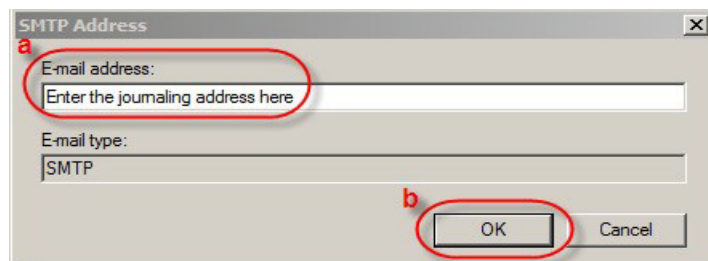
1. Select Start > All Programs > Microsoft Exchange Server 2010 > Exchange Management Console.
2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Recipient Configuration.
4. Click Mail Contact under Recipient Configuration.
5. In the Mail Contact page (a), click New Mail Contact in the Actions pane (b).
6. Select the New Contact option (a) and then click Next (b).
7. In the New Mail Contact window, type Journaling in the First Name field, Contact in the Last Name field and Journaling Contact in the Alias field (a). Click Edit (b).



The 'New Mail Contact' dialog box is shown. On the left, a sidebar contains four items: 'Introduction' (selected), 'Contact Information', 'New Mail Contact', and 'Completion'. The main area is titled 'Contact Information' and contains the following fields and controls:

- A checkbox labeled 'Specify the Organizational unit rather than using a default one:' with a 'Browse...' button next to it.
- A red box labeled 'a' highlights the 'First name:' field (containing 'Joumaling'), the 'Initials:' field (empty), and the 'Last name:' field (containing 'Contact').
- A 'Name:' field containing 'Joumaling Contact'.
- An 'Alias:' field containing 'JoumalingContact'.
- An 'External e-mail address:' field with an 'Edit...' button next to it, which is circled in red and labeled 'b'.
- At the bottom are 'Help', '< Back', 'Next >', and 'Cancel' buttons.

8. Type the journaling address (a) and click OK (b).



The 'SMTP Address' dialog box is shown. It contains the following fields and controls:

- A red box labeled 'a' highlights the 'E-mail address:' field, which contains the placeholder text 'Enter the journaling address here'.
- An 'E-mail type:' field containing 'SMTP'.
- A red box labeled 'b' highlights the 'OK' button.
- A 'Cancel' button is also present.

NOTE The journaling address is unique to your organization. If you were provided with this address, please contact customer support.

9. Click Next.

10. Click New.
11. Click Finish.

Create an SMTP send connector

1. Select Start > All Programs > Microsoft Exchange Server 2010 > Exchange Management Console.
2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Organization Configuration.
4. Click Hub Transport.
5. Click the Send Connectors tab.
6. In the Actions pane, click New Send Connector.
7. Type Journaling Connector for the Name field, for the Select the intended use for this Send connector drop-down list, select Custom (a). Click Next (b).

New Send Connector

Introduction

This wizard helps you create a new Send connector. After you create the Send connector, right-click it in the work pane and then click Properties to configure other properties that aren't shown in this wizard.

Name:

Journaling Connector

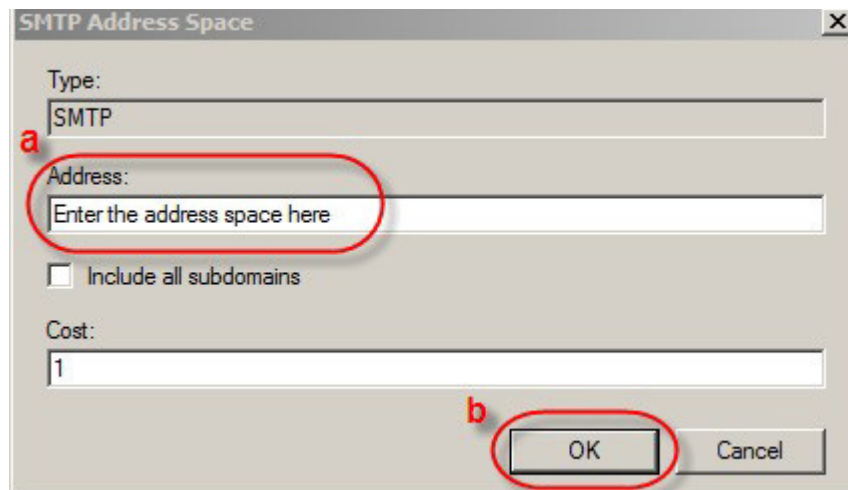
Select the intended use for this Send connector:

Custom

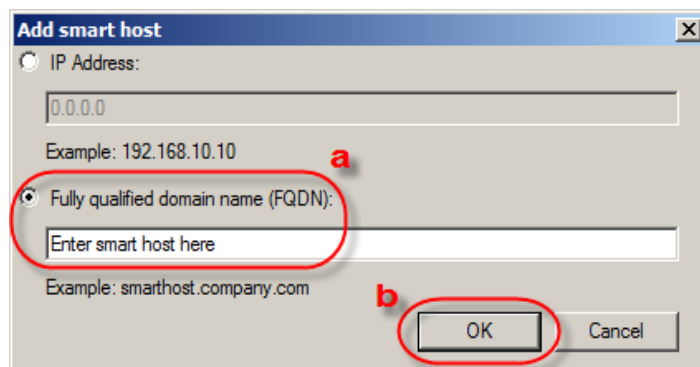
Description: Select this option to create a customized connector, which will be used to connect with systems that are not Exchange servers.

Help < Back Next > Cancel

8. Click Add. The SMTP Address Space window opens.
9. In the Address field, type the Address Space (a). Leave the cost at 1 and then click OK (b).



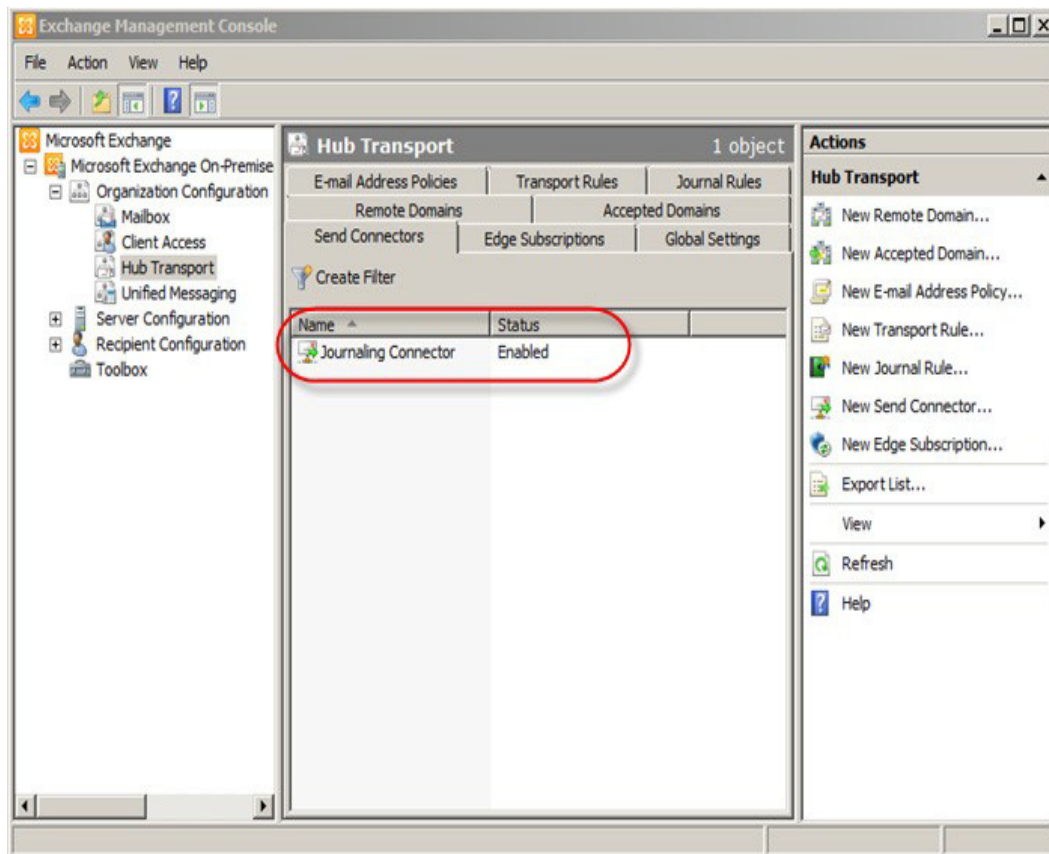
10. Click Next.
11. Select the Route mail through the following smart hosts option and then click Add.
12. Select the Fully qualified domain name (FQDN) option, type the smart host provided to you and then click OK.



13. Click Next.
14. Select None for the Configure smart host authentication settings and then click Next.

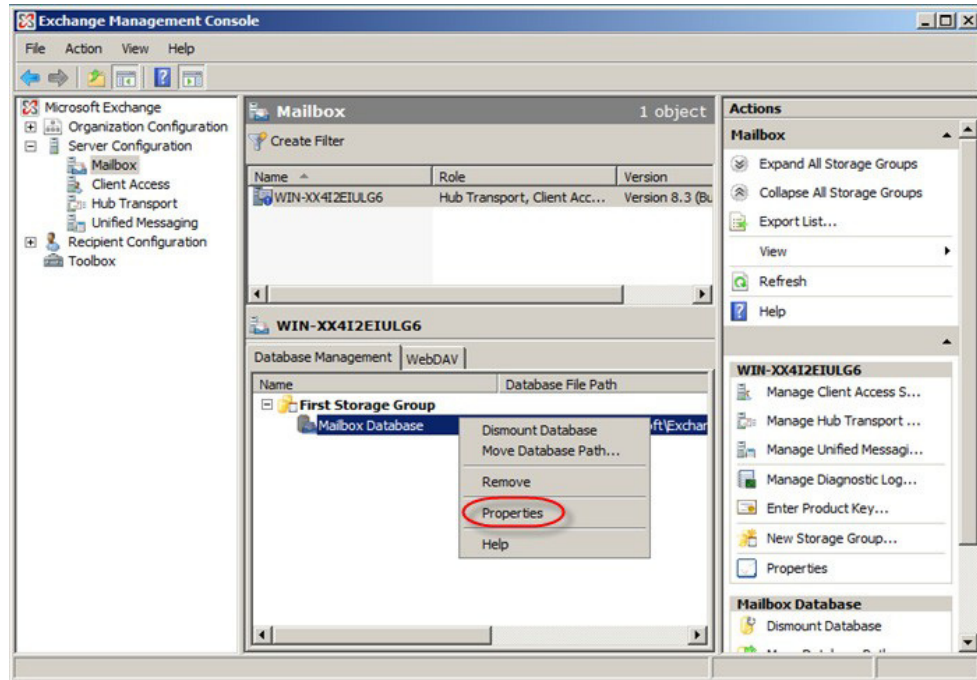
NOTE Exchange 2010 servers automatically send all outbound email via TLS encryption: no outbound security configuration is required by the Administrator.

15. Click Next.
16. Click New.
17. Click Finish. The configured send connector is shown below.

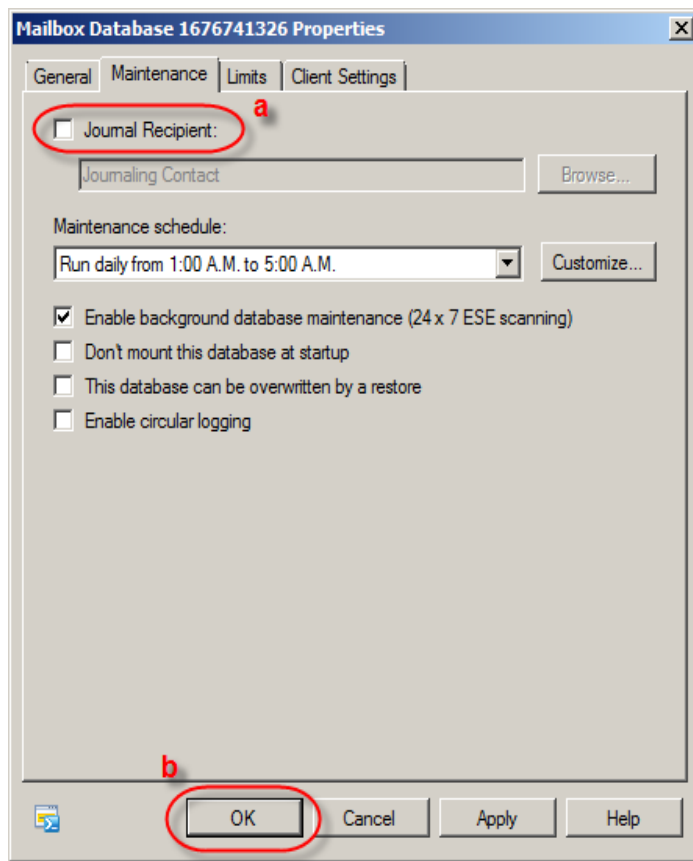


Activate journaling

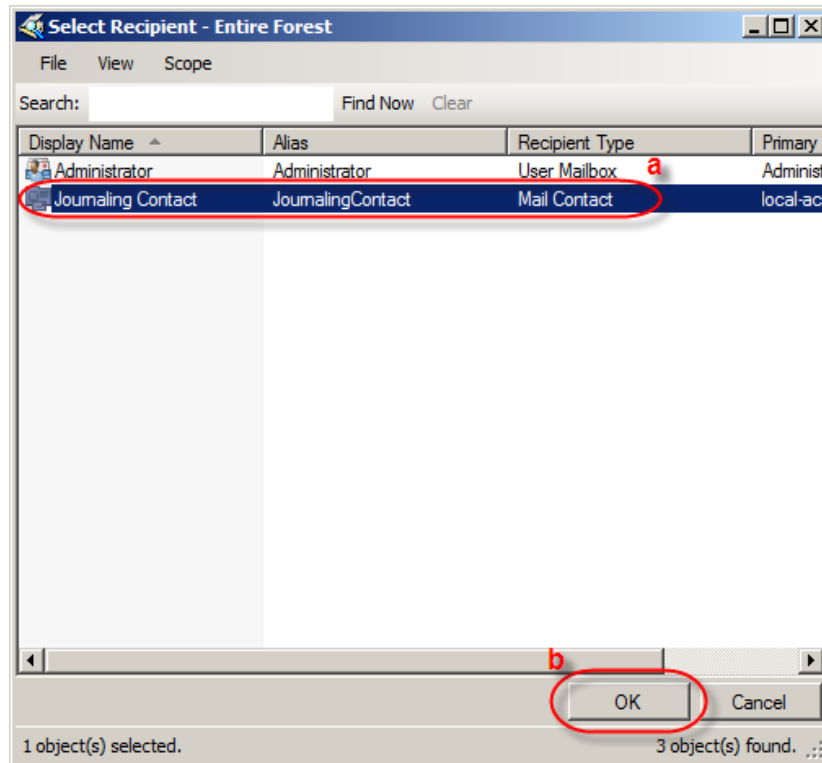
1. Select Start > All Programs > Microsoft Exchange Server 2010 > Exchange Management Console.
2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Organization Configuration.
4. Click Mailbox.
5. In the Database Management tab, right click your mailbox database and select Properties.



6. Click the Maintenance tab.
7. Select the Journal Recipient check box (a), and then click Browse (b).



8. Select Journaling Contact (a) and then click OK (b).



9. Click OK. Message journaling is now activated.

Implement journal rules (select users only)

1. Select Start > All Programs > Microsoft Exchange Server 2010 > Exchange Management Console.
2. Click the + sign to the left of your Exchange server.
3. Click the + sign to the left of Organization Configuration.
4. Click Hub Transport.
5. Click the Journal Rules tab.
6. In the Actions pane, click New Journal Rule. The New Journal Rule window appears.
7. In the Rule Name field, type Journaling Rule (a) and then click Browse (b).

New Journal Rule

This wizard helps you create a new journal rule. When enabled, the new journal rule is executed on your organization's Hub Transport servers.

Rule name:
Journaling Rule

Send Journal reports to e-mail address:
Browse...

Scope:
☒ Global - all messages
☐ Internal - internal messages only
☐ External - messages with an external sender or recipient

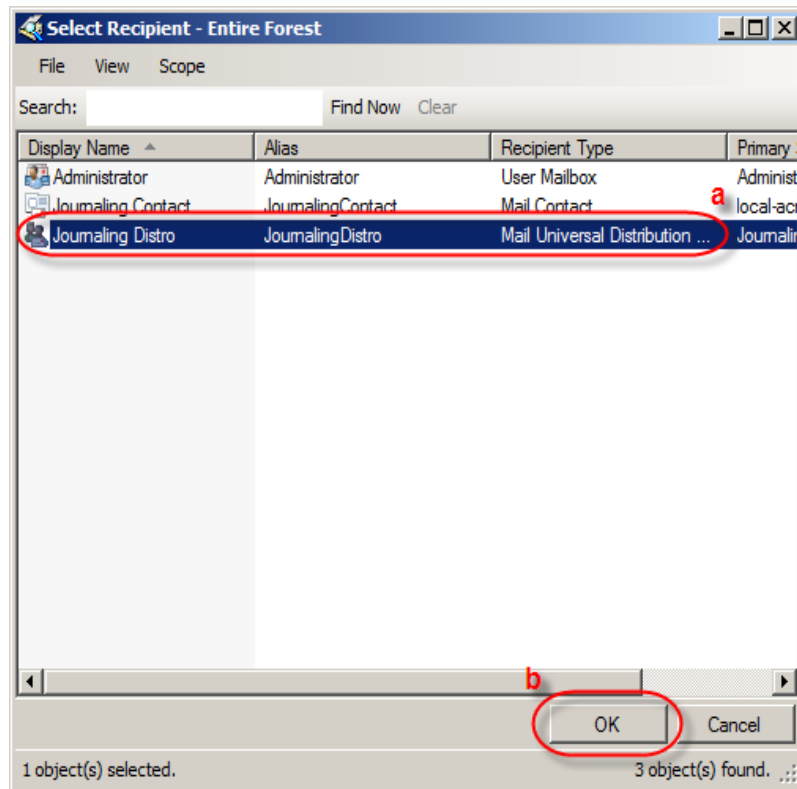
☐ Journal messages for recipient:
Browse...

☒ Enable Rule

To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL).

Help < Back New Cancel

8. Select Journaling Contact from the list and then click OK.
9. Select the Journal messages for recipient check box and then click Browse.
10. Select Journaling Distro from the list (a) and click OK (b).



- Click OK to complete configuration of journal rules for select users in your organization.

Configuring Exchange-Server Journal Polling from the Juniper ATP Appliance CM Web UI

1. From the Juniper ATP Appliance Central Manager Config> System Profiles> Email Collector, 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.

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
GSS Settings
Web Collectors
Email Collectors
Secondary Cores
Golden Image VMs
Licensing
Backup/Restore
Test Malware Detection

Capture Method:
☒ BCC
☐ JATP MTA Receiver
☐ Collect from Juniper Cloud

Email Server:

Protocol:
☒ AUTO
☐ IMAP
☐ POP3
☐ POP3L

SSL:
☒ Enabled
☐ Disabled

Recipient Email Address:

Password:

Domain:

Fetch Interval (min):

Keep Mail on Server:
☐ Keep
☐ Delete

Enabled:
☐ Enabled
☐ Disabled

Cancel

Current Email Collectors

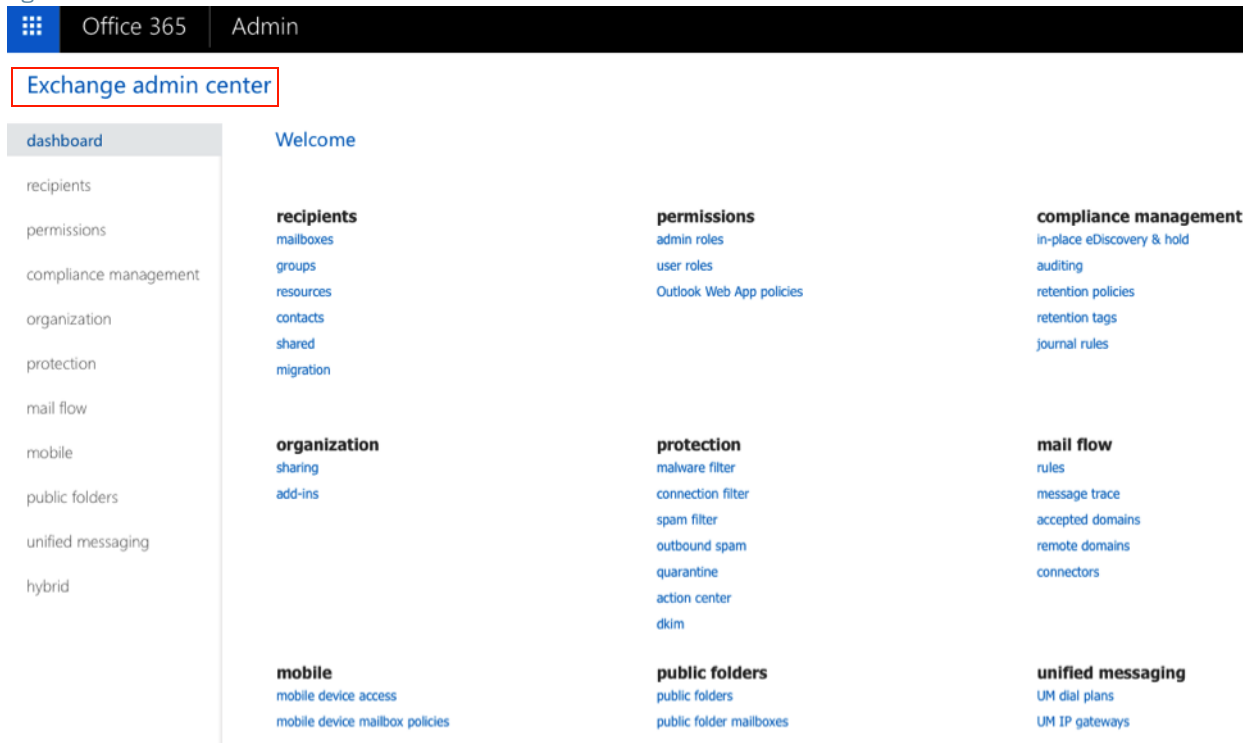
Capture Method	Details	Enabled	Actions
JATP MTA Receiver	MTA Receiver IP: 10.2.118.35 Recipient Email: journal@67.91.204.16 Receive from my Email Servers only: Yes	Yes	Delete Edit
BCC	Email Server: imap.zoho.com Recipient Email Address: email_user2 Protocol: IMAP SSL: Enabled Keep Mail on Server: Delete 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 Poll Interval (min): 5	No	Delete Edit
BCC	Email Server: 192.168.1.202 Recipient Email Address:	No	Delete Edit

Configuring Office 365 Journaling

To set up Office 365 Journaling for Juniper ATP Appliance email mitigation:

1. Log in to the Microsoft Office 365 Admin Center.
2. From the Office 365 Admin Center, select Admin Centers > Exchange.

Figure 5 Microsoft Office 365 Admin Center



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

Figure 6 Setting a New Journal Rule

new journal rule

Apply this rule...

*Send journal reports to:

Name:

*If the message is sent to or received from...

*Journal the following messages...

Save Cancel

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 7 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

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 8 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 ▾

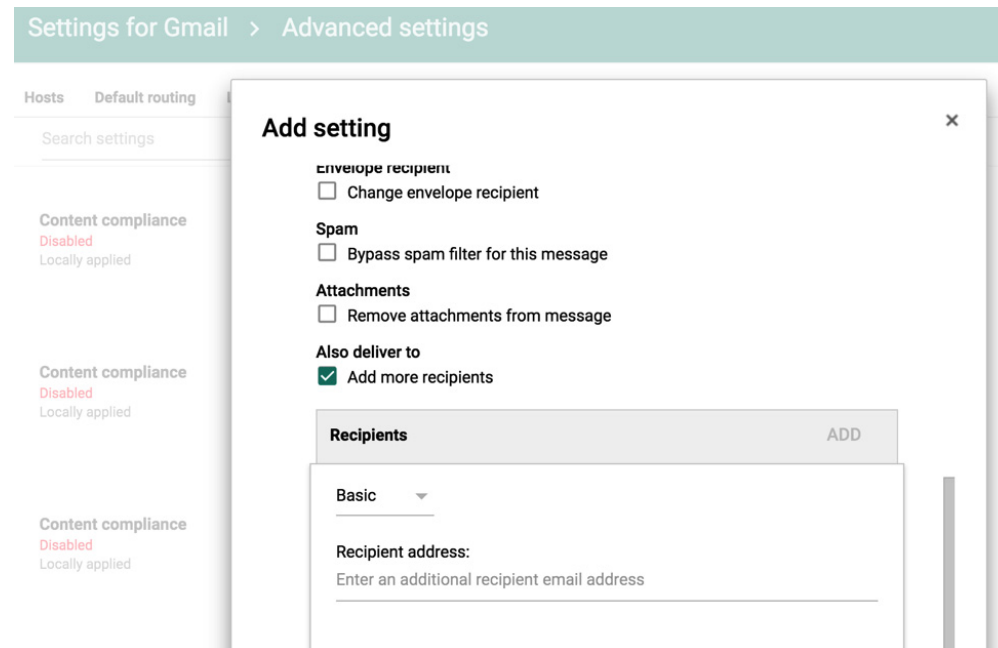
Headers

☐ Add X-Gm-Original-To header

CANCEL SAVE

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

Figure 9 Setting the Juniper ATP Appliance MTA as the Gmail Recipient: JATP_mta@FQDN



- Refer to the Juniper ATP Appliance Operator's Guide for information about configuring email detection mitigations.

Core/CM and All-in-One Email Collector Installation Options

Table 3-1 Email Collector Install Options

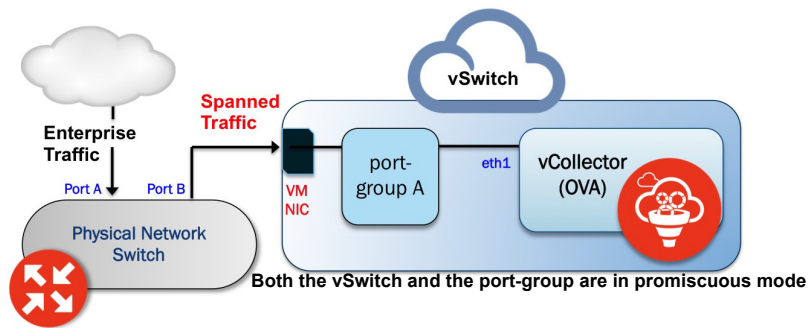
Product Component	Deployment Location(s)	Model Options
Juniper ATP Appliance Core Engine	Locate anywhere in the enterprise network, in a clustered deployment, and/or in remote branch office(s)	Juniper ATP 700 Appliance
Juniper ATP Appliance Virtual or Secondary Core Engine (Windows)	Locate anywhere in the enterprise network and/or in remote branch office(s); Connected logically to the Primary Core.	Juniper ATP Appliance, OVA VM, vCore for AWS
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.	Juniper ATP Appliance Web Collector
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 Mac OS X	Locate anywhere in the enterprise network and/or in remote branch office(s); Connected logically to the Primary Core.	Juniper ATP Appliance on Mac Mini Device
Juniper ATP Appliance All-In-One	Locate anywhere in the enterprise network. (Central Manager Core Collector)	Juniper ATP 700 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

NOTE For hardware installation instructions, refer to the **JATP700 Appliance Hardware Guide**.

Installing the Juniper ATP Appliance Collector Open Virtual Appliance (OVA)

Juniper ATP Appliance's extensible deployment options include a Virtual Collector (vCollector) 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, 5.5 and 6.0. Virtual Collector models supporting 25 Mbps, 100 Mbps, 500 Mbps and a 1.0 Gbps are available.

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).



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.

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	Processorspeed 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 Deployment vSwitch Setup

1. Identify the physical network adapter from which the spanned traffic is received, then create a new VMware Virtual Switch and associate it with the physical network adapter.
2. Click on Virtual Switch Properties. On the Ports tab, select vSwitch and click on the Edit button.
3. Select the Security tab and change Promiscuous Mode to accept, then click OK. Click OK again to exit.
4. Create a new port-group "vtraffic" in the Virtual Switch. This new port-group will be assigned to your vCollector later. See [vSwitch Tip](#) below for information about troubleshooting this setup.

To install the Juniper ATP Appliance OVA to a VM

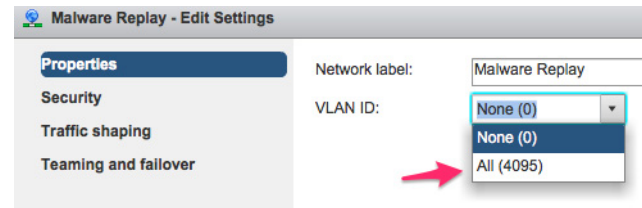
1. Download the Juniper ATP Appliance OVA file from the location specified by your Juniper ATP Appliance sales representative to a desktop system that can access VMware vCenter.
2. Connect to vCenter and click on File>Deploy OVF Template.
3. Browse the Downloads directory and select the OVA file, then 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 Collector is Juniper ATP Appliance Virtual Collector Appliance. If desired, enter a new name for the Virtual Collector.
7. Choose the Data Center on which the vCollector will be deployed, then click Next to view the Host/Cluster page.
8. Choose the host/cluster on which the vCollector will reside, then click Next to view the Storage page.
9. Choose the destination file storage for the vCollector 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 two vCollector interfaces:
 - Management (Administrative): This interface is used to communicate with the Juniper ATP Appliance Central Manager (CM). Assign the destination network to the port-group that has connectivity to the CM Management Network IP Address.
 - Monitoring: This interface is used to inspect and collect network traffic. Assign the destination network to a port-group that is receiving mirrored traffic; this is the port-group "vtraffic" configured in the requirements section above. 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 Virtual Collector; it should be in the same subnet as the management IP address for the Juniper ATP Appliance Central Manager.
 - Netmask: Assign the netmask for the Virtual Collector.
 - Gateway: Assign the gateway for the Virtual Collector.
 - DNS Address 1: Assign the primary DNS address for the Virtual Collector.
 - DNS Address 2: Assign the secondary DNS address for the Virtual Collector.
12. Enter the Search Domain and Hostname for the Virtual Collector.

13. Complete the Juniper ATP Appliance vCollector Settings:
 - New Juniper ATP Appliance CLI Admin Password: this is the password for accessing the Virtual Collector from the CLI.
 - Juniper ATP Appliance Central Manager IP Address: Enter the management network IP Address configured for the Central Manager. This IP Address should be reachable by the Virtual Collector Management IP Address.
 - Juniper ATP Appliance Device Name: Enter a unique device name for the Virtual Collector.
 - Juniper ATP Appliance Device Description: Enter a description for the Virtual Collector.
 - Juniper ATP Appliance Device Key Passphrase: Enter the passphrase for the Virtual Collector; 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.
14. Do not check the Power-On After Deployment option because you must first (next) modify the CPU and Memory requirements (depending on the Virtual Collector model--either 100Mbps, 500Mbps, or 1Gbps. It is important to reserve CPU and memory for any virtual deployment.
15. To configure the number of vCPUs and memory:
 - A. Power off the virtual collector.
 - B. Right click on the virtual collector -> 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.
16. To configure CPU and memory reservation:
 - A. For CPU reservation: Right click on vCollector-> 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 vCollector -> 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.
17. If Hyperthreading is enabled, perform the following selections:
 - A. Right click on the virtual collector -> Edit settings.
 - B. In the Resources tab, select HT Sharing: None for Advanced CPU.
18. Power on the Virtual Collector.

TIP vSwitch Setup Troubleshooting: If your Virtual Collector is not seeing traffic, (1) confirm your environment setup [ESXi installation with OVA installation of a Juniper ATP Appliance vCollector; your vNIC for traffic collection is connected to a tap-aggregation switch]. (2) Verify symptoms [ESXi host-level interface monitoring shows expected tap traffic levels; TCPdump packet capture shows only spanning-

tree traffic and no data; basic system configuration conforms to documentation. Probable Solution: If the switch port preserves VLAN tags (trunking), set the VMkernel adapter to just look at ALL (4095) VLANs and not only at default VLAN (0) as shown in Settings below:

vSwitch VLAN
Troubleshooting
Config in port-groups



TIP Juniper generates an .ovf and a .vmdk file for every release. 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.

Installing and Configuring the AWS vCore AMI

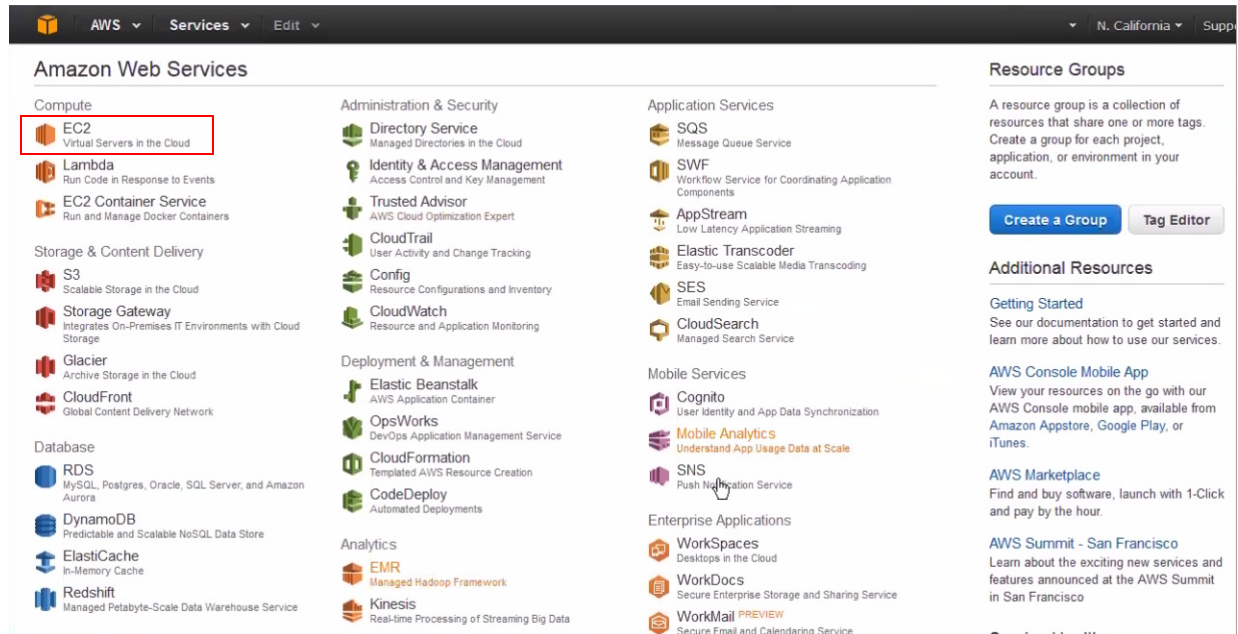
Juniper ATP Appliance vCore for AWS requires both Juniper ATP Appliance and AWS licensed accounts. The installations and configuration process uses both the Amazon AWS Management Console (Part 1) as well as the Juniper ATP Appliance vCore Central Manager Web UI and CLI (Part 2).

NOTE After purchasing the vCore AMI license, share the vCore AMI with your AWS customer account by using the AWS Management Console to configure and launch the vCore AMI. Refer to the Juniper ATP Appliance vCore for AWS Quick Start Guide for more information.

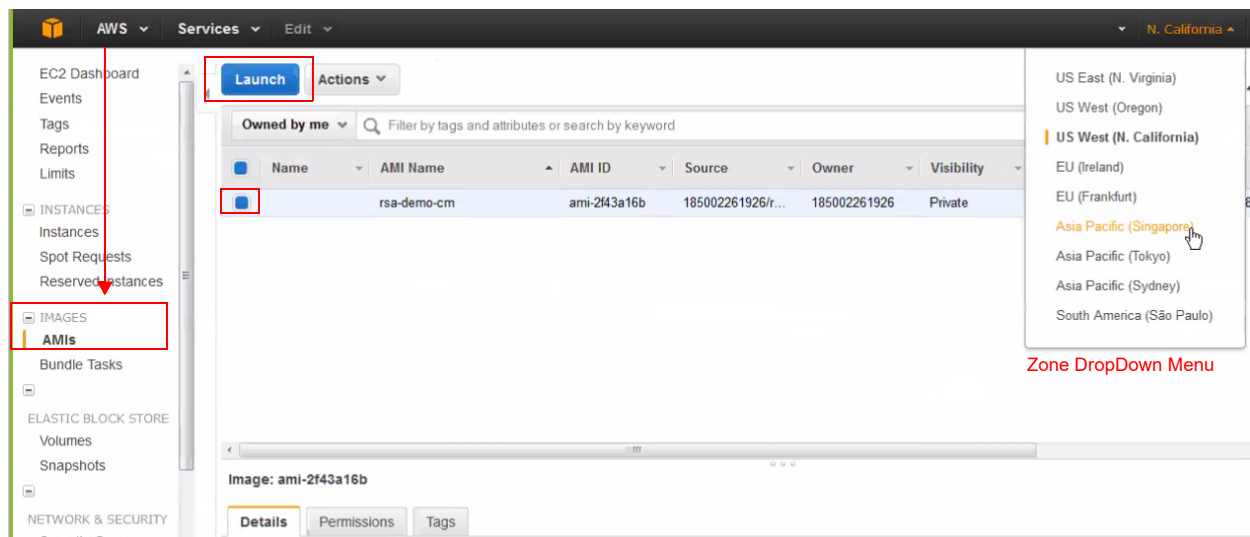
A general AWS AMI configuration workflow is provided below; be sure to refer to the AWS Management Console operations guide for more detailed console usage information.

Part 1- Amazon AWS Management Console vCore AMI Configuration

1. Log into your AWS database account at the Amazon AWS Management Console.
`console.aws.amazon.com`
2. From the AWS Management Console Dashboard, select EC2 services.



3. In EC2 Services, click the IMAGES>AMIs option from the left menu of the AWS Console. Also click on the drop-down menu to change the image ownership type from "Owned by Me" to "Private Images":



4. Select the Juniper ATP Appliance AMI image to be installed by clicking its radio button in the table.
5. From the Zone DropDown menu, select the Zone for which the AMI is to be configured. In our example, the Juniper ATP Appliance "rsa-demo-cm" AMI is selected. (The Juniper ATP Appliance AMI will have been shared with you before you launch the AWS Core.)
6. Click Launch to begin configuration of this Juniper ATP Appliance vCore AMI instance, in EC2, for your enterprise.

Step 2: Choose an Instance Type

	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
<input type="checkbox"/>	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High
<input checked="" type="checkbox"/>	Compute optimized	c4.xlarge	2	3.75	EBS only	Yes	Moderate
<input type="checkbox"/>	Compute optimized	c4.xlarge	4	7.5	EBS only	Yes	High
<input type="checkbox"/>	Compute optimized	c4.2xlarge	8	15	EBS only	Yes	High
<input type="checkbox"/>	Compute optimized	c4.4xlarge	16	30	EBS only	Yes	High
<input type="checkbox"/>	Compute optimized	c4.8xlarge	36	60	EBS only	Yes	10 Gigabit
<input type="checkbox"/>	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate

Cancel Previous Review and Launch Next: Configure Instance Details

7. From the “Choose an Instance Type” page, select an instance type for the AMI. In our example, we selected “c4 large”. Click Next: Configure Instance.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances

Purchasing option ☐ Request Spot Instances

Network Create new VPC

Subnet Create new subnet

Auto-assign Public IP

Placement group

IAM role Create new IAM role

Shutdown behavior

Enable termination protection ☒ Protect against accidental termination

Cancel Previous Review and Launch Next: Add

8. From the “Configure Instance Details” page, select an existing customer-defined Virtual Private Cloud (VPC) from the Network dropdown menu; in our example, we’ve selected rsa-demo-1.

To create a new VPC, click the Create New VPC link and follow the stepped procedure.

9. Define the VPC subnet in the Subnet field; in our example, we used AWS 10.2.0.0/16.

To create a new subnet, click the Create New Subnet link and follow the stepped procedure.

10. Confirm that the subnet is using an Auto-Assigned Public IP, as in the example shown above. This allows the Juniper ATP Appliance vCore to be accessed from the Internet.

11. Click to Enable termination protection to protect against accidental termination.

NOTE Each AMI instance uses a private IP and a public IP. If you are planning on installing one vCore + Central Manager with several Secondary Core, you must have a public IP address assignment. Note that the Secondary Core does not need a public IP because it does not contain a Web UI.

ALSO: Some enterprises connect their AWS VPC to a private network using VPN. In this case, there is no need to assign a public IP to the subnet because internet access can be configured via the VPN.

12. Click Next: Add Storage.

NOTE Click "Encrypted" to encrypt the data volume.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda1	snap-1e873827	512	General Purpose (SSD)	1536 / 3000	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	snap-af7b6e96	1024	General Purpose (SSD)	3072	<input checked="" type="checkbox"/>	Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag](#)

13. Juniper ATP Appliance already provides 1 TeraByte of storage in the Core. Due to the limitations of the AWS storage volume max size, there is no need for further configuration on this page; do not add extra storage to the vCore. Click Next.

Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum) Value (255 characters maximum)

Name test-awscore-doc-1

Create Tag (Up to 10 tags maximum)

Cancel Previous **Review and Launch** **Next: Configure Security**

14. From the "Tag Instance" page, click Create Tag and enter a tag name and description. Click Next: Configure Security to proceed.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name: launch-wizard-3

Description: launch-wizard-3 created 2015-04-23T14:25:25.902-07:00

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0

Add Rule

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel Previous **Review and Launch**

15. A security group is essentially a firewall in AWS. Most customers already have a preexisting firewall, so choose Select an existing security group, or Create a new security group. Do ensure there are rules in the Security Group that allow communication between AWS Core and AWS Secondary Cores.
16. If creating a new security group, enter a name and description in the Security Group Name field and the Description field, respectively.
17. Enter port designation; Juniper ATP Appliance vCore only allows for port 22, 80 and 443. Click Next.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server, allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Security Group ID	Name	Description	Action
sg-85c273e0	default	default VPC security group	Copy to clipboard
sg-31c57454	SSH-HTTPS-ALL	launch-wizard-3 created 2015-04-10T21:33:29.359-07:00	Copy to clipboard

Inbound rules for sg-31c57454

Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0

Buttons: Cancel, Previous, Review and Launch

NOTE You can configure an SSH key although the Juniper ATP Appliance vCore already includes password protection. To add extra protection, add a key pair first, then use Juniper ATP Appliance password for CLI-only login. AWS requires you to set a key pair. You will not be able to use a pem-only login.

18. To configure an SSH Key, select an existing key pair or create a new key pair:

Step 7: Review Instance Launch

Security Group ID: sg-31c57454

All selected security groups inbound rules:

Security Group ID	Type	Protocol	Port Range	Source
sg-31c57454	SSH	TCP	22	0.0.0.0/0
sg-31c57454	HTTP	TCP	80	0.0.0.0/0
sg-31c57454	HTTP	TCP	80	0.0.0.0/0

Instance Details, Storage, Tags

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

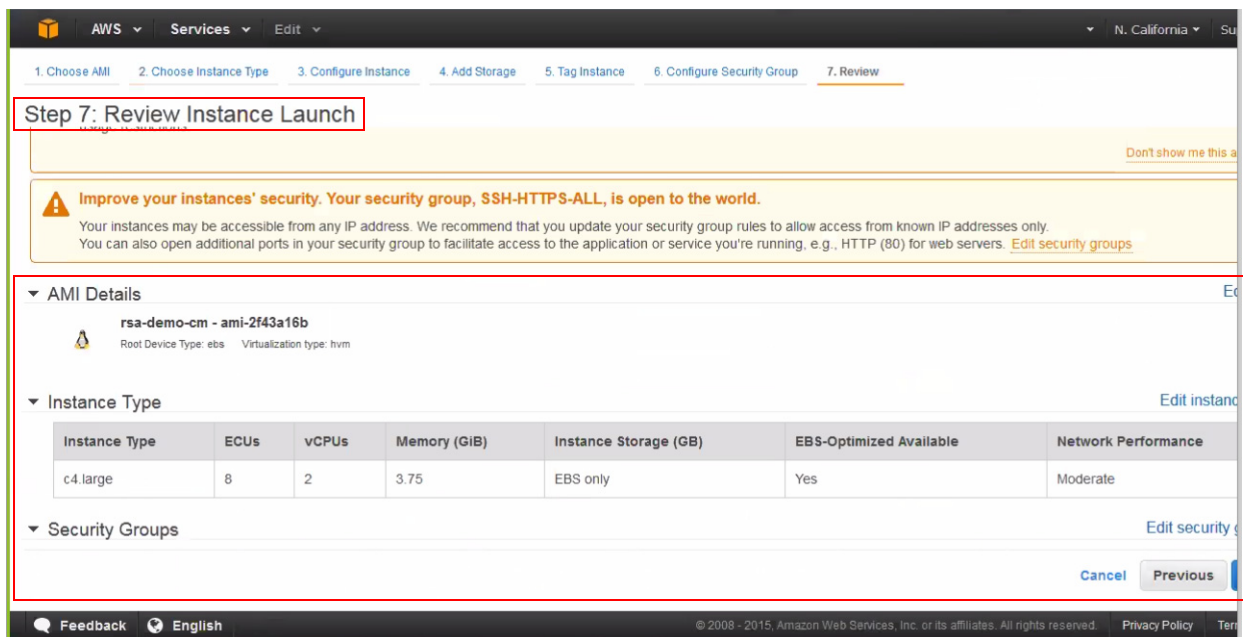
Select a key pair

- rsa-demo-1
- rsa-demo-1
- shelini-1
- test-allen-1
- test-allen-2
- test-core1

Buttons: Cancel, Launch Instances

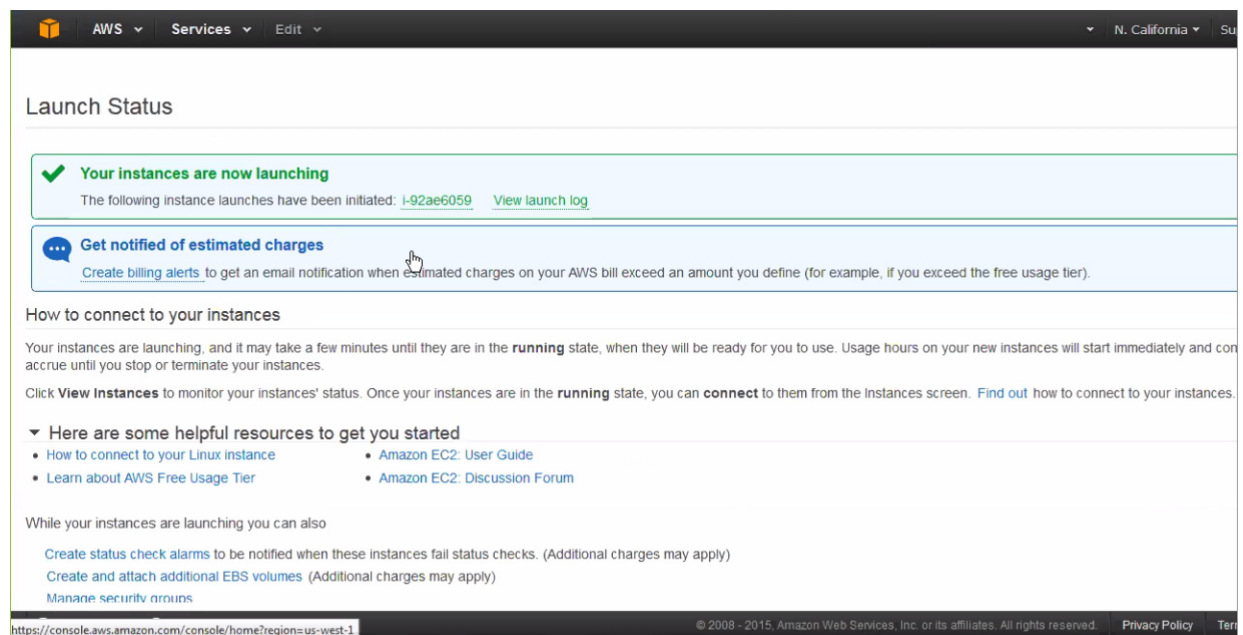
19. If selecting an existing security group, select then choose from the list and click Next.

The “Review Instance Launch” page displays:



20. From the “Review Instance Launch” page, review the Instance Launch details, then either click Edit Instance to make changes, or click Launch to instantiate.

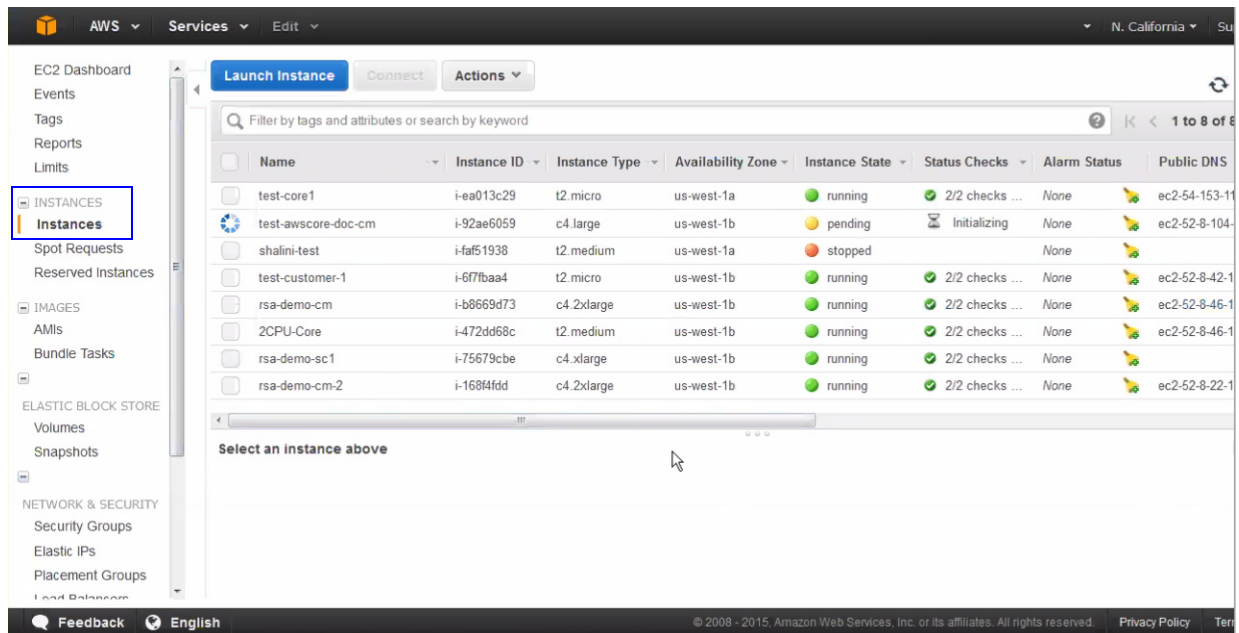
The Launch Status window displays:



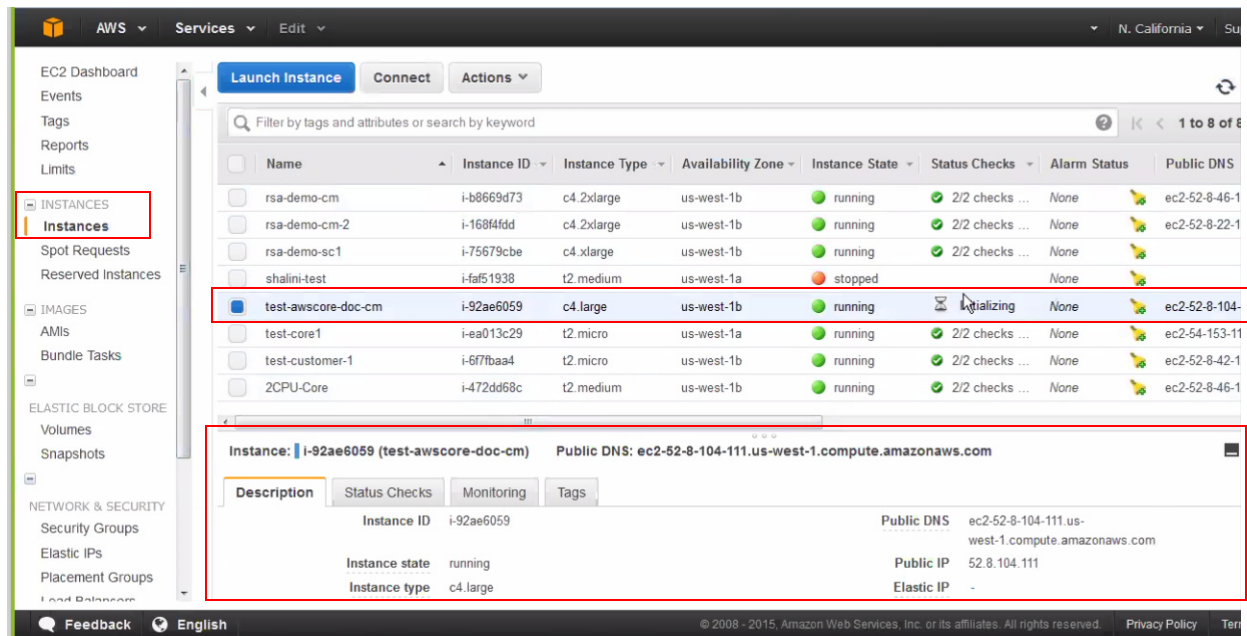
Part 2 - Running the Juniper ATP Appliance vCore AMI Instance

Next, you will initialize the Juniper ATP Appliance vCore AMI Instance from the AWS Management Console, then verify the AMI at the Juniper ATP Appliance Central Manager CLI using the **show ip** command.

1. Open the AWS Management Console Instances page to view the launched AMI Instance status. When a launched Instance finishes initializing, it will display a green icon to indicate “running” status.



2. Select the launched Instance then open the panel at the bottom of the Instances table to review Instance details.
3. Copy the Instance ID and the Instance Type “c4-large2.” for the vCore CLI configuration.



NOTE It is very important to be aware that the private IP address is the DHCP setting, and it will stay static in AWS and should never change during proper operations.

Note also that you cannot change the AMI hostname, although you can change the DNS if necessary.

About DNS: Because the AWS vCore is not located in the enterprise, the reverse DNS on threat targets do not resolve to the expected target hostname. This is rarely confusing when connected via VPN from the corporate network to the VPC. Generally, internal DNS servers are not exposed outside the enterprise, so Juniper ATP Appliance cannot configure the AWS vCore to reach an internal DNS server. If the internal DNS server uses an outward facing IP address and you, as admin, are willing to allow connections to it, this is a reasonable solution. Note that the DNS server that the vCore uses will not have the DNS information of the networks where the Juniper ATP Appliance Traffic Collector is located. This is typical of distributed deployments where the Traffic Collector and the Core/CM are not located in the same enterprise networks.

4. Copy the Public IP address to access the vCore AWS Instance CLI via SSH/Putty:

```

Using username "root".
root@10.2.123.12's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Thu Apr 23 14:35:13 PDT 2015

System load:  0.17          Processes:    282
Usage of /:   15.3% of 901.25GB   Users logged in:  0
Memory usage: 39%              IP address for eth0: 10.2.123.12
Swap usage:   0%

Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have new mail.
Last login: Thu Apr 23 11:21:53 2015 from 10.3.1.210
root@testbed2:~# ssh a

```



```

$ ssh 528.104.111 -PuTTY
help      Display an overview of the CLI syntax
history   Display the current session's command line history
server    Change to the server configuration mode
wizard     Run the configuration wizard

rsa-demo-cml# server
Entering the server configuration mode...
rsa-demo-cml(server)# set uipasswd
Enter the current password of CLI admin:
Error occurred when configuring system service

rsa-demo-cml(server)# set uipasswd
Enter the current password of CLI admin:
Enter the new password of the Central Manager UI account:
Retype the new password of the Central Manager UI account:
Password changed successfully!
rsa-demo-cml(server)# show ip
Private IP Address: 10.2.0.169
Public IP Address: 52.8.104.111

rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server)#
rsa-demo-cml(server) # show ip
Private IP Address: 10.2.0.169
Public IP Address: 52.8.104.111
rsa-demo-cml(server) #
```

6. After launching the AWS Core, the AMI vCore instance will boot up just like a regular appliance, and after the vCore comes up, the next step is to run CLI setup wizard at the vCore CLI just like a regular virtual Core. Refer to the [Juniper ATP Appliance Core/Central Manager Quick Start Guide](#) for instructions on running the wizard to configure a Virtual Core. Also in the Quick Start Guide is information about installing additional Cores, Clustered Cores, Secondary Cores or OVA Cores.

7. To create Secondary Cores for this AWS vCore, return to the AWS Management Console and launch a few more AMI Instances, then login to their CLIs via SSH and point those vCore Central Manager IP Addresses to the primary vCore CM. This process is described in the Juniper ATP Appliance Core/Central Manager Quick Start Guide in the section on Clustered Deployments.

8. For information about installing and configuring Juniper ATP Appliance Traffic Collectors for AWS vCore deployments, refer to Juniper ATP Appliance Traffic Collectors Quick Start Guide.

NOTE Verify that there are no firewall rules blocking the outbound connections to the AWS Core. Be aware, however, that Outbound CnC detection traffic is blocked from leaving the AWS detection VMs.

9. View the AWS configuration from the Juniper ATP Appliance Central Manager Web UI; refer to the section in this guide [Accessing the Juniper ATP Appliance Central Manager Web UI on page 40](#) for information about accessing and navigating the CM Web UI.

On the Central Manager Config>Golden Image VMs page, note that 32-bit images are available for AWS; see figure below for reference.

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 system settings and profiles. The main content area is titled 'Config' and shows the 'Golden Image VMs' section. A form for adding a new VM image is visible, with fields for 'Image Name', 'Description', 'VNC ID', 'Architecture' (set to 32-bit), and 'Disk Size (GB)' (set to 20). Below the form is a table titled 'Current VM Images' with columns for 'Description', 'Enabled', 'Status', and 'Actions'. The table contains one entry: 'GI - Demo', which is not enabled and is in a 'Running' status with VNC ID 1. The actions for this entry are 'Controls', 'Delete', and 'Edit'.

Verifying AWS Configurations

To verify interface configurations, use the following CLI commands (refer to the Juniper ATP Appliance CLI Command Reference for more information):

Table 3-2 CLI Commands

vCore CLI (Mode) & Command	Purpose
JATP (diagnosis) # setupcheck all	Run a check of all system components
JATP (server) # show interface	Verify interface connectivity and status
JATP (server) # show ip <interface>	Verify traffic [example: show ip eth1]
JATP (server) # ping x.x.x.x	Ping connected devices.
JATP (server) # show ip	Display AWS public and private IP addresses.

Table 3-2 CLI Commands

vCore CLI (Mode) & Command	Purpose
JATP (server) # shutdown	Shutdown before moving a devices to a different location, or to perform server room maintenance etc

NOTE: Be sure to refer to the Juniper ATP Appliance CLI Command Reference for more information.

Configuring Juniper ATP Appliance Email Traffic Collection

When powered up, the Juniper ATP Appliance Collector performs its boot process and then displays a CLI login prompt. Use the following procedure to configure the Juniper ATP Appliance Server using the CLI command line and Configuration Wizard.

NOTE FOR OVA DEPLOYMENTS: this configuration process is optional and can be skipped because these settings are addressed during OVA deployment to the VM vSwitch.

TIP Integration requirements for the Email Collector: Microsoft Exchange 2010+

To Configure the Collector Configuration Wizard

1. At the login prompt, enter the default username `admin` and the password `1JATP234`. Review the displayed EULA and press `q` to continue.
2. When prompted to accept the Juniper ATP Appliance End User License Agreement (EULA), enter `yes`. Configuration cannot continue until the EULA is accepted.
3. At the prompt, enter a new CLI administrator password. Weak passwords are not accepted. Note that the CLI admin password is maintained separately from the Juniper ATP Appliance Central Manager Web UI interface.
4. When prompted with the query "Do you want to configure the system using the Configuration Wizard (Yes/No)?", enter `yes`.

5. Next, respond to the Configuration Wizard questions as follows in the Configuration Wizard section below.

Configuration Wizard Prompts	Customer Responses/Actions
Use DHCP to obtain the IP address and DNS server address for the management interface (Yes/No)?	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred. Recommended: Respond with no:
Note: Only if your DHCP response is no, enter the following information when prompted: a. IP address b. Netmask c. Enter a gateway IP address for this management (administrative) interface:	Enter a gateway IP X.X.X.X and quad-tuple netmask using the form 255.255.255.0 (no CIDR format). a. Enter an IP address b. Enter a netmask c. Enter a gateway IP address.
d. Enter primary DNS server IP address. e. Do you have a secondary DNS Server (Yes/No). f. Do you want to enter the search domains? g. Enter the search domain (separate multiple search domains by space):	d. Enter the DNS Server IP address e. If yes, enter the IP address of the secondary DNS server. f. Enter yes if you want DNS lookups to use a specific domain. g. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com
Restart the eth0 interface (Yes/No)?	Enter yes to restart with the new configuration settings applied.
Enter a valid hostname.	Type a unique hostname when prompted; do not include the domain; for example: JuniperATP1
[OPTIONAL] If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed: Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)? Enter IP address for the alternate-exhaust (eth2) interface: Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0) Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example: 10.6.0.1) Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8) Do you have a secondary DNS server for the alternate-exhaust (eth2) interface? Do you want to enter the search domains for the alternate-exhaust (eth2) interface? Note: A complete network interface restart can take more than 60 seconds	Enter yes to configure an alternate eth2 interface. Enter the IP address for the eth2 interface. Enter the eth2 netmask. Enter the gateway IP address. Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface. Enter yes or no to confirm or deny an eth2 secondary DNS server. Enter yes or no to indicate whether you want to enter search domain.

Enter the following server attributes: Central Manager (CM) IP Address:	Enter the CM external IP address, not the loopback, in order to register with and view the Collector in the CM Web UI.
Device Name: (must be unique)	Enter the JuniperATP Collector device name; this identifies the Collector in the Web UI.
Device Description	Enter a device Description
Device Key PassPhrase	Enter the same PassPhrase used to authenticate the Core to the Central Manager.
NOTE: Remember this passphrase and use for all distributed devices!	

NOTE Enter CTRL-C to exit the Configuration Wizard at any time. If you exit without completing the configuration, you will be prompted again whether to run the Wizard. You may also rerun the Wizard at any time with the CLI command **wizard**. Please refer to the CLI Guide for more information.

The Traffic Collector will now automatically “call home” to the Central Manager to announce it is online and active. Wait ~5 minutes and confirm Collector connectivity from the JuniperATP Web UI, as described further below.

When the Configuration Wizard exits to display the CLI, you may use the commands listed in [Verifying Configurations and Traffic from the CLI on page 39](#) to view interface configurations and to whitelist an Email Collector (in distributed systems) if one is already installed and configured. Special characters used in CLI parameters must be enclosed in double quotation marks.

To exit the CLI, type **exit**. Be sure to confirm Collector activity from the JuniperATP Central Manager Web UI (below).

```
JATP (collector) # exit
```

Setting the same Device Key Passphrase on all Juniper ATP Appliance Devices

The same device key must be set on all Juniper ATP Appliance devices in your network, no matter how remote the distributed devices may be. To set a device key passphrase, SSH into the device, login, and use the following CLI commands:

```
JATP (server) # set passphrase <strongPassphraseHash>
JATP (server) # show device key
```

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

Verifying Configurations and Traffic from the CLI

To verify interface configurations, use the following CLI commands. Refer also to the Juniper ATP Appliance CLI Command Reference for more information and to set traffic-filter and x-forwarded-for configurations:

Table 3-3 Configurations and Traffic CLI

CLI Mode & Command	Purpose
JATP (diagnosis) # setupcheck all	Run a check of all system components

Table 3-3 Configurations and Traffic CLI

CLI Mode & Command	Purpose
JATP (server) # show interface	Verify interface connectivity and status
JATP (server) # show ip <interface>	Verify traffic [example: show ip eth1]
JATP (server) # ping x.x.x.x	Ping connected devices.
JATP (diagnosis) # capture-start <IP address> <interface>	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats (not part of the Collector traffic capture engine).
JATP (server) # shutdown	Shutdown before moving a devices to a different location, or to perform server room maintenance etc

NOTE: Be sure to refer to the Juniper ATP Appliance CLI Command Reference for more information. Special characters used in CLI parameters must be enclosed in double quotation marks.

Accessing the Juniper ATP Appliance Central Manager Web UI

To access the Juniper ATP Appliance Central Manager (CM) Web UI, use HTTP/HTTPS and enter the configured Juniper ATP Appliance CM IP address or hostname in a web browser address field, then accept the SSL certificate when prompted. Login is required

To Log in to the Central Manager Web UI

1. In the Juniper ATP Appliance Login window, enter the default username `admin` and the password `juniper`.

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

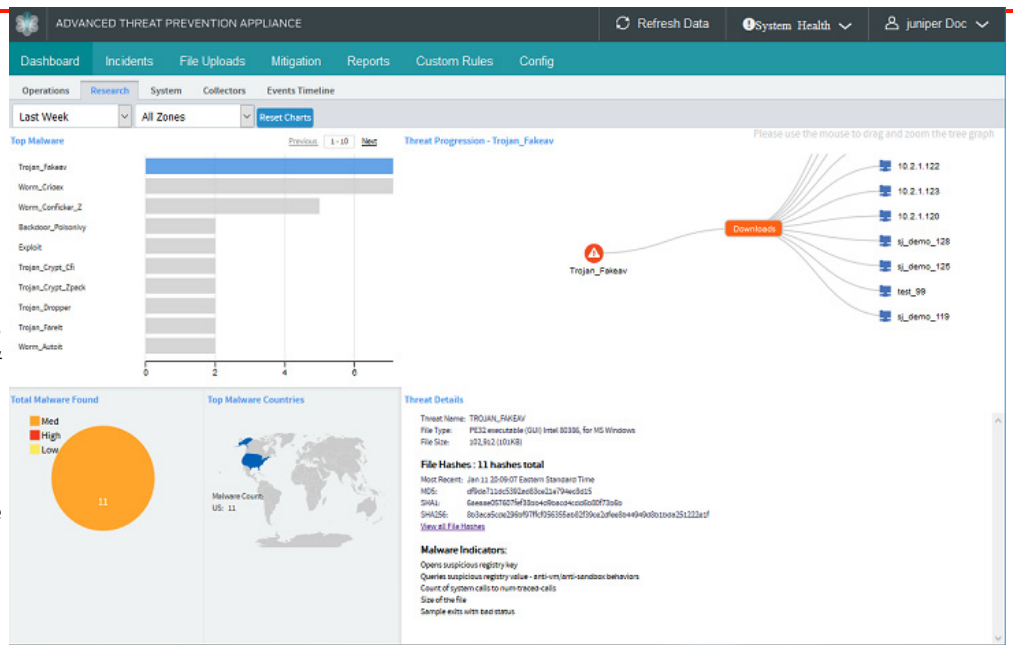
2. When prompted to reset the password, re-enter the password `juniper` as the "old" password, and enter a new password (twice).
3. At login, the Juniper ATP Appliance Central Manager Dashboard is displayed, as shown below. The Dashboard tab includes aggregated malware detection information and provides system status and health information
4. Configuration informations for Email Collectors and MTAs are made from the Configuration tab. Refer to the Juniper ATP Appliance Operator's Guide for more information.

Figure 4 Central Manager Dashboards

Web UI

Navigation Tabs

- **Dashboards**
Review malware summaries, lateral progressions and trends
- **Incidents**
View detected incidents and their behaviors
- **File Uploads**
Submit files for malware analysis
- **Mitigation**
Perform immediate threat verification & mitigation actions
- **Reports**
Configure & view malware activity and audits
- **Custom Rules**
Create and Manage custom security rules
- **Configuration**
Config and modify Juniper ATP Appliance Settings



- The Juniper ATP Appliance CM Dashboard views (Operations | Research | System | Collectors [Web | Email]) provide in-context and aggregated malware detection information as well as system status and health statistics.

The Juniper ATP Appliance CM Dashboard provides in-context and aggregated malware detection information for web and email traffic as well as system status and health information. Additional configurations are made from the Configuration tab. Refer to the Juniper ATP Appliance Operator's Guide or online help for more information.

Use the Config tab to verify that the new Collector is calling the Central Manager (CM) Web UI, and is online and actively inspecting and collecting traffic.

What to Do Next?

- Navigate to the Configuration tab and select System Settings> Licensing from the left panel; upload your license key (obtained from your sales representative).
- Use the Central Manager (CM) Web UI Dashboard and Config pages to confirm traffic monitoring and detection activity. The CM updates security intelligence every 5 minutes, so you may need to wait 5 minutes to see activity at the Web UI.
- Review the Juniper ATP Appliance Product Release Notes for current release information.
- Review the Juniper ATP Appliance Core/Central Manager Quick Start Guide if planning to install additional Cores, Clustered Cores, Secondary Cores or OVA Cores.
- Review the Juniper ATP Appliance vCore for AWS Quick Start Guide if planning to install additional Cores, Clustered Cores, Secondary Cores or OVA Cores.
- Review the Juniper ATP Appliance All-in-One Quick Start Guide for information about All-in-One platform installation and configuration.
- For Email Traffic Collector deployments, refer to the Juniper ATP Appliance Field Guide for information about Email Journaling and Gmail BCC configuration.
- Review the Juniper ATP Appliance Web Traffic Collector Quick Start Guide if planning to install additional or remote Web or Email Traffic Collectors.

- Refer to the Juniper ATP Appliance Mac Mini OS X Engine Quick Start Guide for information about installing a Mac Mini Detection Engine.
- Refer to the Juniper ATP Appliance CLI Command Reference for information about Collector CLI commands.
- Refer to the Juniper ATP Appliance Operator's Guide for information about all products and usage.
- Refer to the Juniper ATP Appliance HTTP API Guide for information about accessing and managing Juniper ATP Appliance advanced threat detection using APIs, including processing data, device and software configuration.
- Refer to the Juniper ATP Appliance CEF Logging Support for SIEM Integration Guide for information about CEF logging.