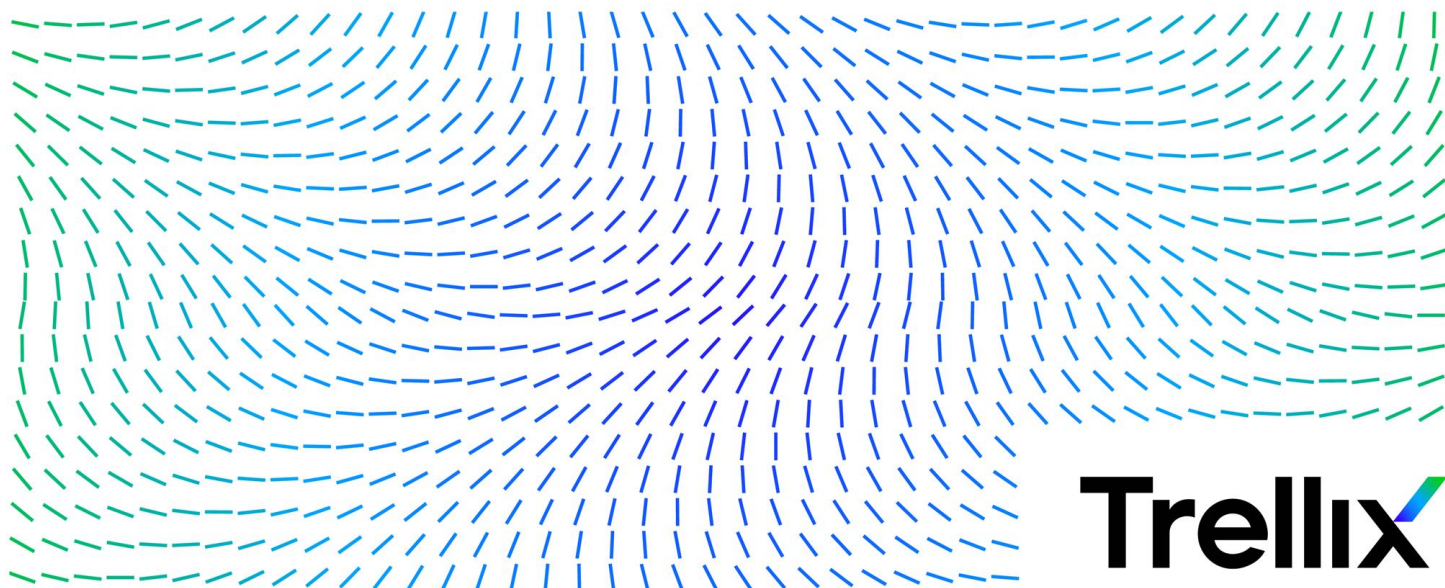


INVESTIGATION ANALYSIS

SYSTEM ADMINISTRATION GUIDE

RELEASE 2.1



Trellix and FireEye are the trademarks or registered trademarks of Musarubra US LLC, Musarubra US LLC, and their affiliates in the US and/or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and/or other countries. Skyhigh Security is the trademark of Skyhigh Security LLC and its affiliates in the US and other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

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

Copyright © 2023 Musarubra US LLC

Investigation Analysis System Administration Guide

Software Release 2.1

Revision 1

Contents

PART I: Overview	10
CHAPTER 1: Getting Started	12
Conventions	13
Software	13
CHAPTER 2: User Interfaces	14
The Web UI	14
Operating Systems and Browser Support for Web UI	14
Screen Resolution Requirements	15
Logging in to the Web UI	15
IA Series Web UI Tabs	15
The Dashboard	16
The Command Line Interface	16
The IPMI	16
CHAPTER 3: Initial Configuration	18
Network Information Requirements	18
Initial Configuration Procedure	19
Configuring Network Settings	20
Logging In	21
PART II: Administration	24
CHAPTER 4: Network Configuration	26
Configuring Eth 0 and Eth 1	26

Configuring the Hostname	27
Configuring the DNS Server	27
Configuring the NTP Server	28
Configuring the DNS Search Domain	29
Configuring the IP Network Parameters	29
Configuring SFP Management Interface for Gen 6 Appliances	30
Configuring the IPMI	31
Testing Connectivity	32
 CHAPTER 5: Time Management	34
Configuring the NTP Server	34
 CHAPTER 6: SNMP Data	36
Prerequisites	36
Configuring SNMP Data	36
SNMP Traps	39
Retrieving SNMP Data Using MIBs	40
Accessing MIBs	41
Requesting SNMP Information	42
 CHAPTER 7: Upgrading Your Investigation Analysis Appliance	44
Upgrading Your Investigation Analysis Appliance Using the Web UI	44
Upgrading Your Investigation Analysis Appliance Using the API	45
Upgrading Your Investigation Analysis Appliance Using the CLI	45
Synchronizing IA and PX	46
 CHAPTER 8: Log Monitoring	48
Accessing Logs	48
Streaming Logs and Viewing Historic Logs	49
 CHAPTER 9: Configuring Syslog Server to Enable TLS Encryption	52
Syslog Certificates	52

Uploading Client Certificate to Syslog Collection	53
Enabling TLS Encryption for Syslog	55
CHAPTER 10: Process Management	58
CHAPTER 11: Clearing Client Data	60
Prerequisites	60
Cleaning Your RAID Device	60
Rebuilding Storage	62
CHAPTER 12: Disk-Mirroring	64
CHAPTER 13: Configuring Session-Reconstruction Parameters	66
PART III: Configuration	68
CHAPTER 14: Clusters	70
IA Clusters	70
Single-Box Cluster	71
Multi-Box Cluster	71
IA Cluster Deployment Considerations	72
IA Cluster Terminology	73
Deploying a New IA Cluster	73
Create Master Node Configuration	74
Create Data Node Configuration	77
Disable Unnecessary Services on Data Node	79
Start the Master Node	79
Start the Data Node	79
Verify the Cluster State using the CLI	80
Verify the Cluster State using the API	80
Expanding an Existing IA Cluster Deployment	81
Adding Nodes to a Single-Node IA Cluster	81

Adding Nodes to a Multinode IA Cluster	81
Recovering Elasticsearch	82
Cluster Maintenance	82
CHAPTER 15: Distributed Search	84
Converting an IA Series Appliance to a Director Node	85
Converting an IA Series Appliance into a Data Node	86
Adding Data Nodes to the Director Node	87
Adding a Data Node to the Director Node	88
Removing a Data Node from the Director Node	89
CHAPTER 16: Multidirector Configuration	90
Configuring Network Connections	91
Preparing an IA Data Node for Multi-Director Configuration	92
Configuring the Single-Box Cluster as a Multi-Box Cluster	93
Configuring the IA Director Node	93
Connecting the IA Director to the IA Cluster	94
Adding a Default Route for Multibox Clusters	95
PART IV: Integrating with IA	98
CHAPTER 17: Configuring PX Metadata through Web UI	100
Viewing the PX Metadata Sources	100
Adding the PX Appliance	101
Generating and Transferring SSH keys	101
Retransferring ACM Keys	102
Configuring Metadata Synchronization	103
Updating the PX Metadata Selection	103
Resynchronizing Network Configuration	103
Deleting the PX Appliance	104

CHAPTER 18: Synching PX and IA Metadata through CLI	106
Prerequisites	106
Configure the IA	106
 CHAPTER 19: Integrating Threat Intelligence	110
Integrating with Mandiant Threat Intelligence	110
Prerequisite	110
Connection Modes	111
Configuring the IA to Mandiant Threat Intelligence Connection	111
Integrating Custom Intel Feeds	113
Prerequisite	113
Configuring a Custom Intel Feed	113
 CHAPTER 20: Integrating with IA for Alerts	116
Configuring Alert Aggregation in the CLI	116
Alert Poll Service	117
Step 1: Configure the Trellix Appliance	117
Step 2: Configure the IA Appliance	117
Alert HTTP Listener	118
Step 1: Configure the IA Appliance	119
Step 2: Configure the Trellix Appliance	119
Step 3: Send a Test Alert	120
 CHAPTER 21: Integrating with the AX Series Appliance for Malware Analysis	122
 CHAPTER 22: Integrating with the Endpoint Security Server for Hostname Data	124
Integrating the Endpoint Security Server and IA Series Appliance	124
Verifying the Endpoint Security Server and IA Integration	125
Changing IA and Endpoint Security Server Configuration Settings After Integration	126
Retrieving Metadata from a Paired Endpoint Security Server	128

PART V: User Management	130
CHAPTER 23: Authentication in the CLI	132
CHAPTER 24: Configuring SAML Authentication	134
CHAPTER 25: Managing User Accounts	138
Roles	138
Adding a User in the CLI	139
Deleting a User in the CLI	139
Editing a User in the CLI	140
Resetting the Passwords for npadmin, npscp, and IPMI Admin Accounts	140
CHAPTER 26: Controlling User Access Using VLAN/QinQ RBAC	142
RBAC Configuration Menu	142
Mapping VLAN/QinQ Ranges to AD Groups	143
Excluding AD Groups from VLAN/QinQ Access Restrictions	144
Appendices	146
APPENDIX 26: Common Access Card (CAC) for Certificate Authentication	147
About CAC for Certificate Authentication	147
Task List for Configuring the Appliance to Use CAC for Certificate Authentication	148
Configuring Custom Web Server Certificates	149
Creating a Custom Self-Signed Web Server Certificate Request	149
Uploading a Custom Self-Signed Web Server Certificate	150
Uploading a Custom CA-signed Web Server Certificate	151
Enabling or Disabling CAC/PIV for Certificate Authentication	152
Enabling or Disabling CAC/PIV for Certificate Authentication Using the Configuration Menu	152

Checking for Revoked Certificates	153
Adding a Local CRL File Using the Configuration Menu	154
Configuring Local CRL File Updates Using the Configuration Menu	156
Adding the OCSP URL Using the Configuration Menu	157
Deleting a CRL File Using the Configuration Menu	158
Refreshing a CRL File Using the Configuration Menu	159
Configuring the User Attributes for Certificate Authentication	160
Configuring the User Attributes for Certificate Authentication Using the Configuration Menu	161
Configuring LDAP for Authorization	163
Selecting the Authorization Type Using the Configuration Menu	164
Configuring an Active Directory Server Using the Configuration Menu	165
Configuring User Mapping Groups Using the Configuration Menu	166
Logging in to the Web UI with Certificate Authentication	168
Index	170
Technical Support	173
Documentation	174

PART I: Overview

This part covers the following topics:

- [Getting Started](#)
- [Initial Configuration](#)
- [User Interfaces](#)

CHAPTER 1: Getting Started

IA is a security analytics platform that allows for centralized search across all connected PX appliances. Analysts look for Layer 7 information across an enterprise. In addition, IA allows for PCAP retrieval from selected flows that were recorded on any connected PX. Analysts can create customized dashboards in multiple configurations to display useful information.

Using IA you can:

- View and share network metadata and activity through easy-to-create custom dashboards.
- Retrieve fast answers with centralized application-level wildcard queries and investigation across packet capture nodes.
- Search indexed metadata from protocols such as HTTP, DNS, SMTP, POP3, IMAP, SSL, TLS, FTP, SSH, MODBUS, MQTT, and RFB.
- Archive and share PCAP files with other analysts during an investigation through integrated case management.

The IA is designed for use by network operations and security personnel with an intermediate knowledge of network protocols.

This *IA System Administration Guide* provides an overview of the Trellix IA series appliance and describes how to use both the Web user interface (Web UI) and the command-line interface (CLI) to configure and manage the appliance's network administration. It is intended for system administrators responsible for deploying, operating, and maintaining the appliance.

Conventions

The following conventions are used in this guide:

Code

Code or shell examples look like this:

`This is a code sample.`

Notes



Items of special note are identified with this symbol.



Items of special important note are identified with this symbol.

Software

OS

The IA software is built on CentOS 7.4 and uses many open source packages.

User Interface

IA provides a user interface implemented as a single-page application (SPA) and offers command-line access for system setup.

CHAPTER 2: User Interfaces

There are three user interfaces available on the appliance:

- Web UI — A Web-based UI used to configure and manage the appliance.
- CLI — A command-line interface used to configure and manage the appliance.
- IPMI Interface — The IPMI Interface allows you to access the appliance and perform recovery activities if it becomes unresponsive.

The Web UI

The appliance Web UI provides a secure HTTPS connection for configuring the appliance. The Web UI functions you have access to depend on the privileges granted by your role.

You access the Web UI by entering the management port's IP address or hostname into a Web browser using HTTPS. The IP address and hostname are set during the initial configuration of the appliance. The hostname must be resolved by a DNS server if you use it to access the Web UI.

HTTP Strict-Transport-Security (HSTS) is also enforced on the IA Web UI. The appliance can now send a 'Strict-Transport-Security' header to a browser. On receiving the header, your browser will connect to the HTTPS site without unencrypted traffic.

Operating Systems and Browser Support for Web UI

Use a recent version of one the following browsers on the system from which you will access the Web UI:

- Internet Explorer
- Microsoft Edge
- Firefox Google

- Chrome
- Safari

Screen Resolution Requirements

The Web UI supports the following screen resolution:

- 1170 x 800 pixels

The minimum width must be 1170 pixels.

Logging in to the Web UI



The user name for the default administrator is `npadmin`.

To log in to the Web UI:

1. Open a Web browser and enter `https://appliance` in the address line, where *appliance* is the IP address or hostname of the appliance. For example, if the configured IP address of the appliance is 10.1.0.1, enter `https://10.1.0.1`. The IP address is configured during the initial start up. See [Initial Configuration](#) on page 18.
2. Click **Proceed** to continue past a warning that appears the first time that you access the IA Web UI.
3. On the login page, enter the user name. The default user name is **npadmin**. Enter the password that was set in the initial configuration.

IA Series Web UI Tabs

This section describes the IA Series Web UI tabs.

- **Dashboard**—Shows a high-level view of the network metadata gathered by the IA Series appliance. Within many panels on the Dashboard, you can click links and buttons to drill down to critical threat information affecting your network. Dashboards are customizable to meet the needs of each analyst.
- **Alerts**—Provides expandable levels of detailed information about the hosts that are infected in the network. Alerts are organized based on severity. The IA Series ingests alerts from other Trellix products, including NX, EX, HX, and PX.
- **Cases**—Allows you to archive and share PCAP files with other analysts during an investigation through integrated case management.

- Malware Analysis—View the results after doing a session analysis on the AX Series platform.
- Appliance Health—Provides appliance and system health information.
- Manage—Provides managed lists, scheduled queries, and import or export dashboards.

The Dashboard

The IA appliance provides customizable views called dashboards that allow analysts to tailor how the information is presented. For example, one analyst may want see a display of email and DNS metadata. Another analyst may be interested in viewing HTTP metadata and trends. Each user can create a customized dashboard.

For details about the Dashboard, see the *Investigation Analysis User Guide*.

The Command Line Interface

The appliance includes a standard command-line interface (CLI) that can be used to configure, manage, and monitor the appliance.

To log into the CLI using a terminal window or SSH client:

1. Using the SSH protocol, log in to the appliance using the management interface's IP address or hostname.

```
$ ssh username@ipAddress | hostName
```

2. When prompted, enter your password.

```
Password: password
```

The hostname > prompt is displayed after you are logged in.

The IPMI

The IPMI allows you to perform the following tasks remotely from a Web browser:

- Cycle the power on your appliance when it is unresponsive.
- Reset the server.
- Access the serial console when the management interface is unavailable or unresponsive.

The IPMI interfaces uses a network connection to the IPMI port of the appliance and is accessed through a secure Web browser session.

The IPMI interface is disabled by default. You must set the IPMI settings during the initial configuration. See [Initial Configuration](#) on page 18.

CHAPTER 3: Initial Configuration

This chapter contains information and instructions for configuring basic network settings for your IA appliance using the CLI.



Trellix highly recommends using the CLI to modify your IA appliance configuration settings. Trellix does not provide technical support for configuration changes made using the shell.

Network Information Requirements

The table below provides the network information requirements.

Network Item	Information Needed
IA Appliance	- Cluster name - name for all of the appliances in the same location. - Hostname - unique name for each appliance. - Elasticsearch does not allow index names with uppercase characters. Cluster names, which are used to create index names, and hostnames must be lowercase when entered in KLISH. - IP address - Subnet mask - Default gateway address
Domain Name Service (DNS)	IP address of one or more DNS Servers

Network Item	Information Needed
Network Time Protocol (NTP) Service (Optional)	IP address of one or more NTP servers
IPMI (Optional)	If you want to access the appliance remotely using the IPMI: • IPMI IP address • IPMI subnet mask • IPMI gateway address

Initial Configuration Procedure

After your Investigation Analysis appliance has been physically added to your network, you must configure the appliance settings during the first boot. For initial configuration, you need a USB keyboard and a monitor with a VGA connection to the appliance.

1. Connect the USB keyboard and monitor to the appliance.
2. Power up the appliance.
3. Press **Enter** to review the EULA.
4. Review the EULA and type **q** when you are finished. Accept the EULA:
Do you accept the FireEye End User License Agreement?: **accept**
5. Press **Enter**.
6. Enter the hostname. The hostname must be different from the Cluster name, but will also be used as the Cluster node name. For example:
Hostname: **cinnamon**
 Elasticsearch does not allow index names with uppercase characters. Cluster names, which are used to create index names, and hostnames must be lowercase when entered in KLISH.
7. If the IA is a Data Node within a multi-box cluster:
Enter **y**.
If the IA is a standalone appliance or a Master-Data Node within a multi-box cluster:
Enter **n**.

8. Enter the Cluster name. This must be different from the hostname. For example:
Cluster name: **cinnamon-cluster**
9. Press **Enter**.
10. You must change your npadmin, npscp, and IPMI passwords.

The password must meet the following criteria:

- 8 characters minimum
- Contain at least 1 character from each of the following categories:
 -  • Uppercase alphabet (A-Z)
 - Lowercase alphabet (a-z)
 - Numbers (0-9)
 - Symbols (!,?, @, etc.)

11. Press any key to continue after you update all three passwords.
12. To customize your system, enter **y**. Continue below with Configuring Network Settings.

Configuring Network Settings

Reference the steps below to complete the initial configuration. If you press enter without providing a new value in any of the following steps, a default value shown inside brackets is used. IP addressed provided must be in valid dotted quad notation. DNS and NTP server addresses must be separated with spaces.

1. Enter the IP address type.
If the IP address is a static address, enter **S**.
If the IP address is a DHCP address, enter **D**.
Press **Enter**.
2. Enter the routable IP address for the appliance. Press **Enter**.
3. Enter the netmask address. Press **Enter**.
4. Press **Enter** when prompted Routable IPv6 Address? []:.
5. Press **Enter** when prompted Prefix Length? []:.
6. Enter the IPv4 address gateway. Press **Enter**.
7. Enter the DNS address. Press **Enter**.

8. Enter the search domain(s) if you will specify non-fully qualified NTP servers in the following step.
If you will not provide an NTP server in the following step, press **Enter** when prompted `Search Domain(s) [ ]:`.
9. Enter a local NTP server, if available. Otherwise, press **Enter** to accept the default option.
10. Enter the IPMI IP address (Optional) or press **Enter** to accept the default option.
11. Enter the IPMI Netmask (Optional) or press **Enter** to accept the default option.
12. Enter the IPMI Gateway Address (Optional) or press **Enter** to accept the default option.
13. To enable the Ether 1 interface, enter **Y**. The Ether 1 interface is used for internal communication between multi-box IA clusters and single-box clusters in multi-director configurations.
14. Your current settings are displayed. Enter **Y** to save your configuration.
15. You see the following prompt:
`Do you want to rebuild storage? [y/n]:`
It is not required to rebuild storage. Capture data on storage disk drives will be erased if you enter **y**.
Enter **n**. Press **Enter**.

The Investigation Analysis restarts.

Logging In

1. Log in with default admin username and the password you selected in the Initial Configuration Procedure.
`hostname login: npadmin`
`password: <password>`

Do not be alarmed if you see the following message after logging in to the IA appliance:

```
SYSTEM CRITICAL - One or more processes (ia-eve-route acm
caseengine flowsummaryservice scheduledsearchservice
 userprofiles-service) not running
```

The services take some time to come up. `ia-eve-route` will not come up until a metadata source is configured. To confirm that services are running, wait a few minutes and then use the `show status` command to show the same output.

2. Enter privileged mode:
`npadmin@hostname> enable`
3. Enter the npadmin password.
4. Enter config mode:
`configure system`

You can now continue to set up the users, PX appliance communication, and other configuration settings for the IA appliance.

PART II: Administration

This part covers the following topics:

- Network Configuration
- Configuring Custom Web Server Certificates
- Time Management
- Configuring SNMP Data
- IA Upgrade Procedure
- Log Monitoring
- Process Management

CHAPTER 4: Network Configuration

The network settings, including IP address, subnet mask, and default gateway, and the Domain Name Service (DNS) server addresses, are defined manually.

There are two management Ethernet interfaces on the IA: Eth0 and Eth1. Eth0 is configured for management, which allows a user to SSH to the device and use a browser to interact with the IA. Eth1 is used for internal communications between the IA and PX. To change network settings, use the CLI.



Trellix highly recommends using the CLI to modify your IA appliance configuration settings. Trellix does not provide technical support for configuration changes made using the shell.

To manually configure the management interface, you must use the Eth1 interface.

Configuring Eth 0 and Eth 1

To configure Eth 0 and Eth 1:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:

```
$ ssh npadmin@10.1.0.1
```


or

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:

```
npadmin@ia# configure system
```

5. Enter the network settings:
`hostname # network`
6. To set the Eth 0, type 8. When prompted, enter the address for eth0.
7. To set the Eth 1, type 9. When prompted, enter the address for eth 1.
8. Type q to save your settings and exit.
9. Type y or n to confirm your changes.
10. Restart networking by typing `restart networking`.

Configuring the Hostname

To configure the hostname:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:
`$ ssh npadmin@10.1.0.1`
or
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:
`npadmin@ia# configure system`
5. Enter the network settings:
`hostname # network`
6. To set the hostname, type 1. At the prompt, enter the hostname and press enter.
7. Type q to save your settings and exit.
8. Type y or n to confirm your changes.
9. Restart networking by typing `restart networking`.

Configuring the DNS Server

To configure the DNS server:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:
`$ ssh npadmin@10.1.0.1`

- or
- ```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  
npadmin@ia> enable
  3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
  4. Enter configuration mode:  
npadmin@ia# configure system
  5. Enter the network settings:  
hostname # network
  6. To set DNS name servers, type 2. When prompted, enter the space-separated list of DNS server addresses and press **enter**.
  7. Type q to save your settings and exit.
  8. Type y or n to confirm your changes.
  9. Restart networking by typing `restart networking`.

## Configuring the NTP Server

### To configure the NTP server:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter the network settings:  
hostname # network
6. To set NTP servers, type 3. When prompted, enter the space-separated list of NTP server addresses and press **enter**.
7. Type q to save your settings and exit.

8. Type y or n to confirm your changes.
9. Restart networking by typing `restart networking`.

## Configuring the DNS Search Domain

To configure the DNS search domains:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter the network settings:  
`hostname # network`
6. To set DNS search domains, type 4. When prompted, enter the space-separated list of DNS search domains and press **enter**.
7. Type q to save your settings and exit.
8. Type y or n to confirm your changes.
9. Restart networking by typing `restart networking`.

## Configuring the IP Network Parameters

To configure the IP network parameters:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`

3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter the network settings:  
`hostname # network`
6. To set IP network parameters, type 5. When prompted, enter the address, netmask, and gateway of the IA.  
  
IPv6 is supported.
7. Type `q` to save your settings and exit.
8. Type `y` or `n` to confirm your changes.
9. Restart networking by typing `restart networking`.

## Configuring SFP Management Interface for Gen 6 Appliances

**Prerequisite:** Disconnect the cable from the 10G-T port and connect it to the SFP management port.

**To configure the SFP management interface:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter the network settings:  
`hostname # network`  
  
1: Node name = 2600-1  
2: DNS Server(s) = 10.128.11.100  
3: NTP Server(s) = 0.pool.ntp.org  
4: Search Domains(s) =  
5: IPv4 Default GW = 10.128.58.193

```

6: IPv6 Default GW =
7: ETH0 Address Configuration
8: ETH1 Address Configuration
9: IPMI Configuration
10: Change interface

```

```

Q: Save changes and exit
C: Cancel changes and exit

```

Select which option you would like to change using the index number:

6. To change the network interface, type 10 and press **Enter**.

```

Available interfaces are:
Currently selected interface- 15FF : 10G-T

```

```

1) 15FF : 10G-T
2) 104E : SFP

```

By default, 10G-T is selected .

7. Select 2 to change the interface to SFP.
8. Type q to save your settings and exit.
9. Type y or n to confirm your changes.

The system restarts after the interface is changed.

## Configuring the IPMI

IPMI is used as a remote troubleshooting interface and allows you to reboot or reimage the unit if it becomes unresponsive. You can set an IP address for this interface during the initial network settings. See [Initial Configuration](#) on page 18. The IPMI configuration is *optional*.

### To configure the IPMI:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

or

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.  

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:  

```
npadmin@ia# configure system
```

5. Enter the network settings:  
`hostname # network`
6. To set the IPMI, type 9. When prompted, enter the IPMI IP address, netmask, and gateway.
7. Type `q` to save your settings and exit.
8. Type `y` or `n` to confirm your changes.
9. Restart networking by typing `restart networking`.

## Testing Connectivity

### To test connectivity:

1. Log in to the IA as `npadmin` using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the `npadmin` password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Test your connectivity and name resolution by pinging a machine with a fully qualified hostname. Use `ping` from the CLI, for example `ping www.google.com`.
6. Type `exit` to return up one level to the CLI.  
Example:  
`ia(config)# ping FireEye.com`



## CHAPTER 5: Time Management

You can set the appliance date and time manually and then use one or more Network Time Protocol (NTP) servers that synchronize the time automatically. You can also specify a secondary NTP server if the primary NTP server is unavailable.

### Configuring the NTP Server

To configure the NTP server:

1. Log into the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Enter configuration mode:  
`hostname # configure system`
5. Enter the network settings:  
`hostname # network`
6. To set NTP servers, type 3. When prompted, enter the space-separated list of NTP server addresses and press **enter**.
7. Type `q` to save your settings and exit.
8. Type `y` or `n` to confirm your changes.
9. Restart networking by typing `restart networking`.



## CHAPTER 6: SNMP Data

Trellix appliances send Simple Network Management Protocol (SNMP) data to communicate abnormal conditions to SNMP managers, administrative computers that monitor and control SNMP data across a network. The IA Series appliance supports both SNMPv2 and SNMPv3 with Enterprise-Specific MIB and trap support. SNMPv3 provides greater data security over SNMPv2 because it adds user authentication and payload encryption to ensure only authorized users can perform read and write operations. SNMPv3 also allows you to create multiple user accounts with assigned SNMP data access rights.



SNMPv3 support is available in IA 1.4.0 and later. Trellix recommends enabling SNMPv3 to send SNMP data.

IA SNMP data includes the following:

- Information that is retrieved (polled) by the SNMP manager. This information is sent in response to requests the SNMP manager sends to the IA appliance.
- Events, known as traps, that are sent (pushed) by the IA appliance to the SNMP manager. Traps typically report alarm conditions such as a disk failure or excessive temperature. They are unsolicited; that is, they are not sent in response to requests from the SNMP manager.

## Prerequisites

- Admin access

## Configuring SNMP Data

To configure SNMPv3 data:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`

or

```
$ ssh npadmin@exampleFQDN
```

2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter the SNMP menu:  
npadmin@hostname(config) # snmp

You will see the following:

- 1: SNMP enabled = False
- 2: SNMP community string = public
- 3: SNMPv3 users =
- 4: SNMP system contact =
- 5: SNMP system location =
- 6: SNMP system name =
- 7: SNMP traps enabled = False
- 8: SNMP trap target(s) =
- 9: SNMP trap string =
- 10: Set SNMP traps

6. Select 3 to enable SNMPv3:

You will see the following:

- a: Add  
d: Delete  
e: Edit  
Press ENTER to go back to the main menu  
using the index letter:

7. Select a to add a user:

Username:



Username length must be greater than 4 characters and less than 32.

8. Enable write access:

Enable write access [y/n]:



User are granted read access by default therefore, any user with write access also has read access.

9. Enter and confirm a user password:



Passwords must be not contain any numeric or special characters.

You will see the following:

```
*** Your passphrase will NOT echo on screen! ***
```

```
Input user passphrase [in alphabets only]:
```

10. Click **Enter** to go back to the main menu.

#### To configure SNMPv2 data:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:

```
$ ssh npadmin@10.1.0.1
```

or

```
$ ssh npadmin@exampleFQDN
```

2. Enter privileged mode:

```
npadmin@ia> enable
```

3. Enter the npadmin password. The password can be 5 to 24 characters long.

```
[sudo] password for npadmin: <password>
```

4. Enter configuration mode:

```
npadmin@ia# configure system
```

5. Enter the SNMP menu:

```
npadmin@hostname(config) # snmp
```

You will see the following:

```
1: SNMP enabled = False
```

```
2: SNMP community string = public
```

```
3: SNMP system contact =
```

```
4: SNMP system location =d
```

```
5: SNMP system name =
```

```
6: SNMP traps enabled = False
```

```
7: SNMP trap target(s) =
```

```
8: SNMP trap string =
```

```
9: Set SNMP traps
```

6. Select 1 to enable SNMP

7. Select y to enable SNMP:

```
Enable snmp [y/n]: y
```

8. Select 2 to change the SNMP community string. Your community string serves like a password. The default community string is `public`.

```
Community string:
```



It is a security risk to leave `public` as the default community string

9. Select 3 to enter the contact name of the administrator responsible for the health of the IA appliance.
10. Select 4 to enter the name of the physical location of the IA appliance.
11. Select 5 to enter the IA appliance name

## SNMP Traps

The IA appliances supports the following SNMP traps:

| SNMP Traps                     | Description                                                                                                |
|--------------------------------|------------------------------------------------------------------------------------------------------------|
| Process down                   | A monitored process is down.                                                                               |
| Process up                     | All processes are running in normal state.                                                                 |
| Health status yellow           | Cluster is in a degraded state.                                                                            |
| Health status red              | Cluster is in a failed state.                                                                              |
| System temperature             | Cluster is above the temperature threshold. The default temperature is 75° Celsius.                        |
| System 1 minute average load   | Load exceeds 60. Trellix recommends maintaining a system load of 20 or below. The default threshold is 60. |
| System 5 minutes average load  | Load exceeds 40. Trellix recommends maintaining a system load of 20 or below. The default threshold is 40. |
| System 15 minutes average load | Load exceeds 40. Trellix recommends maintaining a system load of 20 or below. The default threshold is 40. |
| Tunnel down                    | A PX connection is down.                                                                                   |
| Tunnel up                      | All PX connections are up.                                                                                 |
| RAID down                      | A logical device on the IA is degraded.                                                                    |
| Disk usage percentage          | The disk usage exceeds a threshold of 85 percent. The default threshold is 85%.                            |

### To configure SNMP traps

1. From the SNMP menu, select option 6 to enable SNMP traps.  
Select y to enable SNMP traps:
2.  
Enable traps [y/n]

3. Select 7 to set the Trap target. Specify targets as host1:port1 host2:port2. Be sure hosts are separated with a space. Note that ports are optional.

SNMP trap target(s):

4. Select 8 to set the Trap string.

Trap string:

5. Select 9 to set the SNMP traps:

You will see the following:

- a: Process down enabled = False
- b: Process restarted enabled = False
- c: Elasticsearch yellow enabled = False
- d: Elasticsearch red enabled = False
- e: Tunnel down enabled = False
- f: Tunnel up enabled = False
- g: RAID failure enabled = False
- h: Disk usage percentage enabled = False
- i: 1 minute average load enabled = False
- j: 5 minute average load enabled = False
- k: 15 minute average load enabled = False
- l: Temperature enabled = False



Each SNMP trap is disabled by default.

6. Select Q to save.

## Retrieving SNMP Data Using MIBs

A Management Information Base (MIB) is a text file written in a specific format in which all of the manageable features of a device are arranged in a tree. Each branch of the tree contains a number and a name, and the complete path from the top of the tree down to the point of interest forms the Object Identifier, or OID. The OID is a string of values separated by periods, such as .1.3.6.1.2.1.1.3.0.

You can send requests for data on an object using the OID, but it can be simpler to use the symbolic name for the object instead. A MIB allows SNMP tools to translate the symbolic names into OIDs before sending the requests to the managed device.

The table below lists the monitoring and status OIDs supported in IA 1.4.1 and higher.

| OID                           | Type   | Description       |
|-------------------------------|--------|-------------------|
| .1.3.6.1.4.1.38885.62.1.1.1.0 | String | Down process list |

| OID                                           | Type    | Description                                              |
|-----------------------------------------------|---------|----------------------------------------------------------|
| .1.3.6.1.4.1.38885.62.1.1.3.x.2.0 (x: 1 ~ 64) | Integer | Status of the monitored process (0: running, 1: stopped) |
| .1.3.6.1.4.1.38885.62.1.5.2.0                 | String  | Health status value ('red': 0, 'yellow': 1, 'green': 2)  |
| 1.3.6.1.4.1.38885.62.1.9.2.0                  | Integer | System 1 minute average load                             |
| 1.3.6.1.4.1.38885.62.1.9.3.0                  | Integer | System 5 minutes average load                            |
| .1.3.6.1.4.1.38885.62.1.9.4.0                 | Integer | System 15 minutes average load                           |
| .1.3.6.1.4.1.38885.62.1.10.1.0                | String  | Down tunnel list                                         |
| .1.3.6.1.4.1.38885.62.1.10.2.0                | Integer | Down tunnel count                                        |
| .1.3.6.1.4.1.38885.62.1.11.3.0                | Integer | Disk usage percentage                                    |
| 1.3.6.1.4.1.38885.62.1.9.1.0                  | Integer | System temperature                                       |
| 1.3.6.1.4.1.38885.62.1.11.11.0                | Integer | RAID controller failed stripes (0 or 1)                  |

## Accessing MIBs

The IA MIB is available on the appliance at `/usr/share/snmp/mibs/IA-MIB.txt`. A typical SNMP browser can retrieve the values the appliance supports, and then display them in a hierarchy so you can navigate to the value you need to include in the request.

### To access MIBs:

1. Log into the CLI on the IA.
2. Enter privileged mode:  
`hostname> enable`
3. Enter the password.  
`[sudo] password for npadmin: <password>`
4. Enter shell:  
`hostname# shell`
5. The MIBs for the IA specific traps are located in `/usr/share/snmp/mibs` on the IA Series appliance.
6. Copy the MIB to `/home/np scp` and pull the MIB from the IA using an SCP client, or SCP the MIB directly to your SNMP manager.
7. In your monitoring system, upload them or copy them to the MIB file directory.

## Requesting SNMP Information

There are two ways to retrieve SNMP information:

- The `snmpget` command retrieves the value of a specific object.
- The `snmpwalk` command walks through the object hierarchy and automatically retrieves the object values for the subtree or node that you specified in your walk command.

SNMP commands are entered from the SNMP manager application. See examples of basic commands that retrieve SNMP information below.

### Example SNMP v2c commands:

| SNMP v2c Command      | Description                        | Example                                                                          |
|-----------------------|------------------------------------|----------------------------------------------------------------------------------|
| <code>snmpget</code>  | Walks all IA SNMP entries.         | <code>snmpwalk -v 2c -c public localhost<br/>iaAgentModules</code>               |
| <code>snmpwalk</code> | Retrieves the down processes list. | <code>snmpget -v 2c -c public localhost<br/>.1.3.6.1.4.1.38885.62.1.1.1.0</code> |



# CHAPTER 7: Upgrading Your Investigation Analysis Appliance

You can upgrade your Investigation Analysis appliance to the latest software release using the Web UI, API, CLI, or shell. Your Investigation Analysis appliance must be running software version 2.0 to upgrade to software version 2.1. Be sure to verify the current release of your IA software before upgrading your appliance software. Follow the steps in this section to upgrade your IA appliance to the latest software version.

-  **IMPORTANT:** Contact Trellix Customer Support to request access to the software release image.
-  **IMPORTANT:** The TrellixInvestigation Analysis2.1 appliance will automatically reboot after the upgrade. Allow for the appliance to finish rebooting before use.
-  **IMPORTANT:** Upgrade the cluster master and data nodes simultaneously. After the cluster master and data nodes are upgraded, then perform the upgrade on the IA director node.

## Upgrading Your Investigation Analysis Appliance Using the Web UI

-  **IMPORTANT:** Starting in IA version 1.4.0 and PX 4.5.1, the IA appliance Web UI uses the Software Update tool to support upgrades.

1. Log in to the IA appliance Web UI.
2. Click the **Manage** menu and select **Software Update**.
3. Click the **MANAGE SOFTWARE** button to open the Upload Software window.
4. Click **CHOOSE FILE** to upload the .iso or .fe software image file you received from Trellix Customer Support.
5. Click the **UPLOAD** button to upload the software image to your IA appliance.

6. Click **All Appliances** to see a list of connected IA appliances and select the appliances you want to upgrade.
7. Click **SOFTWARE UPDATE** to open the software update window.
8. Click the IA Software drop-down arrow and select the IA software image you uploaded in step 4 and step 5.
9. Click **Update** to upgrade your selected IA appliances with the latest software image.

## Upgrading Your Investigation Analysis Appliance Using the API

 **IMPORTANT:** Starting in IA version 1.4.0, you can upgrade your Investigation Analysis appliance using the API.

 **IMPORTANT:** When using the API to upgrade your IA data nodes connected to an IA master node, upgrade the master node only. After the master node upgrade is complete, each data node receives the software upgrade from the master node automatically.

1. Enter the following cURL command to upload the IA 2.1 image to your IA appliance using the API:

```
curl -X POST -u <username:passwd> -k -F "update=@/path/to/updates/file" https://<IA_Address>/updates/v1
```

2. Verify that the IA 2.1 image is uploaded:

```
curl -u <username:passwd> -k https://<IA_Address>/updates/v1
```

3. Enter the following cURL command to apply the IA 2.1 upgrade:

```
curl -X POST -u <username:passwd> -k https://<IA_Address>/updates/v1/IA1.5.0.xxxxx/apply
```

## Upgrading Your Investigation Analysis Appliance Using the CLI

Follow these steps to upgrade your Investigation Analysis appliance to software version 2.1 using the CLI.

 **IMPORTANT:** Installing 2.1 upgrade will automatically reboot the IA at completion. Packet capture is interrupted during the upgrade.

1. Using an SCP client, transfer the software image to `/home/npscp/transfer` and verify the md5sum.  
`scp IA-1.5.0.xxxxx.fe /home/npscp/transfer`
2. Log in to the IA and enter the shell.
3. In the CLI, enter `configure system` and then `upgrade`. The upgrade window opens.
4. Select the listed update file which is **IA-1.5.0xxxx** and confirm the selection. The upgrade is installed and the IA appliance restarts, running release 2.1.

## Synchronizing IA and PX

 **IMPORTANT:** Only synchronize the Packet Capture and Investigation Analysis appliances if network configuration settings have been changed between upgrades.

1. On the Investigation Analysis appliance, log into the CLI.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the password:  
`hostname # password`
4. Enter configuration mode:  
`hostname # configure system`
5. Enter the metadata menu:  
`hostname (config) # metadata`
6. Select **H** to synchronize the Investigation Analysis network configuration with the Packet Capture appliance.
7. Select **Q** to quit.



## CHAPTER 8: Log Monitoring

The IA Series appliance includes commands to monitor the system. You can monitor IA-specific logs and manage processes in KLISH. Shell access is not required to access logs.

The following logs are available:

| Log Name      | Description                                              |
|---------------|----------------------------------------------------------|
| auth          | Displays an auth log of the system.                      |
| system        | Displays a system log (npulse.log).                      |
| message       | Displays logs from /var/log/messages.                    |
| elasticsearch | Displays an elasticsearch log for all the elastic nodes. |
| nginx         | Displays logs for access and error from /var/log/nginx.  |
| audit         | Displays audit logs from /var/log/audit.                 |

## Accessing Logs

To access the IA Series appliance logs:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.  

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:  

```
npadmin@ia# configure system
```
5. Enter the log you want to view:  

```
npadmin@ia(config) # show log <log name>
```

  
For example,  

```
npadmin@ia(config) # show log elasticsearch
```

The log appears. Press **q** at anytime to exit from the log.

## Streaming Logs and Viewing Historic Logs

The following commands are available to stream and view historic logs:

| Command                 | Description                                                       |
|-------------------------|-------------------------------------------------------------------|
| <code>continuous</code> | Streams the selected log.                                         |
| <code>history</code>    | Displays all historic logs stored on the IA for the selected log. |

### To continuously stream a log:

1. Log in to the IA as `npadmin` using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```
3. Enter the `npadmin` password. The password can be 5 to 24 characters long.  

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:  

```
npadmin@ia# configure system
```
5. Enter the log you want to stream:  

```
npadmin@ia(config) # show log <log name> continuous
```

  
For example:  

```
npadmin@ia(config) # show log elasticsearch continuous
```

  
The log appears. Press **q** at anytime to exit from the log.

### To view a historic log:

1. Log in to the IA as `npadmin` using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```

3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`

4. Enter configuration mode:  
`npadmin@ia# configure system`

5. Enter the historic log you want to view:  
`npadmin@ia(config) # show log <log name> history`

For example:

`npadmin@ia(config) # show log elasticsearch history`

The historic log appears. Press `q` at anytime to exit from the log.



# CHAPTER 9: Configuring Syslog Server to Enable TLS Encryption

You can enable TLS encryption for logs that are transmitted from your Investigation Analysis appliance to the syslog server to achieve additional security.

**To enable TLS encryption for syslog communication:**

1. Generate syslog certificates on the syslog server and save them in the appropriate locations. See [Syslog Certificates](#) below.
2. Upload certificates to the syslog collection. See [Uploading Client Certificate to Syslog Collection](#) on the next page.
3. Enable TLS for syslog communication. See [Enabling TLS Encryption for Syslog](#) on page 55.

## Syslog Certificates

To establish trust between the syslog client (Investigation Analysis appliance) and the syslog server, you need to generate the CA certificates for both server and client, copy the server certificates to the syslog server, and upload client certificates to your Investigation Analysis appliance.

1. Generate the following certificates on the syslog server:
  - CA certificate on syslog server
  - Certificates for client—**rsclient-cert.pem**; **ca.pem**
  - Certificates for rsyslog server—**rsserver-key.pem**; **rsserver.cert**; **ca.pem**
2. Copy the **ca.pem**, **rsserver.cert**, and **rsserver-key.pem** certificates to the **/etc/pki/tls/private/** path in the syslog server and make changes in the syslog configuration file.
3. Upload the **ca.pem** and **rsclient-cert.pem** certificates to your Investigation Analysis appliance using the API. See [Uploading Client Certificate to Syslog Collection](#) on the next page.

# Uploading Client Certificate to Syslog Collection

You can upload the syslog client certificates to the Syslog collection of your Investigation Analysis appliance using the following request:

POST `https://<IA_IP_address>/config/v1/certmgmt/collection/syslog/upload`



**NOTE:** To use this request, you must belong to the sudo group.

## Required header:

`--user <username>:<password>`

## Request body (form-data):

`{ca: 'TEXT'}`

## Options

- `IA_IP_address`—IP address of the Investigation Analysis appliance running the Investigation Analysis API.
- `username`—Administrator user name.
- `password`—Administrator password.

## Parameters

- `ca` (string)—The name of a certificate you want to upload to the syslog collection.

## Example

POST `https://<IA_IP_address>/config/v1/certmgmt/collection/syslog/upload`

## Required header:

`--user npadmin:hammerhead`

## Request body:

```
{
 ca :@ca.pem
}
```

## Response Fields

- Response Code—A standard HTTP response code.
- Response Message—A standard HTTP response message.
- Date—Standard HTML date format.

## Example

HTTP/1.1 100 Continue

HTTP/1.1 200 OK

Date: Tue, 24 Jan 2017 18:38:24 GMT

```
[
 "1b7c60e9327d5e67de7f381c1bab873d7494dd0b56cd6230253b18ba3cdd3698",
 "987ab86dcf7879812e123f12bb8976cc8670a9870d987ee780134b76deadbeef"
]
```

## cURL Code Sample: Uploading Client Certificate

The code sample was run with cURL 7.57.0.

```
curl -k --user npadmin:hammerhead
https://xxx.xxx.xxx.xxx/config/v1/certmgmt/collection/syslog/upload -X POST -
F "ca=@ca.pem"
```

This cURL sample includes the following options:

- **-k**—This option explicitly allows cURL to perform insecure SSL connections and transfers, which allows you to test your SSL connection without installing a CA certificate.
- **--user npadmin:hammerhead**—Replace npadmin with the user name of the administrator for your Investigation Analysis appliance. Replace hammerhead with the administrator password for your Investigation Analysis appliance.
- **https://xxx.xxx.xxx.xxx/config/v1/certmgmt/collection/syslog/upload**—The request URL. Replace xxx.xxx.xxx.xxx with the IP address of your Investigation Analysis appliance.
- **-X POST**—This option specifies using the POST method.
- **-F "ca=@ca.pem"**—This option specifies the certificate to be uploaded to the syslog collection. Replace ca.pem with the name of the certificate you want to upload.

## Results

This example uploads ca.pem certificate to the syslog collection.

Similarly, you can upload rslclient-cert.pem certificate by replacing ca.pem with rslclient-cert.pem.

## Enabling TLS Encryption for Syslog

To enable TLS encryption for syslog:

1. SSH to the Investigation Analysis appliance as an administrator.
2. Enter the administrator password.
3. Enter privileged mode:  
npadmin@ia> enable
4. Enter the configuration menu:  
npadmin@ia> configure system
5. Enter the syslog configuration menu:

```
npadmin@ia(config)# syslog
```

The syslog menu appears:

```
1: Enable log shipping = False
2: Logging level = info
3: Logging target(s) = 10.128.20.111:6514
4: Logging export protocol = tcp
5: Enable TLS = False

```

```
Q: Save changes and exit
```

```
C: Cancel changes and exit
```

Select which option you would like to change using the index number.

6. Press 5 to enable TLS.
7. Press y to confirm.
8. Select Q to save the changes and exit.



# CHAPTER 10: Process Management

The IA Series appliance includes commands to debug the system. You can start, stop, restart, and show the status of individual processes in KLISH. Shell access is not required to debug issues. In addition to controlling the lifecycle of the application, you can also follow the logs for individual component or choose to dump all the logs.

The following commands are available for process management:

| Command                                                           | Description                                                                                                                                                                                                                |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>process dump</code>                                         | Dumps the last 1000 entries from the log.                                                                                                                                                                                  |
| <code>process manage &lt;processname&gt; &lt;operation&gt;</code> | Manages the process lifecycle. The available operations are: <ul style="list-style-type: none"><li>• <code>start</code></li><li>• <code>stop</code></li><li>• <code>restart</code></li><li>• <code>status</code></li></ul> |
| <code>process tail</code>                                         | Tails the log for the process. To exit the tail command, enter press <b>CTRL-C</b> .                                                                                                                                       |

## To manage a process:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter the process management action you want to complete:  
`npadmin@ia(config)# process manage <processname> <operation>`

For example:

```
npadmin@ia(config)# process manage elasticsearch status
```

Or:

```
npadmin@ia(config)# process dump elasticsearch
```

# CHAPTER 11: Clearing Client Data

The IA CLI `raid-wipe` menu allows you to securely erase the IA appliance RAID device used for PX traffic metadata. You can remove the data from each file system you want to clear. The table below provides a description for each file system and the type of data removed. Completely wipe (erase) the IA RAID device used for PX traffic metadata.

| Partition Type | Description                                                                   | Data Removed                                            |
|----------------|-------------------------------------------------------------------------------|---------------------------------------------------------|
| NPSTORE        | This file system stores all PCAP data and artifacts from bulk PCAP downloads. | Download PCAP, stored PCAP, and bulk download artifacts |
| Elastic        | This file system stores all Elasticsearch data.                               | All Elasticsearch data.                                 |
| CMA            | This file system stores all unprocessed metadata.                             | Unprocessed metadata                                    |

## Prerequisites

- Admin access

## Cleaning Your RAID Device

To configure a RAID device clean operation:

1. Log in to the IA as `npadmin` using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```

3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>

4. Enter configuration mode:  
npadmin@ia# configure system

5. Enter the raid-wipe menu:  
npadmin@hostname(config)# raid-wipe

You will see the following:

**wipe**

Securely removed collected data

1. File partitions to shred/wipe: No partition selected.
2. Verbose Mode: False
3. Shred iteration:
4. Zero Drives:

- A. Apply the shred of filesystem.
- C. Cancel the shred.

Enter the option from above to execute:

6. Enter 1 to select the partition you want to clean:

You will see the following"

**wipe**

Securely removed collected data

1. NPSTORE:
2. ELASTIC:
3. CMA:

Press Enter to go back to the main menu.

Enter the number for the Filesystem you want to include in the SHRED:

7. Select the number (1,2 or 3) for the file system you want to shred. You can include a single file system or multiple file systems in the shred.
8. Select option 2 to enable Verbose mode:
9. Select option 3 to enter the number of shred iterations. You can select up to 9 iterations. The default is 1.

Enter the number of iterations for sherd [1-9]:

10. Select option 4 to enable zero drives. This will zero out each and every sector and byte in the drive after shredding.
11. Select option A to include the file system in the shred.



A file system shred results in a permanent loss of all data in each file system included in the RAID device wipe. You cannot retrieve the file system data after it is deleted.

12. You will see the following warning:  
verify the action

WARNING            WARNING            WARNING            WARNING            WARNING

Continuing this action will result in the permanent  
loss of data on the following file systems:

ELASTIC

Data on these file systems can not be retrieved after this action is  
initiated.

You must enter 'DELETE' to proceed and remove the data.  
Any other response will return to the previous menu.  
Proceed?:

13. Type **DELETE** to confirm file system shred.
14. Press **Enter** to go back to the raid-wipe menu.

## Rebuilding Storage

You can rebuild the storage erased with the `build local` command.



**IMPORTANT:** System processes restart during storage reconstruction.

### To rebuild all your Investigation Analysis storage:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>

4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Rebuild the storage. By default, storage is rebuilt to its former location.  
`npadmin@hostname> build local`

A new storage configuration is immediately built.

## CHAPTER 12: Disk-Mirroring

Trellix x600 appliances ship with a secondary SSD installed, which enables you to have a more streamlined disaster-recovery plan. You can enable disk mirroring feature to mirror files present on the primary SSD to the secondary SSD. Disk-mirroring enables you to use the secondary SSD as a fallback operating system drive.

If you opt to mirror the disks during the first-run, the entire primary disk will be copied to the secondary SSD. After the initial copy, you should be able to boot the appliance through the secondary disk by changing the BIOS boot order. Disk-mirroring is not done automatically at any point.

To mirror disks using the CLI:

1. Log in to the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the admin password:  
`[sudo] password for <npadmin>: <password>`
4. To mirror disks at any point of time:  
`hostname # storage mirror-disk`
5. Press **y** to confirm the mirroring of the primary SSD to the secondary SSD.
6. Press **y** to acknowledge disk-mirroring wipes the data on the secondary SSD.



# CHAPTER 13: Configuring Session-Reconstruction Parameters

You can configure the session-reconstruction parameters in the **pivotengine** menu.

**Prerequisite:** Admin access.

**To configure session-reconstruction parameters:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter the pivotengine menu:  
npadmin@hostname(config) # pivotengine  
PivotEngine/Session Reconstruction Parameters  
  
Thumbnail Generation: Disabled  
Assymmetric Flow Stitching: Disabled  
VLAN Tracking: On  
-----  
A: Toggle the Asymmetric Stitching of flows  
T: Toggle whether to generate thumbnail or not  
V: Toggle VLAN Tracking for reconstruction  
Q: Exit and Save

Select which option you would like to change:

6. Press **A** to toggle the status of asymmetric stitching of flows.

By default, "Asymmetric Stitching of flows" is disabled so that the Packet Capture appliance can see bi-directional traffic on each configured capture interface. If your deployment has one capture interface / PX that records the inbound traffic while another capture interface / PX records the outbound traffic, you need to enable this option.

7. Press **T** to toggle the status of thumbnail generation.

When enabled, the **Artifacts** tab shows thumbnails for extracted artifacts after a successful session.

8. Press **V** to toggle the status of VLAN Tracking for reconstruction.

When enabled, Suricata will look for the same VLAN ID tag in incoming and outgoing flows during session reconstruction. If incoming traffic has a VLAN ID tag and outgoing traffic doesn't have a VLAN ID tag or vice versa, Suricata will not consider it as a session.

9. Press **Q** to save the settings and exit the pivotengine menu.

## PART III: Configuration

---

This part covers the following topics:

- [Clusters](#)
- [Distributed Search](#)



# CHAPTER 14: Clusters

This chapter covers the following topics:

- [IA Clusters](#) below
- [Deploying a New IA Cluster](#) on page 73
- [Expanding an Existing IA Cluster Deployment](#) on page 81
- [Recovering Elasticsearch](#) on page 82

## IA Clusters

In an IA cluster, multiple IA appliances work cooperatively to store and retrieve data. An IA Cluster is formed when an IA appliance is configured or connected in a way that enables distributed storage and search. This approach uses the distributed features of Elasticsearch for operation. This is similar to, but different from the IA distributed search set up. See [Distributed Search](#) on page 84.

In an IA Cluster, every IA appliance runs multiple Elasticsearch nodes within the box, which makes every IA appliance a cluster. There are two types of IA clusters: a single-box cluster and a multi-box cluster.

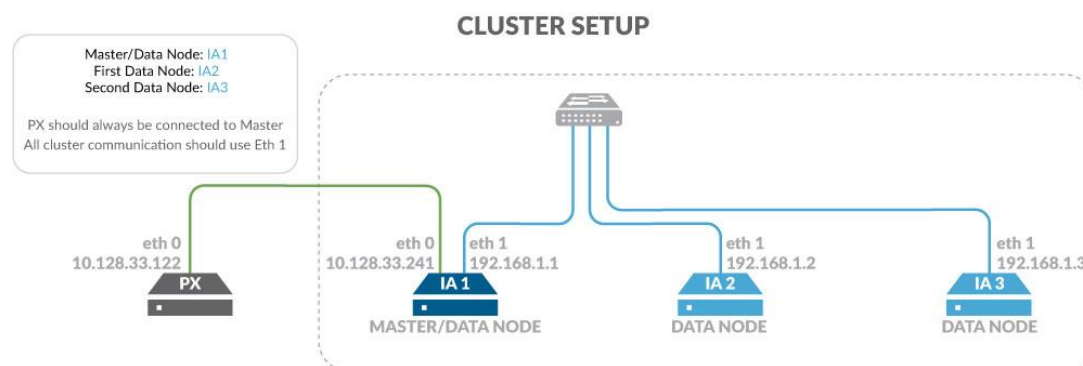


Figure 14-1 IA Clusters

| IA Cluster Components | Definitions                                                                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Master-Data Node      | Collects metadata from one or more connected PX appliances and evenly distributes the data load between itself and one or more connected IA data nodes. |
| Data Node             | IA appliances used to store and search metadata distributed by the connected Master-Data Node.                                                          |

## Single-Box Cluster

A Single-Box IA cluster is formed when an IA appliance has two internal data nodes that store data and allow it to be searched. One internal node functions as a Master Data Node and the other internal node functions as a data node. The Master Data Node collects metadata from the connected PX appliance and evenly distributes the data load between itself and the data node.

## Multi-Box Cluster

A Multi-Box IA cluster is formed when multiple IA appliances are connected together and configured to store data and allow it to be searched. This cluster configuration significantly increases the storage and search capacity of your IA appliances and utilizes the Master Data Node and data node designation in a different way.

In a multi-box cluster, a single IA appliance serves as the Master node because it contains a master-data node and a data node. This appliance is connected to one or more PX appliances and one or more IA appliances, and coordinates the effort of the IA cluster. The Master node is necessary for the multi-box cluster operation and interaction with the IA Web UI. The other IA appliances that make up the multi-box cluster only contain data nodes that are used to store and search metadata.

Each IA Cluster has a name that uniquely identifies it. Each master or data node also has a node name that uniquely identifies it.

Terms used to describe an “IA Cluster” and a distributed search configuration are common to both deployments but have different meanings. This section focuses on IA Clusters. Any references to distributed search terminology will be called out explicitly.

Here is an overview of the basic steps in the cluster deployment process:

1. Choose the deployment option.
2. Configure the master nodes.

3. Configure the data nodes.
4. Start/Restart nodes.

## IA Cluster Deployment Considerations

Here are some scenarios that are likely to occur when deploying an IA Cluster:

- **Single Node Cluster**—A single IA appliance fills the role of both master and data node and no other appliances are part of the cluster. This is the default behavior of an IA appliance.
- **Deploying a New Cluster**—When using an IA cluster, and no other existing IA appliances will be part of the cluster.
- **Expanding an Existing IA Deployment**—This is when an existing IA Cluster is deployed and is in operation. Deployment personnel should plan on an availability outage associated with the deployment, as existing IA appliances or services may need to be restarted.

There are a number of considerations when planning to deploy an IA cluster:

- **Connectivity requirements**—IA appliances participating in the cluster will need to communicate with each other on an isolated, private network. You will need to select a private IP address range and node names for each IA participating in the cluster.
- **Security considerations**—IA appliances that are part of a cluster need to communicate over a trusted network connection. Untrusted devices present on that network may add security risks. Use the eth1 network interface and an isolated, private network for intra-cluster communication. PX appliances can be connected to this private network for the purpose of dedicated metadata exchange.
- **Removing Data Nodes**—Data is shared across all the nodes in the cluster. If you remove a node from the cluster, that data is no longer accessible, the cluster status will change to RED, and cluster performance may diminish. Restoring the node that has the data can restore the cluster state.
- **Configuring the Shard Count Per Index**—By default, each IA host in a cluster has 4 shards because each IA appliance is a cluster that has two internal data nodes. The CLI menu allows you can configure the shard count per index for an IA cluster. Use the Editing IA Cluster Configuration menu to set the shard count to 4 times the number of IA hosts in a cluster. For example, if you have one IA hosts in a cluster, set the shard count to 4. If you have two IA hosts in a cluster set the shard count to 8.



Shard allocation menu can be found on the KLISH. In case of a failure, shards can be reallocated to recover Elasticsearch.

## IA Cluster Terminology

IA appliances participating in an IA Cluster are likely to be a master node, a data node, or both. Master nodes coordinate the effort of the IA cluster and are necessary for cluster operation and interaction with the IA Web UI. Data nodes are used to store and search metadata.

Each IA Cluster has a cluster name that uniquely identifies it. Each master or data node also has a node name that uniquely identifies it.



If you rename an IA Cluster your data will be lost, but will still appear on a connected PX.

## Deploying a New IA Cluster

This section provides instructions for deploying a new IA multibox cluster. If you need to expand your existing IA cluster, see [Expanding an Existing IA Cluster Deployment](#).

The deployment process entails creating configuration files for each node and then copying the files to the appropriate device. You can configure an IA cluster through the cluster setup and maintenance menu in KLISH.



During the IA first run on the CLI, you are required to select if the IA is part of a multi-box cluster or a single-box cluster. Select 'y' for 'yes' if it is a multi-box cluster otherwise select 'n' for 'no'.

This table summarizes the node configuration.

| Node Configuration                       | Sample Setting                                                                                                                                                                                                                                                                                               |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (N) Node name:                           | ia1<br><br>Must be unique within the cluster.<br><br> Elasticsearch does not allow uppercase characters in index names. Cluster names, used to create index names, and hostnames must be lowercase when entered in KLISH. |
| (M) Device is configured as master node: | True                                                                                                                                                                                                                                                                                                         |
| (D) Device is configured as data node:   | True                                                                                                                                                                                                                                                                                                         |
| (A) Disable _all field in ES Index:      | False                                                                                                                                                                                                                                                                                                        |

## Create Master Node Configuration

Before you create the Cluster Master node, you must set up the initial IA configuration.

- Configure the cluster name with a unique name.
- Configure the node name with a unique name. This name is the IA hostname.
- Configure the network settings for `eth0` and `eth1`.
- Apply the configuration settings, and then reboot into the IA appliance.
- Ensure that the interfaces have the configured settings.

This table summarizes the cluster communication settings.

| Cluster Communication               | Sample Settings                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (R) Cluster name:                   | <p>clus-1</p> <p>This name must be the same for all nodes in the cluster.</p> <p> Elasticsearch does not allow uppercase characters in index names. Cluster names, which are used to create index names, and hostnames must be lowercase when entered in KLISH.</p> |
| (U) Unicast ping IP address (port): | <p>192.168.1.1:9300</p> <p>This is a private <code>eth1</code> IP address of the master. In a multibox cluster, the data node Unicast ping IA address should match the <code>eth1</code> IP address of the master data node and default port of 9300.</p>                                                                                            |
| (B) Bind host IP address:           | <p>192.168.1.1</p> <p>The IP addresses for cluster nodes discovery requests, always set to the private <code>eth1</code> IP address of the IA data node that you are configuring.</p>                                                                                                                                                                |
| (P) Publish host IP address (port)  | <p>192.168.1.1</p> <p>Always set to the private <code>eth1</code> address of the IA data node that you are configuring.</p>                                                                                                                                                                                                                          |
| (S) Per Index default shard count:  | <p>4</p> <p>The Per Index shard count is twice the number of IA appliances in your multibox IA cluster. For example, if you have one IA host</p>                                                                                                                                                                                                     |
| (H) HTTP enabled:                   | True                                                                                                                                                                                                                                                                                                                                                 |
| (T) Multi-IA Cluster:               | Yes                                                                                                                                                                                                                                                                                                                                                  |

| Cluster Communication            | Sample Settings                                                                                     |
|----------------------------------|-----------------------------------------------------------------------------------------------------|
| (G) Gateway Recovery node count: | This option must be configured with 2 for a single node cluster and with 4 for a multinode cluster. |

For more information, see [Initial Configuration](#) on page 18.

**To start the cluster setup:**

1. Log in to the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Enter configuration mode:  
`hostname # configure system`
5. Enter cluster setup:  
`user@hostname(config)# cluster setup`



The script indicates that its purpose is for configuring IA Clusters and not for Distributed Search (director).

6. Choose **yes** to continue.
7. From the IA Cluster Configuration menu, choose  
(E) Edit/review cluster configuration.

8. From the edit configuration menu, choose the following:
- **Node name:** Must be unique within the cluster.
  - **Master node:** `true`
  - **Data node:** `true`
  - **Cluster name:** Must be lowercase and must be the same for all nodes in the cluster. Note this name for data node setup.
  - **Unicast ping address:** Change the Unicast ping IP address and add `<eth1-ip>:9300` (e.g. `192.168.2.1:9300`). The data node Unicast ping IP address should match the `.eth1` IP address of the master data node and default port of 9300.
  - **Bind host IP address:** Specify the IP address(es) that the master should listen on. Set this to the private `eth1` IP of the IA appliance you are configuring.
  - **Publish host IP address (port):** Specify the IP address the to accept connection requests. Set this to the private `eth1` IP of the IA appliance you are configuring.
  - **Per index default shard count:** Set the shard count to 4 times the number of IA appliances in your multi-box IA cluster. For example, if you have one IA host in a cluster, set the shard count to 4. If you have two IA hosts in a cluster, set the shard count to 8.
  - **HTTP enabled:** `true`

Your configuration should look similar to this:

#### Editing IA Cluster Configuration

```

Node Configuration
(N) Node name: ia1
(M) Device is configured as master node: true
(D) Device is configured as data node: true
Cluster Communication
(R) Cluster name: clus-1
(U) Unicast ping IP address (port): 192.168.1.1:9300
(B) Bind host IP address: 192.168.1.1
(P) Publish host IP address (port): 192.168.1.1
(S) Per index default shard count: 4
(H) HTTP enabled: true
```

-----  
Q: Quit and return to main menu

Select an option:

9. Select **T** to turn on the cluster.
10. Press the **Q** key to quit and return to the main menu.

**To save and transfer the cluster configuration:**

1. Select **S** to save and transfer cluster configuration.
2. When prompted to enter the configuration file name, accept the default or enter the desired name.  
The screen indicates the location of the configuration file.
3. Choose an option:
  - To install the configuration on the local machine, indicate yes when prompted.
  - To transfer the configuration to a remote host to be installed later, indicate yes when prompted.
1. The system will prompt for the remote host name. The npscp account will need to be enabled on the remote host, and you will need the credentials for that account.
2. When prompted for a destination location, accept the default.

## Create Data Node Configuration

You can configure each data node using the CLI cluster setup menu.

**To create a data node configuration file:**

1. On the IA, log in to the CLI.
2. Enter privileged mode:  
hostname > enable
3. Enter the default admin password:  
hostname # hammerhead
4. Enter configuration mode:  
hostname # configure system
5. Enter cluster setup:  
user@hostname(config)# cluster setup



The script indicates that its purpose is for configuring IA clusters and not for distributed search (director).

6. Choose **yes** to continue.

7. From the IA cluster configuration menu, choose  
(E) Edit/review cluster configuration.
8. From the edit configuration menu, choose the following:

| Node Configuration            | Setting                                                                                                                                                                                                                                        |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node Name                     | Must be unique within the cluster.                                                                                                                                                                                                             |
| Master Node                   | False.                                                                                                                                                                                                                                         |
| Data Node                     | True.                                                                                                                                                                                                                                          |
| Cluster Name                  | Must match the cluster name specified in the master node configuration.                                                                                                                                                                        |
| Unicast ping address          | Must match the private <code>eth1</code> IP master node IP address and default port of 9300. For example, 192.168.1.1:9300.                                                                                                                    |
| Bind IP address               | Specify any IP address that the data node should listen on. This address should match the address for the <code>eth1</code> interface. For example, 192.168.1.2.                                                                               |
| Publish host IP address       | Specify any IP address that the data node should publish on. This address should match the address for the <code>eth1</code> interface. For example, 192.168.1.2.                                                                              |
| Per index default shard count | Set the shard count per indexed data to 4 times the number of IA hosts in a your IA cluster. For example, If you have one IA host in the cluster, set the shard count to 4. If you have two IA hosts in the cluster, set the shard count to 8. |
| HTTP Enabled                  | False.                                                                                                                                                                                                                                         |

9. Select `T` to turn on the cluster.
10. Press the `Q` key to quit to the main menu.
11. When prompted to enter the configuration file name, accept the default or enter the desired file name.  
The screen indicates the configuration file location.
12. Choose an option:
  - To install the configuration to the local machine, indicate yes when prompted.
  - To transfer this configuration to a remote host to be installed later, indicate yes when prompted.

The system prompts for the remote host name. The npscp account must be enabled on the remote host. You will need the credentials for that account.

13. When prompted for a destination location, accept the default.

## Disable Unnecessary Services on Data Node

Several services that are enabled from the default IA configuration are unnecessary for Data Node operation. Disable these unnecessary services.

**To disable unnecessary services on data node:**

1. Log into the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Enter configuration mode:  
`hostname # configure system`
5. Enter cluster hardening:  
`user@hostname(config)# cluster hardening enable`
6. When services are disabled, you should see this message:  
`Services disabled and stopped.`

## Start the Master Node

Your cluster is now properly configured. Reboot the IA appliance.

**To reboot the master node:**

1. Log in to the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Reboot the appliance.  
`hostname # reboot`

## Start the Data Node

After the master node is running, you can restart each data node.

To reboot the data node:

1. Log in to the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Reboot the appliance.  
`hostname # reboot`

## Verify the Cluster State using the CLI

When at least one data node is connected, you can query the master node with the `show cluster` command. This command displays `cluster health` and `node`. The `cluster health` section gives a high-level summary of the cluster status. An important indicator here is `status`, which should be green.

The `node status` section indicates which nodes are connected to the cluster and which role they play. You will see the master and data nodes that are configured in this IA Cluster.

### To verify the cluster on the master node:

1. Log into the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Display the cluster:  
`user@hostname(config)# show cluster`

## Verify the Cluster State using the API

You can verify the cluster state using Elasticsearch web APIs.

### To verify the cluster state using the Web UI and API:

1. Log in to the IA Web UI. Open a Web browser and type `https://appliance` in the address line, where *appliance* is the IP address or hostname of the appliance. For example, if the configured IP address of the appliance is 10.1.0.1, type:  
`https://10.1.0.1`
2. Enter this URL, where *iaipaddress* is the IP address to the IA master node:  
`https://iaipaddress/elasticsearch/_cat/nodes`

3. Check the overall cluster health by entering this URL where *iaipaddress* is the IP address to the IA master node:  
`https://iaipaddress/elasticsearch/_cat/health`

## Expanding an Existing IA Cluster Deployment

This section discusses the steps needed to expand an IA cluster deployment. If you are deploying a new IA Cluster, see [Deploying a New IA Cluster](#) on page 73.

This section assumes that a master node is configured and is in operation. Expanding an IA Deployment can involve adding new nodes to a single node cluster or adding new nodes to a multinode cluster.

### Adding Nodes to a Single-Node IA Cluster

If you are expanding a single node IA Cluster, the existing node becomes the cluster master. To prepare a single-node cluster for this role, you must create and install a master node and configure the master firewall to allow communication with data nodes.

The steps needed to perform these tasks are described in the previous section under the following topics:

- [Create Master Node Configuration](#) on page 74
- [Start the Master Node](#) on page 79

After the master node is configured, the IA Cluster is ready for further expansion. Continue with [Adding Nodes to a Multinode IA Cluster](#) below.

### Adding Nodes to a Multinode IA Cluster

To expand a multinode IA Cluster, you need the cluster name and the master node IP address to create configurations for each new data node. You must configure the master node for further expansion, as discussed in the previous topic.

After you configure the master node, you can configure new data nodes and add them to the cluster. To add data nodes, you must create, install, and configure firewall settings for each data node.

The steps are described in the following topics:

- [Create Data Node Configuration](#) on page 77
- [Disable Unnecessary Services on Data Node](#) on page 79
- [Start the Data Node](#) on page 79

# Recovering Elasticsearch

When Elasticsearch fails or is in a unhealthy state, the ES status indicator appears red due to red indices containing unassigned shards. You can recover it automatically or manually.

The automatic option will allow watchdog to delete all the red indices and reset Elasticsearch. The manual option will provide you with two sub-options. You can reallocate the unassigned shards to the master node or another available node or delete all the red indices.

When the Elasticsearch returns to its healthy state, the status indicator appears green.

## Cluster Maintenance

To maintain a cluster:

1. Log in to the Investigation Analysis CLI.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Enter configuration mode:  
`hostname # configure system`
5. Enter the cluster maintenance menu:  
`user@hostname(config)# cluster maintenance`

The **Elasticsearch Maintenance** menu appears.

```
(S) Shutdown Cluster
(M) Maintenance
(C) Cancel and Exit
Enter your choice:
```

6. (Optional) Press **S** to shutdown the cluster.
7. Press **M** to enter the maintenance mode.

The **Elasticsearch Maintenance** menu is displayed.

Menu:

```
(N) No of days for which to keep the index Open
(C) Cancel and Exit
(X) Save and Exit
```

8. Press **N** and press **Enter** to set the time period in days, for which you need to retain the data on your Investigation Analysis appliance. This period is called the retention period. After the retention period, the older data on your appliance is automatically deleted to accommodate new data.

9. Enter any value between 1 and 1000, and then press **Enter**.

You cannot set the retention period as more than 1000 days. If you enter a value beyond 1000, the following error message is displayed: "Not a valid input. Try again".

10. Click **X** to save and exit.

## CHAPTER 15: Distributed Search

Distributed search enables you to search across multiple IA devices and retrieve PCAP data from multiple PX packet capture appliances. Distributed search requires one IA appliance set up as the director node and other IA appliances set up as the data nodes. This setup is similar to the IA cluster setup. See [Clusters](#) on page 70.

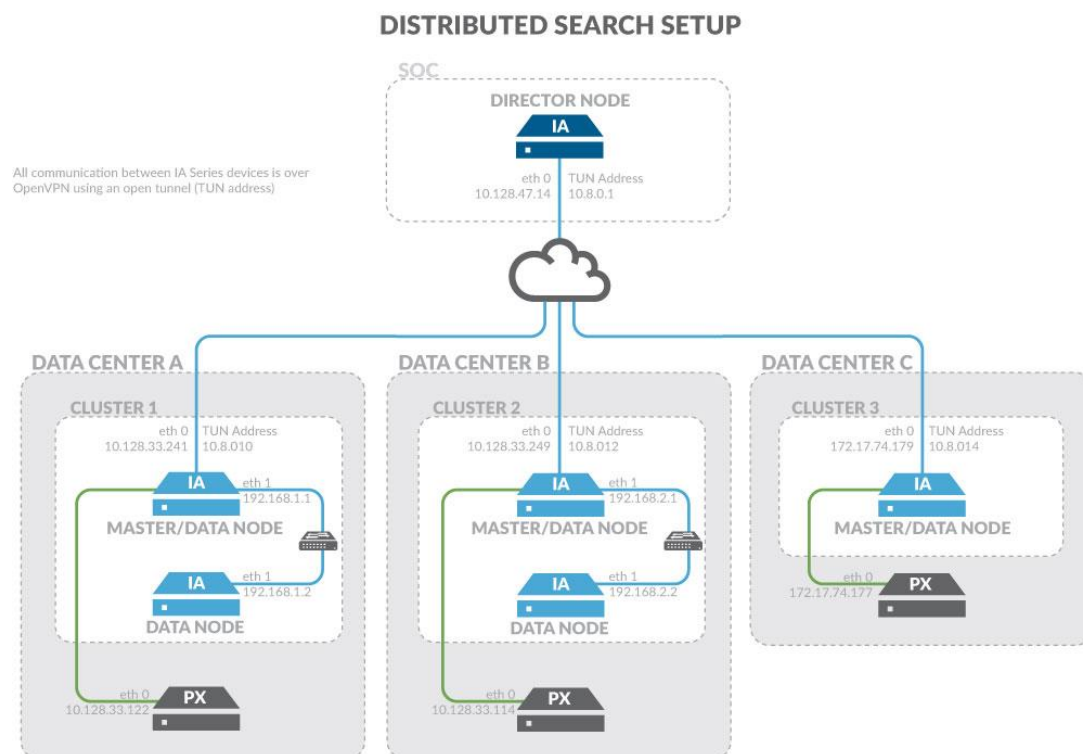


Figure 15-1 Distributed Search

| Distributed Search Components | Definitions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Director node                 | <p>An IA appliance that is a centralized location from which to initiate distributed searches to the data nodes. The director node does not collect metadata directly from IA data nodes or PX appliances but can pull PCAP from any connected PX appliance.</p> <p> By default, all IA appliances are configured as a master data node. Use the CLI to change your IA appliance master data node configuration to a director.</p> |
| Master data node              | An IA appliance that is connected to one PX appliance and one or more IA data nodes or multiple PX appliances and one or more IA data nodes. The master data node collects metadata from connected PX appliances and shares the data load across the connected IA data nodes.                                                                                                                                                                                                                                       |
| Data node                     | IA appliances connected to the Master Data Node and used to store and search metadata.                                                                                                                                                                                                                                                                                                                                                                                                                              |

In distributed search, multiple IA appliances, known as IA clusters, operate independently. IA director nodes query these devices. This approach relies on Elasticsearch tribe nodes to operate.

To configure IA for distributed search, open the following ports on any firewall between the data nodes and the director node:

- TCP 22 on both sides.
- TCP and UDP 1194 on both sides.

## Converting an IA Series Appliance to a Director Node

Converting an IA appliance to a director node erases Elasticsearch data, and the appliance becomes an aggregation unit.

Perform this procedure on the IA Series appliance that you want to convert to a director node.

**To convert an IA Series appliance into a director node in the CLI:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter director mode:  
`npadmin@ia# director`
6. Select **y** to confirm that you want to convert the appliance into a director node.
7. Select **y** to configure the OpenVPN. This process might take 2 minutes.

Your IA appliance is now a director node. You must add master data nodes to the configuration. See [Adding Data Nodes to the Director Node](#) on the next page.

## Converting an IA Series Appliance into a Data Node

Converting an IA Series appliance to a data node stops indexing and Elasticsearch while the change takes effect. Perform this procedure on the IA Series appliance that you would like to convert to a data node.

**To convert an IA Series appliance to a data node:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`

5. Enter data node:  
`npadmin@ia# datanode`
6. Select **a**, and then enter the director node's IP address.
7. You will see messages about validation and then OpenVPN and PX\_ACM restarting.
8. You will see a confirmation screen:  
currently part of tribe node setup...

## Adding Data Nodes to the Director Node

You must add the data nodes to the director node. Perform this procedure on the director node.

### To add data nodes to the director node:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter director mode:  
`npadmin@ia# director`
6. Select **a** to add a data node.
7. Enter the cluster name that you want to join:  
`clus-1`
8. Enter the cluster master hostname. This must be a FQDN or an eth0 IPv4 address.  
`10.128.33.249`
9. Enter the cluster network subnet in CIDR notation. Press enter if adding single-host cluster.  
`2.2.2.0/8 validation 2.2.2.0/8 against`



This is the address range used for eth1 of the data nodes. For example, your cluster network subnet might use range 2.2.2.0/24.

10. Enter the elasticsearch cluster bind\_host (eth1 IP Address of cluster master):  
2.2.2.249  
key generation successful. Moving the key to the client now.
11. When prompted enter the npscp user password of the host:  
The authenticity of host '10.128.33.249 (10.128.33.249)' can't be established.  
ECDSA key fingerprint is  
14:6d:4f:65:4b:37:6b:03:50:5a:0a:45:b7:fd:67:b0.  
Are you sure you want to continue connecting (yes/no)? yes  
warning: Permanently added '10.128.33.249' (ECDSA) to the list of known hosts.  
npscp@10.128.33.249's password:  
clus-1.tar.gz 100% 5395 5.3KB/s 00:00  
Transfer completed SUCCESSFULLY 10.128.33.249  
Transfer of keys was successful. You will need to go to the Data Node and accept the keys now.
12. Select q to quit and save changes.

You must now go to the data node CLI and associate it with this director. This is explained in [Adding a Data Node to the Director Node](#) below.

## Adding a Data Node to the Director Node

This section provides instructions for adding your IA data node to your IA director node.

**To add a data node to the director node:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter data node:  
npadmin@ia# datanode

6. Select option A to add the director.
7. Enter the IP address of the director.

## Removing a Data Node from the Director Node

Perform this procedure on the data node that you would like to remove from the director node.

**To remove a data node from the director node:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter data node:  
npadmin@ia# datanode
6. Select r to remove the appliance as part of the setup.
7. Confirm the removal of the data node.

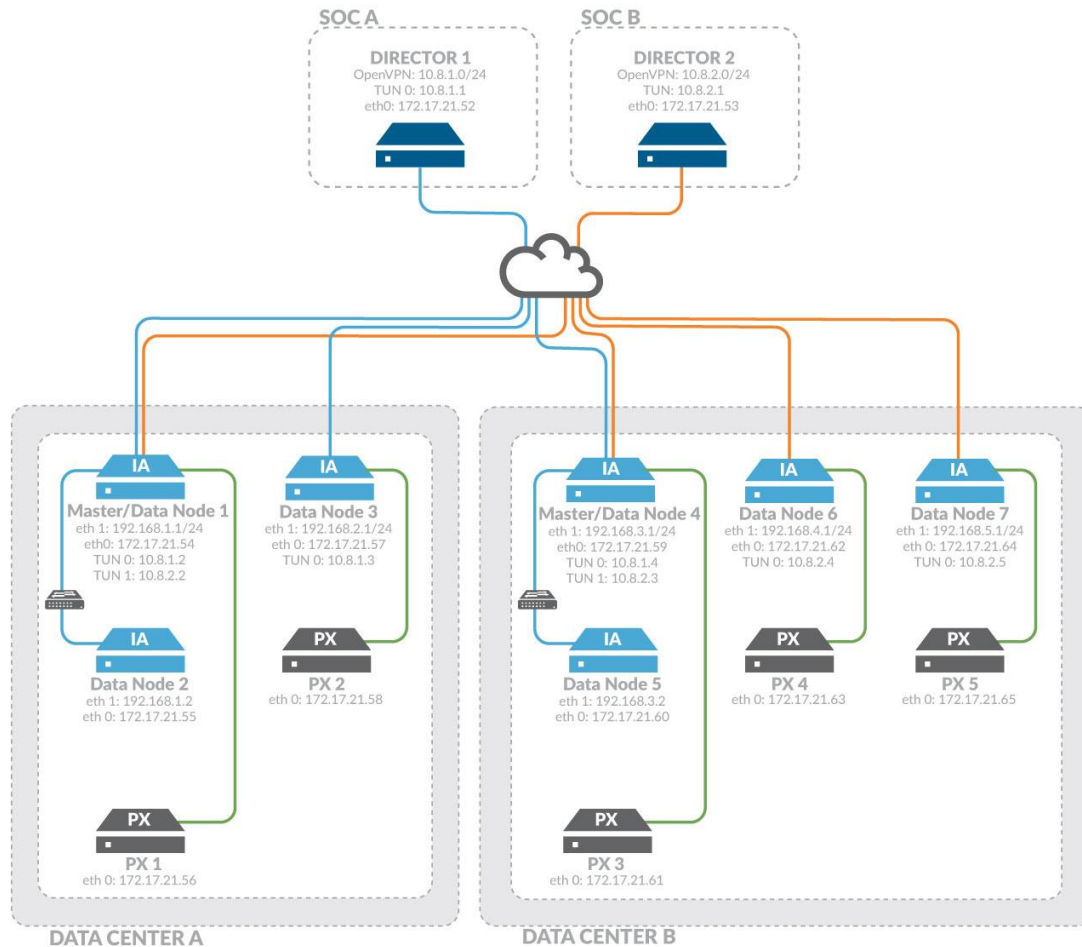
## CHAPTER 16: Multidirector Configuration

IA supports multidirector configuration, which allows your IA data nodes to simultaneously connect to multiple directors.

You can use a multidirector configuration to establish regional and global IA directors to accomplish these tasks:

- Manage your IA clusters
- Share or allocate your IA data views among multiple directors
- Increase IA appliance visibility across your enterprise
- Create a backup for your primary IA director.

## MULTI-DIRECTOR TOPOLOGY



## Configuring Network Connections

IA data nodes and director nodes must follow specific network connection requirements for a multidirector configuration. Follow these guidelines to establish your multidirector setup:

- Each data node must use `eth1`, with separate and private subnet addresses, to connect and communicate with an IA director.



`eth0` is configured for management, which allows users to SSH to the device and use a browser with the IA Web UI.

- To connect with multiple directors, a single-box cluster must be configured as a multibox cluster.

- IA directors must have a unique, nonoverlapping subnet for their OpenVPN IP range.

## Preparing an IA Data Node for Multi-Director Configuration

To set up a multidirector configuration, you must first configure the IA data node as a cluster and set up the eth1 IP address.

If your IA data nodes already are configured as a multibox cluster, then you can use the instructions in this section and [Configuring the Single-Box Cluster as a Multi-Box Cluster](#) on the next page to verify your network settings, or you can go to [Configuring the IA Director Node](#) on the next page to set up your IA Directors.



For a single-box IA cluster serving as a data node, eth1 does not require a physical connection. However, for the multidirector setup to work, it does require an IP address.

In a single-box IA, eth0 is physically connected to the management network. However, eth1 also must be configured to the private subnet that is not routable on the host network. For example, it may use an IP in the CIDR range 192.168.2.0/24 if that is not routable in the customer environment.

### To make the IA data node compatible with a multidirector setup:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.  

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:  

```
npadmin@ia# configure system
```
5. Enter network mode:  

```
npadmin@ia141host(config)# network
```
6. Select option **9**, and then enter a private eth1 IP address and subnet. For example, IP address 192.168.1.1 and subnet 255.255.255.0. Record the eth1 address and subnet for later use.
7. Click **Enter** at the **Routeable IPv6 Address** prompt and the **Prefix Length** prompt.

8. Enter Q to save changes and exit. You will be able to verify, correct, and confirm your network settings.

## Configuring the Single-Box Cluster as a Multi-Box Cluster

Next, set up the single-box cluster as multibox cluster, and then change the publish host and bind host to the new eth1IP address.

**To configure a multi-box cluster configuration and modify the public host and bind host:**

1. Enter cluster setup mode:  
`npadmin@ia141host(config)# cluster setup`
2. Enter y at the prompt:  
`Do you want to configure an IA Cluster (y/n)?`
3. Select option E to edit and review the IA cluster configuration.  
`select an option: E`
4. Select option T to enable the multibox cluster configuration.  
`select an option: T`



After enabling the multibox cluster, your IA data node network settings update the Unicast and Bind host IP address with the eth1 IP address.

No port is required.

5. Record the IA data node `cluster` name in option R.
6. Type Q to save changes and exit.

## Configuring the IA Director Node

Now that your IA data node is configured as a multibox cluster and ready to connect to the IA director, you must configure your IA director. Repeat the steps in this section for your each IA director in your multidirector setup.

**To configure an IA Director for a Multi-Director setup:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`

4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter director mode:  
npadmin@ia# director
6. Select option **S** to configure the OpenVPN subnet and enter 10.8.1.0/24 for the first director. You can use 10.8.2.0/24 for the second IA director.
7. Select **P** to configure the OpenVPN protocol, and then select one of the following:
  - u4: UDPv4
  - t4: TCPv4
  - u6: UDPv6
  - t6: TCPv6



**Caution:** Changing the OpenVPN protocol disconnects the existing data nodes.

8. Select option **A**, and then complete each setting below to add the data node to a multibox cluster with the cluster name and eth0 IP address.

You will see the following:

- Enter the cluster name of the IA data node:
- Enter the master eth0 IP address:
- Is the cluster you are adding a multi-box cluster (y/n):y
- Enter the ES Cluster Network Subnet in CIDR notation:  
192.168.1.1/24
- Enter the elasticsearch cluster bind\_host (eth1 IP address of the cluster master): 192.168.1.1

## Connecting the IA Director to the IA Cluster

The IA Director generates a configuration package for the IA data node that allows a connection between to the two appliances. After accepting the data node configuration keys, you can connect the IA director to the IA cluster. You must log into the IA data node and accept the configuration package to continue.

**To accept the data node transfer keys and connect to the IA director and IA cluster:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
or  
\$ ssh npadmin@exampleFQDN

2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter datanode mode:  
`npadmin@ia# datanode`
6. Select option **A** to enter the IA Director eth0 management IP address.
7. Select **Q** to save and quit.

## Adding a Default Route for Multibox Clusters

When you add a multibox IA cluster to a director, you must also add a default route between each data node of the multibox cluster and the cluster master.

**To add a default route for each data node in your multibox clusters:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter datanode mode:  
`npadmin@ia# datanode`
6. Select option **A** to add your data node to the director.  
`A: Add this IA as a cluster host to a Director`  
`#: Remove this IA from a Director`  
`Q: Quit`  
`Select an option: A`
7. Enter the OpenVPN IP of the director.  
`Adding this host as a cluster master to the director.`  
`Enter the IP of the director you are trying to connect to:`

8. Enter the `eth1` IP address of the master node of your multibox cluster. This is the `eth1` IP address of the cluster master node.

This step requires the configuration package generated by the IA director for your IA data node. You must first configure the connection between your IA director and IA cluster. See [Connecting the IA Director to the IA Cluster](#) on page 94.



If no configuration package for your IA data node exists, then this error message appears in the CLI:

```
Required pay load from the Director not present
```

```
Press any key to continue
```

9. Select `Q` to save and quit.



## PART IV: Integrating with IA

---

This part covers the following topics:

- [Configuring PX Metadata through Web UI](#) on page 100
- [Synching PX and IA Metadata through CLI](#) on page 106
- [Integrating Threat Intelligence](#) on page 110
- [Integrating with IA for Alerts](#) on page 116
- [Integrating with the AX Series Appliance for Malware Analysis](#) on page 122
- [Pairing the NX Series Appliance and PX Series Appliance](#) on page 1



# CHAPTER 17: Configuring PX Metadata through Web UI

You can integrate the PX appliances with your Investigation Analysis appliance through the Investigation Analysis Web UI to configure the PX appliances as the metadata sources of your Investigation Analysis appliance. You can also specify the protocols (from the list of supported PX protocols) whose metadata is received by your IA appliance. You can perform the following tasks through the Investigation Analysis Web UI:

- [Viewing the PX Metadata Sources](#) below
- [Adding the PX Appliance](#) on the next page
- [Generating and Transferring SSH keys](#) on the next page
- [Configuring Metadata Synchronization](#) on page 103
- [Retransferring ACM Keys](#) on page 102
- [Updating the PX Metadata Selection](#) on page 103
- [Resynchronizing Network Configuration](#) on page 103
- [Deleting the PX Appliance](#) on page 104

## Viewing the PX Metadata Sources

To view the information of all the PX appliances connected to your Investigation Analysis appliance, navigate to **MANAGE > Configure System > PX Metadata** in the IA Web UI. The connected PX appliances act as metadata sources for your Investigation Analysis appliance. On the **PX Metadata** page, the following data is displayed:

- IP addresses of all the PX appliances.
- Metadata synchronization status.
- The network port over which the communication is established between the PX and the Investigation Analysis appliances.
- Metadata source directory of each PX appliance.
- Health status of each PX appliance: tunnel and rsync connection status.

# Adding the PX Appliance

Adding the PX appliances through the Investigation Analysis Web UI pairs the PX appliances with your Investigation Analysis appliance. Pairing a PX appliance with your IA appliance configures the PX appliance as a metadata source of your Investigation Analysis appliance.

**To add a PX series appliance to your Investigation Analysis appliance:**

1. Log in to the Investigation Analysis Web UI.
2. Navigate to **MANAGE > Configure System > PX Metadata**.
3. Click **ADD PX** in the upper-right corner of the page.
4. To configure the PX setup:
  1. Enter the PX appliance IP address.
  2. Set the PX appliance **Source Directory** and **Timeout** values.

By default, the source directory is set to **data**. The default timeout value is set to **5** seconds.
  3. Click **NEXT**.
5. To authenticate the pairing of the specified PX appliance with your Investigation Analysis appliance:
  1. Enter the PX admin credentials in the **user name** and **password** fields.
  2. Click **LOGIN & PAIR**.
6. In the **Metadata Selection** page, select the PX protocols whose metadata is received by your IA appliance.

By default, all the supported protocols are selected.
7. Click **Update**.

After you pair a PX appliance with your Investigation Analysis appliance, you need to generate the SSH keys in your Investigation Analysis appliance and transfer them to all the paired PX appliances. See [Generating and Transferring SSH keys](#) below.

## Generating and Transferring SSH keys

To enable the PX appliances (paired with your Investigation Analysis appliance) to communicate with your Investigation Analysis appliance, you need to generate the SSH keys in your Investigation Analysis appliance and transfer them to all the paired PX appliances. Your Investigation Analysis appliance can then receive the PX search data.

**To generate and transfer the SSH keys from your Investigation Analysis appliance to all the connected PX appliances:**

1. Log in to the Investigation Analysis Web UI.
2. Navigate to **MANAGE > Configure System > PX Metadata**.
3. Click **GENERATE SSH KEYS**.
4. If the SSH key already exists, the following message is displayed:  
/data/config/ia/keys/<iatunnel\_tunnel> already exists. Do you want to overwrite?. Click **OK**.
5. In the **PX Login** screen, enter the administrator credentials for the displayed PX appliance to authenticate the transfer of the SSH key to the PX appliance and click **NEXT**.
6. Continue to enter the administrator credentials for all the other PX appliances that are displayed in the wizard to authenticate the transfer of the SSH keys to all the paired PX appliances.
7. Click **LOGIN & TRANSFER**.

A confirmation message is displayed if the transfer is successful.

## Retransferring ACM Keys

You can generate new ACM keys and transfer them to any paired PX appliance to reestablish the connection between your Investigation Analysis appliance and the PX appliance.

**To generate and transfer the ACM keys from your Investigation Analysis appliance to any connected PX appliance:**

1. Log in to the IA Web UI.
2. Navigate to **MANAGE > Configure System > PX Metadata**.
3. Click the **gear** icon ( in the **Actions** column) corresponding to the PX appliance to which you wish to retransfer the ACM keys from your Investigation Analysis appliance.
4. Click **Retransfer ACM Key**.
5. On the **PX Login** screen, enter the administrator credentials for the PX appliance to authenticate the transfer, and then click **LOGIN & TRANSFER**.

A confirmation message is displayed if the transfer is successful.

# Configuring Metadata Synchronization

To configure the metadata synchronization of the PX appliances paired with your Investigation Analysis appliance:

1. Log in to the Investigation Analysis Web UI.
2. Navigate to **MANAGE > Configure System > PX Metadata**.
3. To enable or disable the metadata synchronization of all the PX series appliances connected to your Investigation Analysis appliance, toggle the **Metadata sync** switch to **ON** or **OFF**, respectively.

## Updating the PX Metadata Selection

You can specify the protocols (from the list of supported PX protocols) whose metadata is received by your Investigation Analysis appliance.

To update the PX metadata selection:

1. Log in to the Investigation Analysis Web UI.
2. Navigate to **MANAGE > Configure System > PX Metadata**.
3. Click the **gear** icon (under the **Actions** column) corresponding to the PX appliance to select the appropriate protocols whose metadata is received.
4. Click **Update Metadata**.
5. In the **PX Login** screen, enter the administrator credentials for the PX appliance to authenticate the metadata selection, and then click **LOGIN & Update**.
6. In the **Metadata Selection** page, select the PX protocols corresponding to which the metadata is transferred to your Investigation Analysis appliance, and then click **UPDATE**.

A confirmation message is displayed if the update is successful.

## Resynchronizing Network Configuration

To resynchronize the network configuration of any connected PX appliance from your Investigation Analysis appliance:

1. Log in to the Investigation Analysis Web UI.
2. Navigate to **MANAGE > Configure System > PX Metadata**.

3. Click the **gear** icon under the **Actions** column corresponding to the PX appliance to which you wish to resynchronize the network configuration from your Investigation Analysis appliance.
4. Click **Re-sync Network Configuration with PX**.
5. In the **PX Login** screen, enter the administrator credentials for the PX appliance to authenticate the resynchronization of network configuration and click **LOGIN & SYNC**.

A confirmation message is displayed if the network resynchronization is successful.

## Deleting the PX Appliance

**To disconnect any PX appliance paired with your Investigation Analysis appliance:**

1. Log in to the Investigation Analysis Web UI.
2. Navigate to **MANAGE > Configure System > PX Metadata**.
3. Click the **gear** icon (under the **Actions** column) corresponding to the PX appliance that you wish to disconnect from your IA appliance and select **Delete**.
4. Click **OK** to confirm.



# CHAPTER 18: Synching PX and IA Metadata through CLI

To synch the PX Series metadata with the IA Series, you will need to set up the configuration on both platforms. The IA appliance has the keys required for the PX to communicate with the IA. You must transfer the keys to the PX. This allows the PX to communicate with IA so that it can receive PX search data.



Use care when entering the PX appliance's IP address or FQDN during the IA configuration. If you enter the wrong IP address or FQDN you will transfer the files to the wrong PX appliance. If you enter an invalid IP address FQDN you will have to wait for the appliance to time out before you can try again.



Only the IA's Eth0 interface is supported for cluster communications.

## Prerequisites

You will need:

- Shell and CLI access to the PX
- Shell and CLI access to the IA
- PX appliance's IP address or FQDN
- Password for the PX NPSCP account

## Configure the IA

To configure the connection between your IA and PX appliance, perform this procedure on your IA Series appliance. After this procedure is complete, you will see the PX appliance's IP address at the top of the Metadata menu.

**To configure the IA to communicate with the PX:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:

```
$ ssh npadmin@10.1.0.1
```

or

```
$ ssh npadmin@exampleFQDN
```

2. Enter privileged mode:

```
npadmin@ia> enable
```

3. Enter the npadmin password. The password can be 5 to 24 characters long.

```
[sudo] password for npadmin: <password>
```

4. Enter configuration mode:

```
npadmin@ia# configure system
```

5. Enter the metadata menu:

```
hostname(config) # metadata
```

You will see the following:

```
Metadata Sync: Off
```

```
Connected PXes:
```

```
T) Toggle metadata import on/off
```

```
A) Add PX
```

```
#) Remove PX
```

```
K) Retransfer ACM Key
```

```
G) Regenerate and transfer SSH Keys
```

```
H) Re-sync Network Config with PX
```

```
Q) Quit
```

6. Select A to add your PX appliance.

```
Please enter selection: A
```

7. Enter the following information to connect your PX appliance:

- a. Enter the PX appliance IP address or FQDN:

```
Enter the PX address:10.1.0.1
```



When using FQDNs for any configuration setting, you must first configure a valid DNS server. See [Chapter 4: Network Configuration](#) for more details.

- b. Enter yes to confirm this connection with the PX appliance:

```
Are you sure you want to continue connecting (yes/no)? yes
```



You will see this questions, only if this is the first time a connection is established with this PX appliance.

- c. Enter the npadmin login credentials for your PX appliance:

Enter the 10.1.0.1 user(npadmin):

Enter password for npadmin:



The admin account must have SUDO and API access.

- d. Customize the PX appliance source directory:

Customize source directory on PX(data):



You can customize the PX appliance source directory or keep the source directory set to data.

- e. Select A to add another PX appliance or Q to quit.



## CHAPTER 19: Integrating Threat Intelligence

Threat intelligence data is made available to the IA appliance through Mandiant Threat Intelligence indicators of compromise (also referred to as indicators or IOCs) and custom intel feeds in Structured Threat Information Expression (STIX) or an OpenIOC format. The IA search engine will use the new IOCs to search indexed metadata and identify threat matches. If a threat match is found, IA will automatically generate a THREAT\_INTEL alert in the Web UI, along with detailed threat intelligence about the attacker and a full Intel report.

Use the IA CLI to configure automatic downloads of the latest Mandiant Threat Intelligence indicators of compromise (IOCs) to your IA appliance and enable your custom IOC or STIX intel feeds.

### Integrating with Mandiant Threat Intelligence

The IA and Mandiant Threat Intelligence integration allows you to scheduled automatic downloads of Mandiant Threat Intelligence indicators of compromise (IOCs) to the Investigation Analysis appliance. The IA search engine will use the new IOCs to search indexed metadata and identify threat matches. If a threat match is found, IA will automatically generate a THREAT\_INTEL alert in the Web UI, along with detailed threat intelligence about the attacker and a full Intel report.

#### Prerequisite

Mandiant Threat Intelligence license keys are required to connect your Investigation Analysis appliance to Mandiant Threat Intelligence.

## Connection Modes

The IA and Mandiant Threat Intelligence integration provides two connection modes for your IA Director and datanode and : Full Mode and Index Only Mode.

| Connection Mode | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full Mode       | The IA appliance (data node or Director node) downloads Mandiant Threat Intelligence indicators, searches for threat matches, and stores the results.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Index Only Mode | <p>The IA appliance (data node or Director node) only stores the match results it receives from an IA appliance in Full Mode. IOC downloads and threat-match searches only occur on the IA appliance in Full Mode.</p> <p> When your IA data node is configured in Index Only Mode, the IA Director must be configured in Full Mode. This configuration allows the data node to forward all IOC requests to the IA Director, which submits all IOC requests from the data node to Mandiant Threat Intelligence, searches for threat matches, stores the results, and pushes the results to the data node.</p> <p>In an IA cluster, all data nodes must be configured to Index Only Mode and the Director must be configured to Full Mode.</p> |

## Configuring the IA to Mandiant Threat Intelligence Connection

Use the CLI to configure the Mandiant Threat Intelligence keys required to connect your Investigation Analysis appliance and Mandiant Threat Intelligence platform.

**To configure your IA and Mandiant Threat Intelligence connection:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable

3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter Threat Intel Configuration mode:  
hostname(config)# threatintel
6. Select K to configure the Mandiant Threat Intelligence keys:  
Enter your choice: K



Contact FireEye support@fireeye.com to request your Mandiant Threat Intelligence API key and Secret key.

7. Enter your Mandiant Threat Intelligence API Key provided by FireEye Support.  
Enter FireEye provided API Key for Mandiant Threat Intelligence:
8. Enter your Mandiant Threat Intelligence Secret Key provided by FireEye Support.  
Enter FireEye provided Secret Key for Mandiant Threat Intelligence:



After your IA and Mandiant Threat Intelligence connection is established, the Mandiant Threat Intelligence indicator search is enabled by default.

9. Enter X to save the Mandiant Threat Intelligence keys and exit.  
Enter your choice: X

**To configure the Run Mode for your IA datanode and IA Director:**

1. From the Mandiant Threat Intel menu, enter option R to configure the run mode for your IA datanode:  
Enter your choice: R
2. Select 0 to configure your IA appliance in Full Mode or select 1 to configure your IA appliance in Index Only Mode:  
(0) Data Node Full Mode—In this mode Data Node will download the indicators, perform the search and store the results.  
(1) Data Node Index Only Mode—In this mode Data Node will only store the results, searches will happen on the Director. Any request to Mandiant Threat Intelligence for context will be forwarded to the director. Director needs to be running in Director Full Mode for this mode to work correctly.

Select the mode you wish to run TIS in: 0

3. Select Q to return the previous menu.

# Integrating Custom Intel Feeds

FireEye Threat Intel Service allows you to use the Investigation Analysis CLI to create feed names and the IA Web UI to upload custom intel feeds in Structured Threat Information Expression (STIX) or OpenIOC format to your IA appliance and map each feed to a specific feed name. You can also enable, disable, and delete your custom intel feeds using the Investigation Analysis CLI. IA will parse the file into IOCs for MD5, URL, IPs, JA3 and JA3S hash values. See the *Investigation Analysis API Guide* or the *Investigation Analysis User Guide* for more information.

Follow the steps in this section to integrate your custom intel feeds with your IA appliance.

## Prerequisite

- IA software 1.4.0 or higher

## Configuring a Custom Intel Feed

Use the CLI to configure your custom STIX or IOC intel feed and create a feed name for your mapped STIX or OpenIOC file, enable, or disable your custom intel feed.

**To create your custom intel feed name:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.  

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:  

```
npadmin@ia# configure system
```
5. Enter Threat Intel Configuration mode:  

```
hostname(config)# threatintel
```
6. Select F to configure a custom intel feed for IOC/STIX file:  

```
Enter your choice: F
```



Custom intel feeds in STIX and OpenIOC format are supported in IA 2.1 only.

7. Select A to add a custom intel feed.

(A) Add custom intel feed for IOC/STIX

(#) Toggle/Delete custom intel feed

(X) Go back to previous menu

Enter your choice: A

8. Enter the feed name:

Enter the feed name to add to the system:



Feed names must be greater than 4 characters and less than 32.

#### To enable or disable a custom intel feed:

1. From the `threatintel` menu, enter the # (number) associated with the custom threat intel feed you want to enable or disable.

Enter your choice:

2. Select T to toggle the intel feed status from enable to disable.

(D) Delete FeedName to the system

(T) Toggle FeedName's status

Enter your choice:

3. Click **Enter** to save the change:

Feedname status toggled

Press enter to continue.

4. Select X to go back to the previous menu.

Enter your choice: X

#### To delete a custom intel feed:

1. From the `threatintel` menu, enter the # (number) associated with the custom threat intel feed you want to enable or disable.

Enter your choice:

2. Select D to delete the intel feed.

(D) Delete FeedName to the system

(T) Toggle FeedName's status

Enter your choice:

3. Select y to delete the intel feed from your Investigation Analysis appliance:

Are you sure you want to delete the feedname y/n ? y

Feedname has been deleted from the system.

Press enter to continue.

4. Click **Enter** to continue.
5. Select x to go back to the previous menu.  
Enter your choice: x

## CHAPTER 20: Integrating with IA for Alerts

There are two ways to integrate with another Trellix appliance to receive alerts. This section covers the following topics:

- [Alert Poll Service](#) on the next page
- [Alert HTTP Listener](#) on page 118

### Configuring Alert Aggregation in the CLI

In the alert aggregation menu, there are two ways to receive alerts:

- [Configuring a poll service](#)
- [Configuring an HTTP server](#)

The poll service will poll the device at a specified period of time in seconds. To use this option, you need to create an API user on each Trellix appliance.

To create an API user, see the *CM Series WSAPI Guide* for the CM, NX, and EX Series appliances, and the *REST API Guide* for the Endpoint Security server.



When using the IA with the CMS WSAPI, the CMS timezone must be set to UTC.

If CMS is using a different timezone, then you should use the HTTP server method to receive alerts.

Specify the IP address or FQDN of the device from which to receive the alerts and the polling interval in seconds. By default, the polling interval is 35 seconds.

To configure the HTTP server to listen for alerts, you specify the username, password, and URL for the device to post the alert. The matching configuration must be entered into the alerting device to tell it where to post its alerts.



The PX alert sources do not need to be configured. The alerts are transferred along with the layer 7 metadata from the PX over the RSYNC channel.



The default configuration in NX is fenet proxy enabled. If fenet proxy is disabled in the NX, the fenotify preference ssl cipher list needs to be changed from Original to Compatible. When fenet proxy is disabled, the Original cipher list is not compatible with the fenotify preference ssl cipher list in IA.

If a CM Series platform in your environment receives alerts from other Trellix appliances, the IA can be configured to pull alerts from the CM.

The IA can receive up to 5,000 alerts per second from the PX.



The IA can receive up to 2,000 alerts per second from the CM, NX, and EX.

The IA can receive up to 1,000 alerts per second from the HX.



You must have a PX Series appliance deployed in your network in order to pivot to the PX or reconstruct PCAP for alerts generated from other FireEye appliances, including NX, EX, HX, and CM Series.

## Alert Poll Service

You can set up the IA to retrieve alerts from other appliances by setting up the Poll Service. You must configure the Trellix appliance sending the alerts and then the IA appliance.



Pulling alerts from NX using WSAPI for IA is not supported.

## Step 1: Configure the Trellix Appliance

You can configure the CM, AX, EX, NX or Endpoint Security server for the IA Poll Service.

**To configure Trellix appliance for the IA Poll Service:**

1. Navigate to the Web UI.
2. Click the **Settings** tab.
3. Click **User Accounts** on the sidebar.
4. Under **Add New User** or **Update User**, enter the **User Name**, which is the login name for the user. It must be between 1 and 16 characters, is case sensitive, and must be unique. Use only letters, numbers, and underscores.
5. Select the **Api Analyst** role from the Role list.
6. Click **Update User**.

## Step 2: Configure the IA Appliance

The IA Poll Service is configured using the CLI.

**To configure the IA for the Poll Service:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter the alert aggregation menu:  
alertaggregator
6. At the alert menu prompt enter the letter T to enable the alert listener.
7. Type A to add a new endpoint. Enter the poll service endpoint configuration:  
username : iatest  
ip\_addr or FQDN : 10.41.131.130  
polling\_frequency : 35  
port: 3000 (HX) or 443 (WSAPI)  
api\_type: HX or WSAPI

## Alert HTTP Listener

You can set up the IA to receive alerts from other appliances by setting up the HTTP Listener. You must configure the IA and then the other appliance(s).

The IA HTTP listener is configured using the CLI.

The IA can receive alerts from the following Trellix appliances:



- NX
- EX
- CM

Endpoint Security does not support the HTTP Listener service with IA.

## Step 1: Configure the IA Appliance

To configure IA appliance for the HTTP Listener:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.  

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:  

```
npadmin@ia# configure system
```
5. Enter the alert aggregation menu:  

```
alertaggregator
```
6. At the alert menu prompt enter the letter T to enable the alert listener.
7. Type H to edit the listener configuration.
8. Enter the HTTP server configuration:  

```
Username: alertuser
```

```
Password: <hidden>
```

Save the username and password. You will need it for step 2 below.

## Step 2: Configure the Trellix Appliance

To configure Trellix appliance for the HTTP Listener:

1. Navigate to the Web UI.
2. Click the **Settings** tab.
3. Click **Notifications** on the sidebar.
4. Confirm that every notification type is configured for HTTP.
5. Select the **http** link in red to open the HTTP Server Listing settings.
6. Add a **Name** and click on **Add HTTP Server**.
7. Check the **Enabled** check box.
8. Add the **Server Url**. The URL for IA is **https://<IPADDR>/alert** or **https://<FQDN>/alert**. For example, an IA appliance with IP address of 10.10.10.10, the Server URL would be **https://10.10.10.10/alert**.
9. Check the **Auth** check box.

10. Add the username and password. This is the username and password that you set in the IA appliance in step 1 above.
11. Under **Delivery**, select Per Event.
12. Check the **SSL Enable** check box.
13. Under **Default Provider**, select Generic.
14. Under **Message Format**, select JSON Normal.
15. Click the **Update** button.

## Step 3: Send a Test Alert

### To send a test alert:

1. Navigate to the Web UI.
2. Click the **Settings** tab.
3. Click **Notifications** on the sidebar.
4. Trigger an alert by clicking **Test-Fire**.
5. You will see a confirmation at the top of the web browser.

### To view the test alert on the IA appliance:

1. From a web browser, navigate to the IA dashboard.
2. Click on the Alert Summary view to open the alerts page.
3. You see a high priority alert.



# CHAPTER 21: Integrating with the AX Series Appliance for Malware Analysis

The Investigation Analysis appliance can extract a suspicious file from the network session and send it directly to the AX Series appliance for analysis. You must integrate the IA Series appliance with the AX Series appliance for malware analysis.

For more information about performing analysis, see the *Investigation Analysis User Guide* and the *AX Series Threat Management Guide*.

**To configure the IA for malware analysis on the AX Series appliance:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.  

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:  

```
npadmin@ia# configure system
```
5. Enter the file analysis menu:  

```
npadmin@ia# fileanalysis
```
6. Select A and enter the AX's IP address or the FQDN.



When using FQDNs for any configuration setting, you must first configure a valid DNS server. See [Chapter 4: Network Configuration](#) for more details.

7. Select U and enter the IA's api\_analyst username.
8. Select P and enter the password for the api\_analyst username.

9. Select L to change the amount of files to send at one time to the AX. The default is 5.  
The range is 1-10.
10. Select X to exit.

# CHAPTER 22: Integrating with the Endpoint Security Server for Hostname Data

The IA Series appliance can integrate, or pair, with an Endpoint Security Server to index host information from private IP addresses monitored by endpoints. After the two appliances are paired, you can use KLISH or the API to index hostnames at a customized frequency. Host destination and source can then be used to retrieve usernames associated with them in the Web UI. Pairing requires Endpoint Security version 4.8 or later.

This section includes the following:

- [Integrating with the Endpoint Security Server for Hostname Data](#) above
- [Verifying the Endpoint Security Server and IA Integration](#) on the next page
- [Changing IA and Endpoint Security Server Configuration Settings After Integration](#) on page 126
- [Retrieving Metadata from a Paired Endpoint Security Server](#) on page 128

 Pairing an Endpoint Security Server to your IA Series appliance may reduce the performance of the IA.

## Integrating the Endpoint Security Server and IA Series Appliance

You can integrate multiple Endpoint Security servers to your IA Series appliance through KLISH or the API. For integration steps using the API, see the *IA Series API Guide*.

**To integrate your HX and IA appliances:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  

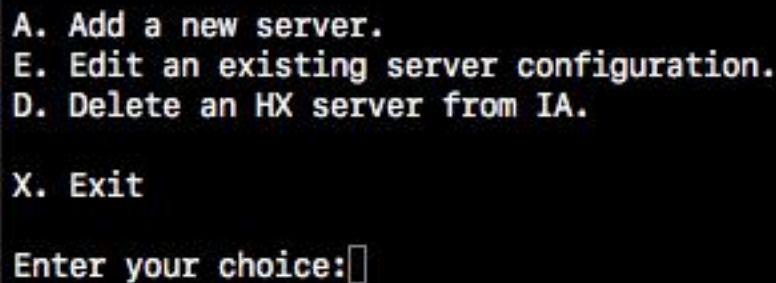
```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```

3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
  4. Enter configuration mode:  
npadmin@ia# configure system
  5. Enter the HX configuration menu:  
npadmin@ia (config)# hx-gw
- You see the following menu:



```
A. Add a new server.
E. Edit an existing server configuration.
D. Delete an HX server from IA.

X. Exit

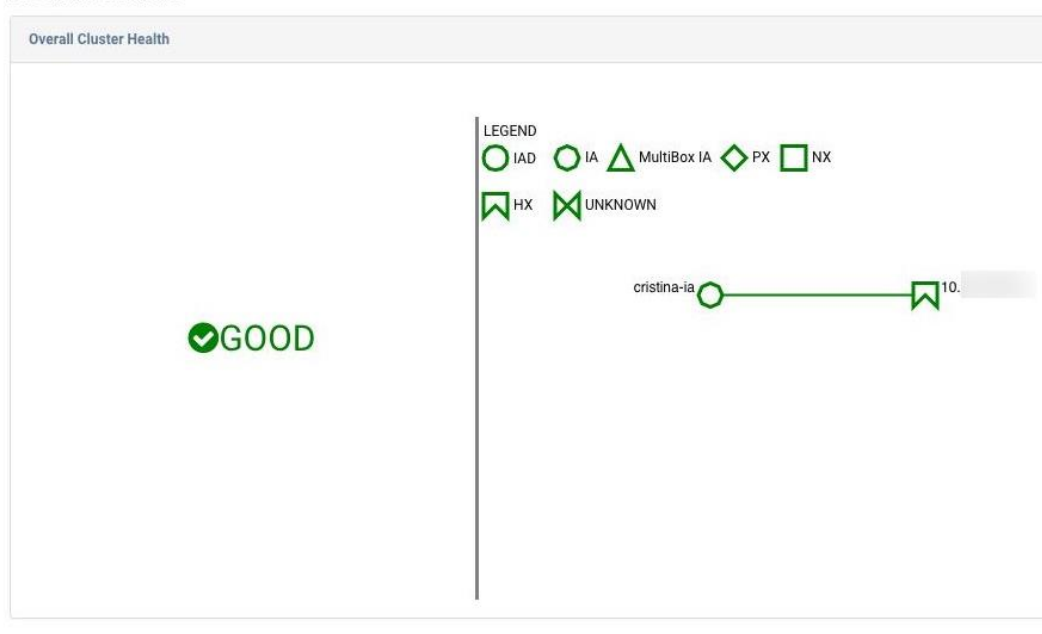
Enter your choice:[]
```

6. Enter A to pair a new server to the IA appliance:
  7. Enter the IP address of the server you want to pair to the IA.
  8. Enter the port number of the IA appliance. The default port value is 3000.
  9. Enter the credentials for the Endpoint Security Server.
  10. Disable SSL verification:  
false
-  Enabling SSL verification in a self-signed certificate HX prevents the HX from connecting to the IA.
11. Press Enter. When pairing is complete, you return to the HX Configuration Menu.

## Verifying the Endpoint Security Server and IA Integration

After you pair your Endpoint Security Server to your IA appliance, the server will appear in the Health Status page of the IA Web UI. The following image shows an example of a properly connected Endpoint Security Server.

## Health Status



For more information on the Health Status page, see the chapter "Monitoring the IA and Paired Appliances" chapter of the *IA Series User Guide*.

# Changing IA and Endpoint Security Server Configuration Settings After Integration

By default, the IA retrieves metadata from the Endpoint Security Server every 30 minutes by default and the Server retrieves data from Agents every 30 minutes. For information about configuring your Server's polling frequency, see the "Configuring Automatic Triage Settings" topic of the *Endpoint Security Server User Guide*. Trellix recommends configuring your IA to index metadata from the Server every 90 minutes in order to capture the most recent information without overwhelming the IA. If the IA indexes data from the Server too frequently, you may experience significant performance issues. The indexing rate can be configured after you pair the two appliances.

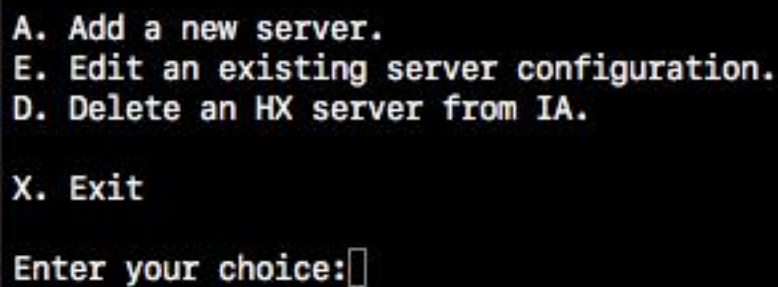
You can also change Endpoint Security Server credentials and SSL verification after integration.



The IP address of a paired Endpoint Server cannot be changed after integration. If an incorrect IP address has been integrated with the IA, FireEye recommends deleting the device and re-adding it with the appropriate IP address.

To configure the indexing rate in KLISH:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter the HX configuration menu:  
npadmin@ia (config)# hx-gw  
You see the following menu:



```
A. Add a new server.
E. Edit an existing server configuration.
D. Delete an HX server from IA.

X. Exit

Enter your choice:[]
```

6. Edit an existing server configuration:  
E

- Each paired HX is assigned a number that appears above its IP address in the HX Server Configuration menu. Enter the index of the paired HX you want to edit. For example, if you only have one paired HX appliance, enter 1.

The **Edit Device Configuration** menu appears:

```
Edit Device Configuration:

ip : 10
username : npadmin
sslVerify : False
hostPollEnabled : True
hostPollInterval : 30m
port : 3000

Note: IP of the device cannot be changed.
It is advised that you delete the device and re-add it with new IP

U. Edit Username
P. Edit Password
T. Toggle the Polling
O. Change polling interval for HX
S. Toggle SSL Verify

X. Save and Return
C. Cancel and Return

Enter your choice:
```

- Enter your choice and edit the configuration. Press enter to apply your change.
- Enter X to save your changes.

## Retrieving Metadata from a Paired Endpoint Security Server

You can retrieve usernames associated with hostnames on-demand in the IA Web UI for one IP address at a time. IP address and hostname information is automatically indexed when the IA syncs up with the server. To configure how often indexing occurs, see [Changing IA and Endpoint Security Server Configuration Settings After Integration](#) on page 126.

**To retrieve usernames from an Endpoint Security Server:**

- In the IA Web UI, search for the IP address of the paired server you want to filter metadata from.
- Scroll to the **Event Table** in the Dashboard.

3. Above the **Event Table**, in the button panel, click the **Edit Columns** button. For more information about the Event Table, see the "The Dashboard" chapter of the *IA Series User Guide*.
4. Select **destinationHostName** or **sourceHostName** from the list of filters. The option you select appears as a new column in the Event Table.
5. In the destinationHostName or sourceHostName column, click the caret next to the hostname you want.
6. Click **getUsername**. A pop-up window appears with the username associated with the hostname indexed from the server appliance.

## PART V: User Management

---

This part covers the following topics:

- [Authentication in the CLI](#)
- [Managing User Accounts](#)
- [Roles](#)



## CHAPTER 23: Authentication in the CLI

The IA uses PAM authentication by default. To select a different authentication, choose from the options below.



If a remote user logs in with the same username as a local user who is already logged in, the remote user is assigned the same role as the local user. When the remote user logs in and the local user with the same name is not present on the IA, then the remote user is assigned the analyst role.

To enable TACACS, RADIUS, AND LDAP authentication for user logins, follow steps below, then choose the option that best suits your needs:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Open the PX authentication configuration:  
`npadmin@hostname(config)# authentication`
6. Type 1 to select which authentication type to use (PAM, LDAP, RADIUS, TACACS+, or Active Directory) and enter the number corresponding to your selection.
7. Type 2 to configure the selected authentication method.

To configure RADIUS and TACACS:



Only IP addresses are permitted for TACACS+ or RADIUS servers. DNS hostnames are not supported for TACACS+ or RADIUS servers.

1. Press 1 to enter a space-separated list of RADIUS/TACACS servers.
2. Press 2 to enter the shared secret to communicating with the servers.

To configure LDAP, chose one of the following three options:

- Press 1 to enter a space-separated list of LDAP servers to authenticate against.
- Press 2 to enter the Object Pk.
- Press 3 to enter the Base DNS for user lookup

# CHAPTER 24: Configuring SAML Authentication

You can enable SAML authentication on your Investigation Analysis appliance (service provider), so that remote users are authenticated by a SAML server (identity provider), before the users can access the Investigation Analysis Web UI.

## Prerequisites:

- Access to the SAML server (IDP)
- Configure the SAML server for Investigation Analysis application

## To configure SAML authentication on your Investigation Analysis appliance:

1. Log into the CLI on your Investigation Analysis appliance.

2. Enter privileged mode:

```
hostname > enable
```

3. Enter the default admin password:

```
hostname # hammerhead
```

4. Enter configuration mode:

```
hostname # configure system
```

5. Enter the SAML Config menu:

```
npadmin@hostname(config)# sam1
```

The **SAML Config** menu is displayed.

```
= SAML Config
```

```
=====
```

```
Configure SAML Authentication
```

1. State [allowed]
2. Attribute for username [sunil]
3. IDP metadata
4. Download SP metadata
5. TLS settings

Select a menu choice by number or an action by letter

```
X - Exit menu
```

```
>
```

6. Press 1 to change the state of the SAML authentication.

7. In the displayed prompt, press **2**, **3**, or **4** to change the state of the SAML authentication to **allowed**, **required**, or **required-force** respectively.

= Choose SAML state

=====

- 1) disabled
- 2) allowed
- 3) required
- 4) required-force

- **disabled**: This mode allows the users to authenticate only through IA. This is the default mode.
- **allowed**: This mode allows the users to authenticate either through IA or SAML.
- **required**: This mode allows the users to authenticate only through SAML.
- **required-force**: This mode automatically redirects the users to the SAML authentication page. As long as the IDP session remains active, you cannot log out of your IA appliance.

8. Press **2** to set the attribute for the user name. Select a letter corresponding to the action you wish to perform.

The user name attribute is used to get the username of the logged-in user. By default, the username is read from the NameID attribute.

9. Press **3** to configure the IDP metadata settings for SAML authentication:

- a. To download the IDP metadata file to your Investigation Analysis appliance, press **1** and enter the metadata fetch URL at the prompt.

You need to get this URL from the SAML server configuration settings.

- b. (Optional) To upload the IDP metadata file to your Investigation Analysis appliance, press **3** and enter the filename of the IDP metadata file that you downloaded and is made available in the transfer directory.

- c. To set the IDP connection timeout, press **2**.

10. Press **4** to download the SP metadata file to the transfer directory. Use SCP to copy the SP metadata file to your Investigation Analysis appliance.

You need to upload this XML file to the SAML server.

11. Press **5** to configure the TLS settings for IDP connection for metadata download.

These TLS settings are used only while downloading the IDP metadata and these validate the SSL certificate of the IDP while connecting to it.

12. Press **S** to save the changes and exit.

**Post-requisite:** Configure the attributes for the users in the SAML server. We have the following roles: "appliance.role", "px.role" and "ia.role". The "appliance.role" can be used if

the roles for a user are the same for both IA and PX. The "ia.role" provides a finer role assignment for a IA appliance. The possible values for these attributes are "uiapi" and "wheel".

A user will now see a SAML option in the login screen. When a user clicks **Login with SAML**, the sign-in screen of the SAML server is displayed, where the user needs to enter the SAML account credentials to access the Investigation Analysis Web UI.



## CHAPTER 25: Managing User Accounts

User accounts must be created before they can log in to the appliance. User accounts include the following information:

- **User Name**—The name with which the user logs in to the appliance.
- **Role**—The role that determines what the user can do on the appliance. For details, see Roles.
- **Password**—The password that along with the user name, authenticates the user and permits access to the appliance.

### Roles

Adding a role lets you set the role ID. Permissions are added to the role.

| Roles            | Description                                         |
|------------------|-----------------------------------------------------|
| Shell (w/Admin)  | Access to the shell and enable commands.            |
| Shell            | Access to the shell commands only.                  |
| UI/API           | Access to the Web UI only.                          |
| UI/API and Shell | Access to the Web UI and shell commands.            |
| All              | This includes all roles (shell, admin, and UI/API). |

## Adding a User in the CLI

1. Log in to the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the admin password:  
`[sudo] password for <npadmin>: <password>`
4. Enter configuration mode:  
`hostname # configure system`
5. Enter the user menu:  
`npadmin@hostname(config)# users`
6. Enter 1 to add a user.
  - a. Enter the user name.
  - b. Enter the full name.
  - c. Set the permissions level for the user. See [Roles](#) on the previous page for more information.
  - d. Confirm whether the values displayed are correct: type `y` to confirm and move to the next setting; type `n` to return to the users menu.
  - e. Set the new user as remote or non-remote: type `y` to specify remote; type `n` to specify non-remote.

A remote or dummy user is a prerequisite for RADIUS/TACACS+ authentication.
  - f. Set the password for a non-remote user.
  - g. Type `y` to confirm the user settings.

## Deleting a User in the CLI

1. Log into the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Enter configuration mode:  
`hostname # configure system`

5. Enter the user menu:  
`npadmin@hostname(config)# users`
6. Select option 2 to delete a user.
  - a. Enter the user name that you want to delete.
  - b. Confirm that you want to delete the user.

## Editing a User in the CLI

1. Log into the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Enter configuration mode:  
`hostname # configure system`
5. Enter the user menu:  
`npadmin@hostname(config)# users`
6. Select option 3 to edit the user.
  - a. Enter the user name that you want to edit.
  - b. Set the permissions level for the user. See [Roles](#) on page 138 for more information.
  - c. Confirm the user settings.

## Resetting the Passwords for npadmin, npscp, and IPMI Admin Accounts

1. Log into the CLI on the IA.
2. Enter privileged mode:  
`hostname > enable`
3. Enter the default admin password:  
`hostname # hammerhead`
4. Enter configuration mode:  
`hostname # configure system`

5. Enter the user menu:

```
npadmin@hostname(config)# users
```

6. You see the following:

```
npadmin@ia123> enable
[sudo] password for npadmin:
npadmin@ia123# configure system
npadmin@ia123(config)# users
```

| UID   | Name  | Roles |
|-------|-------|-------|
| ----- | ----- | ----- |
| ----- |       |       |
| ----- |       |       |
| ----- |       |       |

- ```
1: Add User
2: Delete User
3: Edit User
4: Change npadmin's Password
5: Change npscp's Password
6: Change IPMI ADMIN user password
```

```
Select which option you would like to change
using the index number. Enter "q" to exit:>
```

7. Select option 4 to edit the npadmin's password.
- Confirm that you would like to change the password.
 - Enter the new password.
 - Confirm the password.
8. Select 5 to edit the npscp user password
- Confirm that you would like to change the password.
 - Enter the new password.
 - Confirm the password.
9. Select 6 to change the IPMI Admin user password.
- Confirm that you would like to change the password.
 - Enter the new password.
 - Confirm the password.
10. Enter q to exit.

CHAPTER 26: Controlling User Access Using VLAN/QinQ RBAC

You can control the visibility of network metadata and packet captures (pcap) on your network by mapping Active Directory (AD) groups to specific ranges of VLANs or QinQ tags. Users who belong to particular AD groups can query traffic only within specified VLAN or QinQ ranges. You can also add AD groups to an exception list to allow the group users to access all traffic that is captured.

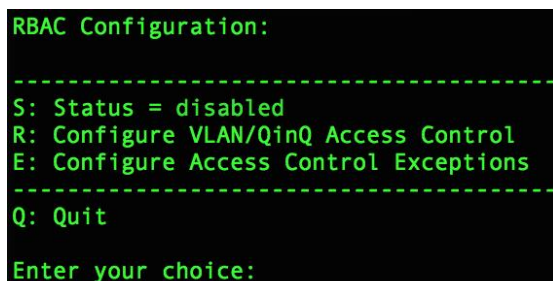
This feature has the following requirements:

- VLAN/QinQ RBAC must be configured on every IA node that is accessed by users. If all IA users only use the IA director, the VLAN/QinQ feature must be configured on the IA director.
- All traffic **MUST** be tagged with either VLAN or QinQ tags. Traffic without tags will be "invisible traffic" that cannot be viewed by any user.
- A user **MUST** match exactly one AD group mapping. If there are no mappings found, then the search will result in an error (unless the user's group is in exception list). If there is more than one matching mapping, the VLAN/QinQ selection for the user is undefined (first match wins).

RBAC Configuration Menu

This feature requires mapping Active Directory Groups to specific ranges of VLANs or QinQ tags. The mappings are defined in the RBAC Configuration menu in the IA CLI.

```
enable
configure system
rbac
```



```
RBAC Configuration:
-----
S: Status = disabled
R: Configure VLAN/QinQ Access Control
E: Configure Access Control Exceptions
-----
Q: Quit
Enter your choice:
```

Three options are listed:

- Enter S to enable to the feature
- Enter R to specify the VLAN and QinQ range to AD group mappings
- Enter E to allow exceptions to the access control specifications

Mapping VLAN/QinQ Ranges to AD Groups

1. In the RBAC Configuration menu, enter option R.

```
RBAC Configuration:
1. VLAN Access Control Policies = 1
2. QinQ Access Control Policies = none
3. Add Access Control Policies
-----
Q: Save changes and exit
C: Cancel changes and exit
```

To list the current VLAN Access control policies, select option 1. To list the existing QinQ Access Control policies, select option 2.

2. Enter 3 to add a new policy.

```
VLAN Access Control Policies = 1
-----
1. eng
   101-101,2049-2049
-----
C: Cancel changes and exit
Enter your choice: █
```

3. Enter the desired mapping in the following format:

- *VLAN mapping:* <group name>, <empty>, <vlan tag>-<vlan tag>
For example: eng,,101-101
- *QinQ mapping:* <group name>, <outer tag>, <inner tag>-<inner tag>
For example: eng-dev,1025,2050-2050

```
Enter up to 10 lines at a time below in CSV format. Enter Ctrl-D to save
VLAN Ex.] <group name>, <empty>, <vlan tag>-<vlan tag>
QinQ Ex.] <group name>, <outer tag>, <inner tag>-<inner tag>

eng,,101-101
eng,,2049-2049
eng-dev,1,102-102
eng-dev,1025,2050-2050
VPNUsers,1,103-103
```

4. To add multiple access control policies at one time, copy and paste up to 10 rules. Each line should be in CSV format and use the syntax provided in the examples.
5. When finished editing, enter Ctrl-D to save your changes.
6. Enter Q on the next screen to commit your changes.
To modify or delete a VLAN or QinQ to group mapping, select the entry number in the VLAN Access Control Policies menu (option 1) or the QinQ Access Control Policies menu (option 2).
7. When all access controls have been specified, enter S in the RBAC Configuration menu to enable the feature.

Excluding AD Groups from VLAN/QinQ Access Restrictions

You can exclude an AD group from VLAN/QinQ RBAC, allowing the group's users to see all traffic.

1. In the top-level RBAC Configuration menu, enter E.

```
RBAC Configuration:
-----
S: Status = disabled
R: Configure VLAN/QinQ Access Control
E: Configure Access Control Exceptions
-----
Q: Quit
Enter your choice:
```

2. Enter the name of the AD group you want to exclude.



IMPORTANT: Users in the excluded groups will be allowed to see all traffic captured.

Appendices

This part includes the following section:

- [Common Access Card \(CAC\) for Certificate Authentication](#) on the next page

APPENDIX 26: Common Access Card (CAC) for Certificate Authentication

This section covers the following information:

- [About CAC for Certificate Authentication](#) below
- Configuring a CA Certificate Bundle
- [Enabling or Disabling CAC/PIV for Certificate Authentication](#) on page 152
- [Checking for Revoked Certificates](#) on page 153
- [Configuring the User Attributes for Certificate Authentication](#) on page 160
- [Configuring LDAP for Authorization](#) on page 163
- [Logging in to the Web UI with Certificate Authentication](#) on page 168

About CAC for Certificate Authentication

A Common Access Card (CAC) or a Personal Identity Verification (PIV) is a smart card that is used by many government employees for all user authentications. Both CAC and PIV use the X.509 standard for a Public Key Infrastructure (PKI) as an authentication mechanism to manage certificates.

The keys and the certificates are stored on the CAC card. CAC satisfies a two-factor authentication (2FA) requirement because you must place a physical card in a CAC reader and know a Personal Identification Number (PIN). The CAC card stores the public certificates and the corresponding private keys that belong to the user.

The certificate is automatically uploaded from the CAC card to the browser, and the user selects an installed certificate to log in. The user is prompted to enter a PIN. If the PIN is validated, the card unlocks a private key that is used to set up a TLS connection with the appliance. The certificate identifies the user and it is used to set up a TLS connection. If the certificate is verified and signed by a trusted Certificate Authority (CA) and has not been revoked, the user is authenticated and can log in to the Web UI. The private key never leaves the CAC card.

CAC for certificate authentication performs the following functions:

- Authentication—Verifies the certificate date, obtains the revocation status of the X.509 certificate through the Online Certificate Status Protocol (OCSP) or the Certificate Revocation List (CRL), and verifies the CA certificate chain.
- Authorization—Maps the X.509 certificate fields to match an entry in the Active Directory (AD) or to match locally configured rules to permit or deny access to the Web UI.

When you enable certificate authentication on the Investigation Analysis appliance, Managed Defense integration with the appliance may not operate as expected. The  Managed Defense service may not have access to the appliance through the Web UI or API if the **fe_services** user is required to use a certificate to log in for user authentication.

Task List for Configuring the Appliance to Use CAC for Certificate Authentication

Complete the steps for configuring the appliance to use CAC for authentication in the following order:

1. Log in to the configuration menu.
2. (Optional) Configure the LDAP settings if you intend to configure the LDAP server to authorize users. For details about how to configure an LDAP server, see [User Management](#) on page 1.
3. Download a CA certificate bundle or add an imported certificate to an existing bundle from a specified URL. For details about uploading a CA-signed certificate to the IA, see [Uploading a Custom CA-signed Web Server Certificate](#) on page 151.
4. Enable policy settings to allow, require, or prohibit for certificate authentication. For details about how to enable policy settings of the Web UI, see [Enabling or Disabling CAC/PIV for Certificate Authentication](#) on page 152.
5. Configure user attributes for certificate authentication. For details about how to configure the user attributes for certificate authentication, see [Configuring the User Attributes for Certificate Authentication](#) on page 160.
6. (Optional) Configure OCSP so that the appliance can validate certificate revocation. For details about how to configure OCSP for certificate validation, see [Adding the OCSP URL Using the Configuration Menu](#) on page 157.
7. (Optional) Refresh the local Certificate Revocation List (CRL) file by downloading a new file from a specified remote location so that the Investigation Analysis appliance can validate certificate revocation. For details about how to refresh a local CRL file for certificate validation, see [Refreshing a CRL File Using the Configuration Menu](#) on page 159.

8. Configure LDAP mappings for authorization if you use an LDAP server to authorize users. For details about how to configure LDAP mappings for authorization, see [Configuring LDAP for Authorization](#) on page 163.

The user can log in to the Web UI for certificate authentication by entering the user name and password provided by the administrator, using a certificate, or both. For details about how to log in to the Web UI, see [Logging in to the Web UI with Certificate Authentication](#) on page 168.

Configuring Custom Web Server Certificates

You can configure Web server certificates by using the `certificates` command in KLISH. This command opens the Web server certificate and Certificate Authority (CA) certificate configuration settings. By default, a self-signed certificate is generated by the IA, but Trellix recommends that you upload a custom certificate to increase the security level of the appliance.

 If you import a custom CA-signed certificate, you must also upload a custom self-signed certificate.

This section includes the following:

- [Creating a Custom Self-Signed Web Server Certificate Request](#) below
- [Uploading a Custom Self-Signed Web Server Certificate](#) on the facing page
- [Uploading a Custom CA-signed Web Server Certificate](#) on page 151

Creating a Custom Self-Signed Web Server Certificate Request

You must generate a certificate request and submit it to a certificate authority before uploading a custom self-signed certificate to the IA.

To create a custom self-signed Web server certificate request:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:

```
$ ssh npadmin@10.1.0.1
```


or

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:

```
npadmin@ia> enable
```

3. Enter the npadmin password. The password can be 5 to 24 characters long.
`[sudo] password for npadmin: <password>`
4. Enter configuration mode:
`npadmin@ia# configure system`
5. Enter the Web server certificate configuration menu.
`npadmin@ia(config)# certificates`
6. Enter **1**. The custom certificate configuration menu appears.
7. Enter **1** to open the certificate signing request (CSR) settings. You see a menu similar to the following:
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:
Email Address []:
Key Size []:
8. Enter the information required of each setting. However, if `key size []` is left empty, the generated private key size defaults to 2048, which meets the security requirements defined by the National Institute of Standards and Technology (NIST).
9. Enter **Y** to confirm the CSR settings are correct. A PEM-encoded request is generated by the system.
10. Copy and paste the PEM-encoded request into a text file and submit the request to a certificate authority.

Uploading a Custom Self-Signed Web Server Certificate

You must upload your custom certificate to the IA after it is signed by a certificate authority. If the certificate is signed by an unknown certificate authority, you must also upload the certificate authority to the IA and configure it in KLISH. The certificate authority file you upload must also be PEM-encoded.

To upload a self-signed server certificate:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:
`$ ssh npadmin@10.1.0.1`
or
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:
`npadmin@ia> enable`

3. Enter the npadmin password. The password can be 5 to 24 characters long.
[sudo] password for npadmin: <password>
4. Enter configuration mode:
npadmin@ia# configure system
5. Enter the Web server certificate configuration menu.
npadmin@ia(config)# **certificates**
6. Enter **1** to replace the default self-signed certificate with a custom certificate. The custom certificate configuration menu appears.
7. Enter **2**. You see the following:
The certificate must first be uploaded to the appliance in pem-encoded format
Server Certificate (path):
8. Enter the PEM-encoded custom certificate. Press **Enter**.

Uploading a Custom CA-signed Web Server Certificate

To upload a custom Web server certificate signed by the Certificate Authority (CA):

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:
\$ ssh npadmin@10.1.0.1

or
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.
[sudo] password for npadmin: <password>
4. Enter configuration mode:
npadmin@ia# configure system
5. Enter the Web server certificate configuration menu.
npadmin@ia(config)# **certificates**
6. Enter **2** to replace the default self-signed certificate with a custom CA-signed certificate.

You see the following:
The certificate must first be uploaded to the appliance in pem-encoded format
CA Certificate (path):
7. Enter the PEM-encoded CA-signed certificate. Press **Enter**.

If you upload a CA-signed certificate to the IA, you must also upload a self-signed certificate. For instructions, see [Creating a Custom Self-Signed Web Server Certificate](#)

[Request](#) on page 149 and [Uploading a Custom Self-Signed Web Server Certificate](#) on page 150.

Enabling or Disabling CAC/PIV for Certificate Authentication

The administrator can make certificate authentication optional, required, or disabled.

- Optional—The user can log in to the Web UI using the user name and password provided by the administrator or using a certificate. For details, see [Logging in to the Web UI with Certificate Authentication](#) on page 168.
- Required—The user must use a certificate to log in to the Web UI. For details, see [Logging in to the Web UI with Certificate Authentication](#) on page 168.
- Disabled—The user cannot log in using a certificate.

 **NOTE:** You cannot use other authentication methods that are already configured to log in to the Web UI.

 **NOTE:** Certificate authentication settings are disabled by default.

Prerequisites

- Admin access to the appliance.
- (Optional) LDAP servers have been configured to authorize users. For details about how to configure an LDAP server, see [User Management](#).
- A Certificate Authority (CA) certificate bundle has been downloaded, and an imported certificate has been added to an existing bundle from a specified URL.

Enabling or Disabling CAC/PIV for Certificate Authentication Using the Configuration Menu

Use the menu options in this section to allow or require certificate authentication in the Web UI.

To enable or disable the policy settings of the Web UI for certificate authentication:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:
\$ ssh npadmin@10.1.0.1
or

- ```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  
npadmin@ia> enable
  3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
  4. Enter configuration mode:  
npadmin@ia# configure system
  5. Enter configuration CAC mode.  
npadmin@ia(config)# **authentication**
  6. In the CAC/PIV configuration menu, select **1** to access the Authentication Mechanism menu.  
Authentication Mechanisms: 1: PAM 2: LDAP 3: Radius 4: TACACS+ 5: Active Directory 6: PKI 7: PKI w/ LDAP 8: PKI w/ Active Directory C: Cancel changes and exit
  7. Depending on the external user management system you use, select a PKI option:
    - Enter **6** if you will not configure LDAP or Active Directory with PKI for authorization.
    - Enter **7** to configure PKI with LDAP for authorization.
    - Enter **8** to configure PKI with AD for authorization.
  8. In CAC/PIV configuration menu, select **2** to configure your selected PKI authorization method.
  9. In the PKI configuration menu, select **1** and enter the status. **If a valid CA-signed certificate is not uploaded to the IA, you will not be able to enable CAC/PIV authentication.**
    - **optional**—Users can log in to the Web UI either using the user name and password provided by their administrator or using an optional X.509 certificate.
    - **required**—Users must log in using a client X.509 certificate for user authentication.
    - **disabled**—The appliance does not accept a client X.509 certificate. Users must log in with user name and password.
  10. Select **Q** to save your settings and exit the menu.

## Checking for Revoked Certificates

You can enable the Investigation Analysis appliance to check for revoked certificates and reject them by using the appliance configuration menu:

- [Configuring Local CRL File Updates Using the Configuration Menu](#) on page 156
- [Adding the OCSP URL Using the Configuration Menu](#) on page 157
- [Adding a Local CRL File Using the Configuration Menu](#) below
- [Deleting a CRL File Using the Configuration Menu](#) on page 158
- [Refreshing a CRL File Using the Configuration Menu](#) on page 159

Both the Online Certificate Status Protocol (OCSP) and the Certificate Revocation List (CRL) protocol are used to validate whether an X.509 certificate has been revoked. If the CRL is configured on the Investigation Analysis appliance, the CRL is used first for certificate verification and then OCSP. By default, OCSP is enabled so that the appliance can verify the status of the certificate.

OCSP servers are also referred as OCSP responders. OCSP allows the appliance to check if a certificate has been revoked without downloading and searching the entire list. If an OCSP URL is found in the certificate, the OCSP responder is queried to determine the status of the certificate revocation. If an OCSP URL is not found in the certificate or the appliance cannot communicate with the OCSP responder from the certificate, a configured default URL is used.

A CRL contains a list of certificates that have been revoked or can no longer be trusted. When a TLS connection is set up with the appliance, part of the authentication process is to validate that the certificate is not listed in the CRL. Each entry in the list corresponds to the certificate number and the date the certificate was revoked.

## Prerequisites

- Admin access to the appliance.
- (Optional) LDAP servers have been configured to authorize users. For details about how to configure an LDAP server, see [User Management](#) on page 1.
- A Certificate Authority (CA) certificate bundle has been downloaded, and an imported certificate has been added to an existing bundle from a specified URL. For details, see [Configuring Custom Web Server Certificates](#) on page 149.
- Certificate authentication has been enabled. For details about how to enable policy settings of the Web UI, see [Enabling or Disabling CAC/PIV for Certificate Authentication](#) on page 152
- A CRL file has already been installed.

## Adding a Local CRL File Using the Configuration Menu

Use the menu options in this section to add a local Certificate Revocation List (CRL) file to the Investigation Analysis appliance. Only one CRL file can be present on the system.

**To add a local CRL file:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter configuration CAC menu.  
npadmin@ia(config)# **authentication**
6. In the CAC/PIV configuration menu, select **1** to access the Authentication Mechanism menu.  
Authentication Mechanisms:  
  - 1: PAM
  - 2: LDAP
  - 3: Radius
  - 4: TACACS+
  - 5: Active Directory
  - 6: PKI
  - 7: PKI w/ LDAP
  - 8: PKI w/ Active Directory
  - C: Cancel changes and exit
7. Depending on the external user management system you use, select a PKI option:
  - Enter **6** if you will not configure LDAP or Active Directory with PKI for authorization.
  - Enter **7** to configure PKI with LDAP for authorization.
  - Enter **8** to configure PKI with AD for authorization.
8. Select **Q** to save your changes and exit to the configure system menu.
9. Enter the CAC/PIV configuration menu.  
npadmin@ia(config)# **authentication**
10. Select **2** to configure PKI.
11. Select **1** to configure the PKI status.
12. Enable PKI.  
Status (disabled, optional, required): **optional**

13. In the PKI Configuration menu, select **3** to enter the CRL Configuration menu. The following appears:

### CRL Configuration:

- 1: CRL Retrieval URL = <none>
- 2: CRL Retrieval interval (hours between refresh) = 1
- 3: Upload CRL file = <none>
- 4: View CRL contents
- 5: Active Directory
- 6: Delete CRL file

```
Q: Save changes and exit
C: Cancel changes and exit
Enter your choice:
```

14. Select **3** to upload a CRL file to the appliance. Upload the CRL file to `/home/npscp/transfer/`.
15. Select **2** to verify the content of the CRL file.

```
-----BEGIN X509 CRL-----
MIIC3jCBxwIBATANBgkqhkiG9w0BAQSFADA0MTIwMAYDVQQDEylGaXJlRXJlIEVudG9vY2VycHJpc2UgRm9yZW5zaWZlIFR1c3QgUm9vdCBDQRCNMTkwjE5MjIxMDM2whcnMzkwMjIwMTAzMDM2WqBfMFOwhwYDVR0jBBgwFoAUKxSmtz0r3WuEUM7DBjNOOW8y9WzkwEAYJKwYBAGCNXUBBAMAQAQwCgYDVR0tUBAMCAQIWHAYJKwYBAGCNXUEBA8XDTM5MDIxOTIyMjAzN1owDQYJKoZIhvcNAQELBQADggIBAJO2SEL8g9K5Ygx0UH7oUrr41SQ06XIFJIIImfQyJS/x1Es+dY5MCPqvV9s3yQpP0Rw+Ck1EwbmYyduT5qh3jCahyhiGQDVB/89pThw+Qo/qw52yzu6g0yL+PjLfa1PSTLYNjWtLhkjwzzMqwzWzp

END X509 CRL-----
```

16. Select **X** to exit the menu.

## Configuring Local CRL File Updates Using the Configuration Menu

Use the menu options in this section to configure local Certificate Revocation List (CRL) file updates. You can configure how often the Investigation Analysis appliance downloads a new local or remote CRL file and specify the remote location of a CRL file.

### To configure local CRL file updates:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  

```
$ ssh npadmin@10.1.0.1
```

  
or  

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:  

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.  

```
[sudo] password for npadmin: <password>
```

4. Enter configuration mode:  
`npadmin@ia# configure system`
5. Enter configuration CAC menu.  
`npadmin@ia(config)# authentication`
6. In the CAC/PIV configuration menu, select **2** to configure the current authentication method.
7. In the PKI Configuration menu, select **3** to enter the CRL Configuration menu. The following appears:  
  
CRL Configuration:  
  
1: CRL Retrieval URL = <none>  
2: CRL Retrieval interval (hours between refresh) = 1  
3: Upload CRL file = <none>  
4: View CRL contents  
5: Active Directory  
6: Delete CRL file  
-----  
Q: Save changes and exit  
C: Cancel changes and exit  
Enter your choice:
8. Select **3** to upload a CRL file to the appliance. Upload the CRL file to  
`/home/npscp/transfer/`.
9. In the CRL Configuration menu, select **1** to enter the URL of the direct path to the certificate file.  
  
The URL is specified with remote server Administrator credentials (<username> and <password>), the remote server (<hostname>), the path and filename in which to save the certificate bundle (<path/filename>) in the following format:  
  
`scp://<username>[:<password>]@<hostname>/<path/filename>`  
  
 **NOTE:** If you do not include the password, the configuration menu prompts for the password and obfuscates the keyboard input as you type it.
10. In the CRL Configuration menu, select **2** to set the time interval in hours for how often the appliance downloads a new CRL file.
11. Select **X** to exit the menu.

## Adding the OCSP URL Using the Configuration Menu

Use the menu options in this section to add the verification OCSP URL so that the appliance can validate certificate revocation. PKI must be selected and CAC must be enabled as the authentication method to add the OCSP URL.

**To add the verification OCSP URL:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system
5. Enter configuration CAC mode.  
npadmin@ia(config)# **authentication**
6. In the CAC/PIV configuration menu, select **2** to configure the current authentication method.
7. Select **2** to add the verification OCSP URL. Press **Enter**.
8. Enter the verification OCSP URL so that certificate revocation can be validated. Press **Enter**.  
  
The configuration of the OCSP URL is displayed in the CAC/PIV configuration menu.
9. Select **S** to save your settings and exit the menu.

## Deleting a CRL File Using the Configuration Menu

Use the menu options in this section to delete a specified Certificate Revocation List (CRL) file from the appliance.

**To delete a local CRL file:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
  
or  
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:  
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
npadmin@ia# configure system

5. Enter configuration CAC menu.  
`npadmin@ia(config)# authentication`
6. In the CAC/PIV configuration menu, select **2** to configure the current authentication method.
7. In the PKI Configuration menu, select **3** to enter the CRL Configuration menu. The following appears:  
CRL Configuration:  
  
1: CRL Retrieval URL = <none>  
2: CRL Retrieval interval (hours between refresh) = 1  
3: Upload CRL file = <none>  
4: View CRL contents  
5: Active Directory  
6: Delete CRL file  
-----  
Q: Save changes and exit  
C: Cancel changes and exit  
Enter your choice:  
  
8. Select **6** to delete the CRL file.

## Refreshing a CRL File Using the Configuration Menu

Use the menu options in this section to refresh a local Certificate Revocation List (CRL) file by downloading a new file from a specified remote location so that the Investigation Analysis appliance can validate certificate revocation. Only one CRL file can be present on the system. When you download a new CRL file, the existing CRL file is automatically deleted.



You must specify the URL of the direct path to the certificate file.

### To refresh a local CRL file:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
`$ ssh npadmin@10.1.0.1`  
or  
`$ ssh npadmin@exampleFQDN`
2. Enter privileged mode:  
`npadmin@ia> enable`
3. Enter the npadmin password. The password can be 5 to 24 characters long.  
[sudo] password for npadmin: <password>
4. Enter configuration mode:  
`npadmin@ia# configure system`

5. Enter configuration CAC menu.

```
npadmin@ia(config)# authentication
```

6. In the CAC/PIV configuration menu, select **2** to configure the current authentication method.

7. In the PKI Configuration menu, select **3** to enter the CRL Configuration menu. The following appears:

```
CRL Configuration:
```

```
1: CRL Retrieval URL = <none>
2: CRL Retrieval interval (hours between refresh) = 1
3: Upload CRL file = <none>
4: View CRL contents
5: Active Directory
6: Delete CRL file

```

```
Q: Save changes and exit
C: Cancel changes and exit
Enter your choice:
```

8. Select **2** to configure the CRL retrieval interval.
9. Select **Q** to save your changes and exit the menu.

## Configuring the User Attributes for Certificate Authentication

An administrator uses the information from the X.509 certificate to identify the user and assign user roles that allow the user to perform certain operations on the appliance. The following table describes the user attributes that are used for certificate authentication.

| Attribute            | Description                                                                                                                                                                                                                                                      |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| x509-cert-subject    | <p>The Distinguished Name (DN) in the Subject field in the certificate. Each entry has a unique identifier.</p> <p>The following example shows the DN format for CAC:</p> <p>C=US, O=Test Government, OU=Test Department, OU=Test Agency, CN=Test Cardholder</p> |
| x509-cert-subject-cn | <p>Common Name (CN) entry from the DN attribute in a certificate. For example, CN=Test Cardholder.</p>                                                                                                                                                           |

| Attribute                    | Description                                                                                                                           |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| x509-cert-san-email          | The email address in the Subject Alternative Name (SAN) field of the certificate. You are allowed to have multiple subfields for SAN. |
| x509-cert-san-email-username | The user name of the email address without the domain name in the certificate.                                                        |
| x509-cert-san-upn            | User Principal Name (UPN) encoded in the Other Name field of the SAN field in the certificate.                                        |

## Prerequisites

- Admin access to the appliance.
- (Optional) LDAP servers have been configured to authorize users. For details about how to configure an LDAP server, see [User Management](#) on page 1.
- A Certificate Authority (CA) certificate bundle has been downloaded, and an imported certificate has been added to an existing bundle from a specified URL.
- Certificate authentication has been enabled. For details about how to enable policy settings of the Web UI, see [Enabling or Disabling CAC/PIV for Certificate Authentication](#) on page 152.

## Configuring the User Attributes for Certificate Authentication Using the Configuration Menu

Use the menu options in this section to configure the user attributes for certificate authentication.

**To configure the user attributes for certificate authentication:**

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:  
\$ ssh npadmin@10.1.0.1  
or

- ```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:
npadmin@ia> enable
 3. Enter the npadmin password. The password can be 5 to 24 characters long.
[sudo] password for npadmin: <password>
 4. Enter configuration mode:
npadmin@ia# configure system
 5. Enter configuration CAC menu.
npadmin@ia(config)# **authentication**
 6. In the CAC/PIV configuration menu, select **1** to access the Authentication Mechanism menu.
Authentication Mechanisms:
 - 1: PAM
 - 2: LDAP
 - 3: Radius
 - 4: TACACS+
 - 5: Active Directory
 - 6: PKI
 - 7: PKI w/ LDAP
 - 8: PKI w/ Active Directory
 - C: Cancel changes and exit
 7. Select **2** to select LDAP.
 8. Select **Q** to save your changes and exit to the configure system menu.
 9. Enter the CAC/PIV configuration menu.
npadmin@ia(config)# **authentication**
 10. Select **2** to configure LDAP.
 - 1: LDAP Server(s) =
 - 2: Base DN = None
 - 3: Bind DN = None
 - 4: Bind Password = None
 - 5: Base Password = None
 - 6: Base Group = None
 - 7: LDAP/AD UIAPI Group = None
 - 8: LDAP/AD Sudo Group = None
 - 9: LDAP/AD SSH Group = None
 - 10: LDAP Domain SID = None
 - 11: LDAP USE SSL = False
 - 12: LDAP USE STARTTLS = False
 - 13: Enable LDAP Group Traversal = False

```
=====
```

 - Q: Save changes and exit
 - C: Cancel changes and exit

11. Make configuration changes to one of the following user attributes. Press **Q** to save your changes and exit the LDAP configuration menu.
 - `x509-cert-subject`—Specifies the name in the subject field in the certificate.
 - `x509-cert-subject-cn`—Specifies the Common Name (CN) from the DN attribute in the certificate.
 - `x509-cert-san-email`—Specifies an email address in the Subject Alternative Name (SAN) field of the certificate. You are allowed to have multiple subfields for SAN.
 - `x509-cert-san-email-username`—Specifies the user name of the email address without the domain name in the certificate.
 - `x509-cert-san-upn`—Specifies the User Principal Name (UPN) that is encoded in the "Other Name" field of the SAN field in the certificate.

Configuring LDAP for Authorization

If you configured an LDAP server to authenticate users, you can configure LDAP mappings for authorization by using the appliance configuration menu:

- [Selecting the Authorization Type Using the Configuration Menu](#) on the facing page
- [Configuring an Active Directory Server Using the Configuration Menu](#) on page 165
- [Configuring User Mapping Groups Using the Configuration Menu](#) on page 166

When the appliance needs to determine the identity of the user, the Subject Alternative Name (SAN) extension with the User Principal Name (UPN) extension in the certificate can be used as an identifier when matching the certificate to an entry in the Active Directory (AD), which is supported by the LDAP protocol.

When the certificate is validated, the AD server uses the Principal Name field (`Principal Name=user@fully.qualified.domain.name`) in the SAN with the UPN of the certificate to search for the user in the Active Directory. The server permits or denies access to the Web UI based on the matched fields.

The user schema name and login name for the LDAP attribute are used to match the configured certificate authorization field. An administrator can configure the LDAP record to map the login name. An administrator can define an LDAP search filter in the configuration that controls which users can log in using a certificate and then can be authorized using LDAP.

Prerequisites

- Admin access to the appliance.
- LDAP servers have been configured to authorize users.
- A Certificate Authority (CA) certificate bundle has been downloaded, and an imported certificate has been added to an existing bundle from a specified URL. For details, see [Configuring Custom Web Server Certificates](#) on page 149.
- Certificate authentication has been enabled. For details about how to enable policy settings of the Web UI, see [Enabling or Disabling CAC/PIV for Certificate Authentication Using the Configuration Menu](#) on page 152.
- User attributes for certificate authentication have been configured. For details about how to configure the user attributes for certificate authentication, see [Configuring the User Attributes for Certificate Authentication](#) on page 160
- Online Certificate Status Protocol (OCSP) has been configured so that the appliance can validate certificate revocation. For details about how to configure OCSP for certificate revocation, see [Adding the OCSP URL Using the Configuration Menu](#) on page 157

Selecting the Authorization Type Using the Configuration Menu

Use the menu options in this section to select a specific authorization method.

To select the authorization type:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:

```
$ ssh npadmin@10.1.0.1
```


or

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:

```
npadmin@ia> enable
```
3. Enter the npadmin password. The password can be 5 to 24 characters long.

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:

```
npadmin@ia# configure system
```
5. Enter configuration CAC configuration menu:

```
npadmin@ia(config)# authentication
```

6. In the CAC/PIV configuration menu, select **1** to access the **Authentication Mechanism** menu.
Authentication Mechanisms: 1: PAM 2: LDAP 3: Radius 4: TACACS+ 5: Active Directory 6: PKI 7: PKI w/ LDAP 8: PKI w/ Active Directory C: Cancel changes and exit
7. Select **5** to choose AD.
Press **Enter**.
8. Select **Q** to save your settings and exit the menu.

Configuring an Active Directory Server Using the Configuration Menu

Use the menu options in this section to configure Active Directory authentication. Because Active Directory (AD) supports the LDAP protocol, the Investigation Analysis appliances can also authenticate through an AD server.

The binding user or `bind-dn` in the Investigation Analysis configuration is a read-only user that is used to query the directory structure starting from the `base-dn`.

To configure Active Directory authentication:

1. Log in to the IA as `npadmin` using the IA IP address or FQDN. For example:

```
$ ssh npadmin@10.1.0.1
```


or

```
$ ssh npadmin@exampleFQDN
```
2. Enter privileged mode:

```
npadmin@ia> enable
```
3. Enter the `npadmin` password. The password can be 5 to 24 characters long.

```
[sudo] password for npadmin: <password>
```
4. Enter configuration mode:

```
npadmin@ia# configure system
```
5. Enter configuration CAC mode.

```
npadmin@ia(config)# authorization
```

6. In the CAC/PIV configuration menu, select **5** to configure AD. The AD configuration menu appears.

```

1: AD Server(s) =
2: Base DN = None
3: Bind DN = None
4: Bind Password = None
5: Base Password = None
6: Base Group = None
7: LDAP/AD UIAPI Group = None
8: LDAP/AD Sudo Group = None
9: LDAP/AD SSH Group = None
10: LDAP Domain SID = None
11: LDAP USE SSL = False
12: LDAP USE STARTTLS = False
13: Enable LDAP Group Traversal = False
=====

Q: Save changes and exit
C: Cancel changes and exit

```

7. Select **1** to configure an LDAP server and host to send LDAP authentication requests. Use the hostname or IP address of the AD server. Press **Enter**.
8. Select **13** to choose the type of encryption (TLS or STARTTLS) for secure connections between the appliance and the Web browser running the Web UI, and to verify remote servers for various client applications. STARTTLS takes an existing insecure connection and upgrades it to a secure connection using SSL/TLS.
Press **Enter**.
9. Select **6** to configure the LDAP user search base (for example, [DC=testad,DC=eng,DC=fireeye,DC=com]).
Press **Enter**.
10. Select **2** to set the Distinguished Name used to bind to the server (for example, [CN=eng-pxbind,OU=UtilityAccounts,OU=Engineering,DC=testad,DC=eng,DC=fireeye,DC=com]).
Press **Enter**.
11. Select **4** to configure the credentials used to bind to the server (for example, P2ssw0rd!).
Press **Enter**.
12. Select **S** to save your settings and exit the menu.

Configuring User Mapping Groups Using the Configuration Menu

Use the menu options in this section to configure user mapping groups for authorization.

To configure user mapping groups:

1. Log in to the IA as npadmin using the IA IP address or FQDN. For example:
\$ ssh npadmin@10.1.0.1

or
\$ ssh npadmin@exampleFQDN
2. Enter privileged mode:
npadmin@ia> enable
3. Enter the npadmin password. The password can be 5 to 24 characters long.
[sudo] password for npadmin: <password>
4. Enter configuration mode:
npadmin@ia# configure system
5. Enter configuration CAC mode.
npadmin@ia(config)# **authorization**
6. In the CAC/PIV configuration menu, select **2** to configure Active Directory. The Active Directory configuration menu appears.

```
1: LDAP Server(s) =
2: Base DN = None
3: Bind DN = None
4: Bind Password = None
5: Base Password = None
6: Base Group = None
7: LDAP/AD UIAPI Group = None
8: LDAP/AD Sudo Group = None
9: LDAP/AD SSH Group = None
10: LDAP Domain SID = None
11: LDAP USE SSL = False
12: LDAP USE STARTTLS = False
13: Enable LDAP Group Traversal = False
```

=====

```
Q: Save changes and exit
C: Cancel changes and exit
```

7. Select **7** to add the user attributes for the X.509 certificates to the uiapi group mapping field for authorization (for example, [CN=eng-pxuiapi,OU=AdminGroups,OU=Engineering,DC=testad,DC=eng,DC=fireeye,DC=com]).

Press **Enter**.
8. Select **Q** to save your changes and exit the menu.

Logging in to the Web UI with Certificate Authentication

You can log in to the Web UI with certificate authentication by entering your account name and password provided by the administrator, using a certificate, or both.

To log in to the Web UI when a certificate is mandatory for user authentication:

1. Go to `https://<appliance>` in the browser, where `<appliance>` is the IP address or hostname of the appliance. For example, if the configured IP address of the appliance is 10.1.0.1, enter `https://10.1.0.1`.
2. On the login page, click **Log in with CAC/PIV**.

To log in to the Web UI when a certificate is optional for user authentication:

1. Go to `https://<appliance>` in the browser, where `<appliance>` is the IP address or hostname of the appliance. For example, if the configured IP address of the appliance is 10.1.0.1, enter `https://10.1.0.1`.
2. On the login page, choose one of the following options:
 - Enter the account name and password your administrator provided and click **Log in**.
 - Click **Log in with CAC/PIV**.

Index

A

About [147](#)

Adding PX [106](#)

admin password [140](#)

Alert Aggregation [116](#)

Alerts [116-118](#)

Authentication [130, 132, 134, 147, 152, 155, 160-161, 165, 168](#)

AX Series Appliance [122](#)

B

Browser Support [14](#)

C

CAC (Common Access Card)

certificate revocation (X.509)

CRL (certificate revocation list)

deleting [158-159](#)

downloading [154, 156](#)

OCSP (Online Certificate Status Protocol)

URL, adding or removing [157](#)

overview [153](#)

user attributes

configuring [161](#)

description [160](#)

LDAP

overview [163-166](#)

overview [147](#)

task list [148](#)

web policy settings

enabling or disabling [152](#)

logging in to Web UI using
certificate [168](#)

CLI [16, 132](#)

CLISH [16](#)

Cluster [70, 72-73, 81](#)

Command Line Interface [16](#)

Configure [71, 74, 100-104, 106, 117, 119, 134, 148](#)

Configuring Eth [26](#)

CRL (certificate revocation list)

deleting [158-159](#)

downloading [154, 156](#)

D

Dashboard [15-16, 128](#)

-
- Data Node [84](#)
 - DHCP [20](#)
 - Disk [39](#), [64](#)
 - Distributed Search [84](#)
 - DNS [12](#), [14](#), [16](#), [18](#), [26](#), [107](#), [122](#), [132](#)
 - F
 - Format
 - PCAP File Format [120](#)
 - FTP [12](#)
 - H
 - Hostname [26](#)
 - HTTP Listener [118](#)
 - I
 - Integration [122](#)
 - IPMI [16](#), [18](#), [31](#)
 - L
 - LDAP [132](#)
 - User Authentication [148](#), [152-155](#), [161-163](#), [165](#), [167](#)
 - LDAP, certificate authorization
 - enabling or disabling [164-166](#)
 - overview [163](#)
 - Load [39](#)
 - Logging In [21](#)
 - M
 - Menu [82](#), [125](#), [142](#), [152](#), [154](#), [156-159](#), [161](#), [164-166](#)
 - Modes
 - Privileged Mode
 - Unprivileged Mode [111](#)
 - N
 - Network [18](#), [24](#), [26](#), [34](#), [36](#), [91](#), [103](#), [107](#), [122](#)
 - Network Configuration [18](#), [26](#)
 - Network Requirements [18](#)
 - npadmin [140](#)
 - NTP Server [18](#), [28](#), [34](#)
 - O
 - OCSP (Online Certificate Status Protocol)
 - URL, adding or removing [157](#)
 - Operating System [14](#)
 - OS
 - CaptureOS [13](#)
 - Other Term
 - Subterm [91](#)
 - P
 - PAM [132](#)
 - Password [16](#), [106](#), [119](#), [138](#), [162](#), [166-167](#)
 - PX Metadata [106](#)
 - R
 - Radius [153](#), [155](#), [162](#), [165](#)
 - RADIUS [132](#)
 - rebuild [62](#)
 - Rebuilding [62](#)
 - Results [55](#)
 - Roles [138](#), [142](#)
 - S
 - Screen Resolution [14](#)
 - Search [12](#), [21](#), [29](#), [68](#), [75](#), [84](#)
 - Shell [48](#), [58](#), [106](#), [138](#)
 - SMTP [12](#)

SNMP [24](#), [36](#)

Software [2](#), [13](#), [44](#)

SSH [12](#), [16](#), [26](#), [55](#), [91](#), [101](#), [107](#), [162](#),
[166-167](#)

SSL [12](#), [55](#), [120](#), [125-126](#), [135](#), [162](#), [166-167](#)

Status [41](#), [125](#), [148](#), [154-155](#), [164](#)

Support [14](#), [44](#), [112](#), [173](#)

Synching PX [106](#)

System [2](#), [12](#), [39](#), [62](#), [100-104](#)

T

TACACS [132](#), [139](#), [153](#), [155](#), [162](#), [165](#)

Temperature [40](#)

Testing Connectivity [32](#)

Time [19](#), [24](#), [34](#)

Time Management [34](#)

U

Upgrade [44](#)

user attributes (X.509)

- configuring [161](#)
- description [160](#)

User Management [138-140](#)

Users [142](#), [153](#)

W

web policy settings

- enabling or disabling [152](#)
- logging in to Web UI using
certificate [168](#)

Web UI [14-15](#)

Technical Support

For technical support, contact Trellix through the Support portal:
<https://www.trellix.com/en-us/support.html>

Documentation

Documentation for all Trellix products is available on the Trellix Documentation Portal:
<https://docs.trellix.com/>

Trellix | 3099 North First Street | San Jose, CA | 1.408.321.6300 | 1.877.347.3393 | www.trellix.com

© 2023 Musarubra US LLC. Trellix and FireEye are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC, and their affiliates in the US and/or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and /or other countries. Skyhigh Security is the trademark of Skyhigh Security LLC and its affiliates in the US and other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

