



AlgoSec Firewall Analyzer

Software Version: A30.10

Administration Guide

View our most recent updates in our online [ASMS Tech Docs](#).

Document Release Date: 4 May, 2020 | Software Release Date: April 2020

Legal Notices

Copyright © 2003-2020 AlgoSec Systems Ltd. All rights reserved.

AlgoSec, FireFlow, AppViz and AppChange are registered trademarks of AlgoSec Systems Ltd. and/or its affiliates in the U.S. and certain other countries.

Check Point, the Check Point logo, ClusterXL, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, INSPECT, INSPECT XL, OPSEC, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UserAuthority, VPN-1, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Cisco, the Cisco Logo, Cisco IOS, IOS, PIX, and ACI are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Specifications subject to change without notice.

Proprietary & Confidential Information

This document contains proprietary information. Neither this document nor said proprietary information shall be published, reproduced, copied, disclosed, or used for any purpose other than the review and consideration of this material without written approval from AlgoSec, 65 Challenger Rd., Suite 310, Ridgefield Park, NJ 07660 USA.

The software contains proprietary information of AlgoSec; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between AlgoSec and the client and remains the exclusive property of AlgoSec. If you find any problems in the documentation, please report them to us in writing. AlgoSec does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of AlgoSec Systems Ltd.

Contents

AFA administration	15
Access the AFA Administration area	15
Quickstart - Configure AFA to analyze devices	16
Logins and other basics	18
Supported browsers	18
Log in to ASMS	18
View ASMS product details	21
Log out of ASMS	22
Manage devices	24
AFA communication protocols	24
Device procedure reference	24
Device icons	25
Add devices to AFA	27
Add device prerequisites	27
Access the DEVICES SETUP page	28
Add cloud devices	32
AWS (Amazon Web Service) accounts in AFA	32
Microsoft Azure subscriptions in AFA	37
Add Check Point devices	41
Check Point network connections	42
Check Point device permissions	42
Add a Check Point Multi-Domain Security Management device	44
Set user permissions	48
Add a Check Point SmartCenter/Gateway	49
Set user permissions	52
Add a Check Point CMA	52
Check Point fields and options	56
Configure one-armed mode manually	61
Enable data collection for Check Point devices	62
Enable data collection via SSH	62

Enable data collection via OPSEC	65
Enable data collection via REST	82
Add Cisco devices	84
Add a CSM-managed Cisco device	84
Cisco IOS routers in AFA	88
Cisco Nexus routers in AFA	94
Cisco ASA firewalls in AFA	99
Cisco Application Centric Infrastructure (ACI) devices in AFA	107
Cisco Firepower devices in AFA	115
Configure one-armed mode manually	120
Add F5 BIG-IP load balancers	120
F5 BIG-IP LTM-only device support	121
F5 BIG-IP LTM and AFM support	125
Add Fortinet devices	129
Fortinet network connections	129
FortiManager device permissions	129
FortiGate device permissions	131
Add a Fortinet FortiManager device to AFA	132
Add a Fortinet FortiGate device to AFA	138
Configure one-armed mode manually	141
Add Juniper devices	141
Juniper NSM devices in AFA	142
Junos Space Security Director devices in AFA	150
Juniper Netscreen devices in AFA	162
Juniper SRX devices in AFA	168
Juniper routers in AFA	175
Configure Juniper STRM to forward logs to a Syslog-ng server	178
Add Palo Alto Networks devices	178
Palo Alto network connections	179
Panorama device permissions	180
Palo Alto Networks Firewall device permissions	181

Add a Palo Alto Networks Panorama	182
Configure one-armed mode manually	187
Add a Palo Alto Networks firewall	187
Add a Symantec Blue Coat	192
Add VMware NSX-V devices	196
Network connectivity	196
Device permissions	196
Add a VMware NSX-V to AFA	198
Required device permissions	200
Baseline configuration compliance	200
Device requirements reference by brand	200
Check Point device requirements	201
Cisco device requirements	201
Arista device requirements	202
Juniper device requirements	202
Fortinet device requirements	202
Palo Alto device requirements	202
F5 device requirements	202
Symantec BlueCoat SGOS device requirements	202
WatchGuard device requirements	202
TopSec device requirements	203
VMware NSX device requirements	203
AWS requirements	203
Azure requirements	203
Add other devices and routing elements	203
Add monitoring and routing devices	203
Add routing elements	207
Add/update multiple devices in bulk	210
Prepare your CSV file	210
Import your CSV file (UI)	212
Import your CSV file (CLI)	213

Bulk import support scope	214
CSV import file format	215
Basic device description headers	216
Access information headers	217
Cisco-related headers	218
CyberArk-related headers	219
Advanced headers	220
Remote management headers	221
Log and monitoring headers	222
Additional headers	224
SNPM polling headers	226
Maintain devices	227
Edit a device's configuration	227
Rename a device	228
Add additional device identifiers for sub-systems	228
Delete a device	229
Update a password for multiple devices	229
Specify routing data manually	231
Specify routing data manually for primary devices	231
Specify routing data manually for sub-systems	232
Specify routing data from the map	233
Integrate AFA and CyberArk	234
ASMS and CyberArk integration architecture	234
Supported devices for CyberArk integration	235
Configure CyberArk AIM for ASMS access	236
Configure CyberArk accounts and permissions	236
Configure CyberArk integration	238
Alternate data collection methods	240
When to use these procedures	240
Recommended device data collection per device type	240
Add a static file device to AFA (UI)	242

Add a static file device to AFA (CLI)	244
Semi-automatic data collection scripts	245
Extend device support	247
Static configuration file support	247
Live monitoring support	247
Static support for generic devices	248
Supported device types	248
Adding Support for a File Device	248
Creating the JSON File	249
Tag Reference	250
config_type	251
device	251
hosts	251
hosts_groups	252
interfaces	252
services	253
services_groups	253
policies	253
rules_groups	254
nat_rules	255
zones	256
routes	256
schedules	256
Sample generic device JSON file	257
Static support troubleshooting	257
Troubleshooting directories and files	257
Generic device monitoring	259
Enable live monitoring support	259
Create data collection files for a generic device	260
Install the new brand	260
Add the device to AFA	261

Collect routing information via SNMP	263
Configuration file example	263
Configuration file example with routing	264
Monitoring support tag reference	265
Tag syntax	265
DEVICE	265
FORM_FIELD	266
CONNECTION_CMD	267
DATA_COLLECTION	268
LOGIN_PROMPT	269
POST_LOGIN_PROMPT	270
COMMANDS_SEQUENCE	271
CMD	272
CMD_VIRT	274
DATA_COLLECTION	276
DIFF	276
EXCLUDE	277
ROUTING	278
FEATURES	279
FEATURE	280
Early availability features	280
Cisco ISE devices in AFA	281
Arista devices in ASMS	284
Enable / Disable map support for Azure	286
Enable /Disable ActiveChange for Azure	288
Enable support for Check Point R80 layers	289
Manage groups	291
About groups in AFA	291
Add groups	291
Edit groups	293
Rename groups	294

Delete groups	295
Manage matrices	296
About AFA matrices	296
Add matrices	297
Edit matrices	299
Rename matrices	300
Delete matrices	301
Manage DR sets	302
Add DR sets	302
Edit DR sets	303
Rename DR sets	305
Delete DR sets	305
Manage the map	307
Complete the map	307
Completed map contents	307
Identify routers to define in AFA	308
Complete the map (CLI)	311
Map completeness CLI tool scope	311
Identify routers to define in AFA	312
Map completeness parameters	314
Troubleshoot traffic simulation queries	316
Edit IP ranges in clouds	319
Remove devices	322
Restore device interfaces	323
Specify routing data manually	324
Schedule analysis	325
Add and edit analysis jobs	325
Delete scheduled jobs	329
Configure real-time monitoring	331
Activate real-time monitoring	331
AFA users and roles	333

AFA authentication	333
AFA user types and permissions	333
Configure user authentication	334
Single Sign On (SSO) and ASMS	335
User authentication via authentication servers	347
Import user data from an LDAP server	358
Configure an LDAP forest	360
Log in when an LDAP forest is configured	367
Manage users and roles in AFA	368
Add or edit users	368
Add and edit user roles	375
Delete AFA users or roles	378
ASMS username and password requirements	379
Import users via CSV	380
Prepare a users CSV file	380
Run the import users script	384
Customize risk and compliance management	386
Customize risk profiles	386
View a risk profile	387
Add a new risk profile	389
Delete a custom risk profile	396
Set a default risk profile	396
Customize risk items	397
Edit, duplicate, or add a custom risk item	397
Risk Info fields	398
Risk Query fields	399
Risk Details fields	400
Delete a risk item	404
Disable a risk item	405
Customize zone types	405
Built-in zone types	406

Add and edit zone types	406
Delete zone types	408
Customize hostgroups	409
Add and edit host groups	409
Delete hostgroups	410
Customize services	411
Add and edit service groups	411
Delete service groups	413
Configure trusted private IP addresses	414
Configure security ratings	415
Security rating calculation	415
Security rating calculation background	416
Customize security rating settings	417
Customize the regulatory compliance report	418
Remove and add compliance reports	419
Supported regulatory compliance reports	420
Customize the compliance score value	422
Customize compliance score severity thresholds	424
Configure the PCI zone	425
Customize baseline configuration profiles	427
Access baseline profiles configuration	427
Add a custom baseline configuration compliance profile	428
Duplicate a baseline configuration compliance profile	430
Edit a baseline configuration compliance profile	432
Delete a custom baseline configuration compliance profile	433
Example: Customize a baseline configuration compliance profile	433
Sample Baseline Configuration Compliance Profile	443
Advanced risk editing	444
Overview	444
Risk item types	445
Traffic risk item guidelines	446

Host group risk item guidelines	448
Property risk item guidelines	449
Rule risk item guidelines	449
Assessment and remedy keywords	451
Configure notifications	455
Schedule dashboard notifications	455
Add and edit dashboard e-mails	455
Deleting Scheduled Jobs	458
Configure event-triggered notifications	458
Supported notifications	459
E-mail Notification Example 1: Analysis completed	459
E-mail Notification Example 2: Changes to policy and risks	459
Configure AFA to send event triggered e-mail notifications	460
Configure device report page messages	462
Define AFA preferences	465
General	466
General Fields	467
Language	468
Display	469
Display Fields	469
Log analysis	470
Log analysis fields	470
Define a device proxy	471
Proxy fields	472
Mail	472
Storage	473
Configure report cleanup	474
Workflow	477
Change request ID format	478
AlgoSec FireFlow	479
BMC Remedy	479

HP ServiceCenter (formerly Peregrine)	481
Other	483
Authentication	484
Backup/Restore	485
Backup and restore prerequisites	486
Backup and restore on distributed architectures	486
Define backup options	487
Back up your system	489
Restore your system	490
Advanced Configuration	491
Add a new AFA configuration parameter and value	491
Advanced AFA configuration parameter reference	492
Customize AFA	508
Custom report pages	508
Create a custom report page	508
Custom report configuration file parameters	509
Extract custom report script flags	510
Custom documentation fields	511
Add documentation fields	511
Enable/Disable documentation fields	512
Custom dashboards and charts	512
Configure custom charts	512
Add a custom chart	513
Chart tag reference	513
Configure a custom dashboard	527
Dashboard tag reference	527
Dashboard configuration example	528
Customize regulatory compliance report	529
Add, remove or customize compliance reports	529
Troubleshooting	533
Troubleshooting and maintenance permissions	533

Entering and exiting debug mode	535
Contact technical support	535
Access log and configuration files	536
Send us feedback	542

AFA administration

This topic lists supported browsers for working with ASMS, as well as a high-level instructions for using the AFA Administration area and setting up your AFA environment.

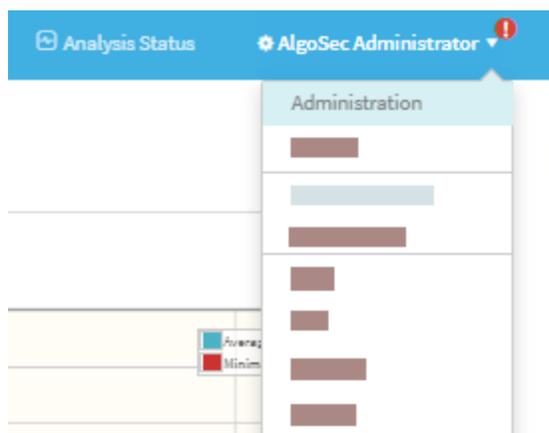
Note: For details about logging in or out of AFA, see [Logins and other basics](#).

Access the AFA Administration area

Most AFA configurations are performed using the AFA Administration area, accessible from the top-right of any AFA page.

Do the following:

In the toolbar, click your username, and then select **Administration** from the dropdown menu.



The Administration area includes the following tabs:

DEVICES SETUP	Manage devices, groups, and matrices. For details, see: <ul style="list-style-type: none"> • Manage devices • Manage groups • Manage matrices
USERS/ROLES	Manage AFA users and user roles. For details, see AFA users and roles .

SCHEDULER	Schedule analysis and notifications. For details, see Schedule analysis .
COMPLIANCE	Manage risk profiles, baseline profiles, and compliance options. For details, see Customize risk and compliance management .
OPTIONS	Configure AFA preferences including report storage options, user authentication options, backup options, and more. For details, see Define AFA preferences .
MONITORING	Configure real-time monitoring. For details, see Configure real-time monitoring .
ARCHITECTURE	Manage Remote Agents or Load Units in a distributed architecture.

Note: The **DOMAINS** tab enables you to segregate data by domain in a Provider Edition environment. For more details, contact AlgoSec customer support.

Quickstart - Configure AFA to analyze devices

This section quickly introduces you to a few typical Administrative tasks and gets you analyzing devices in minutes.

Do the following:

1. **Collect your device policy automatically.** Add devices for which you want to activate data collection. For more details, see [Manage devices](#).
2. **Configure AFA to run a nightly analysis.** Once you have defined your devices for automatic data collection, you can schedule periodic analyses overnight, or at any other schedule of your choice.

For more details, see [Schedule analysis](#).

3. **Configure email notifications.** AFA can send a variety of e-mail messages to you and to your team members when reports are ready or when changes are made on the monitored security devices. Additionally, you can schedule e-mails which

contain dashboards.

For more details, see [Configure notifications](#).

4. **Manage user access.** The AFA Web GUI allows you to view your reports on a secure web server, and lets you provide access to the reports to authorized team members.

Standard or Read-Only access can be granted to each user for each device separately. The Web GUI also allows authorized users to start analyses, to customize the resulting reports, and to run traffic simulation queries on them. AFA administrators may also use the Web GUI for administrative configurations.

For more details, see [AFA users and roles](#).

Logins and other basics

This topic describes the very basics of working with ASMS, such as logging in and out and supported browsers.

Supported browsers

View ASMS in one the following web browsers, at screen resolution of **1920x1080** or above.

- **Mozilla Firefox**
- **Google Chrome**
- **Microsoft Edge**
- **Internet Explorer 11** and higher. Internet Explorer 8.0 is supported for FireFlow requestors only.

Log in to ASMS

Log in to ASMS from any desktop computer using the credentials provided by an AFA administrator.

Do the following:

1. In your browser, navigate to **https://<algosec_server>** where **<algosec_server>** is the ASMS server IP address or DNS name.

If a warning message about the web server's certificate appears, click **Accept** or **OK**. For more details, contact your network administrator.

The **Security Management Suite** login page appears.

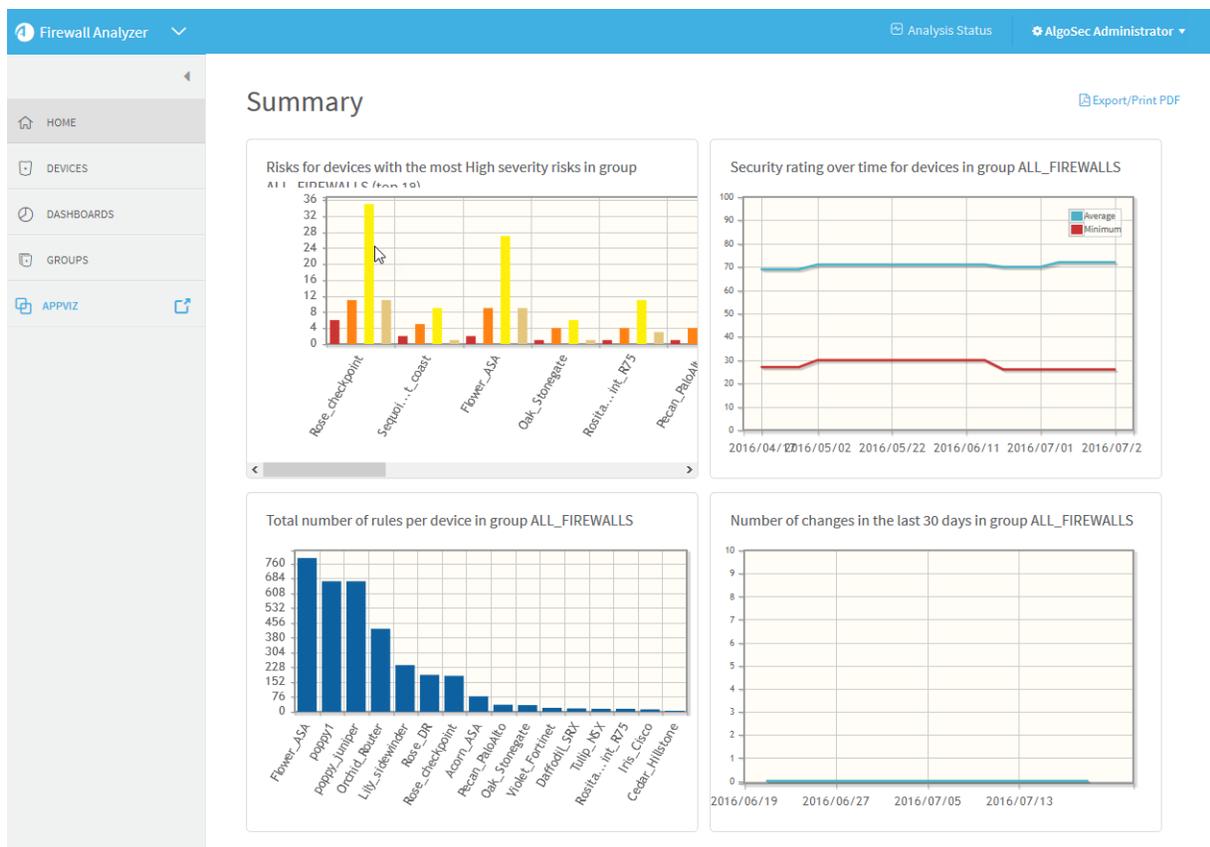


The screenshot shows the login interface for the AlgoSec Security Management Suite. At the top right, there is a link labeled "About". The logo for "algosec" is prominently displayed in the center, with the "a" in a blue circle. Below the logo, the text "Security Management Suite" is centered. There are two input fields: "User Name" and "Password". Below these fields is a blue "Login" button.

2. In the **Username** and **Password** fields, enter your username and password, and click **Login**.

You are logged in, and ASMS displays AFA by default.

For example:

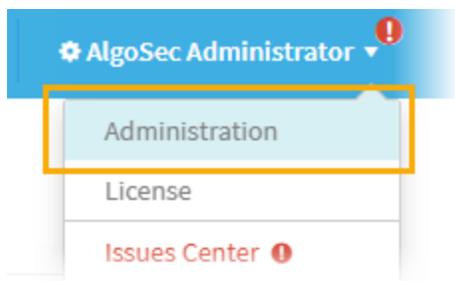


Switch ASMS products

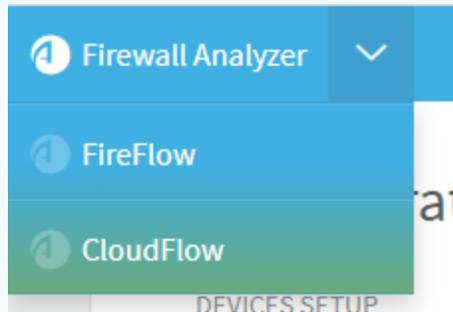
If you are a user in multiple ASMS products, such as AFA, FireFlow, and AppViz, switch between products using the dropdown at the top-left, above the main menu.



If you are an administrator for any of these products, the relevant administration menu is available from your user dropdown at the top-right:



Note: CloudFlow is now accessible from inside ASMS. Click the dropdown at the top-left and select **CloudFlow**.



For more details, see our [CloudFlow Help Center](#).

Adjust your screen space

To adjust the screen space available for your main workspace, hide, display, or change the size of the main menu on the left.

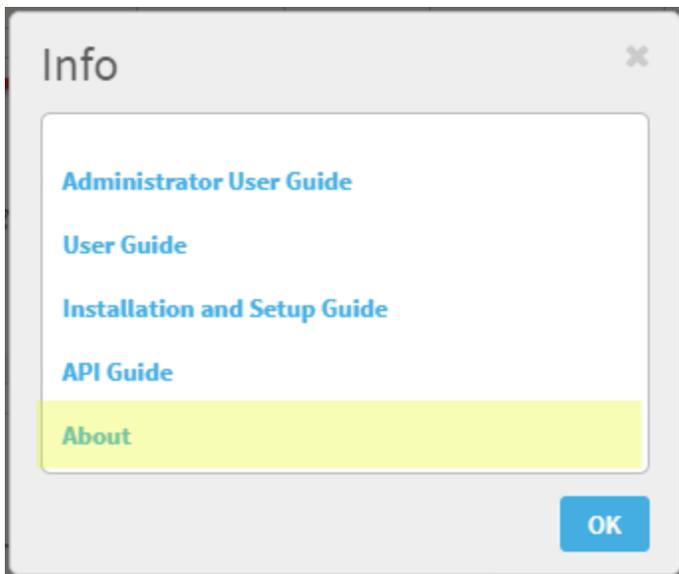
- **To adjust the size of the main menu**, hover between the menu and the workspace and drag the border left or right.
- **To collapse the menu entirely**, click  at the top. When collapsed, click  to expand it again.

View ASMS product details

This procedure describes how you can identify your AFA, FireFlow, or AppViz installation version and build number.

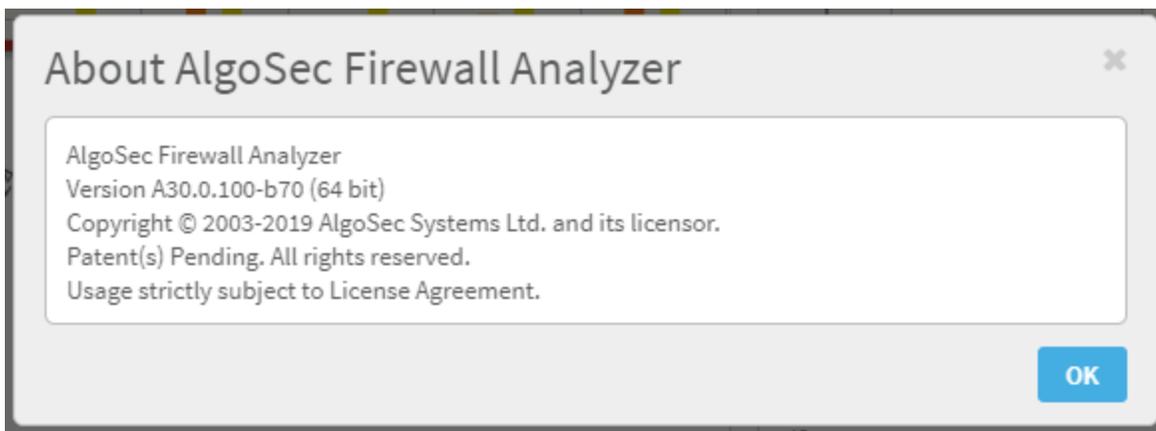
Do the following:

1. In the toolbar, click your username and then select **About** or **Info**.
2. For example, if you're in AFA, in the **Info** dialog, click **About**.



The **About** dialog appears, showing details about the product you have installed.

For example:



Note: If you are running the FIPS 140-2 compliant version of AFA, this information is indicated in the window.

Log out of ASMS

Log out of ASMS by clicking your username at the top right, and selecting **Logout**.

You are logged out of all ASMS products available to you.

Note: If Single Sign On is configured, you must browse to the **Logout** page hosted on your IdP to log out.

For more details, see the *AlgoSec Firewall Analyzer Administrator Guide*.

Manage devices

AFA manages your network security by collecting data from the devices defined in AFA.

Depending on the device's support and the options you enable, add a device to AFA to enable AFA to automatically obtain the device's policy, routing, configuration, and logs.

AFA collects data via analysis or monitoring processes, at configurable intervals.

 [Add / Remove Layer 2 Devices](#): Watch to learn how to manage Layer 2 devices in AFA.

AFA communication protocols

AFA uses encrypted SSH, SOAP, REST or OPSEC communication to access the devices, depending on the available API for the device.

AFA encrypts any stored passwords using the advanced and highly-secure 128 bit AES encryption method (Advanced Encryption Standard).

Once the credentials used to access the device are entered and encrypted in AFA, system administrators can collect device data continuously, without compromising security or having to enter a password each time.

Device procedure reference

For details about adding devices to AFA, see the following:

Generic procedures	<ul style="list-style-type: none">• Add devices to AFA• Add other devices and routing elements• Add/update multiple devices in bulk• Required device permissions• Maintain devices• Specify routing data manually• Integrate AFA and CyberArk
---------------------------	---

Device-specific procedures	<ul style="list-style-type: none"> • Add cloud devices • Add Check Point devices • Add Cisco devices • Add F5 BIG-IP load balancers • Add Fortinet devices • Add Juniper devices • Add Palo Alto Networks devices • Add a Symantec Blue Coat • Add VMware NSX-V devices
-----------------------------------	--

Device icons

Once added to AFA, each device type is shown in the device tree and across the AFA interface using an icon that represents the device's brand or function.

Icon	Description
	Cisco ASA, ACE, IOS Router, or Nexus Router device or security context
	Cisco ACI VRFs and other elements in the Cisco ACI fabric
	Check Point Multi-Domain Security Management (MDSM), Security Management (SmartCenter), or CMA device
	Juniper NetScreen, NSM, SRX, Space, M/E Router, Juniper (non-M/E) router, or Juniper Secure Access (SSL VPN) device
	Fortinet FortiGate or FortiManager device
	Symantec Blue Coat device
	Linux netfilter - iptables device
	Microsoft Azure device
	Palo Alto Networks Firewall or Panorama device
	F5 BIG-IP

Icon	Description
	Forcepoint (McAfee) Security Management Center (formerly known as StoneGate) or Sidewinder device Note: Supported only if the device had been added in an ASMS version earlier than A30.00. For details, see Deprecated devices .
	Topsec Firewall device
	WatchGuard device
	Hillstone Networks device Note: Supported only if the device had been added in an ASMS version earlier than A30.00. For details, see Deprecated devices .
	VMware NSX device
	Amazon Web Services (AWS)
	Avaya - Routing Switch
	Brocade VDX device
	H3C device
	SECUI MF2 device
	Routing Element
	Device configuration file
User-defined icons	A custom device brand. For details, see Extend device support .

Deprecated devices

Support for the Forcepoint brands (Sidewinder, StoneGate) and Hillstone was deprecated in ASMS version A30.00.

If you had defined these devices in an earlier version of ASMS, these devices are still available to you, with all the existing capabilities, but you cannot add new ones after upgrading.

We recommend backing up device data before or after upgrading and then removing these devices from AFA. Make sure to download any report zip files for the device before deleting.

For more details, see the relevant [AlgoPedia](#) KB article.

Additionally, all references to Cisco ASA devices also refer to legacy PIX and FWSM devices. To add a new ASA device to your ASMS system, select ASA options.

Add devices to AFA

This topic provides an introduction on adding devices to AFA so that you can start collecting data automatically.

Add device prerequisites

Before adding a new device to AFA, ensure that your environment is set up to accept communication between AFA and the device.

Manage ports	<p>Note: Make sure to open the necessary port between each device and the AlgoSec server, depending on the protocol being used to connect to the device.</p> <p>Note: In the case of a distributed architecture, open the port between the device and the specific Remote Agent or Load Unit managing each device.</p>
Device permissions	<p>You may need to configure device user permissions to enable AFA to collect data from your device.</p> <p>For details, see Required device permissions.</p>

Access the DEVICES SETUP page

This procedure describes how to access the **DEVICES SETUP** page for each device type.

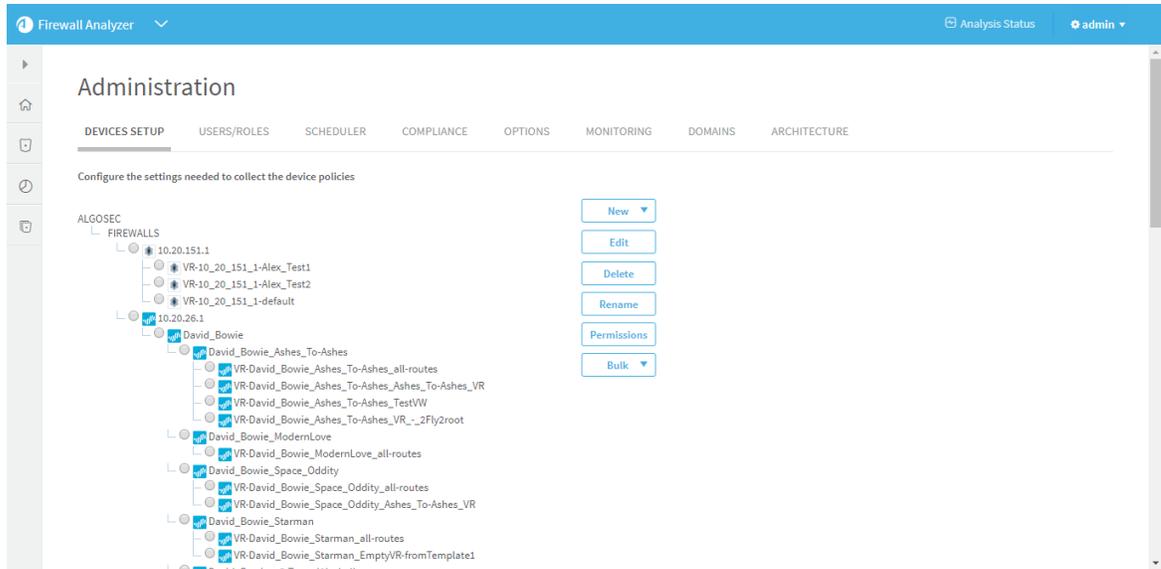
Note: Before you start, ensure that your environment is configured to allow communication between AFA and your device. For details, see [Add device prerequisites](#).

Do the following:

1. Access the **DEVICES SETUP** page in the **Administration** area as follows:

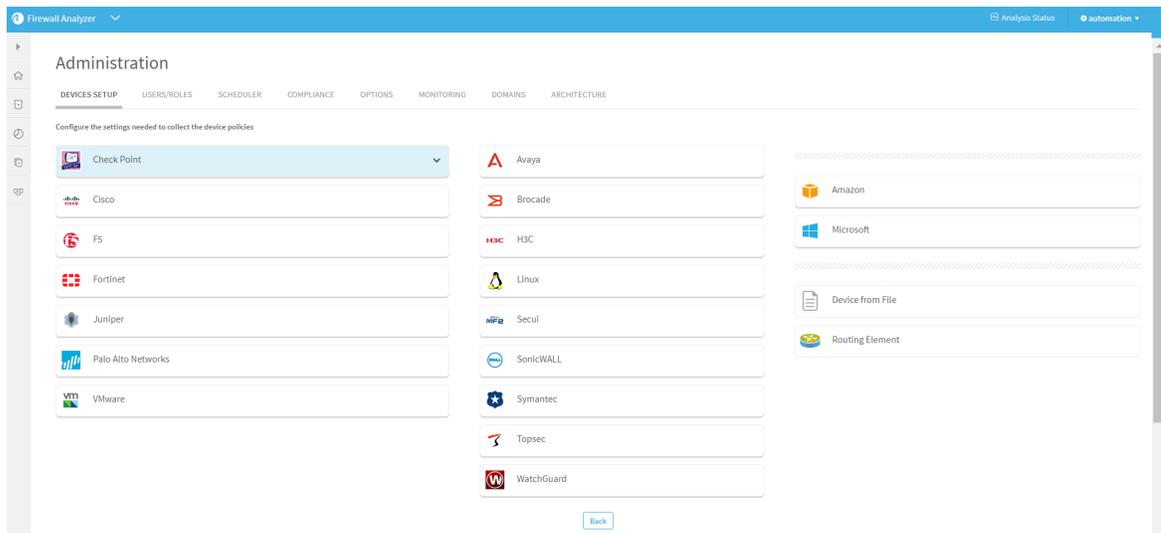
<p>From the main menu on the left</p>	<p>Click Devices, Groups, or Matrics, and then click the  Configure .. button.</p> <p>Note: This button is visible to AFA administrators only.</p>
<p>From the Administration area</p>	<p>In the toolbar, click your username, and select Administration.</p> <p>In the Administration area, click the DEVICES SETUP tab.</p>

The **DEVICES SETUP** tab appears. For example:



2. Click **New** ▼ and select **Devices**.

A selection of vendors appears:



3. Select a vendor, and then a device type.

4. A device form appears, specific to the device type you selected.

For example:

1 Firewall Analyzer Analysis Status AlgoSec Administrator

Administration

DEVICES SETUP USERS/ROLES SCHEDULER COMPLIANCE OPTIONS MONITORING DOMAINS ARCHITECTURE

Configure the settings needed to collect the device policies

vendor device [- Step 1/n]

Access Information

Type: Firepower

Host: (?)

User Name:

Password:

Geographic Distribution

Device managed by (?): Central Manager ▼

ActiveChange

Enable ActiveChange (?)

Cancel Back Next

5. Populate the fields as needed to complete the configuration, clicking **Next** or **Back** as needed.

For more details, see [Device procedure reference](#).

Specify a Syslog-ng server

Many device brands support the ability to send log messages to an external Syslog-ng server.

When relevant, do the following:

- [Select a syslog-ng server](#)
- [Add a new syslog-ng server](#)
- [Edit an existing device](#)

Select a syslog-ng server

Select the syslog-ng server from the list of those already defined in AFA.

Select **localhost** to use the built-in syslog-ng server. No credentials are required for this server.

Note: The **localhost** option is recommended when it is not practical to allocate a dedicated syslog-ng server, such as when you have a small number of devices, are using AFA for evaluation purposes, and so on.

Add a new syslog-ng server

To add a new syslog-ng server, such as if you had one existing before installing AFA, do the following:

1. Click **New** and enter the following details:

Syslog-ng host	The syslog-ng server's host name or IP address.
User Name / SSH User Name	The user name for connecting to the syslog-ng server. Note: If the specified user does not have root permissions, then logs will not be collected for the device until you have manually reloaded the syslog-ng server configuration.
Password / SSH Password	The password for connecting to the syslog-ng server.

2. Click **Test Connectivity** to test connectivity to the defined syslog-ng server.

A message informs you whether AFA connected to the syslog-ng server successfully, and the new syslog-ng server is automatically selected in the **Syslog-ng server** drop-down list.

Tip: Save the device configuration to make this syslog-ng server available for other devices as well.

Edit an existing device

To edit an existing syslog-ng server, do the following:

1. Select the syslog-ng server that you want to edit, and click **Edit**.
2. Edit the properties as needed, and click **OK**.
3. Click **Test Connectivity** to test connectivity to the defined syslog-ng server.

A message informs you whether AFA connected to the syslog-ng server successfully.

➔ **See also:**

- [Defining Check Point Devices](#): Training video about collecting data from a few Check Point devices
- [Defining Cisco, Fortinet, Juniper, McAfee & Palo Alto Devices](#): Training video about collecting data from several different device brands

Add cloud devices

This topic describes how to add an AWS account or Azure subscription to AFA, to be managed and analyzed similarly to on-premises devices.

AWS (Amazon Web Service) accounts in AFA

Add an AWS account to AFA to analyze data using the AWS access key ID you provide.

Analyzed data includes all of the security groups protecting EC2 instances and application load balancers (ALBs), from all AWS regions related to the configured access key. AFA separates these instances into groups called **security sets**. Each AWS security set is a group of instances or ALBs with the same security group and network ACLs, as well as network policies.

For details, see:

- [Network connection](#)
- [Device access requirements for AWS](#)
- [Add an AWS account to AFA](#)

Network connection

The following diagram shows an ASMS Central Manager or Remote Agent connecting to an AWS account via HTTPS-REST (TCP/443).



Tip: ASMS also supports connecting to AWS via a proxy server, which can be configured when adding the device to AFA. For more details, see [Define a device proxy](#).

Device access requirements for AWS

ASMS requires the following permissions for your AWS accounts:

Device analysis

AFA requires minimal read-only access permissions to access AWS and collect data.

This includes the following AWS access keys:

- Access Key ID
- Secret Access Key

We recommend creating a specific IAM user with access keys instead of relying on root user access keys.

This IAM user must have **AmazonEC2ReadOnlyAccess** permissions.

For example:

		Policy Name ↕	Attached Entities ↕	Creation Time ↕	Edited
<input type="checkbox"/>		AmazonEC2ContainerServiceforEC2Role	0	2015-03-19 14:45 EST	2015-
<input type="checkbox"/>		AmazonEC2ContainerServiceFullAccess	0	2015-04-24 12:54 EST	2015-
<input type="checkbox"/>		AmazonEC2ContainerServiceRole	0	2015-04-09 12:14 EST	2015-
<input type="checkbox"/>		AmazonEC2FullAccess	0	2015-02-06 13:40 EST	2015-
<input checked="" type="checkbox"/>		AmazonEC2ReadOnlyAccess	0	2015-02-06 13:40 EST	2015-
<input type="checkbox"/>		AmazonEC2ReportsAccess	0	2015-02-06 13:40 EST	2015-

Tip: You can also use the credentials of another AWS account using the **Assume-Role** functionality. For more details, see [AWS account fields and options](#).

ActiveChange

When ActiveChange is enabled, the IAM user must have read-only permissions, plus the following additional permissions:

- **AuthorizeSecurityGroupIngress**
- **RevokeSecurityGroupEgress**
- **RevokeSecurityGroupIngress**
- **AuthorizeSecurityGroupEgress**

For example:

Actions **Specify the actions allowed in EC2** ? Switch to deny permissions !

[close](#)

Q Security

<input checked="" type="checkbox"/> AuthorizeSecurityGroupEgress ?	<input checked="" type="checkbox"/> AuthorizeSecurityGroupIngress ?	<input checked="" type="checkbox"/> RevokeSecurityGroupIngress ?
<input type="checkbox"/> DescribeSecurityGroupReferences ?	<input type="checkbox"/> CreateSecurityGroup ?	<input type="checkbox"/> UpdateSecurityGroupRuleDescript... ?
<input type="checkbox"/> DescribeSecurityGroups ?	<input type="checkbox"/> DeleteSecurityGroup ?	<input type="checkbox"/> UpdateSecurityGroupRuleDescript... ?
<input type="checkbox"/> DescribeStateSecurityGroups ?	<input checked="" type="checkbox"/> RevokeSecurityGroupEgress ?	

Add an AWS account to AFA

Do the following:

1. Access the **DEVICES SETUP** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Amazon > Web Services (AWS) EC2**.
3. Configure the fields and options as needed.

AWS account fields and options

Access Information	<p>The device type is automatically defined.</p> <p>In the Name field, enter the name that you want to appear in the device tree for this account.</p> <div style="background-color: #e6f2e6; padding: 5px; border: 1px solid #ccc;"> <p>Tip: Use the account's host or route name.</p> </div>
Additional Information	<p>Enter the following details to define access to your AWS account:</p> <ul style="list-style-type: none"> • AWS Access Key ID. Enter your access key, supplied by Amazon. • AWS Secret Key ID. Enter your secret key, supplied by Amazon. • Regions. Select a region. For example: <ul style="list-style-type: none"> ◦ All ◦ China (Beijing) • Assume Role for a Different Account. Select to define this AWS account with the credentials of another AWS account that is already defined in AFA. <p>When selected, also define the Target Account Role ARN (the Amazon Resource Name (ARN) of the role to assume.)</p> <p>For more details, see Device access requirements for AWS.</p>

Route Collection	<p>Select one of the following to determine how AFA should acquire the device's routing data.</p> <ul style="list-style-type: none"> • Automatic. Automatically generate routing data upon analysis or monitoring. • Static Routing Table (URT). Take the device's routing data from a static file that you provide. <p>For details, see Specify routing data manually.</p>
Proxy	<p>Click Set Proxy Server to configure a proxy server to connect all cloud devices defined in AFA, including both AWS and Azure.</p> <p>For more details, see Define a device proxy.</p>
ActiveChange	<p>Select Enable ActiveChange for this device.</p>
Options	<p>Select the following options for your AWS account as needed:</p> <ul style="list-style-type: none"> • Real-time change monitoring. Select this option to enable real-time alerting upon configuration changes. For more details, see Configure real-time monitoring. • Set user permissions. Select this option to set user permissions for this device.

4. Click **Finish**. The new device is added to the device tree.

5. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

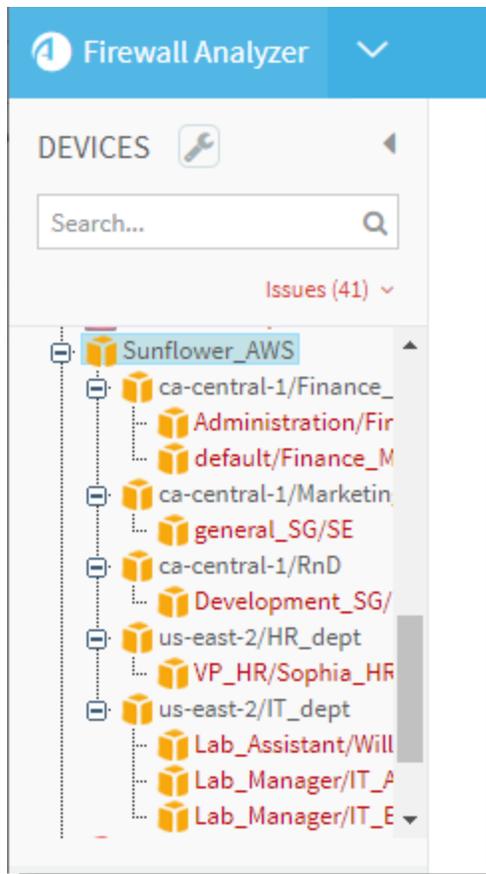
To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the subscription is added.

In the device tree, AWS subscriptions are shown in three levels: the user account, region/VPC, and security set.

For example:



Microsoft Azure subscriptions in AFA

When you add an Azure subscription to AFA, all VMs related to your subscription are represented in the device tree.

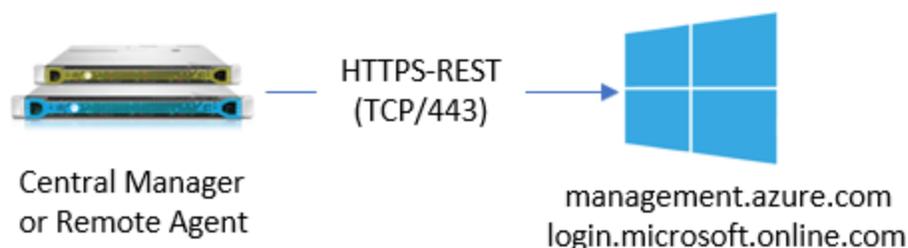
AFA separates the instances into groups called **security sets**. Each Azure security set is a group of VMS with the same security group and subnet security groups, as well as network policies. VMs with no security groups are assigned to a security set called **Unprotected VMs**. To enable accurate traffic simulation, AFA automatically creates a rule to allow all traffic for these VMs.

For more details, see:

- [Network connection](#)
- [Device requirements for Azure](#)
- [Add a Microsoft Azure subscription to AFA](#)

Network connection

The following diagram shows an ASMS Central Manager or Remote Agent connecting to an Azure subscription via HTTPS-REST (TCP/443).



Tip: ASMS also supports connecting to Azure via a proxy server, which can be configured when adding the device to AFA. For more details, see [Define a device proxy](#).

Device requirements for Azure

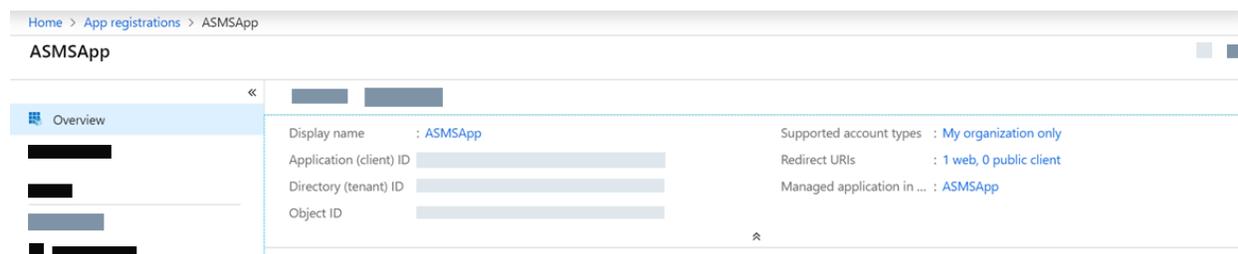
ASMS requires the following permissions for your Azure subscriptions:

Device analysis

AFA requires minimal **Reader** access permissions defined for the subscription to access Azure and collect data.

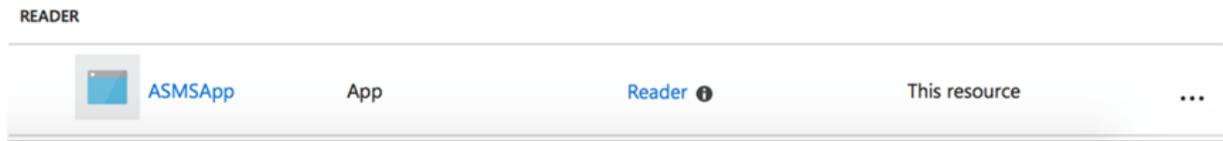
We recommend creating an App Registration with specific permissions instead of sharing an account with other applications.

For example:



The IAM permissions should be **Reader**.

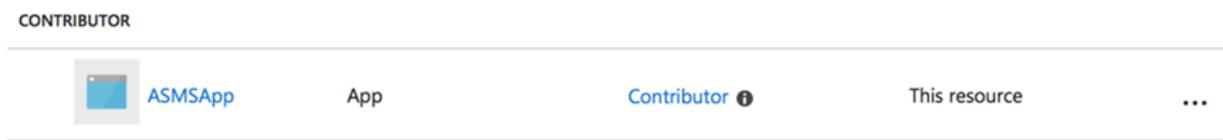
For example:



ActiveChange

When ActiveChange is enabled, the IAM user permissions must be updated to **Contributor**.

For example:



Add a Microsoft Azure subscription to AFA

Do the following:

1. In your Azure account, configure an Active Directory Application to use to connect to AFA.

For details, see [How to configure a Microsoft Azure Active Directory application in AlgoPedia](#).

2. In AFA, access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
3. In the vendor and device selection page, select **Microsoft > Azure**.
4. Configure the fields and options as needed.

Azure subscription field and options

Access Information	<p>Enter the following details:</p> <ul style="list-style-type: none"> • Name. The Azure account's host name or IP address. • Subscription ID. The Azure account's subscription ID. • Tenant ID. The Active Directory Application tenant ID. For more details, see Azure documentation. • Application ID. The application client ID. • Key. The application key.
Route Collection	<p>Select one of the following to determine how AFA should acquire the device's routing data.</p> <ul style="list-style-type: none"> • Automatic. Automatically generate routing data upon analysis or monitoring. • Static Routing Table (URT). Take the device's routing data from a static file that you provide. For details, see Specify routing data manually.
Proxy	<p>Click Set Proxy Server to configure a proxy server to connect all cloud devices defined in AFA, including both AWS and Azure.</p> <p>For more details, see Define a device proxy .</p>
ActiveChange	<p>Select Enable ActiveChange for this device.</p>
Options	<p>Select the following options for your AWS account as needed:</p> <ul style="list-style-type: none"> • Real-time change monitoring. Select this option to enable real-time alerting upon configuration changes. For more details, see Configure real-time monitoring. • Set user permissions. Select this option to set user permissions for this device.

5. Click **Finish**.

The new device is added to the device tree.

6. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

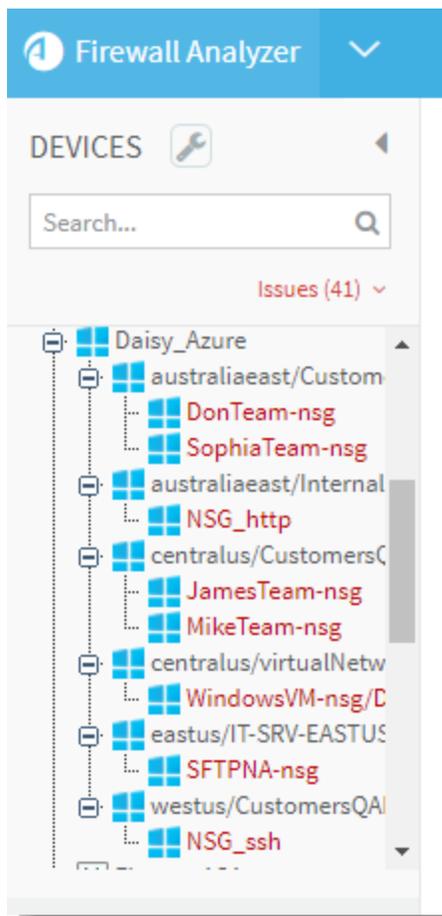
To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the account is added.

In the device tree, Azure has a three-tier hierarchy: subscription, region/VNet, and then security set.

For example:



Add Check Point devices

This topic describes how to add Check Point MDSM, SmartCenter / Gateway, or CMA devices, as well as fields and options shared by all of these device types.

Note: You must also perform procedures on your devices, depending on how you connect to the device from AFA. For details, see [Enable data collection for Check Point devices](#).

Tip: Watch a training video on how AFA can collect data from a few Check Point devices. See [Defining Check Point Devices](#) on the AlgoSec portal.

Check Point network connections

The following diagrams shows an ASMS Central Manager or Remote Agent connecting to a Check Point MDSM, CMA, or Smart Center device, and a Check Point Gateway. Check Point versions R80 or higher have an additional connection via HTTP-REST.



Note: If your CLM/MLM log servers reside on separate hosts, you'll need to connect to these separately from ASMS.

Check Point device permissions

AFA can collect data or logs via SSH or OPSEC. For Check Point versions R80 and higher, you must also define data collection via REST.

ASMS requires the following permissions for each type of connection to your Check Point devices:

Connections via OPSEC (recommended)

ASMS requires minimal read-only CPMI and LEA OPSEC object permissions to connect to Check Point devices, and automatically initiates log collection via the defined LEA connection.

In the Check Point interface, define your permissions as follows:

CPMI	Select the following CPMI permissions: <ul style="list-style-type: none"> • Allow access via Management Portal and SmartConsole Applications • Permissions > Read Only All. To use ActiveChange, select Read/Write All.
LEA	On the LEA Permissions tab, under Permissions to Read Logs , select Show all log fields .

Note: Create a separate OPSEC Object and permissions profile for ASMS use only. Using the **Administrator** profile results in failures due to Check Point configurations.

For more details, see [Create a Check Point OPSEC Certificate for Check Point Devices \(R77 and Lower\)](#).

Connections via SSH

ASMS must have SSH access to the relevant management and log devices, such as PV-1, CMA, SmartCenter, external log server, or CLM.

- For **SecurePlatform (SPLAT)**, ASMS must be allowed to switch to **expert** mode.
- For **Solaris/RHEL/IPSO**, ASMS must connect as the **root** user.

Public key authentication is also supported. In such cases, the following permissions are required:

Read	AFA requires read permissions on the domain folders, such as \$FWDIR/conf or \$FWDIR/log .
Write	AFA writes a package containing the required configuration in the /tmp or /var/tmp directory, based on the device platform, such as SP or Solaris. AFA also requires write permissions in the \$FWDIR/conf directory for temporary log files.
Execute	AFA runs several commands on the management device, including fwm logexport for logs and cpstat for routing.

For more details, see [How to Configure the AlgoSec Firewall Analyzer SSH Client to Use Public Key Authentication](#) in AlgoPedia and [Enable data collection via SSH](#).

REST connections (R80 and higher only)

When using a Check Point device version R80 or higher, AFA also collects data via REST, in addition to OPSEC or SSH.

In addition to OSPEC or SSH permissions, ASMS must have permissions to execute REST calls to the Check Point Security Management Server.

- Minimum permissions required is **Read Only All**.
- When ActiveChange is enabled, the minimum permissions are **Read Write All**.

For more details, see [Enable data collection via REST](#)

Add a Check Point Multi-Domain Security Management device

Check Point Multi-Domain Security Management (MDSM) integrates multiple 'firewalled' networks within a single administrative framework. These devices consolidate multiple SmartCenter Servers, referred to as Customer Management Add-ons (CMAs), on a single host.

AFA analyzes the Filter Module security policy via a secure connection to the MDSM server.

Note: Multi-Domain Security Management, or MDSM, refers to both MDSM and

Provider-1 devices.

Do the following:

1. Access the **DEVICES SETUP** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Check Point > Multi Domain Security Management (Provider-1)**.

Configure the fields and options on the page as needed. For details, see [Check Point fields and options](#).

Note: If you select to enable ActiveChange, the **ActiveChange License Agreement** appears. Select the **I agree** checkbox, and then click **OK**.

3. Click **Next**.

The fields on the **Check Point - Multi-Domain Security Management (Provider-1) - Step 2/3** page differ, depending on whether you selected to connect to the device via SSH or OPSEC.

4. Do one of the following:

OPSEC	Recommended. Enter the IP address of the CMA that manages the devices you wish to analyze.
SSH	Select the CMA that manages the devices you wish to analyze by clicking the relevant row.

5. Click **Next**.

The **Check Point - Multi-Domain Security Management (Provider-1) - Step 3/3** page appears.

This page displays a table listing all the devices that are managed by the Check Point MDSM, including standalone devices and virtual systems.

6. **Optional:** Configure AFA to use logs created by a managed device or virtual system.

Tip: This enables AFA to detect certain policy optimization information, such as unused rules.

Do the following:

- a. In the **Add Device** column, select the check box next to the device's name.
- b. In the **Log Analysis** column, select one of the following:
 - **None.** Disables logging.
 - **Standard.** Enables logging.
 - **Extensive.** Enables logging and the Intelligent Policy Tuner.
- c. In the **Log Server** column, click **Settings**. Then, do one of the following:
 - Select the log server you want to use from the drop-down list.
 - Select **Other** and enter the log server's name manually.

Click **OK** when you're done.

- d. **SSH only:** To edit SSH definitions, **Edit SSH definitions**.

In the **Check Point Log Server SSH Setup** dialog, do the following:

- Specify whether this log server is part of a **Multi-domain log module (MLM/CLM)** or a **Stand-alone log server**.
 - Populate the fields as needed. For details, see [Log Server fields](#).
- e. **OPSEC only:** To test OPSEC connectivity to the defined log server, click **Test OPSEC connectivity**.

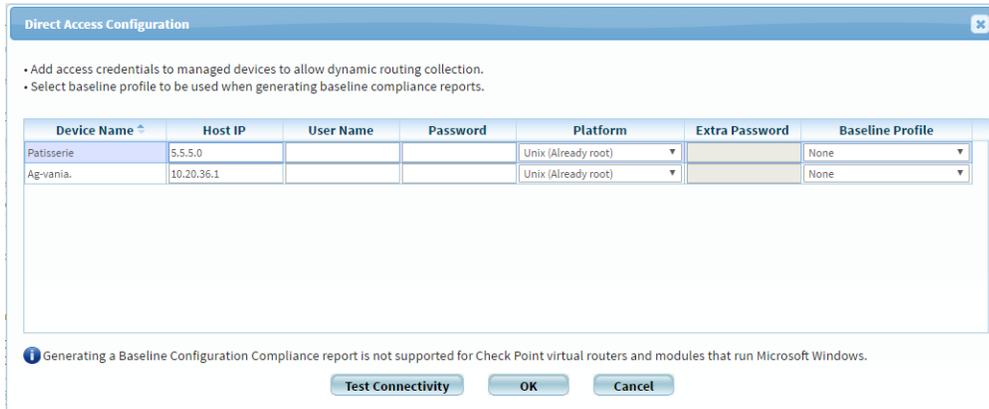
A message informs you whether AFA connected to the log server successfully.

- f. Click **OK**.

7. **Optional:** Enable AFA to generate baseline compliance reports and/or allow dynamic routing collection for all managed devices.

Do the following:

- a. In the **Direct access to managed devices** area, click .
- b. The **Direct Access Configuration** dialog box appears.



The dialog box titled "Direct Access Configuration" contains the following instructions and table:

- Add access credentials to managed devices to allow dynamic routing collection.
- Select baseline profile to be used when generating baseline compliance reports.

Device Name	Host IP	User Name	Password	Platform	Extra Password	Baseline Profile
Patisserie	5.5.5.0			Unix (Already root)		None
Ag-vania.	10.20.36.1			Unix (Already root)		None

Generating a Baseline Configuration Compliance report is not supported for Check Point virtual routers and modules that run Microsoft Windows.

Buttons: **Test Connectivity**, **OK**, **Cancel**

- c. Complete the fields as needed. For details, see [Baseline Configuration Compliance fields](#)

Note: Specifying this information for a device triggers a direct SSH connection to the device.

- d. Click **OK**.

8. Complete the remaining fields as needed. For details, see [Additional Check Point options](#).
9. Click **Finish**.

The new device is added to the device tree.

Set user permissions

If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account. To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

Add a Check Point SmartCenter/Gateway

Check Point products are based on a distributed architecture, where a typical Check Point deployment is composed of a Filter Module or device and the SmartCenter Server.

- **A standalone deployment** is the simplest deployment where the SmartCenter Server and the Filter Module are installed on the same machine.
- **A distributed deployment** is a more complex deployment where the Filter Module and the SmartCenter Server are deployed on different machines.

AFA provides an analysis of the Filter Module's security policy via a secure connection to the SmartCenter server.

Tip: Watch a training video on how AFA can collect data from a few Check Point devices. See [Defining Check Point Devices](#) .

Do the following:

1. Access the **DEVICES SETUP** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Check Point > Security Management (SmartCenter)**.

Configure the fields and options on the page as needed. For details, see [Check Point fields and options](#).

Note: If you select to enable ActiveChange, the **ActiveChange License Agreement** appears. Select the **I agree** checkbox, and then click **OK**.

3. Click **Next**.

The **Check Point - Security Management (SmartCenter) - Step 2/2** page appears, displaying a table that lists all the devices that are managed by the

Check Point SmartCenter/Gateway, including standalone devices and virtual systems.

4. **Optional:** Configure AFA to use logs created by a managed device or virtual system.

Tip: This enables AFA to detect certain policy optimization information, such as unused rules.

Do the following:

- a. In the **Add Device** column, select the check box next to the device's name.
- b. In the **Log Analysis** column, select one of the following:
 - **None.** Disables logging.
 - **Standard.** Enables logging.
 - **Extensive.** Enables logging and the Intelligent Policy Tuner.
- c. In the **Log Server** column, click **Settings**. Then, do one of the following:
 - Select the log server you want to use from the drop-down list.
 - Select **Other** and enter the log server's name manually.

Click **OK** when you're done.

- d. **SSH only:** To edit SSH definitions, **Edit SSH definitions**.

In the **Check Point Log Server SSH Setup** dialog, do the following:

- Specify whether this log server is part of a **Multi-domain log module (MLM/CLM)** or a **Stand-alone log server**.
 - Populate the fields as needed. For details, see [Log Server fields](#).
- e. **OPSEC only:** To test OPSEC connectivity to the defined log server, click **Test OPSEC connectivity**.

A message informs you whether AFA connected to the log server successfully.

- f. Click **OK**.

5. **Optional:** Enable generation of baseline compliance reports and/or allow dynamic routing collection for all managed devices.

To do so, in the **Direct access to managed devices** area, click **Configure**.

The **Direct Access Configuration** dialog box appears.

Device Name	Host IP	User Name	Password	Platform	Extra Password	Baseline Profile
Patisserie	5.5.5.0			Unix (Already root)		None
Ag-vania.	10.20.36.1			Unix (Already root)		None

Generating a Baseline Configuration Compliance report is not supported for Check Point virtual routers and modules that run Microsoft Windows.

Test Connectivity OK Cancel

Complete the fields as needed, and click **OK**. For details, see [Baseline Configuration Compliance fields](#).

Note: Specifying this information for a device triggers a direct SSH connection to the device.

- Complete the remaining fields using the information in Check Point Options Fields (see [Additional Check Point options](#)).
- Click **Finish**.

The new device is added to the device tree.

Set user permissions

If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account. To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

Add a Check Point CMA

You can add single Customer Management Add-ons (CMAs) using the following procedure.

Tip:

- Add multiple CMAs at once by adding a Check Point MDSM. For details, see [Add Check Point devices](#).
- Watch a training video on how AFA can collect data from a few Check Point devices. See [Defining Check Point Devices](#) .

Do the following:

1. Access the **DEVICES SETUP** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Check Point > Single CMA**.
Configure the fields and options on the page as needed. For details, see [Check Point fields and options](#).

Note: If you select to enable ActiveChange, the **ActiveChange License Agreement** appears. Select the **I agree** checkbox, and then click **OK**.

3. Click **Next**.

The **Check Point - Single CMA - Step 2/2** page appears, displaying a table that lists all the devices that are managed by the Check Point CMA, including standalone devices and virtual systems.

4. **Optional:** Configure AFA to use logs created by a managed device or virtual system.

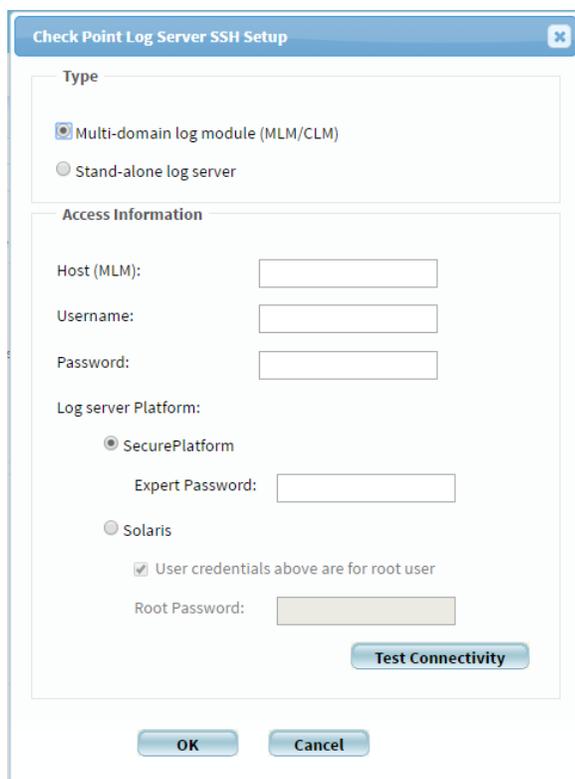
Tip: This enables AFA to detect certain policy optimization information, such as unused rules.

Do the following:

- a. In the **Add Device** column, select the check box next to the device's name.
- b. In the **Log Analysis** column, select one of the following:
 - **None.** Disables logging.
 - **Standard.** Enables logging.
 - **Extensive.** Enables logging and the Intelligent Policy Tuner.
- c. In the **Log Server** column, click **Settings**. Then, do one of the following:
 - Select the log server you want to use from the drop-down list.
 - Select **Other** and enter the log server's name manually.

Click **OK** when you're done.

- d. **SSH only:** To edit SSH definitions, **Edit SSH definitions**.



The screenshot shows the "Check Point Log Server SSH Setup" dialog box. It has a title bar with a close button. The dialog is divided into two main sections: "Type" and "Access Information".

Type:

- Multi-domain log module (MLM/CLM)
- Stand-alone log server

Access Information:

Host (MLM):

Username:

Password:

Log server Platform:

- SecurePlatform
 - Expert Password:
- Solaris
 - User credentials above are for root user
 - Root Password:

At the bottom of the "Access Information" section is a "Test Connectivity" button. At the bottom of the dialog are "OK" and "Cancel" buttons.

In the **Check Point Log Server SSH Setup** dialog, do the following:

- Specify whether this log server is part of a **Multi-domain log module (MLM/CLM)** or a **Stand-alone log server**.
 - Populate the fields as needed. For details, see [Log Server fields](#).
- e. **OPSEC only:** To test OPSEC connectivity to the defined log server, click **Test OPSEC connectivity**.

A message informs you whether AFA connected to the log server successfully.

- f. Click **OK**.

5. **Optional:** Enable generation of baseline compliance reports and/or allow dynamic routing collection for all managed devices.

To do so, in the **Direct access to managed devices** area, click **Configure**.

The **Direct Access Configuration** dialog box appears.

Device Name	Host IP	User Name	Password	Platform	Extra Password	Baseline Profile
Patisserie	5.5.5.0			Unix (Already root)		None
Ag-vania.	10.20.36.1			Unix (Already root)		None

Generating a Baseline Configuration Compliance report is not supported for Check Point virtual routers and modules that run Microsoft Windows.

Test Connectivity OK Cancel

Complete the fields as needed, and click **OK**. For details, see [Baseline Configuration Compliance fields](#).

Note: Specifying this information for a device triggers a direct SSH connection to the device.

6. Complete the remaining fields using the information in Check Point Options Fields (see [Additional Check Point options](#)).
7. Click **Finish**. The new device is added to the device tree.
8. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Check Point fields and options

Check Point devices include the following types of fields and options:

Access Information

Host	Enter the host name or IP address of the device.
R80 or higher	Select this option for devices versions R80 or higher. For R80 devices, you must configure the Management API Settings of the device to accept API calls from the IP address of the AlgoSec server. For more information, see Enabling REST Calls to the Security Management Server (see Enable data collection via REST).

Connect via	<p>Specify how AFA should connect to the device, by selecting one of the following:</p> <ul style="list-style-type: none"> • SSH: Connect via SSH (Secure Shell protocol). This option is not available when adding a single Check Point CMA. • OPSEC (NGX R60 or higher): Connect via OPSEC. Recommended. <p>To specify a custom port, select Custom Port and enter the port number.</p> <p>Note: For Windows environments, only OPSEC is supported.</p> <p>Tip: Configure AFA to connect to the device using SSH with Public-Key authentication. To do so, select the Use public key authentication in data collection check box in the General sub-tab of the Options tab in the Administration area. For details, see Define AFA preferences.</p>
User Name / Password	<p>Type the user name and password to access the device.</p> <p>These fields only appear if you selected R80 or higher or you selected SSH in the Connect via area.</p> <p>For more details, see Required device permissions.</p>
SecurePlatform	<p>Choose this option to specify that the device is installed on a Check Point SecurePlatform operating system.</p> <p>You must complete the Expert Password field.</p> <p>This field only appears if you selected SSH in the Connect via area.</p>
Expert Password	<p>Type the expert password, which allows access to all the functions on the SmartCenter server required for this process.</p> <p>This field only appears if you selected SSH in the Connect via area.</p>

Solaris / RedHat Linux	Choose this option to specify that the device is installed on a Solaris or RedHat Linux operating system. This field only appears if you selected SSH in the Connect via area.
User credentials above are for root user	Select this option to specify that the user name and password entered in the User Name and Password fields are the credentials for the Solaris root user. If you clear this option, you must complete the Root Password field. This field only appears if you selected SSH in the Connect via area.
Root Password	Type the root password for Solaris. This field only appears if you selected SSH in the Connect via area.
High Availability	Select this option to configure High Availability for CMAs. Important: AFA connects to the HA cluster using the active IP address, not the virtual IP address. You must configure access rules for each device in the cluster to allow this traffic. This field only appears if you selected OPSEC in the Connect via area. It is not relevant for Check Point MDSM.
Secondary Security Management (SmartCenter)	Type the secondary CMA. This field only appears if you selected OPSEC in the Connect via area. It is not relevant for Check Point MDSM.

Geographic Distribution

In the **Device managed by** field, select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

Log Collection

Select the log collection method to use.

If you choose **SSH**, you must enable AFA to analyze application control traffic logs. For more details, see [Enable data collection via SSH](#). If you do not perform this step, then information related to application control traffic will not appear in the device report's **Policy Optimization** page.

This area only appears if you selected **OPSEC** in the **Connect via** area.

OPSEC Setup

This area enables you to specify which certificate to use for OPSEC access to the device.

For more information, see [Specifying a Certificate for OPSEC Access to the Check Point Device](#) (see [Enable data collection via OPSEC](#)).

This area only appears if you selected **OPSEC** in the **Connect via** area.

ActiveChange

This area only appears if you selected **OPSEC** in the **Connect via** area.

Select to **Enable ActiveChange** to enable ActiveChange for the device.

Note: This option is unavailable for version R80 or higher.

Log Server fields

Check Point log server fields include the following:

Host (MLM)	Type the host name or IP address of the log server.
Username	Type the user name to use for SSH access to the log server.
Password	Type the password to use for SSH access to the log server.
Secure Platform	Choose this option to specify that the log server is installed on a Check Point SecurePlatform operating system. You must complete the Expert Password field.

Expert Password	Type the expert password, which allows access to all the functions on the log server required for this process.
Solaris	Choose this option to specify that the log server is installed on a Solaris operating system.
User credentials above are for root user	Select this option to specify that the user name and password entered in the Username and Password fields are the credentials for the Solaris root user. If you clear this option, you must complete the Root Password field.
Root Password	If you use a user <i>other than</i> "root" for accessing the Solaris OS, type the root password for Solaris.
Test Connectivity	Click this button to test connectivity to the defined log server. A message informs you whether AFA connected to the log server successfully.

Baseline Configuration Compliance fields

Check Point baseline configuration compliance fields include the following:

Host IP	Type the IP address of the device.
User Name	Type the user name to access the device.
Password	Type the password to access the device.
Platform	Select the device's platform. This field only appears for Check Point devices.
Extra Password	Type the password to use for running OS commands on the device. This field only appears for Check Point devices.

Baseline Profile	<p>Select the baseline compliance profile to use.</p> <p>The drop-down list includes all baseline compliance profiles in the system. For more information on baseline compliance profiles and instructions for adding new baseline compliance profiles, see Customizing Baseline Configuration Compliance Profiles (see Customize baseline configuration profiles).</p> <p>To disable Baseline Compliance Report generation for this device, select None.</p>
Test Connectivity	<p>Click this button to test connectivity to the defined device.</p> <p>A message informs you whether AFA connected to the device successfully.</p>

Additional Check Point options

Check Point devices have the following additional options:

Real-time change monitoring	<p>Select to enable real-time alerting upon configuration changes.</p> <p>For more details, see Configure real-time monitoring.</p>
Set user permissions	<p>Select to set user permissions for this device</p>
Collect audit logs from CLM	<p>Select to collect audit logs from a CLM.</p> <p>Note: When this option is enabled, all modules must be configured to collect logs from <i>the same CLM</i>.</p>
Log collection frequency	<p>Enter the interval of time in minutes, at which AFA should collect logs for the Check Point device.</p>

Configure one-armed mode manually

AFA automatically identifies Check Point CloudGuard devices in one-armed mode, when the device has a single interface. If your device has multiple interfaces and one-armed mode is not identified automatically, configure this for your device manually.

Do the following:

1. On the AFA machine, access your device configuration **meta** file as follows:

```
/home/afa/.fa/firewalls/<device_name>/fwa.meta
```

where **<device_name>** is the name of the device listed. If your device is listed multiple times, enter the longer name.

2. On a new line, enter:

```
is_steering_device=yes
```

3. Run an analysis on the device to update the device data in AFA.

Enable data collection for Check Point devices

In order for AFA to collect data from a Check Point device, you must configure certain settings on the device itself. AFA collects data from Check Point devices using either SSH or OPSEC, and for Check Point versions R80 and above, AFA collects data via REST (along with either SSH or OPSEC). You must enable the data collection requirements for every method you use.

Note: In addition to the requirements listed below, ensure that the user that AFA is using to access the device has the required permissions. The minimum permission required is **Read Only All**. When the device is using ActiveChange, the minimum permission is **Read Write All**. For more details, see [Required device permissions](#).

For more details, see [Add Check Point devices](#).

Enable data collection via SSH

This procedure describes how to enable AFA to process Check Point application control traffic logs.

AFA can be configured to collect logs from a Check Point device via SSH, but special configuration is required on the Check Point device. Application control traffic logs

include the `app_rule_id` field, and this field is masked by default for the SSH log collection user that is specified when adding the device to AFA. As a result, AFA cannot process application control logs that are collected via SSH, nor use them to generate information for the **Application Control Rules Cleanup** area of the device report's **Policy Optimization** page.

In order to enable AFA to process application control traffic logs, you must modify permissions for the `app_rule_id` field on the Check Point device, as described in the following procedure.

Note: For R80 and above, AFA collects data via REST (along with either SSH or OPSEC). For more details, see [Enable data collection via REST](#).

Do the following:

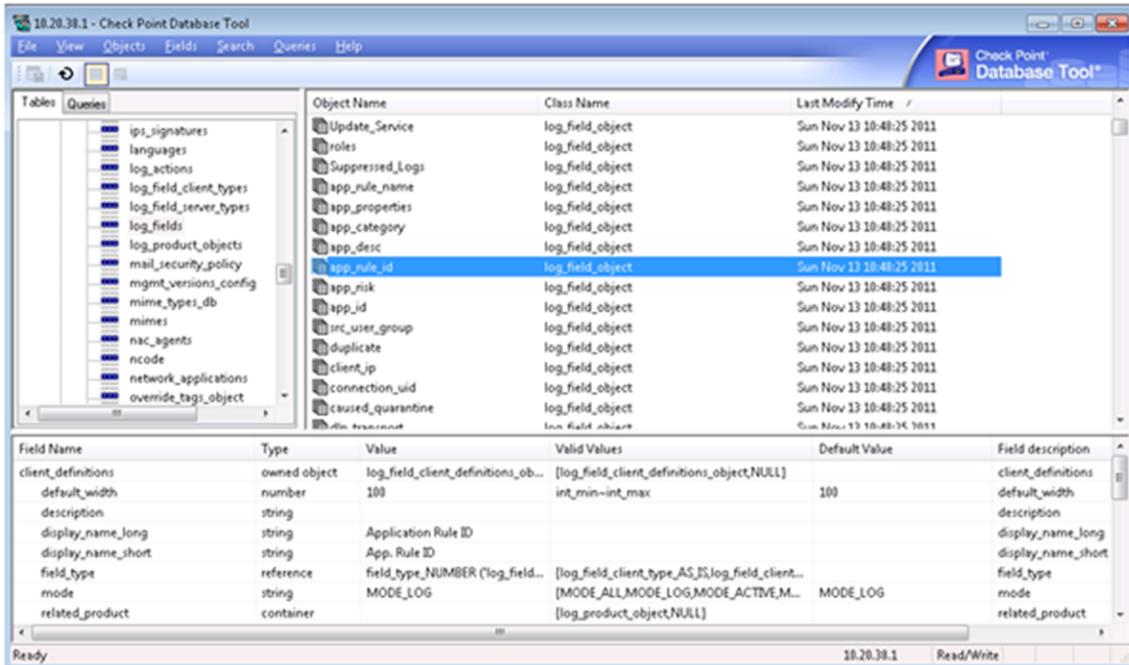
1. Run **GuiDBedit.exe**, and connect to the Check Point device's management station.

The management station is typically located at **C:\Program Files (x86)\CheckPoint\SmartConsole\RXX\PROGRAM**

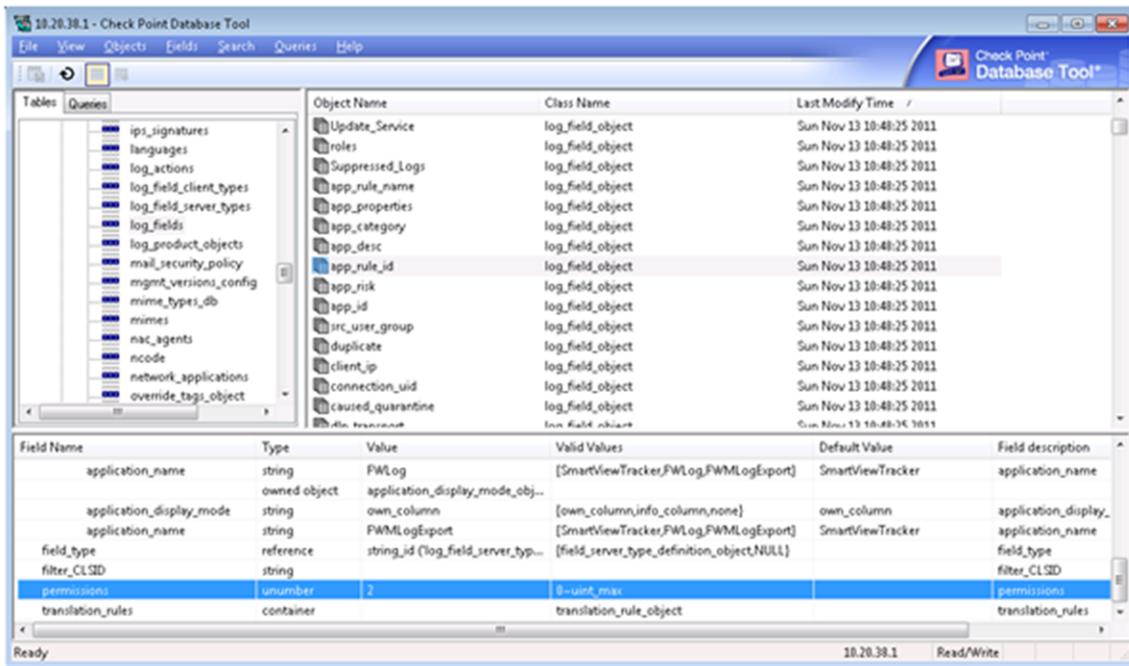
where **RXX** is the version number.

2. In the left pane, navigate to **Other > log_fields**.
3. In the right pane, click on **app_rule_id**.

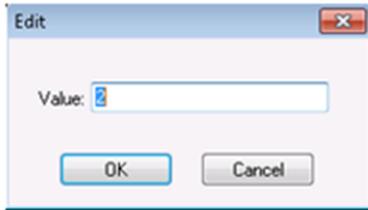
The bottom pane displays the fields that are displayed for **app_rule_id**.



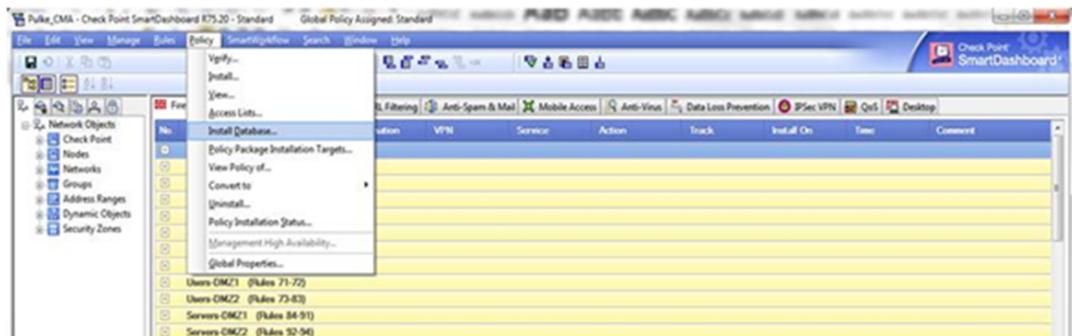
4. In the bottom pane, double-click on the **permissions** field.



The **Edit** dialog box appears.



5. In the **Value** field, change the value from **2** to **0**.
6. Click **OK**.
7. Save your changes and exit the program.
8. If the device sends its traffic logs to a log server other than the management station (for example, a CLM or external log server), do the following:
 - a. Connect to the Check Point device's management station via SmartDashboard.
 - b. Re-install the Check Point database on the log server, by selecting **Policy** and then **Install Database** from the main menu.



- c. Exit the program.

Enable data collection via OPSEC

This procedure describes how to specify a certificate for OPSEC access to a Check Point device, which must be performed in the **Check Point - Multi-Domain Security Management (Provider-1) - Step 1/3** or **Check Point - SmartCenter or CMA - Step 1/2** page after selecting OPSEC as the connection method.

Do the following:

1. Create a certificate for your device. For more details, see:
 - [Create a Check Point OPSEC Certificate for a MDSM \(R80 and Higher\)](#)
 - [Create a Check Point OPSEC Certificate for a CMA/SMC \(R80 and Higher\)](#)
 - [Create a Check Point OPSEC Certificate for Check Point Devices \(R77 and Lower\)](#)
2. In AFA, in the **OPSEC Setup** area, click **Certificate**.

The **Retrieve a new OPSEC certificate** dialog box appears.

3. Complete the fields as follows:

OPSEC Application Name	Type the OPSEC application name, as specified in the OPSEC certificate. The default value is "AlgoSec".
One Time Password	Type the one-time password, as specified in the OPSEC certificate.
Advanced	Click to display advanced fields. The CPMI Authorization Type , CPMI Port , LEA Authorization Type , and LEA Port fields appear.

CPMI Authorization Type	Select the CPMI authorization type.
CPMI Port	Type the CPMI port number. The default value is 18190.
LEA Authorization Type	Select the LEA authorization type.
LEA Port	Type the LEA port number. The default value is 18184.

- Click **OK** to retrieve the certificate from the Check Point SmartCenter, CMA or MDSM server.

Once the certificate is installed, a confirmation window appears.

- Click **OK**.

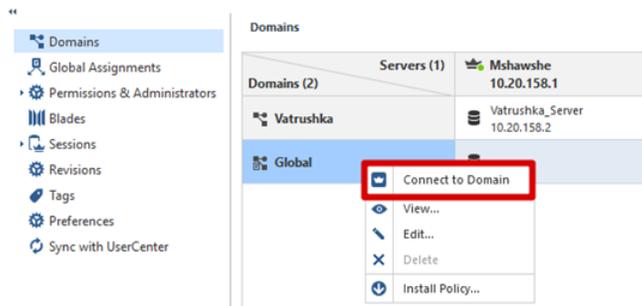
The **OPSEC Setup** area displays the certificate date and time of creation.

Create a Check Point OPSEC Certificate for a MDSM (R80 and Higher)

In order for AFA to collect data from a CheckPoint MDSM via OPSEC, a global certificate needs to be created for authentication and security purposes. The certificate is created using Check Point's **SmartConsole** for the PV-1.

Do the following:

- Connect to the SmartConsole, selecting the **MDS** domain.
- Right-click **Global** and select **Connect to Domain**.

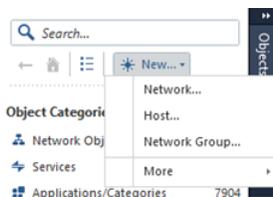


3. Create a network object for the host that will run AFA

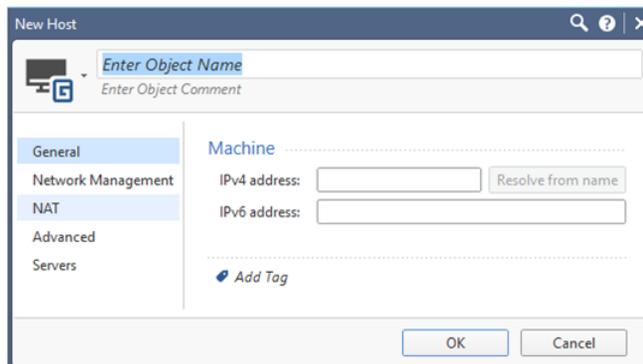
Note: If a network object for the host is already defined, you can skip this step.

Do the following:

- a. Click **New**, and then **Host**.



The **New Host** window appears.



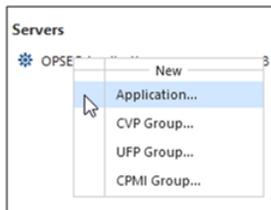
- b. Complete the **Object Name** and **IPv4 Address** fields with the name and address of the host that will run AFA.
- c. Click **OK**.

4. Create an OPSEC application object for this network object.

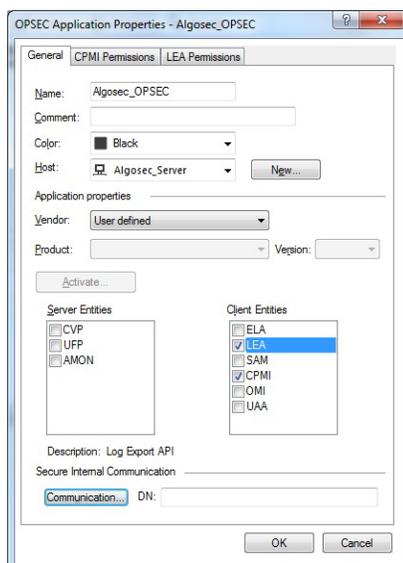
Note: If an OPSEC application object is already defined, you can skip this step.

Do the following:

- a. In the **Object Categories**, under **Servers**, select **OPSEC Applications > Application**.



The **OPSEC Application Properties** dialog box appears.



- b. In the **OPSEC Application Properties** dialog, define the following:

Name	Enter the OPSEC application name. Note: Record the name you entered here. You'll need to specify this name in AFA when you retrieve the certificate.
Host	Select the host to run AFA.

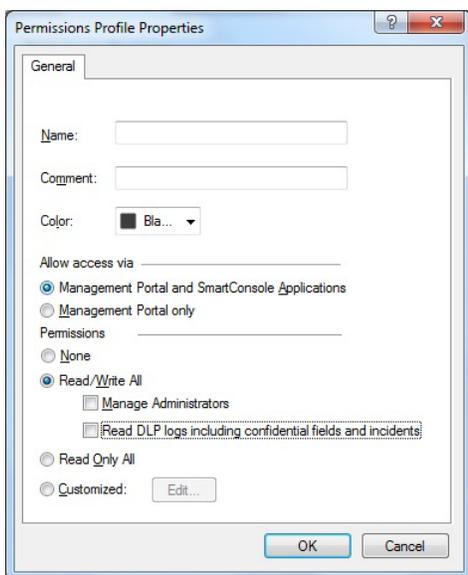
Object Entities	Select the LEA and CPMI items.
------------------------	--

The **LEA Permissions** and **CPMI Permissions** tabs appear.

- c. In the **CPI Permissions** tab, select **Permissions Profile**, and then do one of the following:
- Select the **super** profile in the list, or any other profile with the required minimum permissions.
 - Create a new permission profile. To do this, click **New**. In the **Permissions Profile Properties** dialog, enter a name for your new profile and select the required permissions.

Minimum permissions required are **Read Only All** access. If you're using ActiveChange, you must have **Read/Write All** access.

For example:



- d. In the **LEA Permissions** tab, select **According to Permissions Profile**, and then do one of the following:

- Select the **super** profile in the list, or any other profile with the required minimum permissions.
- Create a new permission profile. To do this, click **New**. In the **Permissions Profile Properties** dialog, enter a name for your new profile and select the required permissions.

Minimum permissions required are **Read Only All** access.

- e. Click **OK**. The **General** tab appears again, with additional options.

5. Create your certificate. Do the following:

- a. Click **Communication**.
- b. In the **Communication** dialog that appears, enter a one-time password , and then enter it again to confirm.

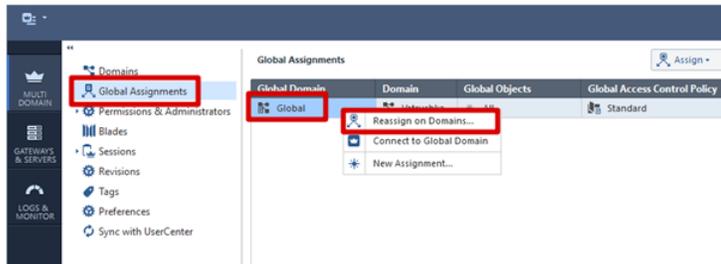
Note: Record the password you entered here. You'll need to specify this name in AFA when you retrieve the certificate.

- c. Click **Initialize**.

The **Trust state** will change from **Uninitialized** to **Initialized but trust not established**. After the certificate is retrieved by AFA, the trust state will change to **Trusted**.

Tip: Create a new certificate if needed by clicking **Reset** and repeating this step.

6. At the top of the screen, click **Publish**.
7. Connect to the MDS (PV-1) console, and select **Global Assignments**.
8. Right-click **Global** and select **Reassign on Domains**.



Continue with [Enable data collection via OPSEC](#).

Create a Check Point OPSEC Certificate for a CMA/SMC (R80 and Higher)

In order for AFA to collect data from a CheckPoint CMA or SMC via OPSEC, a local certificate needs to be created for authentication and security purposes. The certificate is created using Check Point's **SmartConsole** for the CMA/SMC.

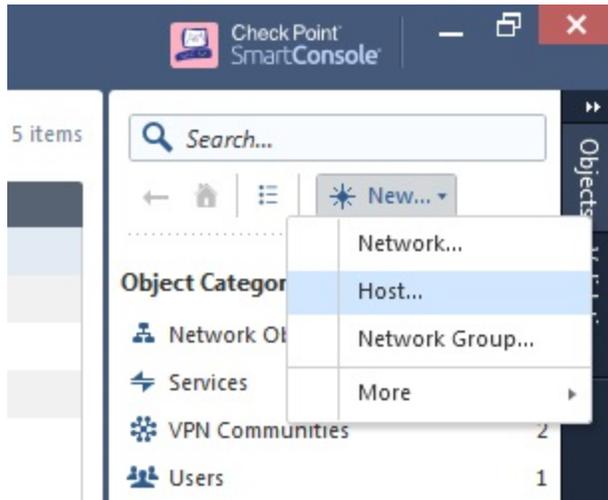
Do the following:

1. Connect to the SmartConsole.
2. Create a network object for the host that will run AFA.

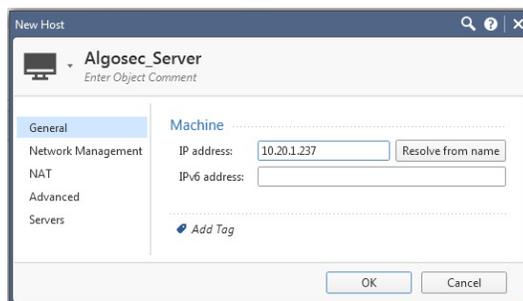
Note: If a network object for the host is already defined, you can skip this step.

Do the following:

- a. In the right pane, click the **New** button and select **Host**.



- b. In the **New Host** dialog, enter the **Name** and **IP address** of the host that will run AFA, and click **OK**.

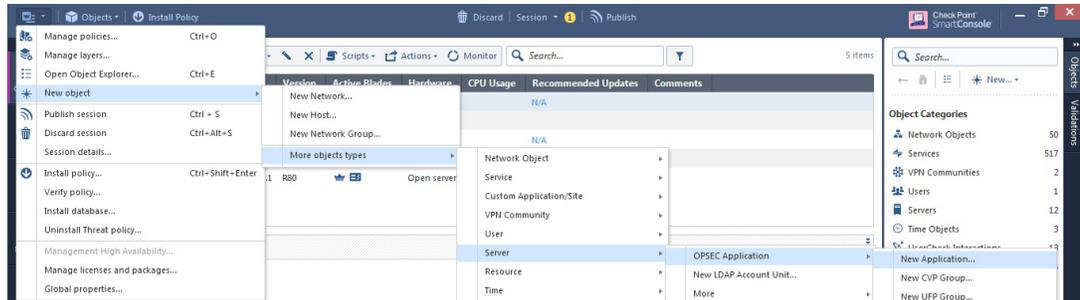


3. Create an OPSEC application object for this network object.

Note: If an OPSEC application object is already defined, you can skip this step.

Do the following:

- a. Click the  icon at the top left of the screen and select:
New object > More object types > Server > OPSEC Application > New Application.



b. In the **OPSEC Application Properties** dialog, define the following:

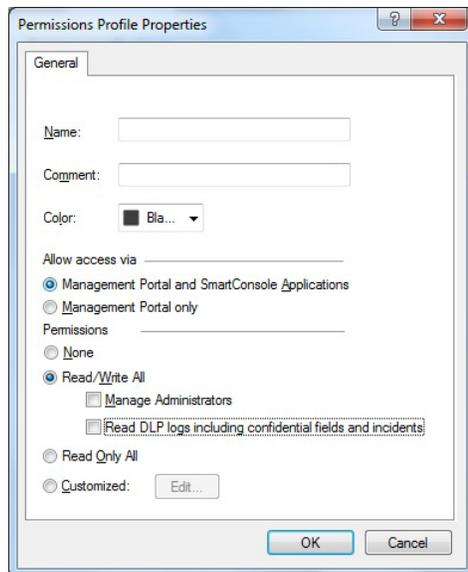
Name	Enter the OPSEC application name. Note: Record the name you entered here. You'll need to specify this name in AFA when you retrieve the certificate.
Host	Select the host to run AFA.
Object Entities	Select the LEA and CPI items.

c. In the **CPI Permissions** tab, select **Permissions Profile**, and then do one of the following:

- Select the **super** profile in the list, or any other profile with the required minimum permissions.
- Create a new permission profile. To do this, click **New**. In the **Permissions Profile Properties** dialog, enter a name for your new profile and select the required permissions.

Minimum permissions required are **Read Only All** access. If you're using ActiveChange, you must have **Read/Write All** access.

For example:



- d. In the **LEA Permissions** tab, select **According to Permissions Profile**, and then do one of the following:
- Select the **super** profile in the list, or any other profile with the required minimum permissions.
 - Create a new permission profile. To do this, click **New**. In the **Permissions Profile Properties** dialog, enter a name for your new profile and select the required permissions.

Minimum permissions required are **Read Only All** access.

- e. Click **OK**. The **General** tab appears again, with additional options.
4. Create your certificate. Do the following:
- a. Click **Communication**.
 - b. In the **Communication** dialog that appears, enter a one-time password , and then enter it again to confirm.

Note: Record the password you entered here. You'll need to specify this

name in AFA when you retrieve the certificate.

- c. Click **Initialize**.

The **Trust state** will change from **Uninitialized** to **Initialized but trust not established**. After the certificate is retrieved by AFA, the trust state will change to **Trusted**.

Tip: Create a new certificate if needed by clicking **Reset** and repeating this step.

5. Reinstall the Check Point database on all existing log servers, including CLMs or external log servers.

Do the following:

- a. At the top of the screen, click **Publish**.
- b. At the top left, click the  icon, and select **Install database**.
- c. In the **Install database** dialog, verify that your CMA is selected, and click **Install**.

Continue with [Enable data collection via OPSEC](#) above.

Create a Check Point OPSEC Certificate for Check Point Devices (R77 and Lower)

In order to collect the policy and routing table from a Check Point FireWall-1 module, AFA can use the OPSEC API. In order for this to happen a certificate needs to be created for authentication and security purposes.

The certificate is created on the SmartCenter server, using Check Point's **SmartDashboard** utility, or on the MDSM server, using Check Point's **Global SmartDashboard** utility.

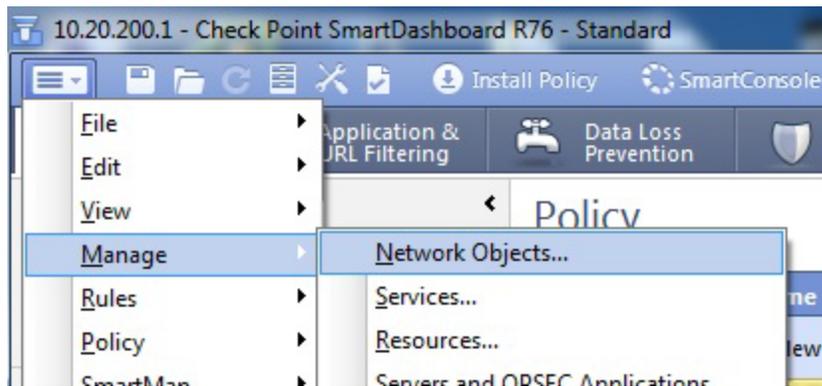
Do the following:

1. Create a network object for the host.

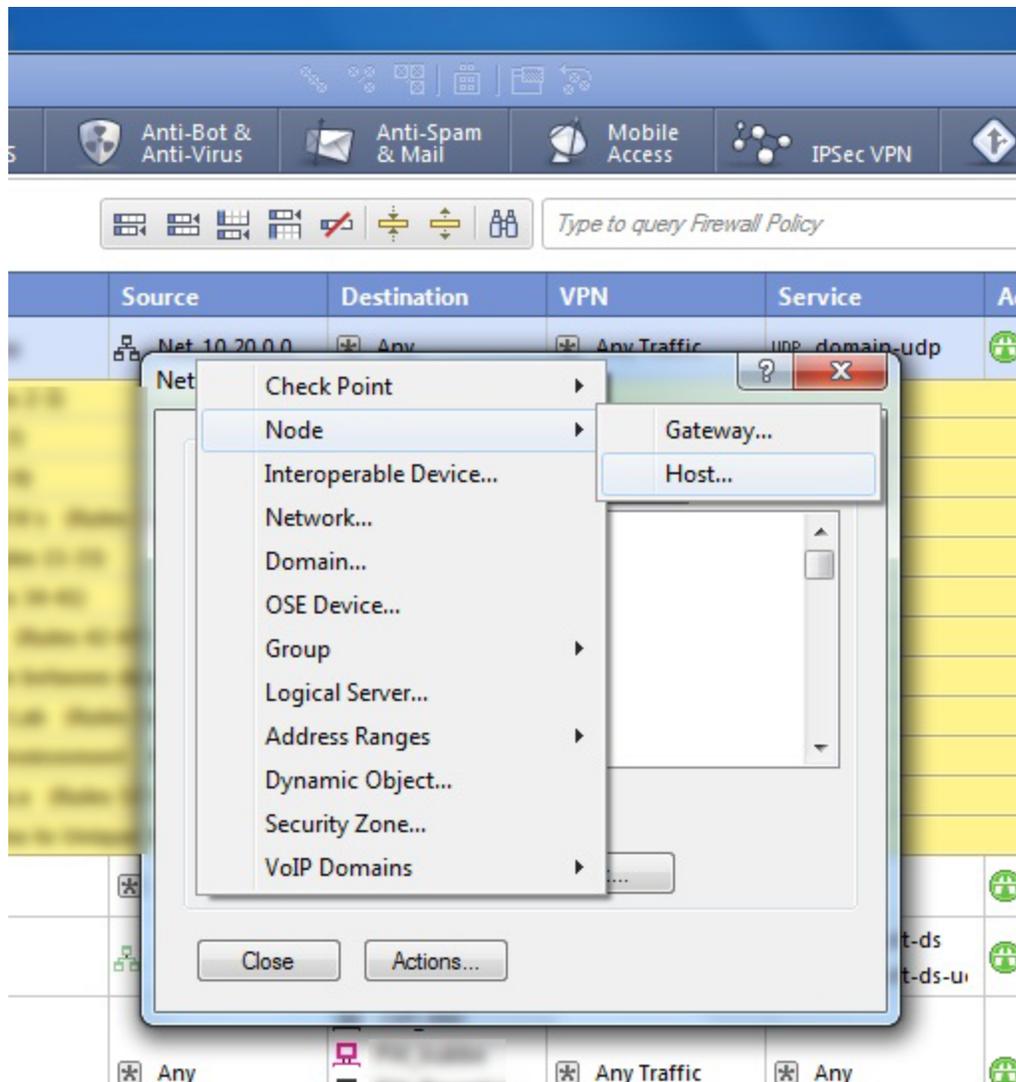
Note: If a network object for the host running AFA is already defined, you can skip this step.

Do the following:

- a. In the main SmartDashboard menu panel, select **Manage > Network Objects**.



- b. Click **New > Node > Host**.



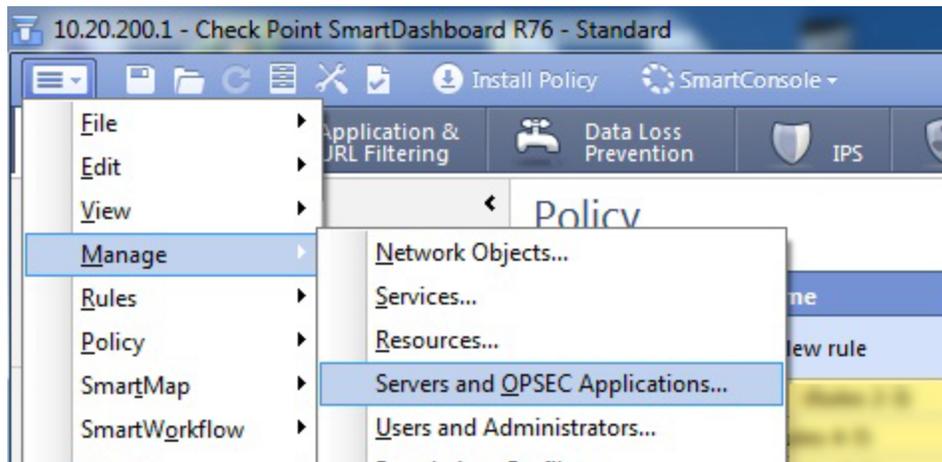
c. In the **Host Node** dialog, enter the **Name** and **IP address** of the host that will run AFA, and then click **OK**.

2. Create an OPSEC application object for this network object.

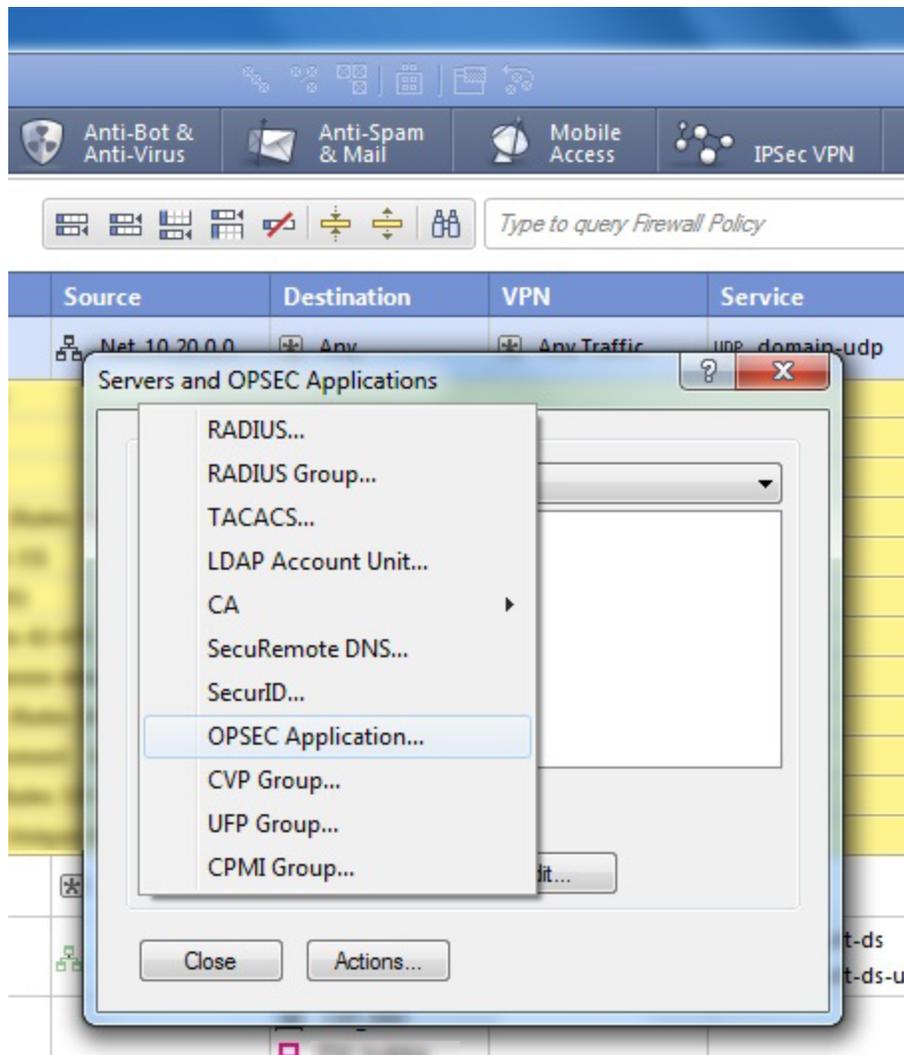
Note: If an OPSEC application object is already defined, you can skip this step.

Do the following:

- a. In the SmartDashboard main menu, select **Manage** and then **Servers and OPSEC Applications**.



- b. In the **Servers and OPSEC Applications** dialog box, click **New > OPSEC Application**.



c. In the **OPSEC Application Properties** dialog, define the following:

Name	Enter the OPSEC application name. Note: Record the name you entered here. You'll need to specify this name in AFA when you retrieve the certificate.
Host	Select the host to run AFA.
Object Entities	Select the LEA and CPMI items.

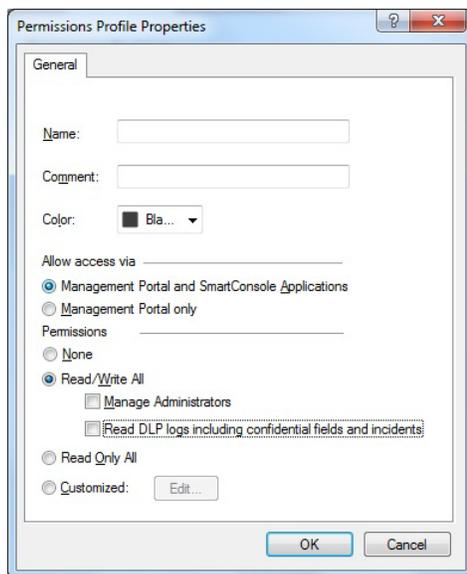
d. In the **CPI Permissions** tab, select **Permissions Profile**, and then do one of

the following:

- Select the **super** profile in the list, or any other profile with the required minimum permissions.
- Create a new permission profile. To do this, click **New**. In the **Permissions Profile Properties** dialog, enter a name for your new profile and select the required permissions.

Minimum permissions required are **Read Only All** access. If you're using ActiveChange, you must have **Read/Write All** access.

For example:



- e. For CheckPoint version R76 or above, in the **LEA Permissions** tab, select **According to Permissions Profile**.

Then do one of the following:

- Select the **super** profile in the list, or any other profile with the required minimum permissions.

- Create a new permission profile. To do this, click **New**. In the **Permissions Profile Properties** dialog, enter a name for your new profile and select the required permissions.

Minimum permissions required are **Read Only All** access.

- f. Click **OK**. The **General** tab appears again, with additional options.
3. Create your certificate. Do the following:
 - a. Click **Communication**.
 - b. In the **Communication** dialog that appears, enter a one-time activation key, and then enter it again to confirm.

Note: Record the key you entered here. You'll need to specify this name in AFA when you retrieve the certificate.

- c. Click **Initialize**.

The **Trust state** will change from **Uninitialized** to **Initialized but trust not established**. After the certificate is retrieved by AFA, the trust state will change to **Trusted**.

Tip: Create a new certificate if needed by clicking **Reset** and repeating this step.

4. Reinstall the Check Point database on all existing log servers, including CLMs or external log servers. Click **Save**, and then selecting **Policy** and **Install Database** from the main menu.

Continue with [Enable data collection via OPSEC](#) above.

Enable data collection via REST

This procedure describes how to enable REST calls to the Security Management Server.

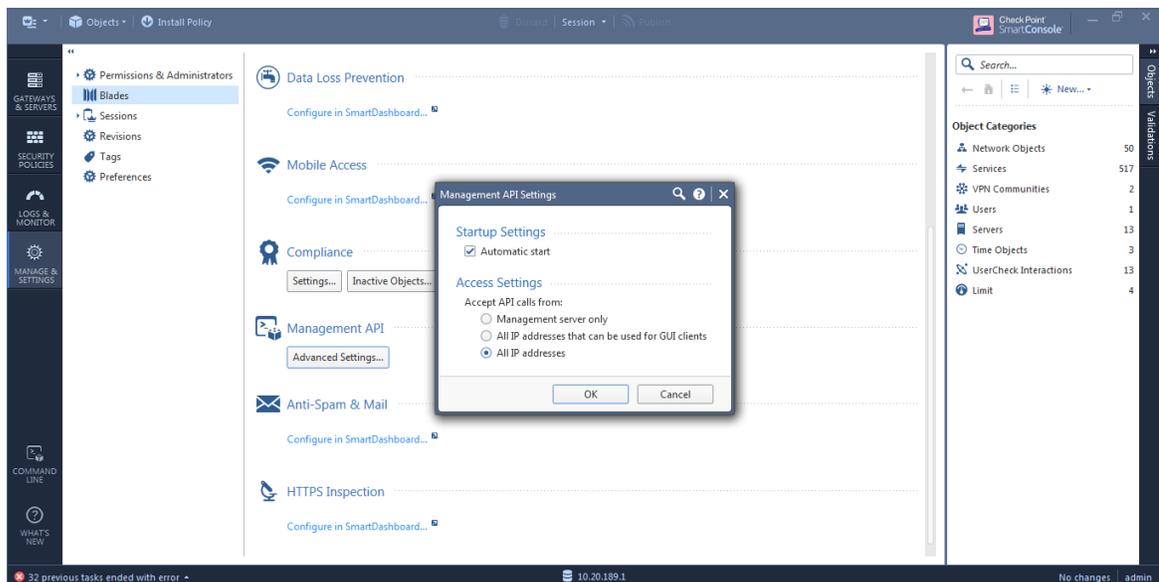
Note: For versions R80 and above, AFA collects data via REST, along with either SSH or OPSEC. In addition to enabling REST, you must also enable SSH or OPSEC as needed.

For details, see [Enable data collection via SSH](#) and [Enable data collection via OPSEC](#).

Do the following:

1. Open a SmartConsole.
2. In the left pane, navigate to **Manage & Settings > Blades > Management API > Advanced Settings**.

The **Management API Settings** window appears.



3. To automatically start the API server at Security Management Server startup, select the **Automatic Start** check box.
4. Select which IP addresses from which the API server accepts requests:

All IP addresses that can be used for GUI clients	API server will accept scripts and web service requests from the same devices that are allowed access to the Security Management Server. Make sure the AFA server is in this list.
All IP addresses	The API server will accept scripts and web-service requests from any device

5. Click **OK**.

In the Management API restart message that appears, click **OK**.



6. At the top, click **Publish**.

7. In the Management Check Point Server CLI, run the **api restart** command, and then exit.

Add Cisco devices

This topic describes how to add Cisco devices to AFA and perform related configurations.

Add a CSM-managed Cisco device

This procedure describes how to add a Cisco device managed by a Cisco CSM. You must add each Cisco device or security context that is managed by a Cisco CSM separately, even if they are managed by the same CSM.

Note: To perform this procedure, you must have a Cisco API license for the CSM device.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Cisco > Point > Firewall via CSM (CSM 4.3 or above)**.
3. Complete the fields as needed, and then click **Finish**.

Access Information

Firewall Host Name	Type the host name of the Cisco device to be analyzed, as it appears in the CSM UI.
CSM Server	Type the host name or IP address of the Cisco CSM server.
CSM User Name	Type the user name to use for SSH access to the Cisco CSM.
CSM Password	Type the password to use for SSH access to the Cisco CSM.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

Select the baseline compliance profile to use, in order to enable generation of Baseline Compliance Reports for this device.

The drop-down list includes all baseline compliance profiles in the system. For more information on baseline compliance profiles and instructions for adding new baseline compliance profiles, see [Customize baseline configuration profiles](#)

Select **None** to disable Baseline Compliance Report generation for this device.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For more information, see [Specify routing data manually](#).

Rules view

Specify how rules should be displayed in device reports:

- **ASDM:** Display rules in the Cisco Adaptive Security Device Manager (ASDM) graphical interface.
- **CLI:** Display rules in command line format.

The default value is **ADSM**.

Note: Intelligent Policy Tuner and the "Unused objects within rules" list are available only with ADSM.

Log Collection and Monitoring

Log collection method	<p>Specify the log collection method that AFA should use when collecting traffic logs for the Cisco device, by selecting one of the following:</p> <ul style="list-style-type: none"> • Hit-counters: Only use hit-counter data. The Change History report page will be based on "last modified" timestamps, and Intelligent Policy Tuner is disabled. • Standard: Use hit-counter data for rule usage, and Syslog data for the Change History report page. Intelligent Policy Tuner is disabled. • Extensive: Combine data from both hit-counters and Syslog. Intelligent Policy Tuner is enabled. <p>The default value is Extensive.</p> <p>Note: The Extensive method is only available when the ADSM is selected in the Rules view area.</p>
Syslog-ng server	<p>If you selected Standard or Extensive in the Log collection method field, you must specify the syslog-ng server. For details, see Specify a Syslog-ng server.</p>
Additional firewall identifiers	<p>Type any additional IP addresses or host names that identify the device. When adding multiple entries, separate values by a ':'. For example: "1.1.1.1:2.2.2.2:ServerName".</p> <p>This is relevant when the device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings. If AFA receives logs with an identifier it does not recognize, the logs will not be processed.</p> <p>Note: This field is only relevant for the parent device. In order to specify additional identifiers for sub-systems (Juniper VSYS/LSYS, Fortinet VDOM, Cisco security context, etc.), see Add additional device identifiers for sub-systems.</p>
Log collection frequency (minutes)	<p>Type the interval of time in minutes, at which AFA should collect logs for the device.</p>

Options

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

The new device is added to the device tree.

- If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

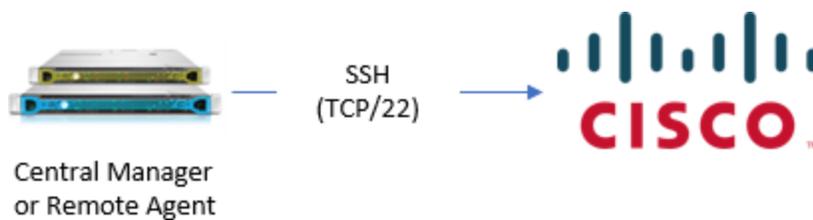
Cisco IOS routers in AFA

The following sections describe how Cisco IOS routers are added to AFA:

- [Network connectivity](#)
- [Device permissions](#)
- [Add a Cisco IOS router](#)

Network connectivity

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a Cisco IOS router.



Device permissions

ASMS requires the following for the user used to access your Cisco IOS routers:

- [Device analysis](#)
- [ActiveChange](#)

Device analysis

ASMS requires the ability to run the following commands on your Cisco IOS routers:

- `show version`
- `show interface`
- `show ipv4 vrf all interface`
- `show ip interface`
- `show ipv6 interface`
- `show ip access-list`
- `show ipv6 access-list`
- `show bgp summary`
- `show running-config`
- `show ip route`
- `show bgp vpn4 unicast labels`
- `show ipv4 vrf all interface brief`
- `show ip route vrf`

Note: Some commands may be relevant only on IOS-XE and IOS-XR devices.

Tip: You may want to create a read-only user with specific permissions to run `show running-config view full`.

For details, see [Defining a limited-privilege Cisco IOS Router user for AFA data collection](#) in AlgoPedia.

ActiveChange

When ActiveChange is enabled, ASMS requires a user that is able to enter privileged mode, using enable credentials (security level **15**).

Add a Cisco IOS router

This procedure describes how to add a Cisco IOS router to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Cisco > IOS Router**.
3. Complete the fields as needed.

Access Information

Enter details for accessing your device.

Host	Enter the device's host name or IP address.
User Name	Enter the username to use for device access via SSH.
Password	Enter the password to use for device access via SSH. Note: For Cisco IOS devices enabled for CyberArk, the Password and Enable User Password must be the same.
Enable User Name	Enter the enable user name to use. Note: This field is required.

Enable User Password	<p>Do one of the following:</p> <ul style="list-style-type: none"> • Enter the enable user password to use. • To specify an empty enable password, enter AlgoSec_no_passwd. • If you do not want AFA to enter the enable mode, enter noenable. <p>Note: For Cisco IOS devices enabled for CyberArk, the Password and Enable User Password must be the same.</p> <p>Note: This field is required.</p>
Retrieve credentials from CyberArk vault	<p>Select this check box to authenticate the device with a CyberArk Vault instead of saving the device credentials on the AFA server.</p> <p>When selected, also enter the following CyberArk details for the device being authenticated via CyberArk:</p> <ul style="list-style-type: none"> • Platform (Policy ID) • Safe • Folder • Object <p>Note: These options only appear when CyberArk is configured in AFA. For details, see Integrate AFA and CyberArk.</p>

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system. For more details, see [Customize baseline configuration profiles](#).

To disable Baseline Compliance Report generation for this device, select **None**.

Note: If this router is divided into VRF modules, Baseline Compliance Reports will only be generated for the root/default VRF.

Advanced

Select the following options as needed:

<p>Include risk analysis and policy optimization</p>	<p>Select this option to include risk analysis and policy optimization analysis in the device's reports.</p> <p>When this is not selected, AFA produces condensed router reports which run as if there is no license for risks, optimization or regulatory compliance. Reports still include policy changes and baseline compliance.</p> <p>This option is disabled by default.</p> <p>Note: Selecting this option will increase the analysis time for this router significantly and might result in performance degradation.</p>
<p>Automatically add/remove VRF instances upon detection (Applies for all Cisco Routers)</p>	<p>Select this option to enable automatic updating of VRF instances for all Cisco routers defined in AFA.</p> <p>The updates will be reflected in the device tree and graphic network map, and the updates will affect the device license usage.</p>

Remote Management Capabilities

Select a data transmission method:

- **SSH** (more secure)
- **Telnet**

Define the following as needed:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
Number of allowed encryption keys	Enter the permitted number of different RSA keys received from this device's IP address. Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc. For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. If this number is set to 1, the connection to the node will fail, resulting in a failed analysis.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

ActiveChange

Select this option to enable FireFlow to generate CLI recommendations and push them to the device.

Checking this box will enable ActiveChange for all the supported Cisco firewalls, Cisco IOS routers, and Juniper SRX firewalls (not only for this device).

Options

Select the following as needed:

Real-time change monitoring	Select this option to enable real-time change monitoring. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

- If you enabled ActiveChange, the **ActiveChange License Agreement** dialog box appears.

Select **I Agree**, and click **OK**.

- Click **Finish**. The new device is added to the device tree.

- If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added. The new device appears in the device tree, including any VRF devices as unique nodes.

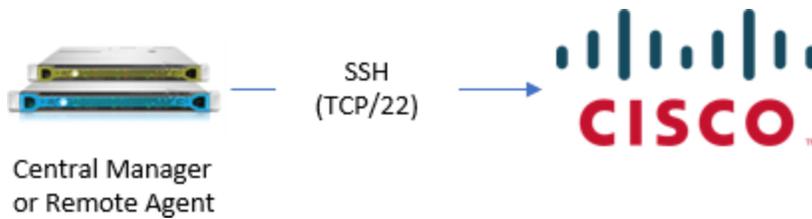
Cisco Nexus routers in AFA

The following sections describe how ASMS connects to Cisco Nexus routers:

- [Network connection](#)
- [Device permissions](#)
- [Add a Cisco Nexus router to AFA](#)

Network connection

The following diagram shows the connection between an ASMS Central Manager or Remote Agent and a Cisco Nexus router over SSH.



Device permissions

To analyze Cisco Nexus router devices, ASMS requires the ability to run the following commands on the Nexus device:

- **show version**
- **show interface**
- **show ip interface**
- **show ip access-list**
- **show running-config**
- **show vdc membership** (For Nexus 7000 and above)
- **show vrf interface | xml**
- **show vrf all interface**
- **show ip route**
- **show ip route vrf all**
- **show vrf all**
- **show bgp vpn4 unicast labels**

For Nexus versions 7000 and above, ASMS must also have permissions to view all VDCs.

Add a Cisco Nexus router to AFA

This procedure describes how to add a Cisco Nexus router to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Cisco > Nexus Router**.
3. Complete the fields as needed.

Access Information

Enter the following details for accessing your device from AFA:

Host	Enter the host name or IP address of the device.
User Name	Enter the user name to use for SSH access to the device.
Password	Enter the password to use for SSH access to the device.
Retrieve credentials from CyberArk vault	<p>Select this check box to authenticate the device with a CyberArk Vault instead of saving the device credentials on the AFA server.</p> <p>When selected, also define the following:</p> <ul style="list-style-type: none"> • Platform (Policy ID) • Safe • Folder • Object <p>Note: These options only appear when CyberArk is configured in AFA. For details, see Integrate AFA and CyberArk.</p>

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system. For more details, see [Customize baseline configuration profiles](#).

Note: To disable Baseline Compliance Report generation for this device, select **None**.

Additional Information

Select the following as needed:

<p>Include risk analysis and policy optimization</p>	<p>Select this option to include risk analysis and policy optimization analysis in the device's reports.</p> <p>When this is not selected, AFA produces condensed router reports which run as if there is no license for risks, optimization or regulatory compliance. Reports still include policy changes and baseline compliance.</p> <p>This option is disabled by default.</p> <p>Note: Selecting this option will increase the analysis time for this router significantly and might result in performance degradation.</p>
<p>Automatically add/remove VRF instances upon detection (Applies for all Cisco Routers)</p>	<p>Select this option to enable automatic updating of VRF instances for all Cisco routers defined in AFA.</p> <p>The updates will be reflected in the device tree and graphic network map, and the updates will affect the device license usage.</p>

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For more details, see [Specify routing data manually](#).

Remote Management Capabilities

Select a data transmission method:

- Telnet
- **SSH (more secure)**

Then define:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
Number of allowed encryption keys	<p>Enter the permitted number of different RSA keys received from this device's IP address.</p> <p>Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc.</p> <p>For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA.</p> <p>If this number is set to 1, the connection to the node will fail, resulting in a failed analysis.</p>

Options

Select the following as needed:

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
------------------------------------	---

Set user permissions

Select this option to set user permissions for this device.

4. Click **Finish**. The new device is added to the device tree.
5. If you selected **Set user permissions**, the **Edit users** dialog box appears.
In the list of users displayed, select one or more users to provide access to reports for this account.
To select multiple users, press the **CTRL** button while selecting.
Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Cisco ASA firewalls in AFA

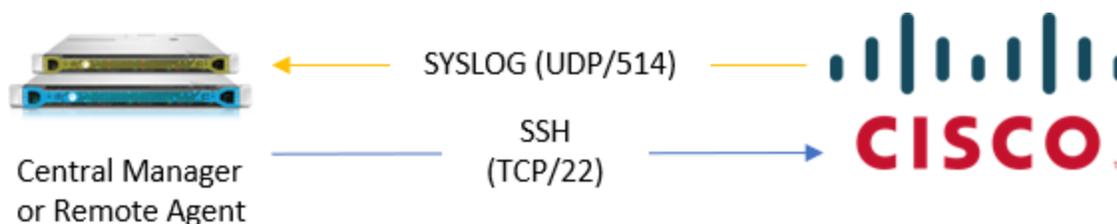
The following sections describe how ASMS connects to Cisco ASA firewalls:

- [Network connection](#)
- [Device permissions](#)
- [Add a Cisco ASA firewall](#)

Note: All references in the ASMS Tech Docs to Cisco ASA devices also refer to legacy PIX and FWSM devices. To add a new PIX or FWSM device to AFA, select ASA options.

Network connection

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a Cisco ASA device:



Device permissions

ASMS requires the following permissions to connect to your Cisco ASA devices:

- [Device analysis](#)
- [ActiveChange](#)
- [Log collection](#)

Device analysis

ASMS requires the ability to run the following commands on your ASA device:

- `show version`
- `show mode`
- `change to system`
- `show context`
- `show access-list`
- `show ipv6 access-list`
- `show running-config`
- `show route`
- `show ipv6`
- `terminal`
- `show cts sgt-map`

Tip: You may want to create a separate user for ASMS, enabling the user to have a security level 5.

For details, see [Defining a limited-privilege PIX/ASA/FWSM user for AFA data collection](#) in AlgoPedia. This procedure is not relevant if you have ActiveChange enabled.

ActiveChange

When ActiveChange is enabled, ASMS requires a user with **read-write** permissions and is able to enter privileged mode, using enable credentials (security level **15**).

Log collection

ASMS supports the ability to collect logs either by receiving Syslog messages from the device, or by collecting Syslog messages from a remote Syslog-ng server.

In either case, make sure that your Cisco ASA device is configured to send CISCO 106100 SYSLOG events to ASMS.

For example:

```
%FWSM-6-106100: access-list acl_ID {permitted | denied | est-allowed}  
protocol interface_name/source_address(source_port) -> interface_name/dest_address(dest_
```

These messages are logged when packets match an ACL statement, if you have the log option for the access-list command configured.

The message level depends on the level defined for the access-list command. By default, this level **6**.

Note: Intelligent Policy Tuner analysis is supported for Cisco ASA versions 7.1 and higher.

To use this feature, the device must send correct log messages, in type **106100**, and the device's ACLs must contain the keyword **log**.

Add a Cisco ASA firewall

This procedure describes how to add a Cisco ASA firewall to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Cisco > ASA**.

3. Complete the fields as needed.

Access Information

Enter details to access your device from AFA:

Host	Enter the device's host name or IP address.
User Name	<p>Enter the user name to use for SSH access to the device.</p> <p>Note: AFA partially supports user awareness for Cisco ASA devices. The network user appears as a field for each rule in the Policy tab, but is not used in traffic simulation queries.</p>
Password	<p>Enter the password to use for SSH access to the device.</p> <p>Note: For Cisco ASA devices enabled for CyberArk, the Password and Enable User Password must be the same.</p>
Enable User Password	<p>Enter the enable user password to use:</p> <ul style="list-style-type: none"> • noenable. Skip running the enable command. • Algosec_no_passwd. The enable password is empty. • Leave the field empty. AFA will issue a login command instead of the enable command, using the same password provided for the SSH connection. <p>Note: For Cisco ASA devices enabled for CyberArk, the Password and Enable User Password must be the same.</p>

Retrieve credentials from CyberArk vault	<p>Select to authenticate the device with a CyberArk Vault instead of saving the device credentials on the AlgoSec server.</p> <p>When selected, also enter the following CyberArk details for the device being authenticated:</p> <ul style="list-style-type: none"> • Platform (Policy ID) • Safe • Folder • Object <p>Note: These options only appear when CyberArk is configured in AFA. For details, see Integrate AFA and CyberArk.</p>
---	--

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

Note: This field is only relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system.

To disable Baseline Compliance Report generation for this device, select **None**.

For more details, see [Customize baseline configuration profiles](#).

Remote Management Capabilities

Select one of the following methods to collect data:

- **SSH** (recommended)
- **Telnet**

Then define:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
Number of allowed encryption keys	Enter the permitted number of different RSA keys received from this device's IP address. Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc. For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. If this number is set to 1 , the connection to the node will fail, resulting in a failed analysis.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For more details, see [Specify routing data manually](#).

Rules View

Specify how rules should be displayed in device reports:

- **ASDM:** Display rules in the Cisco Adaptive Security Device Manager (ASDM) graphical interface.
- **CLI (Default):** Display rules in command line format.

Note: Intelligent Policy Tuner and the **Unused objects within rules** list are available only with ADSM.

Log Collection and Monitoring

Define the following as needed:

<p>Log collection method</p>	<p>Specify the log collection method that AFA should use when collecting traffic logs for the Cisco device, by selecting one of the following:</p> <ul style="list-style-type: none"> • Hit-counters: Only use hit-counter data. The Change History report page will be based on last modified timestamps. Intelligent Policy Tuner is disabled. • Standard: Use hit-counter data for rule usage, and Syslog data for the Change History report page. Intelligent Policy Tuner is disabled. • Extensive (Default): Combine data from both hit-counters and Syslog. Intelligent Policy Tuner is enabled. <p>Note: This method is available only when ADSM is selected in the Rules view area. For details, see Rules View.</p>
<p>Syslog-ng server</p>	<p>If you selected Standard or Extensive in the Log collection method field, you must specify the syslog-ng server. For details, see Specify a Syslog-ng server.</p>

Additional firewall identifiers	<p>Enter any additional IP addresses or host names that identify the device. When adding multiple entries, separate values by a colon (:).</p> <p>For example: 1.1.1.1:2.2.2.2:ServerName.</p> <p>This is relevant when the device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings. If AFA receives logs with an identifier it does not recognize, the logs will not be processed.</p> <p>Note: This field is only relevant for the parent device, and not for sub-systems. For more details, see Add additional device identifiers for sub-systems</p>
Log collection frequency (minutes)	<p>Enter the interval of time in minutes, at which AFA should collect logs for the device.</p>

ActiveChange

Select this option to enable FireFlow to generate CLI recommendations and push them to the device.

Checking this box will enable ActiveChange for all the supported Cisco firewalls, Cisco IOS routers, and Juniper SRX firewalls (not only for this device).

Options

Select the following as needed:

Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring.</p>
Set user permissions	<p>Select this option to set user permissions for this device.</p>

4. If you enabled ActiveChange, the **ActiveChange License Agreement** dialog box appears.

Select **I Agree**, and click **OK**.

5. Click **Finish**. The new device is added to the device tree.

6. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added. Any configured contexts on the ASA device are also imported.

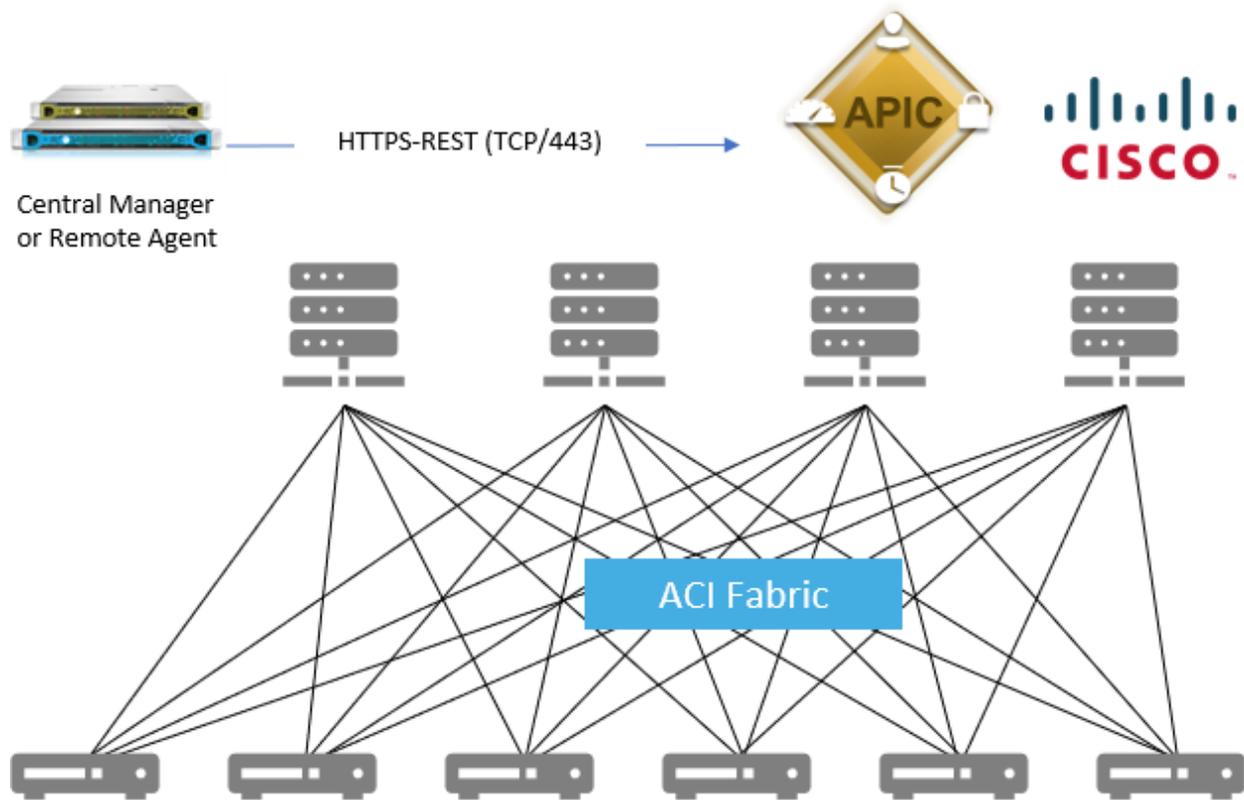
Cisco Application Centric Infrastructure (ACI) devices in AFA

The following sections describe how ASMS connects to Cisco ACI devices:

- [Network connectivity](#)
- [Device permissions](#)
- [Add a Cisco \(ACI\) to AFA](#)

Network connectivity

The following image shows an ASMS Central Manager or Remote Agent connecting to a Cisco ACI APIC and fabric.



Device permissions

ASMS requires the following permissions to access Cisco ACI devices:

- [Device analysis](#)
- [ActiveChange](#)

Device analysis

ASMS requires minimal, read-only access permissions to access Cisco ACI devices and collect data.

The user defined on the ACI APIC controller must have a minimum of **readPriv** permissions on **Security Domains All**.

For example:

Properties

Login ID: admin
 First Name: Algosec
 Last Name: Administrator
 Phone:
 Email:
 Description: optional

Account Status: Active Inactive
 Account Expires: No Yes
 UNIX User ID: 15374
 Security Domains:  

Name	Access
Security Domain all	
Role admin	writePriv

ActiveChange

When ActiveChange is enabled, ASMS requires **writePriv** permissions on **Security Domains All**.

For example:

Properties

Login ID: admin
 First Name: Algosec
 Last Name: Administrator
 Phone:
 Email:
 Description: optional

Account Status: Active Inactive
 Account Expires: No Yes
 UNIX User ID: 15374
 Security Domains:  

Name	Access
Security Domain all	
Role admin	writePriv

Add a Cisco (ACI) to AFA

This procedure describes how to connect Cisco ACI devices to AFA. AFA always connects to Cisco ACI devices via REST.

Note: To identify service graph data in queries and change requests, you must specifically configure AFA to recognize that data. For details, see [Configure support for Cisco service graphs](#).

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Cisco > Application Centric Infrastructure (ACI)**.
3. Populate the fields as follows:

Access Information

Enter details to access your device from AFA:

Host	Enter the device's host name or IP address. Tip: Typically, your APIC cluster has three nodes. Specify the host name or IP address of only one of the APIC nodes. If the node you added goes down, you'll need to switch your AFA device configuration to another node. Edit the device configuration in AFA and enter the host name or IP address of that second node.
User Name	Enter the user name to use to access the device.
Password	Enter the password to use to access the device.

Geographic Distribution

Select a remote agent to perform data collection for the device, if relevant.

To configure the device to be managed locally, select **Central Manager**.

Route Collection

Determine how AFA acquires the device's routing information. Select one of the following:

- **Automatic.** AFA automatically generates the device's routing upon analysis or monitoring.
- **Static Routing Table (URT).** AFA takes the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

ActiveChange

Select this option to enable FireFlow to generate CLI recommendations and push them to the device.

Checking this box will enable ActiveChange for all the supported Cisco firewalls, Cisco IOS routers, and Juniper SRX firewalls (not only for this device).

Options

Select either of the following options:

- **Real-time change monitoring.** Enable real-time alerting upon configuration changes. For details, see [Configure real-time monitoring](#).
 - **Set user permissions.** Set user permissions for this device.
4. If you enabled ActiveChange, the **ActiveChange License Agreement** dialog box appears.
Select **I Agree**, and click **OK**.
 5. Click **Finish**. The new device is added to the device tree.
 - **ACI devices** appear in the device tree in a two-tier hierarchy, including both APICs and tenants.

- **EPGs** are shown with the following syntax: **<application_profile>/<EPG_name>**. For more details, see [EPG identification and supported contract scopes](#).
- Any **VRFs** on the map are shown with the following syntax: **<Tenant_name>/<VRF_name>**
- **vzAny objects** are shown with the following syntax: **<VRF_name>/vzAny**. AFA updates the contents of these objects upon change monitoring and analysis.

6. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added. The ACI and each ACI tenant is displayed in the device tree.

EPG identification and supported contract scopes

During analysis, AFA reads all configuration data from ACI and saves EPG values according to the following logic:

- If an EPG is associated to specific VMs, their IP addresses are saved as the EPG value.
- Otherwise, AFA reads the subnets associated with the Bridge Domains (BD) and considers these subnets for the EPG(s) connected to that BD.

The AFA **Policy** tab displays the following contract scopes for ACI EPGs:

- **ApplicationProfile**. Supported when the contract is assigned to an EPG that belongs to a single Application Profile.
- **Global**. Not supported for imported or exported contracts

- **Tenant.**
- **VRF.** If the source or destination belong to different VRFs, AFA shows expanded rules, one for each VRF.

Configure support for Cisco service graphs

If you want to be able to identify service graph data in queries and change requests, you must specifically configure AFA to recognize that data.

Do the following:

1. Ensure that your device has the following vendor property definition: **fiip_additional_devices_set_support = yes.**

This parameter is set to **yes** by default, and is defined in the `/home/afa/.fa/config` file.

2. Create a CSV file named **devicesSetDefinition.csv**. Save this file on the AFA machine, in the `/home/afa/.fa/` directory.
3. Populate the **devicesSetDefinition.csv** file with tenant, service graph, and device mapping data, as shown in the following example:

Tenant Name	Service Graph Redirect Name	Devices
Jasmine_ACI	SG_HTTP_S	CKP1, F51
Jasmine_ACI	SG_HTTP3	PAN1
Flower_ACI	SG_eCommerce	PAN1, PAN2
Begal_ACI	SG_2	FP1, F52
Begal_ACI	SG_SQL	FP1, F52

Note: In this file, device names must be exact matches to the names used to identify the devices in ASMS.

4. Create another CSV file, in the same `/home/afa/.fa/`, named **devicesSetConnection.csv**.

5. In the **devicesSetConnection.csv** file, define the network logic used to define the service graph redirect. Use source and destination addresses, as shown in the following example:

Source	Destination	Tenant Name	Service Graph Redirect Name
10.1.0.0-10.1.0.255.255	10.2.1.6	Jasmine_ACI	SG_HTTP_S
10.1.0.0-10.1.0.255.255	10.2.1.6	Jasmine_ACI	SG_HTTP_S
10.1.1.3	10.2.1.6	Jasmine_ACI	SG_HTTP3
10.5.7.3-10.5.7.8	10.9.1.5	Flower_ACI	SG_eCommerce
192.1.1.3	192.2.1.6	Begal_ACI	SG_2
0.0.0.0-255.255.255.255	10.3.1.1	Begal_ACI	SG_SQL

Service graph data is now recognized in AFA queries and FireFlow change requests.

Tip: Alternately, advanced administrators can configure a script that resolves service graph redirects based on any custom logic using FireFlow ticket fields as parameters.

We recommend contacting AlgoSec professional services to configure this sort of custom logic.

Configure firewalls in path (FIP) functionality for ACI tenants and VRFs

By default, AFA query results include ACI tenants with either of the following criteria:

- ACI tenants with a BD that intersects with the query source or destination
- ACI tenants where one or more of the tenant's VRFs is included in the query path

ASMS administrators can configure AFA to identify ACI tenants only when the tenant's VRF is included in the query path. Do the following:

1. On your AFA machine, browse to and open the **devicedriver-cisco-aci.properties** file for editing. This file is located in the **/data/algosec-ms/config** directory on your AFA machine.

2. Update the `devicedriver.cisco.aci.protectedCloudHostsEnabled` parameter value to `false`.

Cisco Firepower devices in AFA

The following sections describe how ASMS connects to Cisco Firepower devices:

- [Network connectivity](#)
- [Device permissions](#)
- [Add a Cisco Firepower](#)

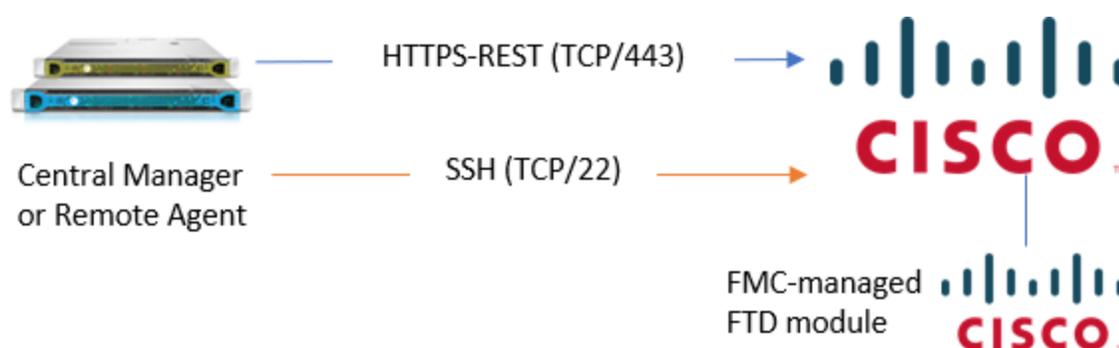
Note: AFA automatically identifies Cisco Firepower devices in service-chaining mode if the device has only a single interface.

If your device has multiple interfaces and service-chaining mode is not identified automatically, configure this for your device manually. For more details, see

[Configure one-armed mode manually](#).

Network connectivity

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a Cisco Firepower device:



Device permissions

ASMS requires the following device permissions to connect to Cisco Firepower devices:

Device analysis

The Cisco Firepower system includes both the Firepower Management Center (FMC) and the Firepower Threat Defense (FTD) firewalls.

AFA manages the FMC directly, mainly supporting the FTD via the FMC API. In addition, AFA collects routing and baseline compliance data directly from the FTD via SSH.

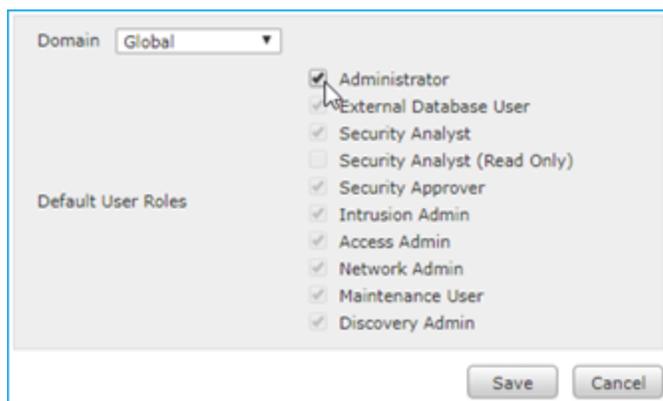
Therefore, AFA must have both of the following access rights:

- **API (HTTPS)** access to the FMC
- **SSH** access to the FTD. AFA does not support direct access to the FDM API.

To connect to your device, ASMS requires a user that is:

- **Dedicated for ASMS.** Connecting to the device using any other user may cause that user to be logged out of the Firepower UI at each monitoring cycle, as well as for any changes made to the Firepower device via ASMS.
- In the **Global** domain
- An **Administrator** user with a **read-only** role.

For example:



Note: The Administrator level role is required due to FMC limitations for fetching Audit logs.

ActiveChange

When ActiveChange is enabled, ASMS requires **read-write** permissions.

The user must continue to maintain **Administrator** permissions.

Add a Cisco Firepower

This procedure describes how to add a Cisco Firepower device to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Cisco > Firepower**.
3. Complete the following fields as needed.

Access Information

Enter details to access the device from AFA:

Host	Enter the hostname or IP address of the FMC.
User Name	Enter the username to use for SSH access to the FMC device. Note: AFA does not support user or network application awareness for Cisco Firepower. The network application appears as a field for each rule in the Policy tab, but is not used in traffic simulation queries.
Password	Enter the password to use for SSH access to the FMC device.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

ActiveChange

Select this option to allow FireFlow to automatically implement changes on the

device.

4. Click **Next** to continue on to the **FirePower - Step 2/2** page. This page lists the FTDs that are managed by the Firepower FMC.

For example:

The screenshot shows the 'Administration' page in the Firewall Analyzer interface. The page title is 'Administration' and the sub-header is 'Firepower - Step 2/2'. Below the sub-header, there is a table with the following data:

<input type="checkbox"/>	Host Name
<input checked="" type="checkbox"/>	10.20.1.78
<input checked="" type="checkbox"/>	10.20.1.79
<input checked="" type="checkbox"/>	10.20.1.16

Below the table, there is a section titled 'Direct access to managed devices' with the text 'Configure direct access to the managed devices in order to:' and a 'Configure' button.

5. To exclude an FTD, clear its check box in the table.
6. Click [Configure](#) to configure details for the selected FTDs.

In the **Direct Access Configuration**, define the **Host**, **User Name**, and **Password**, and **Baseline Profile** for each FTD.

Tip: To disable Baseline Compliance Report generation for this device, select

None.

For more details, see [Customize baseline configuration profiles](#).

For example:

Device Name	Host IP	User Name	Password	Baseline Profile
CertFTD1	10.20.101.1	admin	*****	Cisco Firepower
CertFTD2	10.20.204.38	admin	*****	Cisco Firepower

Click **Test Connectivity** to test the connections to the FTDs defined, and then click **OK**.

Note: You must specify the credentials for each FTD in order for AFA to collect routing data it needs to accurately analyze the device.

7. Select the following as needed:

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

8. If you enabled ActiveChange, the **ActiveChange License Agreement** dialog box appears.

Select **I Agree**, and click **OK**.

9. Click **Finish**.

The new device is added to the device tree.

10. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Configure one-armed mode manually

AFA automatically identifies Cisco Firepower devices in one-armed mode, when the device has a single interface. If your device has multiple interfaces and one-armed mode is not identified automatically, configure this for your device manually.

Do the following:

1. On the AFA machine, access your device configuration **meta** file as follows:

```
/home/afa/.fa/firewalls/<device_name>/fwa.meta
```

where **<device_name>** is the name of the device listed. If your device is listed multiple times, enter the longer name.

2. On a new line, enter:

```
is_steering_device=yes
```

3. Run an analysis on the device to update the device data in AFA.

Add F5 BIG-IP load balancers

This topic describes how to add F5 load balancers to AFA, including LTM-only devices and LTM and AFM devices.

If you have both LTM and AFM devices, and you do not need FireFlow support, use the **LTM and AFM** option. If you have only an LTM device, or if you have both but need FireFlow support, use the **LTM-only** option.

F5 BIG-IP LTM-only device support

This section describes how AFA connects to F5 BIG-IP LTM-only load balancers.

- [Device permissions](#)
- [Add an F5 BIG-IP LTM-only device to AFA](#)

Device permissions

The user connecting to the F5 device can have any role, but the User Partition must be **ALL**.

Terminal access must be set to **tmsh** or **Advanced shell**.

Add an F5 BIG-IP LTM-only device to AFA

This procedure describes how to add an F5 BIG-IP LTM-only device to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. On the vendor and device selection page, select **F5 > BIG-IP LTM Only**.
3. Complete the fields as needed, and then click **Finish**.

Access Information

Type	F5 BIG-IP LTM Only This field is read-only.
Host	Enter the host name or IP address of the device.
User Name	Enter the user name to use for SSH access to the device.
Password	Enter the password to use for SSH access to the device.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system. For more details, see [Customize baseline configuration profiles](#).

To disable Baseline Compliance Report generation for this device, select **None**.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

Remote Management Capabilities

This area enables you to select a define a data transfer method. Only **SSH** is supported, using either the default or a custom port.

Define the following as needed:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
--------------------	---

Number of allowed encryption keys	<p>Enter the permitted number of different RSA keys received from this device's IP address.</p> <p>Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc.</p> <p>For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. If this number is set to 1, the connection to the node will fail, resulting in a failed analysis.</p> <p>Default = unlimited</p>
--	--

Log Collection and Monitoring

Define the following as needed:

Log collection method	<p>Specify the log collection method that AFA should use when collecting audit logs for the F5 load balancer, by selecting one of the following:</p> <ul style="list-style-type: none"> • Extensive (Default): Not applicable. Intelligent Policy Tuner (IPT) is not available for F5 devices. • Standard: Use Syslog data for the Change History report page. IPT is disabled. • None. Disables the other Log Collection and Monitoring fields. <p>Note: This device type supports audit logs only.</p>
Syslog-ng server	<p>If you selected Standard or Extensive in the Log collection method field, you must specify the syslog-ng server.</p> <p>For details, see Specify a Syslog-ng server.</p>

Additional firewall identifiers	<p>Enter any additional IP addresses or host names that identify the device. When adding multiple entries, separate values by a colon (:).</p> <p>For example: 1.1.1.1:2.2.2.2:ServerName.</p> <p>This is relevant when the device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings. If AFA receives logs with an identifier it does not recognize, the logs will not be processed.</p> <p>Note: This field is only relevant for the parent device, and not for sub-systems. For more details, see Add additional device identifiers for sub-systems</p>
Log collection frequency (minutes)	<p>Enter the interval of time in minutes, at which AFA should collect logs for the device.</p> <p>The default value is 60.</p>

Options

Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes. For more details, see Configure real-time monitoring,</p>
Set user permissions	<p>Select this option to set user permissions for the device.</p>

The new device is added to the device tree.

- If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

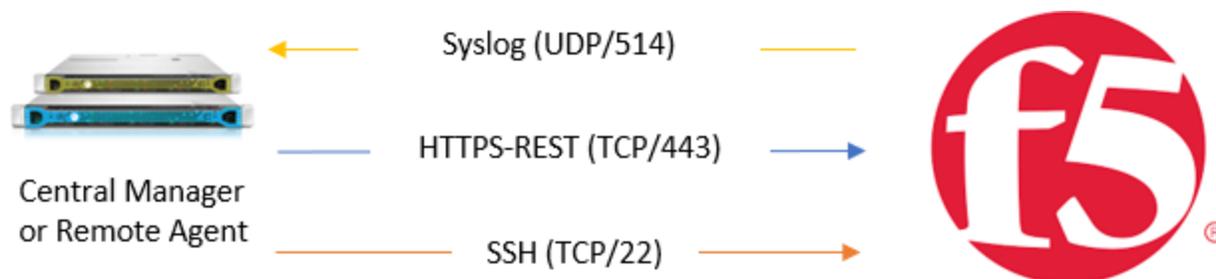
F5 BIG-IP LTM and AFM support

This section describes how AFA connects to F5 BIG-IP LTM and AFM devices.

- [Network connection](#)
- [Device permissions](#)
- [Add an F5 BIG-IP LTM and AFM to AFA](#)

Network connection

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a F5 BIG-IP LTM and AFM device.



Device permissions

ASMS requires an **Administrator** role on all partitions to access your F5 BIG-IP LTM and AFM device for basic analysis and change management. Additionally, **Tmsh** for terminal access is required for Baseline Compliance functionality.

For more details, see [F5 BIG-IP LTM+AFM - data collection authentication method](#) in AlgoPedia.

Add an F5 BIG-IP LTM and AFM to AFA

This procedure describes how to add an **F5 BIG-IP LTM and AFM** device to AFA, and should be used when your device uses AFM and you do not need FireFlow support.

Note: If you need FireFlow support, add a F5 BIG-IP LTM Only device. For details, see [Add an F5 BIG-IP LTM-only device to AFA](#).

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. On the vendor and device selection page, select **F5 > BIG-IP LTM and AFM**.
3. Complete the fields as needed, and then click **Finish**.

Access Information

Type	F5 BIG-IP LTM and AFM This field is read-only.
Host	Enter the host name or IP address of the device.
User Name	Enter the user name to use for access to the device.
Password	Enter the password to use for access to the device.
Retrieve credentials from CyberArk vault	<p>Select this check box to authenticate the device with a CyberArk Vault instead of saving the device credentials on the AlgoSec server.</p> <p>When selected, also enter the following CyberArk details for the device being authenticated via CyberArk:</p> <ul style="list-style-type: none"> • Platform (Policy ID) • Safe • Folder • Object <p>Note: These options only appear when CyberArk is configured in AFA. For details, see Integrate AFA and CyberArk.</p>

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system. For more details, see [Customize baseline configuration profiles](#).

To disable Baseline Compliance Report generation for this device, select **None**.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

Log Collection and Monitoring

Define the following as needed:

Log collection method	<p>Specify the log collection method that AFA should use when collecting audit logs for the F5 load balancer, by selecting one of the following:</p> <ul style="list-style-type: none"> • Extensive (Default): Not applicable. Intelligent Policy Tuner (IPT) is not available for F5 devices. • Standard: Use Syslog data for the Change History report page. IPT is disabled. • None. Disables the other Log Collection and Monitoring fields. <p>Note: This device type supports audit logs only.</p>
------------------------------	---

Syslog-ng server	<p>If you selected Standard or Extensive in the Log collection method field, you must specify the syslog-ng server.</p> <p>For details, see Specify a Syslog-ng server.</p>
Additional firewall identifiers	<p>Enter any additional IP addresses or host names that identify the device. When adding multiple entries, separate values by a colon (:).</p> <p>For example: 1.1.1.1:2.2.2.2:ServerName.</p> <p>This is relevant when the device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings. If AFA receives logs with an identifier it does not recognize, the logs will not be processed.</p> <p>Note: This field is only relevant for the parent device, and not for sub-systems. For more details, see Add additional device identifiers for sub-systems</p>
Log collection frequency (minutes)	<p>Enter the interval of time in minutes, at which AFA should collect logs for the device.</p> <p>The default value is 60.</p>

Options

Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes. For more details, see Configure real-time monitoring.</p>
Set user permissions	<p>Select this option to set user permissions for the device.</p>

- If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

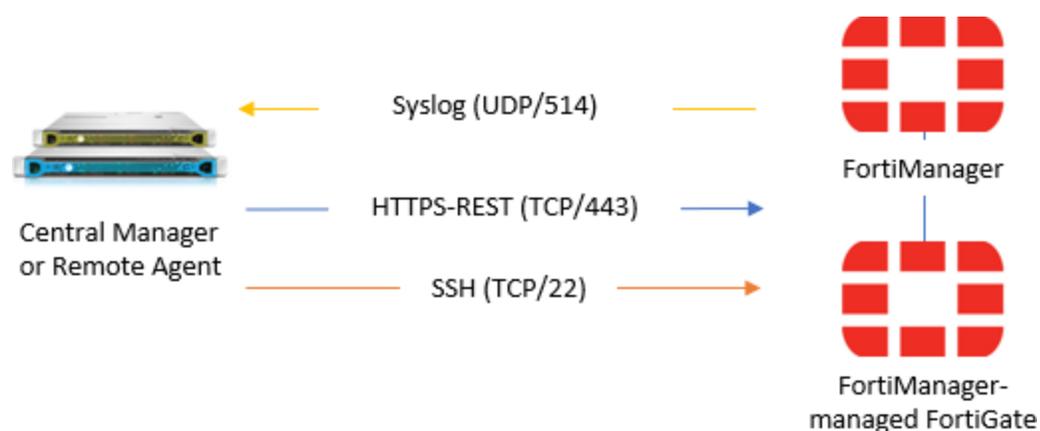
A success message appears to confirm that the device is added.

Add Fortinet devices

This topic describes how Fortinet FortiManager and FortiGate devices are connected to AFA.

Fortinet network connections

The following image shows an ASMS Central Manager or Remote Agent connected to Fortinet FortiManager and FortiGate devices.



Note: If syslog messages are sent via FortiAnalyzer device, a separate connection is required.

FortiManager device permissions

ASMS requires the following permissions when connecting to FortiManager devices:

Device analysis

AFA requires a user account with **Restricted_User** permissions to connect to the FortiManager device.

Read-only permissions are sufficient, as shown in the example below (click to expand):

The screenshot shows the 'Edit Profile' configuration page for a user named 'Restricted_User'. The profile is of type 'System Admin'. The permissions table below shows that 'None' is selected for all listed categories.

Category	Read-Write	Read-Only	None
System Settings	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Administrative Domain	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FortiGuard Center	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
License Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Advanced	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Device Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Add/Delete/Edit Devices/Groups	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Retrieve Configuration from Devices	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Revert Configuration from Revision History	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Terminal Access	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Manage Device Configurations	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Provisioning Templates	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
SD-WAN	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Policy & Objects	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Global Policy Packages & Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Assignment	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy Package & Objects	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Policy Check	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Install Policy Package or Device Configuration	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Import Policy Package	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Interface Mapping	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
AP Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
FortiClient Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
FortiSwitch Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
VPN Manager	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Note: FortiManager v5.2.3 and above with REST access must have permissions for rpc-permit (set **rpc-permit read**).

ActiveChange

When ActiveChange is enabled, AFA requires a user account with **Super_User** permissions with read-write permissions.

For example:

The screenshot shows the 'System Settings' interface with the 'Edit Profile' configuration page. The profile name is 'Super_User' and the description is 'Super user profiles have all system and device privileges enabled.' The profile type is set to 'System Admin'.

	<input checked="" type="radio"/> System Admin	<input type="radio"/> Restricted Admin	
	Read-Write	Read-Only	None
System Settings	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Administrative Domain	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiGuard Center	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
License Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firmware Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Advanced	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Device Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Add/Delete/Edit Devices/Groups	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Retrieve Configuration from Devices	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Revert Configuration from Revision History	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Terminal Access	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Manage Device Configurations	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provisioning Templates	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
SD-WAN	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policy & Objects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Global Policy Packages & Objects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Assignment	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policy Package & Objects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Policy Check	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Install Policy Package or Device Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Import Policy Package	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interface Mapping	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
AP Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiClient Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiSwitch Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
VPN Manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Note: FortiManager v5.2.3 and above with REST access and ActiveChange must have read-write permissions for rpc-permit (set `rpc-permit read-write`).

FortiGate device permissions

AFA requires read-only permissions to connect to Fortigate devices.

In the FortiGate web interface, in the **Admin Profile** configuration > **Access Control**, select an option that is at least **read-only**.

- If device configuration consists of VDOMs, the user must be configured with **set scope global**. Users configured with **set scope vdom** are not supported for AFA.
- If the FortiGate device is defined directly in AFA as opposed to via a FortiManager device, AFA does not support a user defined only on the managing FortiManager.

Add a Fortinet FortiManager device to AFA

This procedure describes how to add a Fortinet FortiManager device to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Fortinet > FortiManager**.
3. Complete the fields as needed.

Access Information

Host	Enter the host name or IP address of the device.
User Name	<p>Enter the user name to use for accessing the device.</p> <p>This user name must be a super-user.</p> <p>If Administrative Domains (ADOMs) are used:</p> <ul style="list-style-type: none"> • To analyze only devices under a specific ADOM, specify a specific ADOM's administrator credentials. • To analyze all devices under all ADOMs, provide the credentials of a global administrator. • When analyzing devices as a global administrator, no other action is required. Otherwise, some manual configuration may be required. Contact AlgoSec support for more information.
Password	Enter the password to use for accessing the device.

Connect via	For FortiManager version 5.2.3 and above, select REST . For earlier versions, select SSH and SOAP . You must enable the relevant web service on the device itself. For more details, see Enable the relevant API in the FortiNet FortiManager device .
Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when REST is selected.

The following fields are relevant only when CyberArk is configured. For details, see [Integrate AFA and CyberArk](#).

Retrieve credentials from CyberArk vault	Select this check box to authenticate the device with a CyberArk Vault instead of saving the device credentials on the AlgoSec server.
Platform (Policy ID)	Enter the Platform for this device which will be authenticated via CyberArk.
Safe	Enter the safe for this device which will be authenticated via CyberArk.
Folder	Enter the folder for this device which will be authenticated via CyberArk.
Object	Enter this device's CyberArk Object.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

ActiveChange

Select **Enable ActiveChange** to enable FireFlow to implement changes on the device.

Log Collection and Monitoring

For AFA to process logs from the devices managed by the FortiManager device you are adding, you may need to specify additional device identifiers.

This is relevant when the sub-device is represented by multiple or non-standard device identifiers. For example, this may be relevant for firewall clusters or non-standard logging settings.

For more details, see [Add additional device identifiers for sub-systems](#).

Define the following values:

Log collection method	<p>Specify whether AFA should collect logs for the device, by selecting one of the following:</p> <ul style="list-style-type: none"> • None: Do not collect logs. • Standard: Enable log collection. • Extensive: Enable log collection and the Intelligent Policy Tuner. <p>The default value is Extensive.</p>
Syslog-ng server	<p>If you selected Standard or Extensive in the Log collection method field, you must specify the syslog-ng server. For details, see Specify a Syslog-ng server.</p> <p>Tip: Alternately, see Configure your FortiManager to forward syslog messages to AFA.</p>
Log collection frequency	<p>Enter the interval of time in minutes, at which AFA should collect logs for the device.</p>

4. If you enabled ActiveChange, the **ActiveChange License Agreement** dialog box appears.

Select **I Agree** and click **OK**.

5. Click **Next** to continue to the **Fortinet FortiManager Step 2/2** page.

This page lists all the devices that are managed by the FortiManager, including standalone devices and virtual systems.

6. **Optional:** Configure AFA to use logs created by a managed device or virtual system

To specify that AFA should use the logs created by a managed device / virtual system, do the following:

- a. In the **Add Device** column, select the check box next to the device's name.
- b. In the **Log Analysis** column, select one of the following:
 - **None** to disable logging.
 - **Standard** to enable logging
 - **Extensive** to enable logging and the Intelligent Policy Tuner.

Note: Using the device's logs enables AFA to detect certain policy optimization information, such as unused rules. This information is displayed in the **Policy Optimization** section of the AFA report.

7. **Optional:** Enable generation of baseline compliance reports:

To enable generation of baseline compliance reports, do the following:

- a. Click [Configure](#).
- b. In the **Direct Access Configuration**, enter the following details, and then click **OK**.

Host IP	Type the IP address of the device.
User Name	Type the user name to access the device.

Password	Type the password to access the device.
Baseline Profile	Select the baseline compliance profile to use. The drop-down list includes all baseline compliance profiles in the system. For more details, see Customize baseline configuration profiles . To disable Baseline Compliance Report generation for this device, select None .
Test Connectivity	Click this button to test connectivity to the defined device. A message informs you whether AFA connected to the device successfully.

Note: Specifying this information for a device triggers a direct SSH connection to the device.

8. Select the remaining options as needed:

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

9. Click **Finish**.

The new device is added to the device tree, and appears with a three tier hierarchy: FortiManager, FortiGate and VDOM.

10. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

11. Enable the relevant API in the FortiNet FortiManager device.

Do the following:

- a. Log in to the FortiManager Web interface, and navigate to the **System Settings > Network settings**.
- b. Configure one of the following, depending on your FortiManager device version:

FortiManager versions 5.2.3 and higher	Connect via REST. Under System Settings > Network > Management Interface > Administrative Access , select: <ul style="list-style-type: none"> • HTTPS • Web Service
FortiManager versions earlier than 5.2.3	Connect via SOAP. Under System Settings > Network > Interface > Administrative Access , select Web Service .

Configure your FortiManager to forward syslog messages to AFA

ASMS can collect log data by receiving syslog messages from the FortiManager device or a FortiAnalyzer, or by collecting syslog messages from a remote syslog-ng server.

This procedure describes how to configure the FortiManager device to send syslog messages to ASMS. For more details, see [Log Collection and Monitoring](#).

Do the following:

1. Log in to your FortiManager web interface, and navigate to the **Log & Report > Log Settings** area.
2. Enable the **Send Logs to Syslog** option, and enter the **IP Address/FQDN** of your AFA server.

Add a Fortinet FortiGate device to AFA

This procedure describes how to add a FortiGate device to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Fortinet > FortiGate**.
3. Complete the fields as needed, and then click **Finish**.

Access Information

Host	Type the host name or IP address of the device.
User Name	Type the user name to use for SSH access to the device.
Password	Type the password to use for SSH access to the device.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Compliance Configuration

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system. For more details, see [Customize baseline configuration profiles](#).

To disable Baseline Compliance Report generation for this device, select **None**.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For more details, see [Specify routing data manually](#).

Remote Management Capabilities

Select a data collection method:

- SSH (more secure)
- Telnet

Then define the following:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
Number of allowed encryption keys	Enter the permitted number of different RSA keys received from this device's IP address. Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc. For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. If this number is set to 1, the connection to the node will fail, resulting in a failed analysis.

Log Collection and Monitoring

Log collection method	<p>Specify whether AFA should collect logs for the device, by selecting one of the following:</p> <ul style="list-style-type: none"> • None: Do not collect logs. • Standard: Enable log collection. • Extensive: Enable log collection and the Intelligent Policy Tuner. <p>The default value is Extensive.</p>
Syslog-ng server	<p>If you selected Standard or Extensive in the Log collection method field, you must specify the syslog-ng server. For details, see Specify a Syslog-ng server.</p>
Additional firewall identifiers	<p>Enter any additional IP addresses or host names that identify the device.</p> <p>When adding multiple entries, separate values with a colon (:). For example: 1.1.1.1:2.2.2.2:ServerName.</p> <p>This is relevant when the device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings. If AFA receives logs with an identifier it does not recognize, the logs will not be processed.</p> <p>Note: This field is only relevant for the parent device. For more details, see Add additional device identifiers for sub-systems.</p>
Log collection frequency	<p>Enter the interval of time in minutes, at which AFA should collect logs for the device.</p>

Options

Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring.</p>
Set user permissions	<p>Select this option to set user permissions for the device.</p>

The new device is added to the device tree with a two tier hierarchy: FortiGate and VDOM.

4. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Configure one-armed mode manually

AFA automatically identifies Fortinet devices in one-armed mode when the device has a single interface, or a single one non-management interface. If your device has multiple non-management interfaces and one-armed mode is not identified automatically, configure this for your device manually.

Do the following:

1. On the AFA machine, access your device configuration **meta** file as follows:

```
/home/afa/.fa/firewalls/<device_name>/fwa.meta
```

where **<device_name>** is the name of the device listed. If your device is listed multiple times, enter the longer name.

2. On a new line, enter:

```
is_steering_device=yes
```

3. Run an analysis on the device to update the device data in AFA.

Add Juniper devices

This topic describes how to add Juniper devices to AFA.

Tip: If you have multiple Juniper Netscreen or SRX devices, we recommend adding the Juniper NSM or Space that manages these devices.

This automatically enables AFA to analyze any devices managed by the NSM or Space device.

Juniper NSM devices in AFA

The following sections describe how Juniper NSM devices are added to AFA:

- [Device permissions](#)
- [Add a Juniper NSM device](#)

Consider the following when adding NSM devices:

Juniper NSM 2007 managing Netscreen devices	If you have a Juniper NSM 2007 managing Netscreen devices, you must add each Netscreen device separately, and specify that the Netscreen device logs are collected from the NSM. For more details, see Juniper Netscreen devices in AFA .
NAT support for SRX devices	NAT is not supported for Juniper SRX devices defined in AFA under an NSM. If you need NAT support, add your Juniper SRX device separately. For details, see Juniper SRX devices in AFA .

Device permissions

AFA requires the following to collect data from NSM devices:

- [Device analysis](#)
- [Log collection](#)
- [Dynamic routing data collection](#)
- [Global zone rule collection for SRX](#)

Device analysis

To collect data from the NSM GUI server via SOAP, the user accessing the NSM must

have the read-only **System Administrator** role.

You may want to create a user specifically for AFA data collection. To create this user, do the following:

Create a read-only NSM user for data collection

1. Log in to the NSM and select **Tools > Manage Administrators and Domains**.
2. Click **+** to create a new administrator.
3. In the **General** tab, enter a name for the user.
4. In the **Authorization** tab, click **Set Password** and set a password for the user.
5. In the **Permissions** tab, click **+**.
6. In the **New Select Role and Domains** dialog, do the following:
 - From the **Role** drop-down list, select **Read-Only System Administrator**.
 - Select the checkboxes for any of the relevant domains.
7. Click **OK** to close any open dialog boxes.

Log collection

To collect log files from the NSM dev server, you must do one of the following:

- Access the NSM dev server as user **root**
- Deploy the **install_nsm_sudo** script on the NSM dev server to change a minimal set of folder permissions. For more details, see [Collecting Logs from Juniper NSM without Using the Root](#) in AlgoPedia.

Dynamic routing data collection

To retrieve dynamic routing data from devices managed by the NSM, the user accessing the NSM must have SNMP access.

For more details, see [Collecting dynamic routes via SNMP for devices managed by NSM](#) in AlgoPedia.

Global zone rule collection for SRX

To collect global-zone rules for SRX devices managed by an NSM, the NSM user defined in AFA must have a role with permissions to view the Junos Global Rulebase. To enable this, do the following:

In the NSM application, navigate to **Administration > Common > Task > Manage administrator and domains > Roles**, and select **View Juno Global Rulebase**.

Add a Juniper NSM device

This procedure describes how to add a Juniper NSM to AFA. AFA uses the NSM API 2008, available in NSM versions 2008 and higher, to connect to the NSM and collect data.

Do the following:

1. Set your NSM device to listen to port **8443** on the IP address of its interface.

For details, see the [Juniper Knowledge Base](#).

2. If you are using a Juniper NSM 2007 or 2008, enable AFA to translate rule numbers to rule IDs.

These rule IDs are available by default in NSM 2009 traffic logs.

Enable rule number translation

Do the following:

- a. In the AFA **Administration** area, navigate to the **OPTIONS > Advanced Configuration** tab.
- b. Click **Add** to add a new parameter. Enter the following details:

Name	Use_Rulenum
Value	yes

- c. Click **OK** and **OK** again to save your changes.

3. Access the **Devices Setup** page. For more details, see [Access the DEVICES SETUP page](#).
4. In the vendor and device selection page, select **Juniper > NSM (NSM 2008 or above)**.
5. Complete the following fields as needed.

Access Information

NSM GUI server	Enter the host name or IP address of the NSM GUI server.
NSM HA Cluster	<p>Select this option to enable a High Availability cluster. If AFA fails to access the primary NSM GUI server, AFA will attempt to access the secondary server instead.</p> <p>If selected, also populate the Secondary NSM GUI server field with the host name or IP address of the secondary server.</p> <p>Note: NSM HA cluster support is only available if the NSM GUI server and Dev server are running on the same server.</p>
User Name	<p>Enter the user name to use for SSH access to the NSM GUI server.</p> <p>Note: AlgoSec recommends using a "read-only" user account on the NSM GUI server.</p> <p>For details, see Device analysis.</p> <p>Tip: Configure AFA to connect to the device using SSH and Public key authentication.</p> <p>Configure this on the Administration > Options > General tab.</p> <p>For details, see Use public key authentication in data collection.</p>
Password	Enter the password to use for SSH access to the NSM GUI server.
Port	<p>Enter the port number to use on the NSM GUI server.</p> <p>Default: 8443</p> <p>Default for NSMXpress appliances: 443</p>

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Log Collection and Monitoring

Do the following:

- a. Ensure that **Collect Logs (via SSH)** is selected to determine that AFA collects traffic logs for the device using SSH.
- b. In the **From** field, select the log source:

NSM (Default)	<p>Under NSM Dev server, select the NSM location:</p> <ul style="list-style-type: none"> • Same as NSM GUI server (default). The NSM Devices server is located on the same machine as the NSM GUI server. • Separate server: The NSM is located separately from the NSM GUI server. If selected, also enter the NSM's host name or IP address. <p>In the SSH User Name and SSH Password fields, enter the credentials used to connect to the NSM.</p> <p>Click Test Connectivity to test the connection.</p> <div style="background-color: #e6f2e6; padding: 5px; margin-top: 10px;"> <p>Tip: When using Juniper's STRM log server, AFA enables you to forward logs to a built-in or external syslog-ng server, which you can define as the relevant log server instead. For more details, see Configure Juniper STRM to forward logs to a Syslog-ng server.</p> </div> <div style="background-color: #e6f2e6; padding: 5px; margin-top: 10px;"> <p>Note: For NSMXpress appliances, the NSM GUI server and the NSM Devices server are installed on the same machine.</p> </div>
-------------------------	---

Syslog-ng	<p>Select an existing syslog-ng server, edit its details, or add a new one.</p> <p>For details, see Specify a Syslog-ng server.</p> <p>Select the NSM forwarding option to indicate that logs are collected on the NSM and then forwarded to the syslog-ng server.</p>
------------------	---

- c. Select **Collect audit logs from the same server** to determine that AFA collects audit logs in addition to traffic logs.
- d. In the **Log collection frequency (minutes)** dropdown, select an interval at which AFA collects logs. **Default** = 60 minutes.

Note: You may need to specify additional device identifiers for AFA to process logs from devices managed by this NSM device. This is relevant when the managed device has multiple or non-standard device identifiers in the logs, such as for firewall clusters or non-standard logging settings. For details, see [Add additional device identifiers for sub-systems](#).

6. Click **Next** to continue to the **Juniper NSM Step 2/2** page.

This page lists the devices that are managed by the NSM, including standalone devices and virtual systems.

Do the following:

Add Device column	Select the checkbox for any devices you want to define via the NSM.
-----------------------------	---

<p>Log Analysis column</p>	<p>Select one of the following to determine log functionality for a selected device:</p> <ul style="list-style-type: none"> • None to disable logging. • Standard to enable logging. • Extensive to enable logging and the Intelligent Policy Tuner. <p>This enables AFA to detect policy optimization data, such as unused rules, and display them in the Policy Optimization section of the AFA report.</p>
<p>Migrate from currently defined Netscreen column</p>	<p>Displayed if you have Netscreen devices managed by this NSM already defined in AFA.</p> <p>Select devices to migrate for AFA to delete them in the background and add them back via the NSM.</p> <p>Note: Juniper SRX devices already defined in AFA cannot be migrated. To define the device as managed by the NSM, first delete the SRX device from AFA, and then redefine via the NSM.</p>

7. (Optional) Enable generation of baseline compliance reports.

Do the following:

- a. Click [Configure](#).
- b. Do one of the following:

<p>Configure direct access for each device</p>	<p>In the Direct Access Configuration dialog, enter the following details:</p> <ul style="list-style-type: none"> • Host IP. Enter the device's IP address. • Username. Enter the username used to access the device. • Password. Enter the password to access the device. • Baseline Profile. Select a baseline profile to use for the device. For details, see Customize baseline configuration profiles. To disable Baseline Compliance Report generation for this device, select None. <p>Click Test Connectivity to test connectivity to the defined device.</p> <p>This triggers a direct SSH connection to the device.</p>
<p>Configure access to managed devices via the NSM</p>	<p>If you do not want to enter credentials for each device and have AFA access them directly, select</p> <p>Access the managed devices through the NSM machine. Then, enter the SSH User Name and SSH Password.</p> <p>AFA connects to the NSM via SSH, and opens another SSH connection from the NSM to each of the selected devices.</p>

8. Complete the remaining fields as needed, and click **Finish**.

Advanced

Select **Display virtual routers (Netscreen devices)** to analyze each virtual router under a Netscreen device separately.

Each virtual router will appear in the device tree immediately below the Netscreen device, and parallel to virtual systems.

Note: This option is not available for Juniper SRX devices defined in AFA via

the NSM. To use this functionality for SRX devices, define them directly in AFA.
For more details, see [Juniper SRX devices in AFA](#).

Options

Select the following as needed:

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

The new device is added to the device tree.

- If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Junos Space Security Director devices in AFA

The following sections describe how ASMS connects to Junos Space Security Director devices:

- [Network connectivity](#)
- [Device permissions](#)
- [Add a Junos Space Security Director device](#)

Consider the following when adding Junos Space Security Director devices to AFA:

Data collection time required

Data collection may take longer on Junos Space than on other brands.

This may have various implications across the system for processes that involve data collection from Junos Space devices.

Upgrades and additional routing instances

Juniper Space devices defined in AFA **before version A30.00** have different behavior and support options.

If you are upgrading, do one of the following:

<p>Upgrading from A30.00 to A30.10 or higher</p>	<p>If you already have a Juniper Space device defined in AFA, edit your Space device in the AFA Administration area to view all updates for Space devices, such as viewing additional routing instances in the device tree and the map.</p> <p>No changes are required. Simply edit the device configuration and click Finish to update the data.</p>
<p>Upgrading with Juniper Space devices added prior to ASMS A30.00</p>	<p>If your Juniper Space device was added prior to ASMS A30.00, you will need to delete this device from AFA and add it back again to implement all new features.</p> <p>For more details, see Delete a device.</p>

SRX devices already defined in AFA

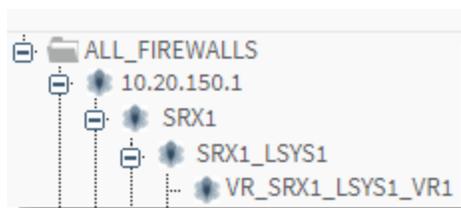
If you have SRX devices already defined in AFA and want to convert them to Juniper Space, first remove the SRX devices and then add them back via Space.

For more details, see [Delete a device](#) and [Juniper SRX devices in AFA](#).

Virtual Router, VRF, and Secure Wire support

When the Juniper Space device manages an SRX device or LSYS, which in turn manages Virtual Routers, VRFs, or Secure Wires, AFA displays these routing instances in AFA the device tree. This provides increased route analysis and automation design at the levels of these routing instances.

For example:



Note: Items not added to the device tree include empty Virtual Routers or LSYSs, unsupported routing instances, and LSYSs that contain only unsupported routing instances.

AFA reports provide the following data, per tree level:

Virtual Router / VRF / Secure Wire level	At the level of the routing instance, AFA displays topology information only, and no policy information. Policy information is displayed at the LSYS level, one node up in the tree.
LSYS level	At the LSYS level, AFA displays policy information only, and no topology information. Topology information is shown at the routing instance level, one node down in the tree.
Management level	Higher up in the tree, at the Space management, AFA displays aggregated information for all child devices, including both policy and topology information.

If you've added new routing instances to your Juniper Space device and want to generate AFA data for these routing instances, edit your Space device in the **AFAAdministration** area.

No changes are required. Simply edit the device configuration and click **Finish** to update the data.

For details, see [Virtual Router, VRF, and Secure Wire support](#).

Inter-VR routing support for route-leaking

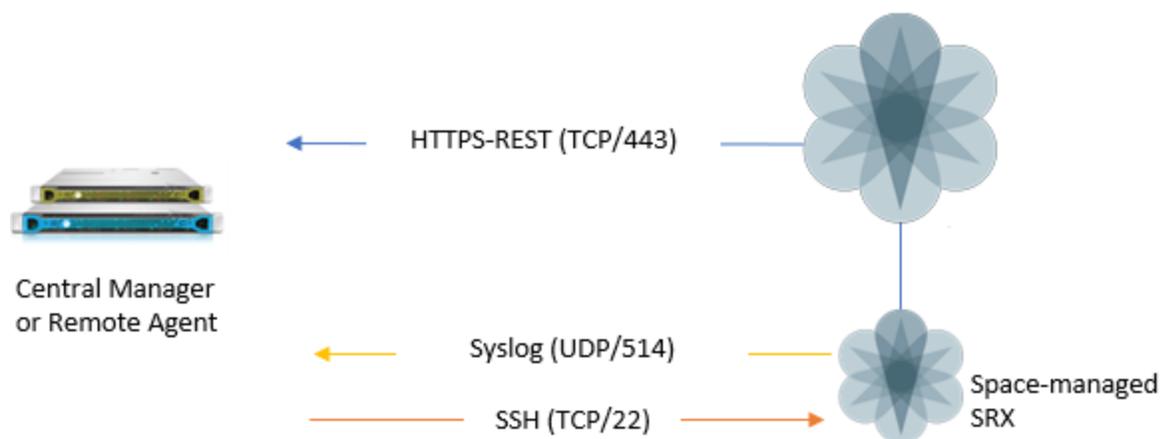
AFA supports RIB groups and next-table commands as next-hop routers (NHRs) for

SRX devices managed by Juniper Space Security Director.

When AFA detects either of these inter-VR routing configurations, it adds fake, or back-plane, interfaces to the Juniper Space's URT file to simulate these connections. These connections can then be displayed on the AFA network map and in query results.

Network connectivity

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a Juniper SPACE device.



Device permissions

ASMS requires the following for the user used to access your Juniper SPACE devices:

- [Device analysis](#)
- [ActiveChange](#)
- [Log collection](#)

Device analysis

- Super administrator permissions on the Juniper SPACE device
- Both GUI and API access enabled
- Full access to all Domains

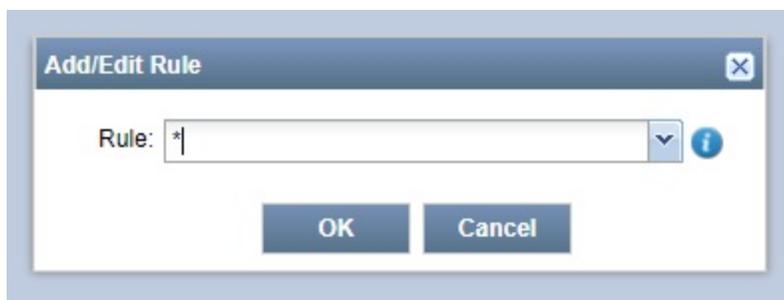
You may want to create a user specifically for AFA data collection. To create this user, do the following:

Create a read-only Juniper Space user for data collection

1. Log in to the **Junos Space - Network Management Platform**.
2. In the **Junos Space - Network Management Platform**, create a new API Access profile.

When adding the new profile, add a new rule with only an asterisk (*) in the name.

For example:



3. Switch to the **Roles** area and create a new role with the following permissions:

Log Collector Management	Read Log Collector info
Event Viewer	View Device Logs
Reports	Reports > View Report

Firewall Policies	<p>The following, without sub-permissions:</p> <ul style="list-style-type: none"> • View Policy • Export Policy • Policy Profiles • Schedulers • AccessProfile • AppFirewall Policy • SSL Proxy Profile • End User Profile • Active Directory • Condition • Environment Variable • Identity Management • Application Signatures
NAT Policies	<ul style="list-style-type: none"> • Export NAT Policy • View NAT Policy • View NAT Dirty Policy • NAT Pools (without sub-permissions) • Ports Sets (without sub-permissions)
VPNs	View VPN
Shared Objects	<p>The following, without sub-permissions:</p> <ul style="list-style-type: none"> • Services • Addresses • Zones Sets • Variables
Security Director Devices	View Security Director Devices

Devices	<ul style="list-style-type: none"> • Unmanaged Devices • Model Devices > <ul style="list-style-type: none"> • View Modeled Instance • View Modeled Device Status • View Configlet • Connection Profiles > View Connection Profile • Device Management > <ul style="list-style-type: none"> • Device Inventory > <ul style="list-style-type: none"> • View Physical Inventory • View Physical Interfaces • View Logical Interfaces • View License Inventory • View Software Inventory • Device Access > SSH to Device • Device Configuration > <ul style="list-style-type: none"> • View Active Configuration (without the sub-permissions) • View Template Association • View Configuration Change Log
Device Templates	Templates > <ul style="list-style-type: none"> • View Template Details • View Template Association
CLI Configlets	<ul style="list-style-type: none"> • Configlets > View CLI Configlet Details • Configuration View > <ul style="list-style-type: none"> • View Configuration View Details • Export Configuration View
Configuration Files	Config Files Management > Export Configuration File
Jobs	Job Management > View Recurrence

Audit Logs	Audit Log > Export Audit Logs
Administration	Fabric (without sub-permissions) Applications (without sub-permissions)

4. Create a new user. When assigning roles, do the following:
 - Select **GUI Access** and **API Access**
 - In the **Exec RPC API Access Profile area**, select the new API access profile that you created in [step 2](#).
 - Select the newly defined role that you created in [step 3](#).
 - In the **Job Management View** area, select to view all jobs.
5. When assigning domains, select all domains, or the **Global** domain.

For more details about how to perform these steps, see [Junos Space - Network Management Platform documentation](#).

ActiveChange

When ActiveChange is enabled, the user connecting to the Junos Space device requires a minimum of **read-write** access via SSH.

Log collection

Configure your system to do one of the following:

- Have syslog messages sent to ASMS directly from the firewall
- Have ASMS collect syslog messages from a remote syslog-ng server

For details, see:

- [Log Collection](#) for Juniper Space
- [Configure Juniper SRX devices to send traffic logs](#)
- [Configure Juniper STRM to forward logs to a Syslog-ng server](#)

Add a Junos Space Security Director device

This procedure describes how to add a Junos Space Security Director device to AFA. Once added, all SRX devices managed by the Space device are also added to AFA, as well as any Virtual Routers or Secure Wires managed by the SRX device or LSYS.

For more details, see [Virtual Router, VRF, and Secure Wire support](#).

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, click **Juniper > Junos Space Security Director**.
3. Complete the fields as needed.

Access Information

Enter the following access details and credentials:

Host	Enter the device's host name or IP address.
User Name	Enter the user name to use to access the device.
Password	Enter the associated password.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

Note: This field is relevant only when a Geographic Distribution architecture is configured.

ActiveChange

Select Enable ActiveChange to configure FireFlow to generate

CLI recommendations and push them to the device.

Log Collection

Define log collection on the device as follows:

Log collection method	<p>Specify whether AFA should collect logs for the device, by selecting one of the following:</p> <ul style="list-style-type: none"> • None: Do not collect logs. • Standard: Enable log collection. • Extensive: Enable log collection and the Intelligent Policy Tuner. <p>The default value is Extensive.</p>
Syslog-ng server	<p>If you selected Standard or Extensive in the Log collection method field, you must also specify the syslog-ng server. For details, see Specify a Syslog-ng server.</p> <p>Note: When using Juniper's STRM log server, we recommend forwarding logs to the syslog-ng server defined in AFA. For more details, see Configure Juniper STRM to forward logs to a Syslog-ng server.</p>
Log collection frequency	<p>Select the interval of time in minutes, at which AFA should collect logs for the device.</p>

Note: In order for AFA to process logs from the devices that are managed by this management device, you may need to specify additional device identifiers. This is relevant when the sub-device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings. For more details, see [Add additional device identifiers for sub-systems](#).

4. If you enabled ActiveChange, the **ActiveChange License Agreement** dialog box

appears.

Select **I Agree** and click **OK**.

5. Click **Next** to continue to the **Junos Space Security Director - Step 2/2** page.

This page lists the devices that are managed by the Juniper Space, including standalone devices and logical systems.

Do the following:

Add Device column	Select the checkbox for any devices you want to define via the Space device.
Log Analysis column	<p>Select one of the following to determine log functionality for a selected device:</p> <ul style="list-style-type: none"> • None to disable logging. • Standard to enable logging. • Extensive to enable logging and the Intelligent Policy Tuner. <p>This enables AFA to detect policy optimization data, such as unused rules, and display them in the Policy Optimization section of the AFA report.</p>

6. **(Optional) Enable generation of baseline compliance reports.**

Do the following:

- a. Click [Configure](#).
- b. In the **Direct Access Configuration** dialog, enter the following details:
 - **Host IP.** Enter the device's IP address.
 - **Username.** Enter the username used to access the device.
 - **Password.** Enter the password to access the device.

- **Baseline Profile.** Select a baseline profile to use for the device. For details, see [Customize baseline configuration profiles](#). To disable Baseline Compliance Report generation for this device, select **None**.

Click **Test Connectivity** to test connectivity to the defined device.

This triggers a direct SSH connection to the device.

7. Select the remaining options as needed:

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

8. Click **Finish**.

The new Space device is added to the device tree, showing each individual device, LSYS, or routing instance configured.

Space devices and the devices they manage appear in the device tree with a potentially four-tier hierarchy. For example: **Juniper Space Security Director (Management Device) > SRX > LSYS > Virtual Router, VRF, or Secure Wire**

For more details, see [Virtual Router, VRF, and Secure Wire support](#).

Note: SRX clusters in passive/active mode appear as a single node in the tree, while SRX clusters in active/active mode appear as two nodes.

Empty routers or LSYSs, unsupported routing instances, or LSYSs that contain only unsupported routing instances, are not added to the device tree.

9. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

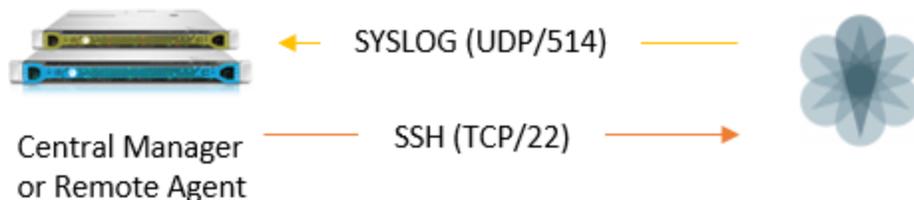
Juniper Netscreen devices in AFA

The following sections describe how ASMS connects to Juniper Netscreen devices:

- [Network connectivity](#)
- [Device requirements](#)
- [Add a Juniper Netscreen to AFA](#)

Network connectivity

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a Juniper Netscreen device.



Device requirements

ASMS requires the following to connect to Juniper Netscreen devices:

- [Device analysis](#)
- [ActiveChange](#)
- [Log collection](#)

Device analysis

The user connecting to the Netscreen device must be a super-user with a minimum of **read-only** access via SSH.

ActiveChange

When ActiveChange is enabled, the user connecting to the Netscreen device requires a minimum of **read-write** access via SSH.

Log collection

ASMS can either receive syslog messages from the device or can collect syslog messages from a remote syslog-ng server.

Tip: We recommend configuring a remote syslog-ng server for log collection whenever possible.

If your system is configured for the Netscreen device to send syslog messages to ASMS, the message format must be configured as follows.

Syslog servers								
No.	Enable	IP / Hostname	Port	Security Facility	Facility	Event Log	Traffic Log	TCP
1.	<input checked="" type="checkbox"/>	192.168.1.2	514	LOCAL0	LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

In such cases, ensure that the TCP option is cleared.

Add a Juniper Netscreen to AFA

This procedure describes how to add a Juniper Netscreen to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Juniper > Netscreen**.
3. Complete the fields as needed:

Access Information

Enter the device's access information and credentials as follows:

Host	Enter the device's host name or IP address.
-------------	---

User Name	Enter the user name to use for SSH access to the device.
Password	Enter the password to use for SSH access to the device.
Retrieve credentials from CyberArk vault	<p>Select to authenticate the device with a CyberArk Vault instead of saving the device credentials on the AlgoSec server.</p> <p>When selected, also define the following:</p> <ul style="list-style-type: none"> • Platform (Policy ID). The Platform for this device which will be authenticated via CyberArk. • Safe. The safe for this device which will be authenticated via CyberArk. • Folder. The folder for this device which will be authenticated via CyberArk. • Object. This device's CyberArk Object. <p>Note: These options only appear when CyberArk is configured in AFA. For details, see Integrate AFA and CyberArk.</p>

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

Note: This field is only relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system.

To disable Baseline Compliance Report generation for this device, select **None**.

For more details, see [Customize baseline configuration profiles](#).

Advanced

Click the arrow next to the **Advanced** heading to display the fields in this area.

Select **Display virtual routers** to analyze each virtual router separately.

When selected, each virtual router will appear in the device tree immediately below the Netscreen device and parallel to virtual systems.

Note: This is required in the rare cases where there are no inter-VR routes to/from a specific VR. In other words, when there is an “isolated” VR.

Remote Management Capabilities

Select one of the following methods to collect data:

- **SSH** (recommended)
- **Telnet**

To specify a custom port, select the **Custom Port** option and enter the port. This is only relevant when SSH is selected.

Tip: Alternately, configure AFA to connect to the device using SSH with Public-Key authentication. To do so, select the **Use public key authentication in data collection** check box in the **General** sub-tab of the **Options** tab in the Administration area.

For details, see [Define AFA preferences](#).

Firewall Log

Configure logging fields as follows:

Collect logs	<p>Specify whether AFA should collect logs for the device, by selecting one of the following:</p> <ul style="list-style-type: none"> • None. Do not collect logs. • Standard. Enable log collection. • Extensive. Enable log collection and the Intelligent Policy Tuner. <p>The default value is Extensive.</p>
From	<p>Specify from where AFA should collect logs, by selecting one of the following:</p> <ul style="list-style-type: none"> • NSM (default). AFA collects logs from the NSM. If selected, also define the following: <ul style="list-style-type: none"> ◦ NSM Dev server. The NSM host name or IP address. ◦ User Name. The user name used to connect to the NSM. ◦ Password. The password used to connect to the NSM. <p>Click Test Connectivity to test your connection to the NSM server.</p> • Syslog-ng. AFA collects logs from a syslog-ng server. If selected, also specify the syslog-ng server. For details, see Specify a Syslog-ng server. <div data-bbox="545 1188 1409 1381" style="background-color: #e6f2e6; padding: 10px; border: 1px solid #ccc;"> <p>Tip: If you are using Juniper's STRM log server, have the messages forwarded to a syslog-ng. For details, see Configure Juniper STRM to forward logs to a Syslog-ng server.</p> </div> <p>The default value is NSM.</p>
Collect audit logs from the same server	<p>Select to specify that AFA uses the same server to collect both traffic and audit logs.</p> <div data-bbox="467 1577 1409 1696" style="background-color: #e6f2e6; padding: 10px; border: 1px solid #ccc;"> <p>Note: If you clear this option, specify a separate set of audit log details, just as you did for the traffic log server.</p> </div>

Additional firewall identifiers	<p>Enter any additional IP addresses or host names that identify the device, separated by colon (:).</p> <p>For example: 1.1.1.1:2.2.2.2:ServerName</p> <p>This is relevant when the device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings. If AFA receives logs with an identifier it does not recognize, the logs will not be processed.</p> <p>Note: This field is not supported for sub-systems, such as Juniper VSYS/LSYS. For more details, see Add additional device identifiers for sub-systems.</p> <p>Note: This field only appears if you selected Syslog-ng in the From field.</p>
Log collection frequency	<p>Enter the interval of time in minutes, at which AFA should collect logs for the device.</p>

ActiveChange

Select Enable ActiveChange to configure FireFlow to generate recommendations and push them to the device.

Note: The ActiveChange area only appears if you selected **SSH** above.

Options

Define the following options as needed:

Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring.</p>
Set user permissions	<p>Select this option to set user permissions for this device.</p>

4. Click **Finish**. The new device is added to the device tree.
5. If you selected **Set user permissions**, the **Edit users** dialog box appears.
 In the list of users displayed, select one or more users to provide access to reports for this account.
 To select multiple users, press the **CTRL** button while selecting.
 Click **OK** to close the dialog.

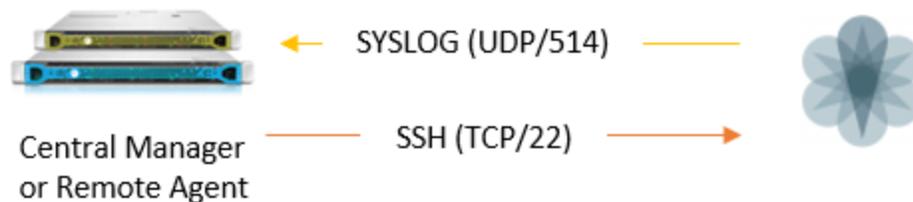
Juniper SRX devices in AFA

The following sections describe how ASMS connects to Juniper SRX devices:

- [Network connection](#)
- [Device permissions](#)
- [Add a Juniper SRX device to AFA](#)
- [Configure Juniper SRX devices to send traffic logs](#)

Network connection

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a Juniper SRX device.



Device permissions

ASMS requires the following permissions for your Juniper SRX routers:

Device analysis

AFA requires permissions to run the following commands on your SRX device:

- show configuration
- show route extensive all
- show configuration groups junos-defaults applications

ActiveChange

When ActiveChange is enabled, ASMS requires a specific user on the SRX device. This user must be a member of the **super-user** login class.

For example, define the SRX user as follows:

The screenshot shows the 'Edit User Management' window with the 'Users' tab selected. An 'Add User' dialog box is open, containing the following fields and values:

Field	Value
User name:	AlgosecUser
User Id:	
Full name:	Algosec Admin
Password:	*****
Confirm password:	*****
Login class:	super-user

Buttons for 'Add...', 'Edit...', and 'Delete' are visible on the right side of the dialog. 'OK' and 'Cancel' buttons are at the bottom of the dialog.

Note: If ActiveChange is not enabled, the user can be in a login-class other than super-user.

For details, see [How to configure a Juniper SRX read-only user with permissions required for AFA data collection](#) in AlgoPedia.

Add a Juniper SRX device to AFA

This procedure describes how to add a Juniper SRX to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Juniper > SRX**.
3. Complete the fields as needed.

Access Information

Enter the device's access information and credentials as follows:

Host	Enter the host name or IP address of the device.
User Name	Enter the user name.
Password	Type the associated password.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system. For more details, see [Customize baseline configuration profiles](#).

Note: To disable Baseline Compliance Report generation for this device, select **None**.

Additional Information

Select **Display virtual routers** to analyze each virtual router separately, enabling advanced routing analysis.

This causes individual virtual routers to appear in the AFA device tree as the last tier (below their LSYS), and AFA provides a report for each router.

When this option is enabled, the analysis AFA provides for the LSYS aggregates the information provided for its VRs and should be used for most AFA analysis capabilities, such as policy optimization recommendations.

The VR analyses provides the ability to:

- Troubleshoot routing/topology issues, such as traffic simulation query results
- Manage risks by focusing on the rules that trigger risks,
- Determine which risky rules to trust

Although the LSYS analysis aggregates the information for each VR under it, the LSYS analysis does not fully contain the information provided in the VR tier analyses.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.

- **Static Routing Table (URT)**. AFA will take the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

Remote Management Capabilities

Select a data collection method:

- **Telnet**
- **SSH** (more secure)

Then, define the following:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
Number of allowed encryption keys	Enter the permitted number of different RSA keys received from this device's IP address. Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc. For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. If this number is set to 1, the connection to the node will fail, resulting in a failed analysis.

Tip: You can configure AFA to connect to the device using SSH with Public-Key authentication. For details, see [Define AFA preferences](#).

Log Collection and Monitoring

Define log collection and monitoring settings as follows:

Log collection method	<p>Specify whether AFA should collect logs for the device, by selecting one of the following:</p> <ul style="list-style-type: none"> • None: Do not collect logs. • Standard: Enable log collection. • Extensive: Enable log collection and the Intelligent Policy Tuner. <p>The default value is Extensive.</p>
Syslog-ng server	<p>If you selected Standard or Extensive in the Log collection method field, you must specify the syslog-ng server. For details, see Specify a Syslog-ng server.</p> <p>Note: When using STRM (Juniper's log server), you can forward the logs to a syslog-ng (AFA's built-in syslog-ng or an external one). Then, you can define this syslog-ng as the relevant log server. For more details, see Configure Juniper STRM to forward logs to a Syslog-ng server.</p>
Additional firewall identifiers	<p>Enter any additional IP addresses or host names that identify the device. Separate multiple entries by colons (:).</p> <p>For example: 1.1.1.1:2.2.2.2:ServerName</p> <p>This is relevant when the device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings.</p> <p>If AFA receives logs with an identifier it does not recognize, the logs will not be processed.</p> <p>Note: This field is only relevant for the parent device, and you may want to specify additional identifiers for sub-systems. For details, see Add additional device identifiers for sub-systems.</p>
Log collection frequency	<p>Select the interval of time in minutes, in which AFA should collect logs for the device.</p>

ActiveChange

Select **Enable ActiveChange** for all supported Juniper SRX firewalls to enable

FireFlow to generate CLI recommendations and push them to the device.

Note: Checking this box will enable ActiveChange for all Juniper SRX firewalls (not only for this device).

Options

Define the following options as needed:

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

- If you enabled ActiveChange, the **ActiveChange License Agreement** dialog box appears.

Select **I Agree** and click **OK**.

- Click **Finish**.

- If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

The new device is added to the device tree, and a success message appears to confirm that the device is added.

Configure Juniper SRX devices to send traffic logs

ASMS can collect log data by receiving traffic logs from the device itself, or by collecting syslog messages from an external, remote syslog-ng server.

Configure this as needed. For details, see the [Juniper Knowledge Base](#).

Juniper routers in AFA

The following sections describe how ASMS connects to Juniper JUNOS routers:

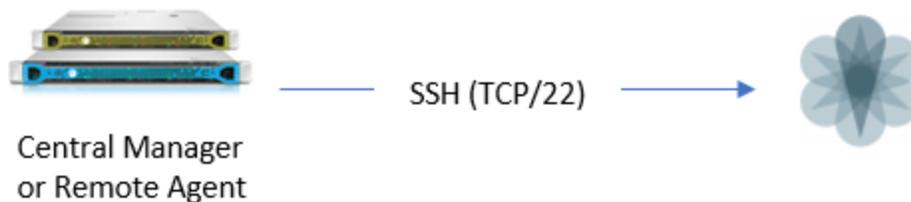
- [Network connectivity](#)
- [Device requirements](#)
- [Add a Juniper router to AFA](#)

Note: Juniper routing devices with large route tables may cause data collection to take longer than usual.

For details about specific routers supported, see the [AlgoSec Support Matrix](#).

Network connectivity

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a Juniper router.



Device requirements

ASMS connects to Juniper routing devices using SSH, and requires a super-user with the following permissions:

- **show version**
- **show route active-path all**
- **show configuration**

Note: If you need to use a user that is not a super-user, contact AlgoSec support.

Add a Juniper router to AFA

This procedure describes how to add a Juniper router to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Juniper > M/E Routers**.
3. Complete the fields as needed.

Access Information

Enter the device's access information and credentials as follows:

Host	Enter the device's host name or IP address.
User Name	Enter the user name used to access the device.
Password	Enter the password used to access the device.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

Note: This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

To disable Baseline Compliance Report generation for this device, select **None**.

The drop-down list includes all baseline compliance profiles in the system. For more details, see [Customize baseline configuration profiles](#).

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

Remote Management Capabilities

Select a method of data transmission:

- **SSH** (recommended).
If selected, AFA also enables you to specify a custom port. Select **Custom Port** and enter the port number.
- **Telnet**

From the **Number of allowed encryption keys** dropdown, select the number of permitted different RSA keys received from this device's IP address.

Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc.

For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. In this case, if the **Number of allowed encryption keys** value was set to **1**, the node connection and subsequent analysis will fail.

Options

Define the following options as needed:

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

4. Click **Finish**. The new device is added to the device tree.
5. If you selected **Set user permissions**, the **Edit users** dialog box appears.
In the list of users displayed, select one or more users to provide access to reports for this account.
To select multiple users, press the **CTRL** button while selecting.
Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Configure Juniper STRM to forward logs to a Syslog-ng server

This procedure describes how to configure Juniper STRM to forward logs to a syslog-ng server.

Do the following:

1. Log in to the STRM Log Manager interface, and click the **Admin** tab.
2. On the left, click **Data Sources > Syslog Forwarding Destinations > Add**.
3. Enter the syslog-ng server's IP address and port, and click **Save**.

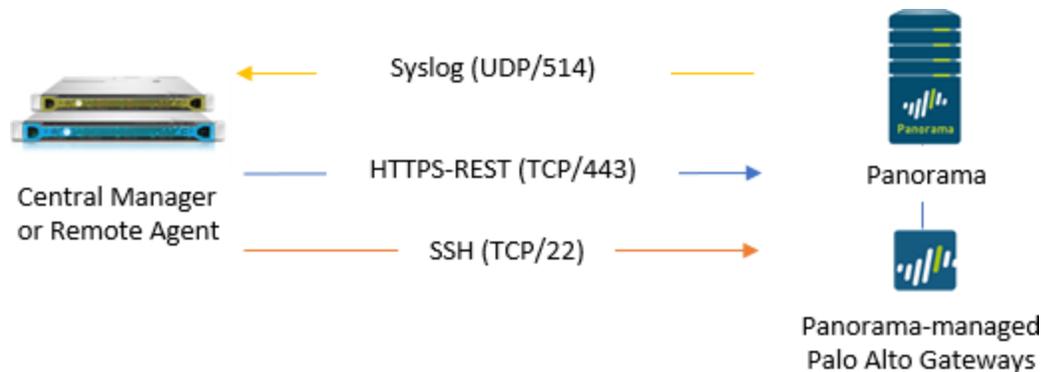
All logs that are sent to the Juniper STRM device will be forwarded to the syslog-ng server.

Add Palo Alto Networks devices

This topic describes how AFA connects to Palo Alto Panorama and firewall devices.

Palo Alto network connections

The following image shows how an ASMS Central Manager or Remote Agent connects to Palo Alto Panorama and Gateway devices.



Note: Log data can also be forwarded from M100/M500 collectors.

Service chaining mode

AFA automatically identifies Palo Alto Panorama devices in service-chaining mode when the device has a single interface, or a single one non-management interface.

If your device has multiple non-management interfaces and service-chaining mode is not identified automatically, configure this for your device manually. For details, see [Configure one-armed mode manually](#).

VR/Vwire and VSYS analysis

Once added, AFA identifies and analyzes individual VR/Vwires for Panorama devices, in addition to analyzing each VSYS. The VSYS analysis aggregates the information provided for its VR/Vwires, and should be used for most AFA analysis features, such as policy optimization recommendations.

VR/Vwire analysis data provides the ability to troubleshoot routing and topology issues, such as traffic simulation query results, manage risks, and determine which risky rules to trust.

Although the VSYS analysis aggregates the information for each VR under it, the VSYS analysis does not fully contain the data provided in the VR tier analysis.

Inter-VR routing / Inter-VSYS support

AFA supports all inter-VR and inter-VSYS cases, whether they are by shared-VR or an explicit inter-VR, by doing the following:

- Using shared VRs
- Using the VR as a next-hop router
- Including the inter-VSYS using the external zones

Note: Shared Gateways are partially supported, only when the virtual router is already included in the DEVICES tree.

When AFA detects either of these inter-VR routing configurations, it adds fake, or back-plane, interfaces to the firewall's VR URT file to simulate these connections. These connections can then be displayed on the AFA network map and in query results.

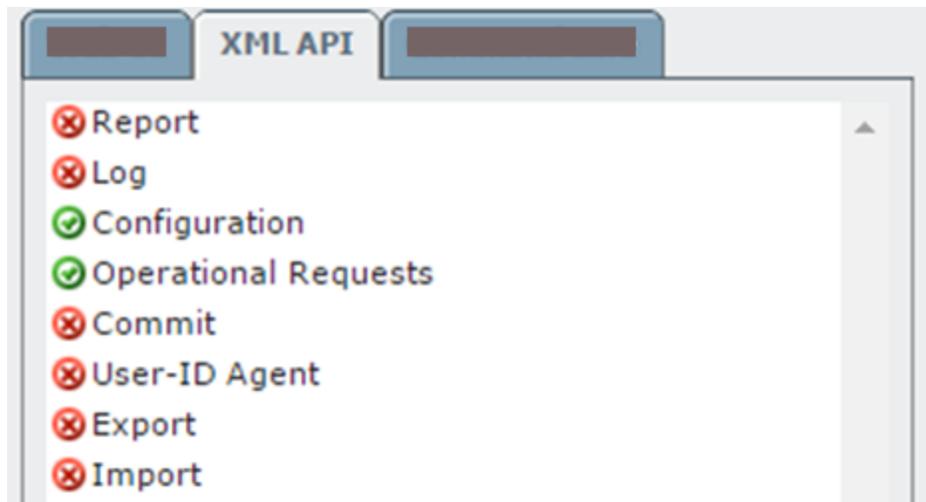
Panorama device permissions

ASMS requires the following device permissions to connect to Palo Alto Panorama devices:

Device analysis

ASMS requires a Panorama REST API account configured with **Configuration** and **Operational Requests** permissions.

For example:



ActiveChange

When ActiveChange is enabled, ASMS requires the additional **Export** permissions as well.

For example:



Palo Alto Networks Firewall device permissions

To connect to Palo Alto firewall devices, ASMS requires one of the following types of users:

- **Superuser** (read-only)
- **Device Admin**
- **Device Admin** (read-only)

If the Palo Alto firewall is a version earlier than 4.1.7, is managed by Panorama, but is defined directly in AFA, ASMS requires one of the following types of users:

- **SuperUser** (read/write)
- **Admin** (read/write)

Add a Palo Alto Networks Panorama

This procedure describes how to add a Palo Alto Networks Panorama device to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Palo Alto Networks > Panorama**.
3. Complete the fields as needed.

Access Information

Host	Enter the host name or IP address of the device.
User name	Enter the administrative user name to use for SSH access to the device. For more details, see Panorama device permissions .
Password	Enter the associated password.
High Availability	Select this option to configure a High Availability cluster. If selected, you must also enter a value for the Secondary field.
Secondary Panorama	Type the host name or IP address for the secondary device.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

ActiveChange

Select this option to enable ActiveChange for the device.

Log Collection and Monitoring

Syslog-ng server	Specify the syslog-ng server. For details, see Specify a Syslog-ng server .
Log collection frequency	Type the interval of time in minutes, at which AFA should collect logs for the device.

You must also configure the device to send syslog messages. For more details, see [Configure log collection on a Panorama device](#).

Note: To process logs from the devices managed by the Panorama, you may need to specify additional device identifiers, especially when the sub-device is represented by multiple or non-standard device identifiers in the logs. This may be relevant, for example, with firewall clusters or non-standard logging systems.

For more details, see [Add additional device identifiers for sub-systems](#).

4. If you enabled ActiveChange, the **ActiveChange License Agreement** dialog box appears.

Select **I Agree** and click **OK**.

5. Click **Next** to display the **Panorama - Step 2/2** page.

This page lists the devices that are managed by the Panorama, including standalone devices and virtual systems.

Tip: Clear any devices that you don't want to add to AFA.

6. Optional: To collect logs created by a managed device / virtual system:
 - a. In the **Add Device** column, select the check box next to the device's name.
 - b. In the **Log Analysis** column, select one of the following:
 - **None** to disable logging.
 - **Standard** to enable logging
 - **Extensive** to enable logging and the Intelligent Policy Tuner.

Note: Using the device's logs enables AFA to detect certain policy optimization information, such as unused rules. This information is displayed in the **Policy Optimization** section of the AFA report.

7. Optional: Enable AFA to generate baseline compliance reports:

- a. Click [Configure](#).
- b. In the **Direct Access Configuration**, enter the following details, and then click OK.

Host IP	Type the IP address of the device.
User Name	Type the user name to access the device.
Password	Type the password to access the device.

Baseline Profile	<p>Select the baseline compliance profile to use.</p> <p>The drop-down list includes all baseline compliance profiles in the system. For more details, see Customize baseline configuration profiles.</p> <p>To disable Baseline Compliance Report generation for this device, select None.</p>
Test Connectivity	<p>Click this button to test connectivity to the defined device.</p> <p>A message informs you whether AFA connected to the device successfully.</p>

Note: Specifying this information for a device triggers a direct SSH connection to the device.

8. Select the remaining options as needed:

Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes.</p> <p>For details, see Configure real-time monitoring.</p>
Set user permissions	<p>Select this option to set user permissions for this device.</p>

9. Click **Finish**. The new device is added to the device tree.

In the device tree, Panoramas are represented with a four tier hierarchy: Panorama, PA firewall, VSYS, and VR/Vwire.

Passive-Active clusters

Passive-Active clusters, including VSYSs and firewalls display as follows:

- Display as a single node on the tree and on the map.
- Cluster display names in the device tree, report, and so on, represent both names of the cluster members. For example: **NODE1_NODE2**

- Sub-nodes of the device, such as a VSYS, follow afterward. For example:
NODE1_NODE2_VSYS1
- **Baseline compliance:** Define the active node details in the device definition wizard.
- For Active-Active clusters, AFA includes both nodes in the tree.

10. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Configure log collection on a Panorama device

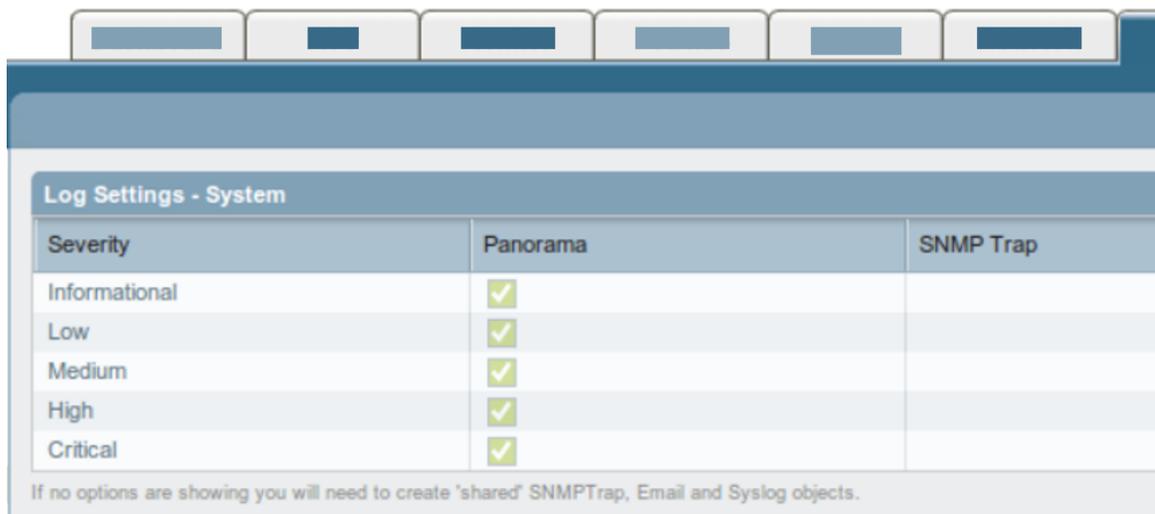
ASMS can collect log data by receiving syslog messages from the Panorama device, or by collecting syslog messages from a remote syslog-ng server.

This procedure describes how to configure the Panorama device to send syslog messages to ASMS. For more details, see [Log Collection and Monitoring](#).

On the Panorama device, do the following:

1. Configure a new **Syslog Server Profile** for the syslog server. For details, see [Palo Alto KnowledgeBase](#).

2. Configure the log settings by selecting all severities. For example:



Configure one-armed mode manually

AFA automatically identifies Palo Alto Panorama devices in one-armed mode when the device has a single interface, or a single one non-management interface. If your device has multiple non-management interfaces and one-armed mode is not identified automatically, configure this for your device manually.

Do the following:

1. On the AFA machine, access your device configuration **meta** file as follows:

```
/home/afa/.fa/firewalls/<device_name>/fwa.meta
```

where **<device_name>** is the name of the device listed. If your device is listed multiple times, enter the longer name.

2. On a new line, enter:

```
is_steering_device=yes
```

3. Run an analysis on the device to update the device data in AFA.

Add a Palo Alto Networks firewall

This procedure describes how to add a Palo Alto Networks firewall to AFA.

Note: Palo Alto Networks firewalls defined directly in AFA do not support the advanced routing analysis provided for Palo Alto Networks devices defined at the Panorama level. AFA does not identify individual VR/Vwires and therefore does not benefit from the routing information they provide.

For more details, see [Add a Palo Alto Networks Panorama](#).

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor device selection page, select **Palo Alto Networks > Firewall**.
3. Complete the fields as needed.

Access Information

Host	Type the host name or IP address of the device.
User Name	Type the administrative user name to use for SSH access to the device. If the device is managed by Panorama and Panorama is used to push all or part of the device's configuration, you must provide a user of the Superuser type. If the device is either not managed by Panorama, or it is managed by Panorama but no configuration is pushed from Panorama towards the device, then you can specify a user name of any of the following types: Superuser, Superuser (Read Only), Device Admin, or Device Admin (Read-Only).
Password	Type the password to use for SSH access to the device.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system. For more information on baseline compliance profiles and instructions for adding new baseline compliance profiles, see Customizing Baseline Configuration Compliance Profiles (see [Customize baseline configuration profiles](#)).

To disable Baseline Compliance Report generation for this device, select **None**.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For more information, see Manually Specifying Routing Information (see [Specify routing data manually](#)).

Remote Management Capabilities

Select a method of data collection:

- **SSH** (more secure)
- Telnet

Then define the following:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
--------------------	--

Number of allowed encryption keys	<p>Enter the permitted number of different RSA keys received from this device's IP address.</p> <p>Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc. For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. If this number is set to 1, the connection to the node will fail, resulting in a failed analysis.</p>
--	--

Log Collection and Monitoring

Specify whether AFA should collect logs for the device, by selecting one of the following:

- **None:** Do not collect logs.
- **Standard:** Enable log collection.
- **Extensive:** Enable log collection and the Intelligent Policy Tuner.

The default value is **Extensive**.

Additionally, define the following values:

Syslog-ng server	<p>If you selected Standard or Extensive in the Log collection method field, you must specify the syslog-ng server. For details, see Specify a Syslog-ng server.</p>
-------------------------	---

Additional firewall identifiers	<p>Enter any additional IP addresses or host names that identify the device.</p> <p>When adding multiple entries, separate values by a colon (:). For example: 1.1.1.1:2.2.2.2:ServerName</p> <p>This is relevant when the device is represented by multiple or non-standard device identifiers in the logs, for example, in cases of firewall clusters or non-standard logging settings. If AFA receives logs with an identifier it does not recognize, the logs will not be processed.</p> <p>Note: This field is not supported for sub-systems (Juniper VSYS/LSYS, Fortinet VDOM, Cisco security context, etc.). To configure additional identifiers for sub-systems, see Adding Additional Device Identifiers for Sub-Systems (see Add additional device identifiers for sub-systems).</p>
Log collection frequency	<p>Type the interval of time in minutes, at which AFA should collect logs for the device.</p>

Options

Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring.</p>
Set user permissions	<p>Select this option to set user permissions for the device.</p>

4. Click **Finish**.

The new device is added to the device tree, with a two tier hierarchy: firewall and VSYS.

5. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

➔ **See also:**

- [AlgoSec & Palo Alto Networks](#)

Add a Symantec Blue Coat

This procedure describes how to add a Symantec Blue Coat device to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Symantec > Blue Coat**.
3. Enter the following fields as needed:

Access Information

Supported Capabilities	Displays a list of supported device capabilities. This field is read-only.
Host	Enter the host name or IP address of the device.
User Name	Enter the user name to use for SSH access to the device.
Password	Enter the password to use for SSH access to the device.

<p>Retrieve credentials from CyberArk vault</p>	<p>Select this check box to authenticate the device with a CyberArk Vault instead of saving the device credentials on the AlgoSec server.</p> <p>If selected, also enter the following details:</p> <ul style="list-style-type: none"> • Platform (Policy ID): The platform to use when authenticating via CyberArk. • Safe: The safe to use when authenticating via CyberArk. • Folder: The folder to use when authenticating via CyberArk. • Object: The device's CyberArk Object. <p>Note: These options only appear when CyberArk is configured in AFA. For more details, see Integrate AFA and CyberArk.</p>
--	--

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Baseline Configuration Compliance

To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.

The drop-down list includes all baseline compliance profiles in the system. For more details, see [Customize baseline configuration profiles](#).

To disable Baseline Compliance Report generation for this device, select **None**.

SNMP Polling

SNMP version	Select the SNMP version in the drop-down menu.
SNMP community	the SNMP community string. This field is only relevant for SNMP v2c .
Security Name (username)	Enter the security name. This field is only relevant for SNMP v3 .
Authentication Protocol	Select an authentication protocol as needed. This field is only relevant for SNMP v3 .
Authentication Password	If you selected an authentication protocol, enter the password. This field is only relevant for SNMP v3 .
Privacy Protocol	Select a privacy protocol as needed. This field is only relevant for SNMP v3 .
Privacy Password	If you selected a privacy protocol, enter the password. This field is only relevant for SNMP v3 .

Additional Information

Enter an **enable** password to use when switching to enabled mode.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

Remote Management Capabilities

Select one of the following methods to collect data:

- SSH (recommended)
- Telnet

Then, enter the following as needed:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
Number of allowed encryption keys	Enter the permitted number of different RSA keys received from this device's IP address. Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, and so on. For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. If this number is set to 1 , the connection to the node will fail, resulting in a failed analysis.

Policy Configuration Method

Select one of the following policy configuration methods:

Visual Policy Manager - VPM	The device policy is configured via the Visual Policy Manager (VPM) only.
Content Policy Language - CPL (Command-Line)	The device policy is configured via <i>both</i> the command line (CPL) <i>and</i> the Visual Policy Manager (VPM).

Options

In this field...	Do this...
Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

4. Click **Finish**. The new device is added to the device tree.
5. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

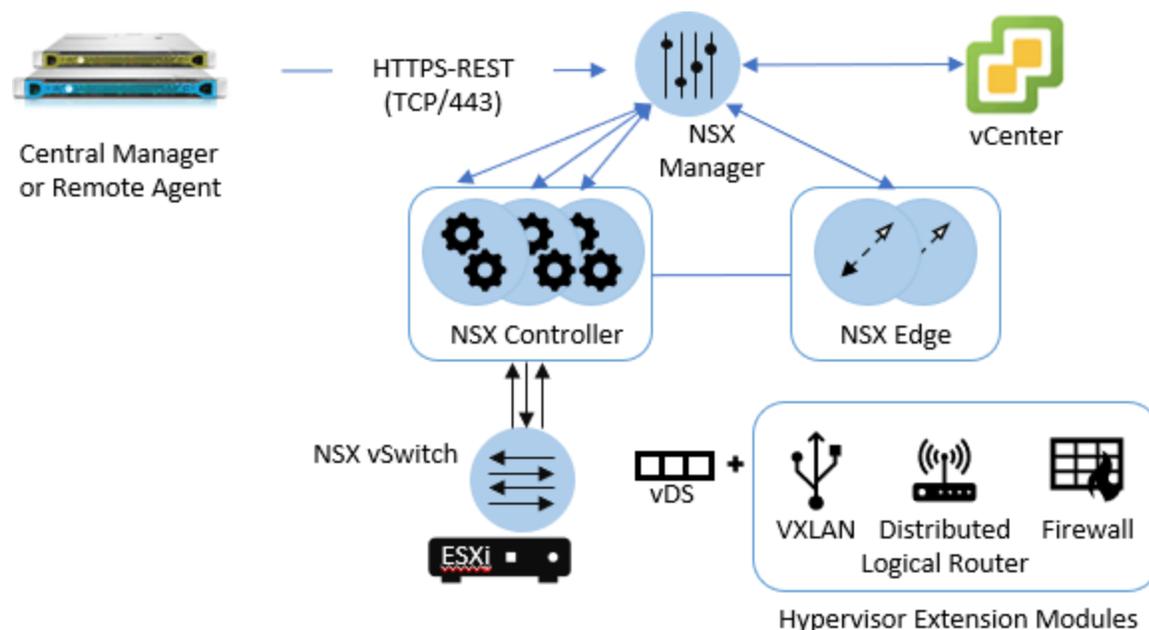
Click **OK** to close the dialog.

Add VMware NSX-V devices

This topic describes ASMS's support for VMware NSX-V devices.

Network connectivity

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a VMware NSX-V device environment.



Device permissions

ASMS requires the following to collect data from VMware NSX-V devices

- [Device analysis](#)
- [ActiveChange](#)

Device analysis

ASMS requires minimal, read-only access permissions to access VMware NSX-V devices and perform data collection.

The user accessing the VMware NSX-V device must have one of the following roles:

- Auditor
- Security Admin
- NSX Admin
- Enterprise Admin

Note: If you are using an NSX Manager, we recommend using the build-in NSX Manager user to connect from ASMS.

ActiveChange

When ActiveChange is enabled, the user connecting to the VMware NSX-V device requires read-write permissions.

- Security Admin
- Enterprise Admin

Note: When adding an NSX-V device to AFA with vCenter permissions, (both Admin and Read Only), the following data will be missing:

- Device version
- Device host name
- NSX Manager IP

Add a VMware NSX-V to AFA

This procedure describes how to add a VMware NSX-V device to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#)
2. In the vendor device selection page, click **VMware > NSX**.
3. Complete the fields as needed.

Access Information

Host	Enter the host name or IP address of the NSX Manager. This is the name that will be displayed in the devices tree.
User Name	Enter the user name to use for REST access to the device.
Password	Enter the password to use for REST access to the device.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Additional Information

Select the **Learning mode** option to specify that AFA traffic simulation should treat traffic that is not specified in a rule as blocked.

In reality, the default behavior for NSX devices is to allow all traffic that is not explicitly blocked. Learning mode enables you to better understand the specific traffic that needs to be allowed on the device.

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

ActiveChange

Select the **Enable ActiveChange** option to enable ActiveChange for the device.

Note: Enabling ActiveChange rollback for this device requires special configuration on the device.

Options

Real-time change monitoring	Select this option to enable real-time change monitoring. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

4. Click **Finish**. The new device is added to the device tree.
5. If you selected **Set user permissions**, the **Edit users** dialog box appears.
In the list of users displayed, select one or more users to provide access to reports for this account.
To select multiple users, press the **CTRL** button while selecting.
Click **OK** to close the dialog.
A success message appears to confirm that the device is added.

Required device permissions

AFA requires certain permissions on devices in order to collect data and support other functionalities. The table below describes AFA's requirements for the user account used to connect to AFA for each brand, as well as any other device requirements. Some permissions are only required for specific AFA features.

This topic describes items required for each device type in order for AFA to collect data and support other features. Some items are only required for specific AFA features.

Baseline configuration compliance

For baseline configuration compliance support, AFA connects via SSH to the device and executes the commands in the specified baseline configuration profile.

The required permissions depend on the profile used, as AFA requires permission to read/execute all commands listed in the profile.

Device requirements reference by brand

Check requirements for the following device brands:

- [Arista device requirements](#)
- [AWS requirements](#)
- [Azure requirements](#)
- [Check Point device requirements](#)
- [Cisco device requirements](#)
- [F5 device requirements](#)
- [Fortinet device requirements](#)
- [Juniper device requirements](#)
- [Palo Alto device requirements](#)
- [Symantec BlueCoat SGOS device requirements](#)
- [TopSec device requirements](#)

- [VMware NSX device requirements](#)
- [WatchGuard device requirements](#)

Note:

Support for the Forcepoint brands (Sidewinder, StoneGate) and Hillstone was deprecated in ASMS version A30.00.

If you had defined these devices in an earlier version of ASMS, these devices are still available to you, with all the existing capabilities, but you cannot add new ones after upgrading.

We recommend backing up device data before or after upgrading and then removing these devices from AFA. Make sure to download any report zip files for the device before deleting.

For more details, see the relevant [AlgoPedia](#) KB article.

Check Point device requirements

See [Check Point device permissions](#).

Cisco device requirements

Cisco ASA	For details, see Device permissions .
Cisco Firewalls via CSM	Requires enabling the CSM API service. To enable this, in the CSM management application, click Tools > Security Manager Administration > API , and check the Enable API Service setting.
Cisco IOS	For details, see Device permissions .
Cisco Nexus	For details, see Device permissions .
Cisco ACI	For details, see Device permissions .
Cisco ISE	For details, see Device permissions .

Cisco Firepower	For details, see Device permissions .
------------------------	---

Arista device requirements

For details, see [Device permissions](#).

Juniper device requirements

Juniper Netscreen	For details, see Device requirements .
Juniper SRX	For details, see Device permissions .
Juniper NSM	For details, see Device permissions .
Junos Space Security Director	For details, see Device permissions .
Juniper M/E Routers	For details, see Device requirements .

Fortinet device requirements

For more details, see [Add Fortinet devices](#).

Palo Alto device requirements

For details, see [Add Palo Alto Networks devices](#).

F5 device requirements

F5 BIG-IP LTM Only	For details, see Device permissions .
F5 BIG-IP LTM and AFM	For details, see Device permissions .

Symantec BlueCoat SGOS device requirements

The user must be able to enter “enable” mode.

For retrieving routing data from the device, SNMP access is required.

WatchGuard device requirements

Read Only permissions are sufficient.

Routing is based on SNMP.

- For default usernames and passwords see here (<https://knowledge.algosec.com/skn/tu/e5269>).
- For further SNMP details, see here (<https://knowledge.algosec.com/skn/tu/e5178>).

TopSec device requirements

For further SNMP details, see here (<https://knowledge.algosec.com/skn/tu/e5178>).

VMware NSX device requirements

For details, see [Device permissions](#).

AWS requirements

For details, see [Device access requirements for AWS](#)

Azure requirements

For details, see [Device requirements for Azure](#).

Add other devices and routing elements

This topic describes how to add monitoring and routing devices and routing elements.

Note: For details about adding devices of specific vendor types to AFA, or importing device data from CSV files, see [Add devices to AFA](#) and [CSV import file format](#).

Add monitoring and routing devices

This procedure describes how to add the following types of monitoring and routing devices to AFA:

- Avaya - Routing Switch
- Brocade VDX
- Cisco ACE
- HP H3C Routers
- Juniper Secure Access (SSL VPN)
- Juniper Routers (non-M/E)
- Linux Netfilter IPtables
- SECUI MF2
- SonicWall
- Topsec Firewall
- WatchGuard

Note: These devices support change monitoring, routing analysis, and baseline configuration compliance only.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select your device type.
3. Complete the following fields as needed, and then click **Finish**.

The fields displayed may differ depending on your device brand and selections.

Access Information fields

Supported Capabilities	Displays a list of device capabilities. This field is read-only and only appears for some devices.
Host	Type the host name or IP address of the device.
User Name	Type the user name to use for SSH access to the device.
Password	Type the password to use for SSH access to the device.

Geographic Distribution fields

Device managed by	Select the remote agent that should perform data collection for the device. To specify that the device is managed locally, select Central Manager . This field is relevant when a Geographic Distribution architecture is configured.
--------------------------	--

Baseline Configuration Compliance

Baseline Configuration Profile	<p>To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.</p> <p>The drop-down list includes all baseline compliance profiles in the system.</p> <p>To disable Baseline Compliance Report generation for this device, select None.</p> <p>For more details, see Customize baseline configuration profiles.</p>
---------------------------------------	--

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For more information, see [Manually Specifying Routing Information](#) (see [Specify routing data manually](#)).

SNMP Polling

Use the following fields to define SNMP polling values. These fields only appear for selected device brands.

SNMP version	Select the SNMP version in the drop-down menu.
SNMP community	Type the SNMP community string. This field is only relevant for SNMP v2c .
Security Name (username)	Type the security name. This field is only relevant for SNMP v3 .
Authentication Protocol	If desired, select the authentication protocol in the drop-down menu. This field is only relevant for SNMP v3 .

Authentication Password	If you selected an authentication protocol, type the password. This field is only relevant for SNMP v3 .
Privacy Protocol	If desired, select a privacy protocol in the drop-down menu. This field is only relevant for SNMP v3 .
Privacy Password	If you selected a privacy protocol, type the password. This field is only relevant for SNMP v3 .

Remote Management Capabilities

Select SSH or Telnet to determine how data is transmitted to AFA.

Note: SSH is more secure than Telnet, however some device brands support only one method.

Then define the following details:

Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
Number of allowed encryption keys	Enter the permitted number of different RSA keys received from this device's IP address. Different RSA keys may be sent from the same IP address in cases of cluster fail-over, device operating system upgrades, etc. For example, if a cluster fail-over occurs, the secondary node will send a new RSA key from the same IP address to AFA. If this number is set to 1 , the connection to the node will fail, resulting in a failed analysis.

Options

Real-time change monitoring	Select this option to enable real-time change monitoring. For more details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

The new device is added to the device tree.

- If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Add routing elements

This procedure describes how to add routing elements to AFA.

Routing elements are generic devices that perform SNMP connections for retrieving routing tables, without collecting configurations.

Note: AFA supports routing elements using SNMPv2c and SNMPv3. The supported MIB is RFC-1213, and the OID fetched from the device is **ipRouteEntry** (object identifier: 1.3.6.1.2.1.4.21.1).

We do not recommend adding devices as routing elements if they have a non-standard routing deployment in addition to the standard RFC1213, such as Cisco Routers. For these devices, the SNMP response does not include crucial information, mainly concerning VRF instances.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, click  **Routing Element** on the right.
3. Complete the following fields as needed and click **Finish**.

Access Information fields

Supported Capabilities	Displays a list of device capabilities. This field is read-only.
Host	Type the host name or IP address of the device.

Geographic Distribution fields

Device managed by	Select the remote agent that should perform data collection for the device. To specify that the device is managed locally, select Central Manager . This field is relevant when a Geographic Distribution architecture is configured.
--------------------------	--

SNMP Polling fields

Use the following fields to define SNMP polling values.

SNMP version	Select the SNMP version in the drop-down menu.
SNMP community	Type the SNMP community string. This field is only relevant for SNMP v2c .
Security Name (username)	Type the security name. This field is only relevant for SNMP v3 .

Authentication Protocol	If desired, select the authentication protocol in the drop-down menu. This field is only relevant for SNMP v3 .
Authentication Password	If you selected an authentication protocol, type the password. This field is only relevant for SNMP v3 .
Privacy Protocol	If desired, select a privacy protocol in the drop-down menu. This field is only relevant for SNMP v3 .
Privacy Password	If you selected a privacy protocol, type the password. This field is only relevant for SNMP v3 .

Route Collection

Specify how AFA should acquire the device's routing information:

- **Automatic.** AFA will automatically generate the device's routing information upon analysis or monitoring.
- **Static Routing Table (URT).** AFA will take the device's routing information from a static file you provide. For details, see [Specify routing data manually](#).

Options

Update Network Map upon routing change	Select this option to enable automatically updating the graphic network map upon routing changes.
Set user permissions	Select this option to set user permissions for this device.

The new device is added to the device tree.

4. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

Add/update multiple devices in bulk

Add multiple new devices or update multiple existing devices in bulk by importing a pre-prepared CSV file. After importing, the new or updated devices appear in AFA like all others.

AFA enables you to do this via the **Administration** area in AFA or via CLI.

For more details, see the [How to Import and Manage Devices in Bulk from a .CSV File](#) AlgoPedia article.

Prepare your CSV file

Prepare your CSV file to import by using the sample provided in the AFA UI, or creating your own from scratch.

Note: The same CSV file cannot be used to both add new devices and update existing devices at the same time.

For more details, see [CSV import file format](#).

Access AFA's sample CSV file

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Click **Bulk** and select **Add/Update devices (CSV)**.
3. Click **Download sample files**.

A **zip** file is downloaded with sample files for various device types.

Add a line to the file for each device you want to add or update, as well as values that correspond to each header.

For details, see [CSV import file format](#).

Prepare a CSV file from scratch

Do the following:

1. Open a text or csv file, and add a list of comma separated column headers. Each column header supports a device property or option.

For details about supported column headers, see [CSV import file format](#).

2. For each device you want to add or update, add a new line with values that correspond to each header.

Note the following:

Adding or updating	Your CSV file can include either devices to add or update, but not both.
Devices that must be handled on their own	<p>The following device types cannot be listed in a CSV file together with other device types:</p> <ul style="list-style-type: none"> • Cisco IOS • Cisco ASA and all types of Cisco firewalls • Juniper Netscreen <p>These devices must be added or updated using a CSV file of their own.</p>
Missing headers	<p>If you are adding new devices, any headers not included in the CSV are assigned with default values.</p> <p>If you are updating existing devices, any headers not included in the CSV are ignored, and no changes are made for those properties in AFA.</p>
Syslog values for sub-systems	If you want to assign syslog identifiers for sub-systems, you must do this as part of an update CSV file. The parent device must already be defined in AFA.

3. Save the file and continue with [Import your CSV file \(UI\)](#).

Tip: Use a CSV file to assign additional device identifiers for primary/parent devices or device subsystems, such as VSYS or VDOM.

In such cases, you only need to include the **name** and **additional_fw_ips** column headers for each device.

For more details, see [Add/update multiple devices in bulk](#) and [Bulk import support scope](#).

Import your CSV file (UI)

This procedure describes how to import a CSV file of device data into AFA via the **Administration UI**.

Note: For more details, see [Prepare your CSV file](#) and [CSV import file format](#).

Do the following:

1. Ensure that the devices listed in your CSV file are online and accessible by AFA via SSH.
2. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
3. Click **Bulk** and select **Add/Update devices (CSV)**.
4. Select to either **Add New Devices** or **Update Devices**.
5. Select your **Device Type**, and then browse to and select your prepared CSV file. For more details, see [Prepare your CSV file](#).

For example:

6. Click **Add** or **Update**.

The configured devices are added to or updated in AFA, and a confirmation message is displayed.

Import your CSV file (CLI)

This procedure describes how to import a CSV file of device data into AFA via CLI commands.

Note: For more details, see [Prepare your CSV file](#) and [CSV import file format](#).

Do the following:

1. Ensure that the devices listed in your CSV file are online and accessible by AFA via SSH.
2. Log in to the AFA server as user **afa** and browse to the directory where the CSV file is saved.
3. Run the following command:

```
import_devices -f <CSVFile> -t <deviceType> [-u ]
```

Where:

-f <CSVFile>	Defines the name of the CSV file. This file must be located in the current directory.
---------------------------	---

-t <deviceType>	Defines the type of devices to import or update. Supported values include: <ul style="list-style-type: none"> • ASA. A Cisco ASA device. • IOS. A Cisco IOS Router. • NSC. A Juniper NetScreen device. • GEN. Any of the other supported device brands. In this case, specify the brand in the CSV brand column. For more details, see CSV import file format. For additional device types and configurations, see Bulk import support scope .
-u	Determines that the script updates existing devices. When absent, the script imports the data as new devices.

The script runs and the devices described in your CSV file are added or updated in AFA.

Bulk import support scope

Each CSV file can include the following types of device data:

- Device data for multiple devices to be added or updated.

You cannot use the same CSV file to add new devices and update existing devices at the same time.

- Device data for multiple device types, except for the following:
 - **Cisco IOS**
 - **Cisco ASA**
 - **Juniper Netscreen**

These device types must be added in CSV files with no other device types listed.

Additionally, the following types of devices and device options must be added or configured manually in the **AFAAdministration** area:

Device types	<p>Add the following types of devices individually in the AFAAdministration area:</p> <ul style="list-style-type: none"> • Management devices, including any device that manages other devices. For example, Juniper NSM, Check Point devices, cloud "device" accounts, and so on. • Routing elements • Cisco Firewall via a CSM • Cisco Application Centric Infrastructure (ACI) • H3c • SECUI MF2
Device options	<p>The following options must be configured manually in the AFAAdministration area after importing:</p> <ul style="list-style-type: none"> • Enabling ActiveChange • Enabling Learning mode for a VMware NSX device. Learning mode causes AFA to treat traffic that is not specified in a rule as blocked. Because the default behavior of an NSX Distributed Firewall is to allow all traffic that is not explicitly blocked, AFA provides this option to enable you to better understand the specific traffic that needs to be allowed on the device. • Specifying the policy configuration method for a Symantec Blue Coat device to VPM. The default is CPL. • Specifying a static URT file.

CSV import file format

This topic lists the headers and values supported for CSV files used to import or update device data in AFA.

Note: Header values are case sensitive. Using header values with different cases from those listed below will cause unexpected results in your file upload.

For more details, see [Add/update multiple devices in bulk](#) and the [How to Import and Manage Devices in Bulk from a .CSV File](#) AlgoPedia article.

Tip: You can also use a CSV file to assign additional device identifiers for primary/parent devices or device sub-systems, such as VSYS or VDOM. In such cases, you only need to include the [name](#) and [additional_fw_ips](#) values.

Basic device description headers

Header name	Description
brand	<p>The device brand. For more details, see Supported device brand values.</p> <p>Required for all devices except for the following:</p> <ul style="list-style-type: none"> • Cisco IOS • Cisco ASA/PIX/FWSM • Juniper Netscreen <p>Specify these brand types in the Bulk Add/Update Device dialog instead.</p>
name	<p>The device ID (tree name).</p> <p>Required for all device types.</p> <p>This is an internal name, usually the name displayed in the tree, without non-alphanumeric characters or spaces.</p> <p>If you're specifying a sub-system, this is the name of the sub-system.</p>
display_name	<p>The name as it appears in the device tree, including spaces and other special or numeric characters.</p> <p>Optional for all devices</p> <p>Default: If this column is missing or empty, the device is added using the device's host name.</p>

Supported device brand values

Enter the following values to indicate device brands:

Analysis and monitoring devices	<ul style="list-style-type: none"> • asa. Cisco ASA • bluecoat. Symantec Blue Coat • f5bigip • f5bigip_afm. F5 BIG-IP LTM and AFM • f5bigip_full. F5 BIG-IP LTM Only • fortigate. Fortinet Fortigate • fwsn (Cisco FWSM) • ios. Cisco IOS • junos. Juniper SRX • junosmxrouter. Juniper M/E Routers • nexus. Cisco Nexus • nsc. Juniper Netscreen • nsx. VMware NSX • paloalto. Palo Alto Networks firewall
Monitoring-only devices	<ul style="list-style-type: none"> • ace. Cisco ACE • avaya. Avaya Routing Switch • brocade. Brocade VDX • junipersa. Juniper Secure Access (SSL VPN) • junosrouter. Juniper Routers (non-M/E) • netfilter. Linux netfilter iptables • sonicwall. SonicWall • topsec. Topsec Firewall • watchguard. WatchGuard

Access information headers

Header name	Description
host_name	The device host name or IP address. Required for all device types.
user_name	The username used to access the device. Required for all device types.

Header name	Description
passwd	<p>The password used to access the device.</p> <p>Required for all device types unless CyberArk authentication is used.</p> <p>Note: For Cisco IOS or ASA devices enabled for CyberArk, the Password and Enable User Password must be the same.</p>
enable_user_name	<p>The enable user name.</p> <p>Relevant and required only for Cisco ISO devices.</p>
epasswd	<p>The enable password.</p> <p>Relevant and required only for the following devices, unless CyberArk authentication is used on these devices:</p> <ul style="list-style-type: none"> • Cisco IOS • Cisco ASA • Symantec Blue Coat <p>For more details, see CyberArk-related headers.</p> <p>Note: For Cisco IOS or ASA devices enabled for CyberArk, the Password and Enable User Password must be the same.</p>

Cisco-related headers

Header name	Description
rules_view	<p>Determines how rules are displayed in device reports, as one of the following:</p> <ul style="list-style-type: none"> • ASDM. (Default) Display rules in the Cisco Adaptive Security Device Manager (ASDM) graphical interface. • CLI. Display rules in command line format. <p>Relevant for Cisco ASA devices only.</p>

CyberArk-related headers

Header name	Description
use_cyberark	<p>Determines whether to use CyberArk authentication:</p> <ul style="list-style-type: none"> • yes • no <p>Required for CyberArk devices.</p>
cyberark_platform	<p>Defines the CyberArk platform name.</p> <p>Required for CyberArk devices.</p>
cyberark_safe	<p>Defines the CyberArk safe.</p> <p>Required for CyberArk devices.</p>
cyberark_folder	<p>Defines the CyberArk folder.</p> <p>Required for CyberArk devices.</p>
cyberark_object	<p>Defines the CyberArk object.</p> <p>Required for CyberArk devices.</p>
cyberark_enable_platform	<p>Defines the CyberArk platform for the enable password.</p> <p>Optional, and relevant only for CyberArk devices.</p>
cyberark_enable_safe	<p>Defines the CyberArk safe for the enable password.</p> <p>Optional, and relevant only for CyberArk devices.</p>
cyberark_enable_folder	<p>Defines the CyberArk folder for the enable password.</p> <p>Optional, and relevant only for CyberArk devices.</p>
cyberark_enable_object	<p>Defines the CyberArk object for the enable password.</p> <p>Optional, and relevant only for CyberArk devices.</p>

Advanced headers

Header name	Description
separate_vrfs	<p>Determines whether to split the device into VRFs:</p> <ul style="list-style-type: none">• yes (Default)• no <p>Relevant only for the following devices:</p> <ul style="list-style-type: none">• Juniper Netscreen• Juniper SRX• Cisco IOS• Cisco Nexus
full_analysis	<p>Determines whether to include risk analysis and policy optimization details in the device reports:</p> <ul style="list-style-type: none">• yes (Default)• no <p>Relevant for Cisco IOS and Cisco Nexus devices only.</p>

Remote management headers

Header name	Description
con	<p>Determines the connection type as one of the following:</p> <ul style="list-style-type: none"> • SSH • SSH (3des). Cisco ASA only • SSH (des). Cisco ASA only • TELNET. For the following device types: <ul style="list-style-type: none"> • Juniper • Cisco • Blue Coat • Fortigate • Palo Alto • Linux Netfilter <p>Required for all devices except the following:</p> <ul style="list-style-type: none"> • VMware NSX • Cisco ACI <p>These devices connect to AFA via REST.</p>
number_of_allowed_encryption_keys	<p>Determines the permitted number of different RSA keys that AFA can receive from the device's IP address, as follows:</p> <ul style="list-style-type: none"> • 1 • 2 • unlimited (Default) <p>Note: Relevant only when using SSH. This might be required in cases of cluster fail-over, device operating system upgrades, and so on.</p>
ssh_port	<p>Defines the port to use for an SSH connection.</p> <p>Relevant only when using SSH.</p> <p>Defaults:</p> <ul style="list-style-type: none"> • 4118 for WatchGuard devices • 22 for all other devices

Log and monitoring headers

Note: Assigning syslog identifiers for sub-systems must be done as a part of *updating* devices in bulk, not as a part of *adding* devices in bulk. The parent device must already be defined in AFA.

Header name	Description
collect_log	<p>Determines whether AFA collects logs for the device:</p> <ul style="list-style-type: none"> • yes • no (Default) <p>Relevant for the following device types:</p> <ul style="list-style-type: none"> • Cisco ASA/FWSM • F5 BIG-IP • FortiGate, • Juniper Netscreen • Juniper SRX • Palo Alto <p>Note: For Cisco ASA and FWSM devices, set to no to enable logging with only hit-counter data.</p>
log_collection_mode	<p>Determines the method for collecting logs for the device:</p> <ul style="list-style-type: none"> • standard. Enable log collection. • extensive. (Default) Enable log collection and the Intelligent Policy Tuner. <p>Relevant when log collection is enabled.</p>

Header name	Description
collect_log_from	<p>Determines whether AFA collects logs from the NSM or a syslog-ng server:</p> <ul style="list-style-type: none"> • nsm (Default) • syslog <p>Relevant for Juniper Netscreen when log collection is enabled.</p> <p>Note: If traffic logs and audit logs are not on the same server, specify the audit log server using additional headers listed below. In such cases, this value defines a value for the traffic log server.</p>
log_host_name	<p>Defines the host name or IP address of the server/device sending logs to AFA.</p> <p>Relevant when log collection is enabled.</p>
log_user_name	<p>Defines the user name used to connect to the server/device sending logs to AFA.</p> <p>Relevant when log collection is enabled.</p> <p>Note: To collect logs from a remote syslog-ng server using a user other than root, you must configure the server separately.</p>
log_passwd	<p>Defines a password for connecting to the server/device sending logs to AFA.</p> <p>Relevant when log collection is enabled.</p>
collect_log_from_adt	<p>Determines whether AFA collects audit logs from the NSM or a syslog-ng server:</p> <ul style="list-style-type: none"> • nsm • syslog <p>Relevant for Juniper Netscreen when log collection is enabled.</p> <p>Note: By default, the audit log server is the same as the traffic log server.</p>

Header name	Description
log_host_name_adt	<p>Defines the host name or IP address of the server/device sending audit logs to AFA.</p> <p>Relevant for Juniper Netscreen when:</p> <ul style="list-style-type: none"> • Log collection is enabled • The audit log server is different from the traffic log server
log_user_name_adt	<p>Defines the user name for connecting to the server/device sending audit logs to AFA.</p> <p>Relevant for Juniper Netscreen when:</p> <ul style="list-style-type: none"> • Log collection is enabled • The audit log server is different from the traffic log server
log_passwd_adt	<p>Defines the password for connecting to the server/device sending audit logs to AFA.</p>
log_collection_frequency	<p>Defines how often AFA collects logs for the device, in minutes.</p> <p>Relevant for Juniper Netscreen when:</p> <ul style="list-style-type: none"> • Log collection is enabled • The audit log server is different from the traffic log server
additional_fw_ips	<p>Defines any additional IP addresses or host names that identify the device, with colon-separated values.</p> <p>Relevant when log collection is enabled.</p>

Additional headers

Header name	Description
collector	<p>Defines a server to manage the device's data:</p> <ul style="list-style-type: none"> • Central Manager (default) • The name of any remote agent <p>Relevant only when AFA is configured for geographic distribution.</p>

Header name	Description
baseline_profile	<p>Defines the baseline compliance profile to use when generating reports for the device.</p> <p>Optional for all devices.</p>
root_psw	<p>Defines a password to increase permissions on the device to root user permissions.</p> <p>Relevant only for Linux Netfilter IPTables</p> <p>Tip: Devices usually block the ability to access the device as user root. Enable root access to the device to improve AFA support.</p>
monitoring	<p>Determines whether to enable real-time alerts for configuration changes:</p> <ul style="list-style-type: none"> • yes. Default for real/live devices. • no. Default for file devices. <p>Optional for all devices.</p> <p>For more details, see Configure real-time monitoring.</p>
set_user_permissions	<p>Determines whether you can set user permissions for the device:</p> <ul style="list-style-type: none"> • yes (Default) • no <p>Optional for all devices.</p>
firewall_users	<p>Defines the users with access to the reports produced for the device.</p> <p>Separate multiple usernames with slashes (/).</p> <p>Relevant when setting user permissions is enabled for the device.</p>

SNMP polling headers

Header name	Description
snmp_version	Determines the SNMP version: <ul style="list-style-type: none"> • snmpv2c • snmpv3 Relevant only for the following devices: <ul style="list-style-type: none"> • Symantec Blue Coat • Juniper Secure Access (SSL VPN) • Linux netfilter iptables • SonicWall • Topsec • WatchGuard • SECUI MF2 • Avaya Routing Switch • Brocade VDX
snmp_community	Defines the SNMP community string. Required and relevant only when using SNMPv2c.
snmp_username	Defines the SNMP Security Name (username). Required and relevant only when using SNMPv2c.
snmp_auth_password	Defines the authentication password. Required and relevant only when: <ul style="list-style-type: none"> • Using SNMPv2c • The authentication protocol is specified
snmp_auth_protocol	Determines the authentication protocol: <ul style="list-style-type: none"> • md5 • sha • empty Required and relevant only when using SNMPv2c.

Header name	Description
<code>snmp_priv_password</code>	<p>Defines the authentication password.</p> <p>Required and relevant only when:</p> <ul style="list-style-type: none"> • Using SNMPv2c • The privacy protocol is specified
<code>snmp_priv_protocol</code>	<p>Determines the privacy protocol:</p> <ul style="list-style-type: none"> • des • aes • empty <p>Required and relevant only when using SNMPv2c.</p>

Maintain devices

This topic includes maintenance procedures administrators may need to perform periodically for devices managed by AFA.

Edit a device's configuration

This procedure describes how to update the configuration for a specific device.

Tip: AFA also supports updating multiple devices in bulk using a CSV file. For more details, see [Add/update multiple devices in bulk](#).

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. From the tree on the left, select the device whose configuration you want to edit, and then click **Edit**.
3. Edit the field definitions as needed, and click **Finish**.

A confirmation message appears. Click **OK** to continue.

Rename a device

By default, the device's display name, used to identify the device throughout AFA, is the device's host name. This procedure describes how to change this display name.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. From the tree on the left, select the device you want to rename, and then click **Rename**.
3. In the **Rename** dialog, enter the new name and click **OK**

A confirmation message appears. Click **OK** to continue.

Add additional device identifiers for sub-systems

If a device is represented by multiple or non-standard device identifiers in the log files collected by AFA, such as firewall clusters or non-standard logging settings, you must configure additional device identifiers to work with AFA.

For parent devices, the AFA configuration enables you to define additional device identifiers when you add or edit the device. This procedure describes how to specify identifiers for subsystems, such as VSYS, VDOM, and so on, as well as for devices managed by a management system such as Juniper NSM or Palo Alto Panorama.

Tip: AFA also enables you to configure device identifiers for parent devices and sub-systems in bulk via CSV. For more details, see [Add/update multiple devices in bulk](#).

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. From the tree on the left, select the device or sub-system you want to add

identifiers for, and then click **Edit** on the right.

3. In the **Edit....** dialog, in the **Log Collection** area, enter any additional IP addresses or host names that identify the device.

Separate multiple values with a colon (:). For example:

1.1.1.1:2.2.2.2:ServerName

Note: The **Log Collection** areas appears only when log collection is supported for the device and relevant to the sub-system.

4. Click **OK**. The additional identifiers are added to the sub-system's definition.

Delete a device

This procedure describes how to delete a device from AFA, such as if it is no longer in use, or needs to be updated in a way that requires you to remove it and add it back again.

Do the following:

1. Before deleting a device from AFA, we recommend that you download all AFA reports for the device to back up the device's historical data.
2. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
3. From the tree on the left, select the device you want to delete, and then click **Delete**.
4. In the verification message that appears, confirm that you do want to delete the device, and then click **OK**.

A confirmation message appears. Click **OK** to continue.

Update a password for multiple devices

This procedure describes how to update and synchronize passwords across multiple devices.

Note: This procedure is not supported for devices configured with CyberArk authentication. For details, see [Integrate AFA and CyberArk](#).

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. On the right, click **Bulk** and select **Update password** from the dropdown menu.
3. In the **Bulk Update Passwords** dialog, select the devices you want to update the password for.

If you have many devices listed, do any of the following to help you locate your device:

Find a device quickly	Enter a name in the box at the top to select it automatically.
Navigate across pages	Click Previous or Next below the grid to navigate back and forth
Sort the grid	Click a column header to sort the devices shown
Filter the grid	Click  in each column header to filter the grid by that column.

4. In the **New password** field, type the new password to use on all selected devices.
5. To get additional permissions for Cisco devices, select the **Enable user password (Cisco Only)** check box and type in another password.
6. Click **Update**.
7. In the **Confirm Password** dialog, confirm the password(s) you just updated, and then click **Confirm**.

The password is updated for all the specified devices.

Specify routing data manually

AFA compiles routing and topology data collected from each device into a unified routing table (URT) file, which stores the data in AFA's generic format. By default, this file automatically regenerated every time the device is monitored or analyzed.

AFA administrators can change the device's routing and topology data by editing the URT file and uploading it to AFA. Uploaded URT files are static representations of the device's routing information. For these devices, AFA will not regenerate updated URT files automatically.

Note: Since AFA doesn't automatically regenerate the URT files if you've uploaded edits, you must manually update the file again for any configuration changes made on the device.

Specify routing data manually for primary devices

This procedure describes how to upload an edited URT file for primary devices. If sub-devices are defined in the URT file, the file is ignored.

This procedure does not affect URT files and data for sub-devices.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. From the tree on the left, select the device you want to edit, and then click **Edit** on the right.
3. On the device configuration page, in the **Route Collection** area, select **Static Routing Table (URT)**.

Do one of the following:

- If you already have a URT defined that you want to edit, click **Download current URT file**.

- To create a new URL file, click **Download Sample** file.
4. Edit the file with the routing information you want to import. For more details, see [How to manually specify routing information for Cisco Layer 2 devices](#) in [AlgoPedia](#).
 5. In AFA, click **Upload new file**, and select the your edited file.
AFA validates your file, and notifies you if any syntax or content error is found.
 6. When complete, click **Finish**.

The new routing table will take affect after the next device analysis.

Specify routing data manually for sub-systems

This procedure describes how to specify routing data manually for a sub-device or sub-system.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. From the tree on the left, select the sub-device or sub-system you want to edit, and then click **Edit** on the right.
3. In the **Edit** dialog that appears, in the **Route Collection** area, select **Static Routing Table (URT)**.

Do one of the following:

- If you already have a URT defined that you want to edit, click **Download current URT** file.
 - To create a new URL file, click **Download Sample** file.
4. Edit the file with the routing information you want to import. For more details, see [How to manually specify routing information for Cisco Layer 2 devices](#) in [AlgoPedia](#).

- In AFA, click **Upload new file**, and select the your edited file.

AFA validates your file, and notifies you if any syntax or content error is found.

- When complete, click **Finish**.

The new routing table will take affect after the next device analysis.

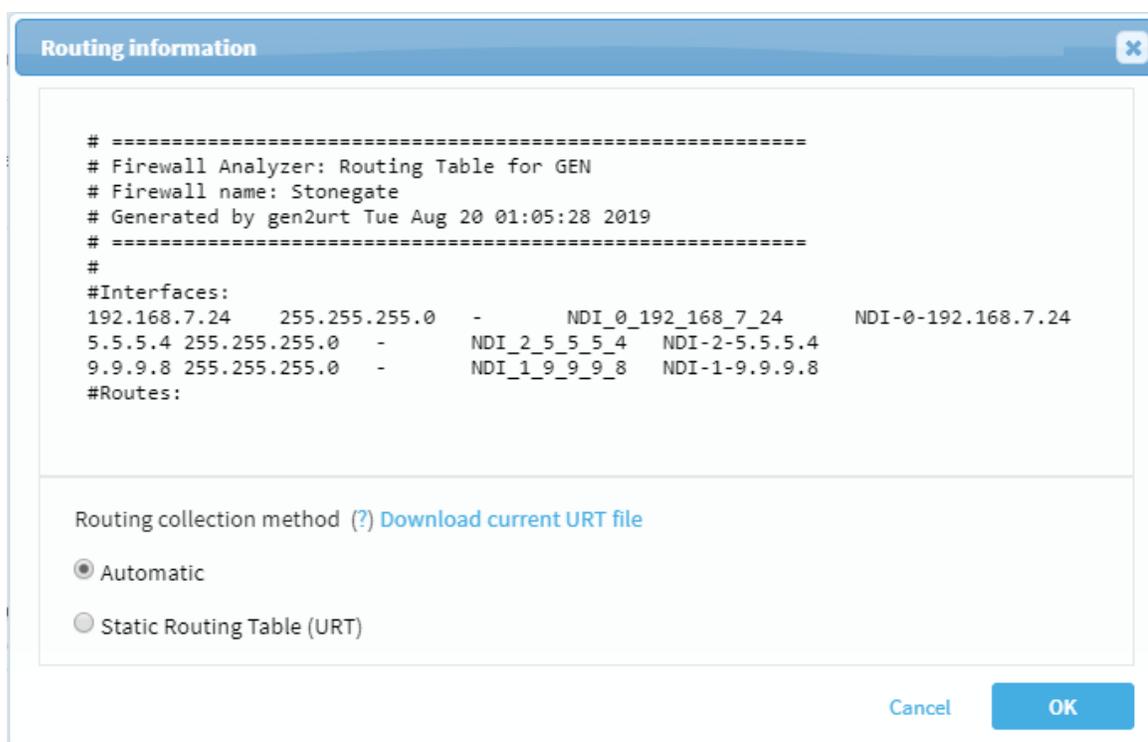
Specify routing data from the map

This procedure describes how to specify routing data manually directly from the map instead of the Devices Setup page.

Do the following:

- In AFA, view the graphic network map. Click **DEVICES**, select a device, and then click **MAP**.
- Locate and right-click the device you want to edit, and select **Routing Information**.

The **Routing information** dialog shows the current URT file. For example:



- Under the file content, click **Static Routing Table (URT)**, and then do one of the

following:

- If you already have a URT defined that you want to edit, click **Download current URT** file.
 - To create a new URL file, click **Download Sample** file.
4. Edit the file with the routing information you want to import. For more details, see [How to manually specify routing information for Cisco Layer 2 devices](#) in [AlgoPedia](#).
 5. In AFA, click **Upload new file**, and select the your edited file.
AFA validates your file, and notifies you if any syntax or content error is found.
 6. When complete, click **Finish**.

The new routing table will take affect after the next device analysis.

Integrate AFA and CyberArk

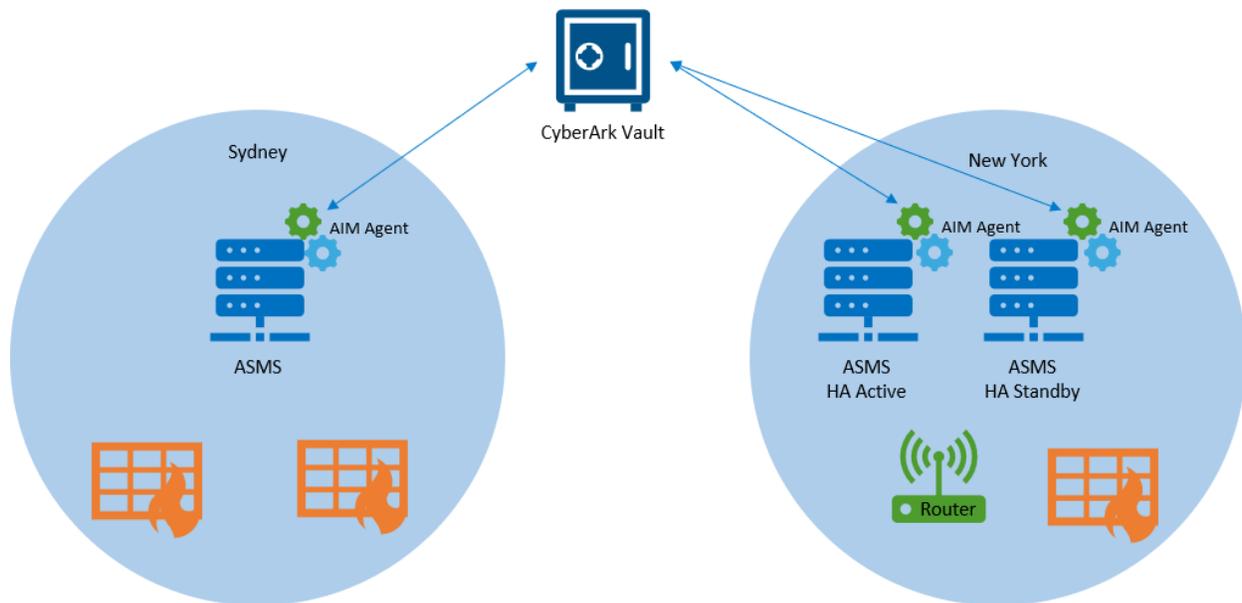
ASMS integrates with CyberArk Vault to enable ASMS access to devices without saving device credentials in ASMS directly. Once configured, ASMS connects to CyberArk to retrieve device credentials, for monitoring, scheduled analysis, or ActiveChange. The actual credential retrieval is transparent to the user.

ASMS supports configuring CyberArk credentials for multiple devices in AFA, becoming more valuable as the number of devices you have in AFA grows.

Note: When integrating with AFA, credentials for syslog collection still need to be provided separately to AFA.

ASMS and CyberArk integration architecture

The following image shows an example of an ASMS-CyberArk integration, with ASMS in a Geographic Distribution and High Availability architecture.



The CyberArk integration is supported for:

- **Standalone** ASMS installations
- Two ASMS machines, serving in **High Availability** or **Disaster Recovery** configurations
- A **Central Manager** with one or more hosts in different geographic locations near each target security device
- Any combination of the last two architectures

The CyberArk AIM agent must be installed on each of the ASMS machines, as each ASMS machine will need to connect to the devices they manage, and require CyberArk credentials.

Supported devices for CyberArk integration

CyberArk integration is supported for the following device brands:

- Fortinet FortiManager
- Juniper Netscreen
- Cisco ASA
- Cisco Nexus

- Cisco IOS
- F5 BIG-IP LTM and AFM
- Symantec Blue Coat

Note: For details about supported versions of CyberArk, contact your AlgoSec customer representative.

Configure CyberArk AIM for ASMS access

Before using CyberArk in ASMS, you must enable ASMS access in CyberArk. This procedure describes how to define an application ID and application details for ASMS in CyberArk's Password Vault Web Access (PVWA).

Do the following:

1. Log in to the PVWA as a user with authorization to manage applications. Add an application, and name it **AlgoSec**.
2. Enable the **Allow extended authentication restrictions** option for the **AlgoSec** application you created. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
3. Specify the application's **Allowed Machines**, and include any of your ASMS machines. This ensures that ASMS can access credentials managed by CyberArk from any machine in your system.

For more details, see the [CyberArk documentation](#).

Configure CyberArk accounts and permissions

This procedure describes how to ensure that CyberArk accounts and permissions are configured as needed for the ASMS integration, and is performed in the CyberArk Vault.

Do the following:

1. In the CyberArk Password Safe, provision any privileged accounts required by the **AlgoSec** application. For each account, make sure to add the **Add accounts** permission.
2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored.
3. Add the Provider users as a Safe Member, with the following permissions:
 - **List accounts**
 - **Retrieve accounts**
 - **View Safe Members**

Tip: If you are installing multiple Provider users, we recommend creating a group for these users and adding the group to the Safe with the required permissions.

4. Add the application, using the **APPID**, as a Safe Member with the **Retrieve accounts** permission only.
5. Additionally, provide the Provider user and the application with the **Access Safe without Confirmation** permission, if your scenario complies with all of the following:
 - Your environment is configured for **dual control**
 - You have a **PIM-PSM environments version 7.2 and lower**
 - The **Safe is configured to require confirmation** from authorized users before passwords can be retrieved

This is not required for Privileged Account Security solutions versions 8.0 and higher.

For more details, see the [CyberArk documentation](#).

Configure CyberArk integration

This procedure describes how to configure specific devices to be authenticated via a CyberArk vault. When configured, the CyberArk configuration fields appear for those devices in the **DEVICES SETUP** page.

Do the following:

1. Complete the integration configuration on the CyberArk side. For details, see:
 - [Configure CyberArk AIM for ASMS access](#)
 - [Configure CyberArk accounts and permissions](#)
2. In the **AFAAdministration** area, navigate to the **Options > Authentication** tab.
3. Scroll down to the **CyberArk** area, and select the **Allow to setup devices with CyberArk credentials management** checkbox.
4. (Optional) Define default values for all devices authenticated via CyberArk, as follows:

Platform (Policy ID)	Enter a default CyberArk Platform.
Safe	Enter a default CyberArk safe.
Folder	Enter a default CyberArk folder. Default : root

5. Click **OK** to save your changes.

From now on, CyberArk options will appear in the **DEVICES SETUP** page for all relevant device brands.

6. (Optional). Configure CyberArk system notifications. The following parameters are disabled by default:
 - **cyberark_connectivity_health_check** - Tests the connectivity between ASMS and the CyberArk vault.

- **suite_cyberark_aim_service** - Checks the status of the CyberArk AIM service (**aimprv**) running on the ASMS host.
7. Configure the specific devices you want to authenticate via CyberArk, either one at a time or in bulk.

For details, see:

- [Device procedure reference](#)
 - [Edit a device's configuration](#)
 - [Add/update multiple devices in bulk](#)
8. Configure the CyberArk Application Access Manager (AAM) agent on all ASMS hosts and configure it to communicate with the CyberArk vault. If you're working in a distributed environment, make sure to configure the AIM agent on all hosts in your system, including the Central Manager, Remote Agents, secondary nodes of all clusters, and so on.

For more details, see the [CyberArk documentation](#).

Alternate data collection methods

This section describes offline device data collection methods that can be used as alternates to on-boarding the device into AFA from the **Administration** area and collecting data automatically.

Note: Since these are static files and not live devices, configuration changes such as dynamic route updates only appear in AFA when you update the file again.

Additionally, AFA cannot track changes in real-time, or track who may have made each change on the device. Updates are represented only in reports generated after the update.

ActiveChange is not supported for file devices.

When to use these procedures

While we recommend that you generally collect data from live devices automatically, this requires that the AFA machine be connected to the device's network.

This may not always be possible, and you may want to analyze devices in a different location, or on a network that you are not able to connect to directly.

Additionally, you may have L3 devices where this data is already collected by an existing toolset.

Note: We recommend that customers ensure that AFA has the most recent device data possible, which helps to provide network map completeness and traffic simulation accuracy.

Complete device data typically involves analyzing your core and distribution layer routing infrastructure as well as firewalls.

Recommended device data collection per device type

Collect data from your devices semi-automatically or manually using scripts provided by AlgoSec.

Each device type has a recommended method, described in the table below.

Note: These procedures are documented in our [Alternate data collection method](#) documentation, on the [AlgoSec portal](#). Use your portal credentials to access them.

Check Point	<p>For details, see:</p> <ul style="list-style-type: none"> • Check Point FireWall-1 devices (semi-automatic). For Check Point FireWall-1 devices running on specific platforms, device data collected includes components of the Check Point file structure and the filter module's routing table. Relevant platforms include Windows, Sun, Nokia, SecurePlatform, Alteon, and Linux. • Check Point devices (manual). Semi-automatic and manual data collection is supported only for Check Point device versions R77.X and below.
Cisco	For details, see Cisco routers and devices .
Juniper	For details, see Juniper devices .
Fortinet Fortigate	For details, see Fortinet Fortigate (manual) .
Palo Alto Networks	For details, see Palo Alto Networks (manual) .
McAfee Firewall Enterprise (Forcepoint Sidewinder)	<p>For details, see McAfee Firewall Enterprise (Sidewinder) (manual).</p> <p>Note:</p> <p>Support for the Forcepoint brands (Sidewinder, StoneGate) and Hillstone was deprecated in ASMS version A30.00.</p> <p>If you had defined these devices in an earlier version of ASMS, these devices are still available to you, with all the existing capabilities, but you cannot add new ones after upgrading.</p> <p>We recommend backing up device data before or after upgrading and then removing these devices from AFA. Make sure to download any report zip files for the device before deleting.</p> <p>For more details, see the relevant AlgoPedia KB article.</p>

Symantec BlueCoat	For details, see Symantec Blue Coat (manual) .
--------------------------	--

Access semi-automatic data collection scripts from the [AlgoSec portal](#). For details, see [Semi-automatic data collection scripts](#).

Depending on your system configuration, device files can also be obtained as follows:

Use a recent AFA report	<p>If you have a live device on another ASMS system, retrieve the full device configuration file from the latest AFA report.</p> <p>For example, you may want to do this when adding a device that already exists in a production system to a testing system as well.</p> <p>For more details, see Access log and configuration files.</p> <p>Tip: If your device is supported only as EA, make sure that the device support is enabled as needed in both your production and testing environments. For details, see Extend device support.</p>
Create a JSON file manually	<p>If you do not have another device to collect the data from, create the file manually.</p> <p>For details, see Static support for generic devices.</p>

Note: AFA does not currently support manual data collection from monitoring devices.

Add a static file device to AFA (UI)

This procedure describes how to add a file device to AFA from the AFAAdministration area.

Note: Alternately, see [Add a static file device to AFA \(CLI\)](#).

Do the following:

1. In AFA, access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).

2. In the vendor and device selection page, click  **Device from File** on the right.
3. In the **Name** field, enter a name for your file device.
4. Select the file you want to analyze by selecting one of the following:

Upload new	<p>Upload a file from your computer. Browse to and select your file. File size must not exceed 20 MB.</p> <p>For larger files, copy the file to the /home/afa/algosec/fwfiles directory, and use the Existing on server option.</p> <p>For more details, see Recommended device data collection per device type.</p>
Existing on server	<p>Select a file already saved on the AFA server, in the /home/afa/algosec/fwfiles directory.</p> <p>Select the file you want to analyze from the dropdown list.</p>

5. Define how AFA should acquire the device's routing information. Select one of the following:

Automatic	<ul style="list-style-type: none"> • Automatic. Automatically generate the device's routing information upon analysis or monitoring. • Static Routing Table (URT). Take the device's routing information from a static file you provide. For more details, see Specify routing data manually.
Static Routing Table (URT).	<p>Take the device's routing information from a static file you provide. For more details, see Specify routing data manually.</p>

6. Select **Real-time change monitoring** option to enable real-time alerting upon configuration changes. For more details, see [Configure real-time monitoring](#).
7. Select **Set user permissions** to set user permissions for this device.
8. Click **Finish**. The new device is added to the device tree.
9. If you selected **Set user permissions**, the **Edit users** dialog box appears.

In the list of users displayed, select one or more users to provide access to reports for this account.

To select multiple users, press the **CTRL** button while selecting.

Click **OK** to close the dialog.

A success message appears to confirm that the device is added. The device is now shown in the device tree in AFA, and will be included in the ALL_FIREWALLS analysis reports.

Add a static file device to AFA (CLI)

This procedure describes how to add a file device to AFA using CLI commands.

Note: Alternately, see [Add a static file device to AFA \(UI\)](#).

Do the following:

1. Place any collected device data files, such as in the following directory on the AFA server: **home/afa/algosec/fwfiles/**

For more details, see [Recommended device data collection per device type](#).

2. Summarize the files in a single CSV file with the following columns:

name	The device's display name, used in the device tree and all other locations around ASMS.
path_name	The location of the device file on the AFA machine, in the /home/afa/algosec/fwfiles directory.
full_analysis	Determines whether to perform full analysis. To optimize performance during device analysis, enter no .

For example:

name	path_name	full_analysis
-------------	------------------	----------------------

MYROUTER	/home/afa/algosec/fwfiles/MyRouter.rd	no
MYNEXUS	/home/afa/algosec/fwfiles/MyNexus.nexus	no

Save the CSV file in the **home/afa/algosec/fwfiles/** directory on the AFA server.

3. Log in to the AFA server as user **afa**.
4. Run **import_devices -t <CSV filename> -f FILE**

where **<CSV filename>** is the name of the CSV file you saved in the previous step.

For example: **import_devices -t BulkL3Devices.csv -f FILE**

When complete, all devices listed in the CSV file are shown in the device tree in AFA, and will be included in the ALL_FIREWALLS analysis reports.

Semi-automatic data collection scripts

Access the data collection scripts used for any semi-automatic process from the [AlgoSec portal](#) (portal user account required).

These scripts use the same commands for copying files and creating directories as are listed in the manual data collection procedures.

Do the following:

1. In your browser, open the [Semi-Automatic Data Collection Procedures](#) AlgoSec portal page.
2. Download the scripts for your device type. Open the files to inspect the scripts as needed.

Firewall-1 scripts for Sun/Nokia/SecurePlatform/Alteon/Linux platforms

If you copy the Firewall-1 Unix data collection script (**ckp_collect**) from a Windows PC to a Sun, Nokia, SecurePlatform, Alteon, or Linux platform, ensure that any carriage returns (^M) added by the Windows system are removed on the target platform.

If you have a compressed **ckp_collect.z** file, expand the file as follows:

Copy the **ckp_collect.z** to a Check Point SmartCenter server running on Sun Solaris, SecurePlatform, or Linux.

Run one of the following commands:

Sun platforms	uncompress ckp_collect.Z
SecurePlatform or Linux platforms	gunzip ckp_collect.Z

The **ckp_collect** and **ckp_log_collect** files are created, and the compressed **ckp_collect.z file** is deleted.

These scripts are ready for you to run as needed.

Extend device support

This section explains how to enable support for devices that are not supported out of the box, and how to manually customize routing information for any device.

ASMS provides the option to enable device support for new devices or to enable additional support for devices supported out of the box.

To enable additional device support utilizing an early availability feature, see [Early availability features](#).

Static configuration file support

You provide a JSON file which represents the device's configuration. This option provides full support in AFA, FireFlow, and AppViz. See [Static support for generic devices](#).

Note: When using this option, updating the device's policy requires updating and replacing the file in AFA (either manually or with a script you provide). Real-time change monitoring is not supported, but the **Changes** tab in reports will reflect changes that are detected by an analysis (as the result of the file being updated).

Note: This device type has a few limitations, due to its static nature. Baseline compliance analysis is not supported. Log collection is not supported, so none of the features which require traffic or audit logs are supported, such as policy optimization recommendations or information about who made a change to the device or when a change was made. Although these devices are supported for FireFlow, they are not supported for ActiveChange.

Live monitoring support

You provide an XML file that describes how to collect data from the device and icons to represent the device brand. This option provides change monitoring, basic routing, and baseline compliance only. See [Generic device monitoring](#).

Static support for generic devices

You can enable Analysis and Monitoring support for generic devices with a JSON file that represents the device's configuration at a single point in time.

Supported device types

The ability to enable AFA support for a generic device is only supported for devices whose policy's conform to one of the following models:

- **Policy-Based.** One set of rules per device across all of its interfaces. For example, Check Point devices.
- **Interface-based.** One set of rules per interface. For example, Cisco devices.
- **Zone-Based.** Each policy rule is defined using a source zone and destination zone. For example, Fortinet devices managed by FortiManager.

Note: Static support is available only for traditional security devices and is not relevant for other sources, such as SDN and cloud.

Adding Support for a File Device

To add and analyze a generic device using a static configuration file, complete the following workflow:

1. Create a JSON file which contains the necessary device configuration items. For details, see [Creating the JSON File](#).
2. Upload the JSON file to AlgoSec Firewall Analyzer as a file device. See [Add other devices and routing elements](#)

Note: Updating the device's policy requires manually updating and replacing the file in AFA. If desired, you can write your own script to automatically update the file in the `/home/afa/algosec/fwfiles` directory.

Creating the JSON File

The following procedure describes how to create the JSON file that represents the device configuration.

To create the JSON file:

1. Review the example file located in `/usr/share/fa/data/plugins/config_parser_template.json`
2. Create your own configuration file according to the template. See [Tag list](#) and [Tag Reference](#).

Note: If the device is a layer 2 device, you must specify this in the device (see [device](#)) tag. For zone based devices, AFA automatically converts the device's topology into layer 3 terminology using a heuristic based on the device's policy. For all other device types, you must provide the device's topology in layer 3 terminology by manually editing the device's URT file. For more details, see [Specify routing data manually](#).

Note: Any rules with NAT must be defined separately from non-NAT rules in the configuration.

3. Rename the file with the suffix ".algosec".
4. As user **afa**, run the JSON validator to verify the JSON file is valid:

```
su - afa
curl --si '127.0.0.1:8080/afa/configParser/validateFile?path=<full path to JSON fi
```

Tag list

Tag	Description
config_type	The policy model.
device	The definition of the device.

Tag	Description
hosts	The host name.
hosts_groups	The host group name.
interfaces	The interface name.
services	The service name.
services_groups	The service group name.
policies	The rule name.
rules_groups	The rules group name. (optional)
nat_rules	The rule name.
global_nat_rules	The global NAT rule name
nat_objects	The NAT object name.
nat_objects_groups	The NAT object group name.
nat_pools	The NAT pool name.
zones	The zone name. (optional)
routes	The route's ID.
schedules	The schedule name. (optional)

➔ See also:

- [Tag Reference](#)
- [Sample generic device JSON file](#)
- [Static support troubleshooting](#)

Tag Reference

Note: In order for the file to function as intended, any special characters used in a string must be escaped with a \.

For comprehensive examples, see Generic Device JSON File Examples (see [Sample generic device JSON file](#)).

config_type

One of the following values:

- **POLICY_BASED**: One set of rules per device across all of its interfaces. For example, Check Point devices.
- **INTERFACES_BASED**: One set of rules per interface. For example, Cisco devices.
- **HOST_BASED**: Device policy refers to the host itself (source or destination is "Me"). For example, Amazon AWS devices.
- **ZONE_BASED**: Each policy rule is defined using a source zone and destination zone. For example, Fortinet devices managed by FortiManager.

device

Parameter	Description
name	Device name.
major_version	Device major version (first number before first dot).
version	Device version.
minor_version	Device minor version (last number of whole version).
policy	Policy name (optional).
is_layer2	1 or 0 . Indicates whether the device is a layer 2 device.

hosts

Parameter	Description
name	Host name.
comment	Host comment, if there is one (optional).
ips	List of host IPs.

Parameter	Description
type	PREDEFINED/ANY/IP_ADDRESS/IP_RANGE/DOMAIN/SUBNET/IPS_LIST
is_negate	true/false (optional)

hosts_groups

Parameter	Description
name	Host group name.
members	List of group members (from hosts hash or from hosts_groups hash).
type	GROUP
is_negate	true/false (optional)

interfaces

Parameter	Description
name	The interface logical name.
enable	enabled/disabled. (optional)
ips	List of interface's IPs in format of: 'IP address/CIDR'.
Hwdevice	The interface physical name.
zone	Interface's zone. (optional)
description	Description. (optional)
rules_groups	<p>List of rules groups that apply to this interface.</p> <p>Note: The name of the rule group should be the same as the rule group id value in rule_group tag.</p> <p>Note: This parameter is only relevant for INTERFACE_BASED configuration.</p>

services

Parameter	Description
name	Service name.
service_definitions	List of service definitions in the following format: <pre>protocol: The protocol name: tcp/udp/icmp/any/protocol number.</pre> <ul style="list-style-type: none"> • src_port: The source port number/source port range (if there is no source port, or range is any, it will be *)/ICMP type. (optional) <pre>dst_port: The destination port number/destination port range. If range is any, it will be *.</pre>
Type	ANY/TCP/UDP/ICMP/TCP_UDP

services_groups

Parameter	Description
name	Service group name.
members	List of group members (from services hash or from services_groups hash).
type	GROUP

policies

Parameter	Description
rule_name	Rule's name as appears in the configuration.
rule_display_name	Display name.
rule_id	Rule's ID - unique identifier of the rule, can be the rule name if it is unique.
line_number	Line number of the rule in configuration file.
rule_num	Rules number (to save order of rules).
src_zone	List of source zones. (optional)
direction	Inbound/outbound. (optional)

Parameter	Description
comments	Rule's comment. (optional)
rule_grp	Group to which the rule belongs. (optional)
log	0/1
enable	Enabled/disabled.
src	List of rule's sources.
service	List of rule's services.
schedule	Schedule name from schedules list. (optional)
action	ALLOW/DENY
dst_zone	List of destination zones.(optional)
dst	List of rule's destinations.
src_nat	List of source NAT hosts/addresses. (optional)
src_nat_type	Source NAT type - one of the values: static/dynamic. (optional)
dst_nat	List of destination NAT hosts/addresses. (optional)
dst_nat_type	Destination NAT type - one of the values: static/dynamic. (optional)
bi-directional	0/1 (optional). Relevant for static NAT for example, MIP in NetScreen.
src_negate	0/1 (optional)
dst_negate	0/1 (optional)
policy	Policy name. (optional)

rules_groups

(optional)

Parameter	Description
name	Rules group name.
enable	Enabled/Disabled.

Parameter	Description
comments	Rules group comment, if there is one (optional).
type	Rules group type (optional)

nat_rules

Parameter	Description
rule_name	Rule's name as appears in the configuration (without canonization).
rule_id	Rule's ID - unique identifier of the rule, can be the rule name if it is unique.
line_number	Line number of the rule in the configuration file.
src_zone	List of source zones.(optional)
rule_display_name	Display name.
direction	Inbound/outbound.(optional)
comments	Rule's comment.(optional)
rule_num	Rules number (to save order of rules).
log	0/1
enable	Enabled/disabled.
src	List of rule's sources.
dst	List of rule's destinations.
src_nat	List of source NAT hosts/addresses.
src_nat_type	Source NAT type - one of the values: static/dynamic .
dst_nat	List of destination NAT hosts/addresses.
dst_nat_type	Destination NAT type - one of the values: static/dynamic .
bi-directional	0/1. (optional) Relevant for static NAT (e.g. MIP in NetScreen)
src_negate	0/1 (optional)

Parameter	Description
dst_negate	0/1 (optional)
service	List of rule's services.
schedule	Schedule name (from schedules list). (optional)
action	ALLOW/DENY
dst_zone	List of destination zones.(optional)

zones

(optional)

Parameter	Description
name	Zone name.
interfaces	List of zone interfaces.
description	Zone's description.

routes

Parameter	Description
id	Route's ID.
interface_name	Logical name. (optional)
route_mask	CIDR of the route.
gateway	Gateway (IP address).
interface	Physical name. (The Hwdevice value specified in the "Interfaces" section.)
route	IP address of the route.

schedules

(optional)

Parameter	Description
name	Schedule name.
start_date	Start date in format of: <code>`ddMMMyyyy, HHmm`</code> .
end_date	End date in format of: <code>`ddMMMyyyy, HHmm`</code> .

Sample generic device JSON file

For sample JSON files, see our online [Tech Docs](#).

Static support troubleshooting

This topic provides troubleshooting information for static devices.

Troubleshooting directories and files

The following table lists directories and files that are relevant for troubleshooting static devices, depending on the scenario.

	Device Definition	Analysis
Working folder	<code>/home/afa/algosec/work/collect_gen-<PID></code> For example: <code>/home/afa/algosec/work/collect_gen-62123</code>	<code>/home/afa/algosec/firewalls/afa-<###></code> For example: <code>/home/afa/algosec/firewalls/afa-88</code>
Configuration file	<code>gen_data.txt</code>	<code><device name>.<device brand suffix></code> For example: <code>10_20_74_1.secui</code> <div style="background-color: #e0f2f1; padding: 5px; margin-top: 10px;"> <p>Note: This file is compressed and contained in the <code>raw_files.zip</code> file at the end of the analysis. This is not done yet when the partner parser is launched.</p> </div>
Log file	<code>/home/afa/.fa-history</code>	<code>/home/afa/algosec/firewalls/afa-<###>/fwa.history</code>

Problem: Analysis failed

Probable cause: The JSON configuration is invalid. The required data is missing and/or the file structure is wrong.

Confirm the issue: Confirm the problem by searching the failed analysis's error log file for the following errors:

- "Invalid JSON format in file: ..."
- "Invalid format in file: ..."
- ".....at /usr/share/fa/bin/config_parser_json2out line ... Error: hash creation failed."

Solution: Identify the problem in the JSON file and fix it.

Do the following:

1. Open an SSH connection to AFA and run:

```
su - afa
```

2. Run:

```
curl -si '127.0.0.1:8080/afa/configParser/validate?path=<full path to JSON file>'
```

3. View the validation results and error messages in the file **ValidationLogs.txt** file.

This file will be in the same directory as the JSON file.

4. Fix the error identified in the error message.

Example

After the analysis failed, search the failed analysis's error logs for the following:

```
Info: running config_parser_json2out -i "gen-algosec_generic_device
.algosec" -o "config_parser.out" malformed JSON string, neither array,
object, number, string or atom, at character offset 163088 (before
"a_ext_10.10.110.88"\n...") at /usr/share/fa/bin/config_parser_json2out
line 33.
Error: hash creation failed.
```

You validate the JSON file (as described in the solution above). The following error message appears in the **ValidationLogs.txt** file:

```
ERROR: [Validator] [2015-10-25 13:23:54,884] [ConfigParserValidatorService
.java{1}::validate{1}:41] Invalid JSON format in file =/home/afa/
algosec_generic_device.algosec
    Line: 6847
    Field: policies -> src
    Error message: Unexpected character ('a' (code 97)): expected a
valid value (number, String, array, object, 'true', 'false' or 'null')
at [Source: java.io.FileInputStream@86daca; line: 6847, column: 14
```

With this information, you recognize that on line **6847** there is a missing quotation mark:

```
"src" : [
    a_ext_10.10.110.88"
],
```

Generic device monitoring

AFA provides the ability to enable live monitoring support for generic devices. The support for these devices is identical to the support provided for monitoring devices supported by AFA out-of-the-box, including real-time change monitoring, basic routing simulation based on an SNMP connection, and baseline configuration compliance analysis.

Note: Reports generated for these devices include device change information and baseline configuration compliance results only.

Enable live monitoring support

To enable live monitoring support, complete the following workflow:

1. Specify the method for collecting data. For details, see [Create data collection files for a generic device](#).
2. Install the new brand. For details, see [Install the new brand](#).
3. Add the device to AFA. For details, see [Add the device to AFA](#).

Create data collection files for a generic device

Note: AFA can connect to the device via SSH or REST, depending on the APIs supported by the device.

Do the following:

1. Open a terminal and log in using the username "afa" and the related password.
2. Copy the file `/usr/share/fa/data/plugins/brand_configuration_template.xml`, and name the new file "`brand_config.xml`".
3. Edit the tags as needed. For details, see [Monitoring support tag reference](#).

To enable SNMP support, make sure to specify the relevant tags. See [Collect routing information via SNMP](#).

4. Create the following graphics files of an icon that represents the device brand, where `<brand_id>` is the Id you defined in the **DEVICE** tag of the `brand_config.xml` file:

File name	Description
<code><brand_id>.16.png</code>	16x16 pixel png
<code><brand_id>.35.png</code>	35x35 pixel png
<code><brand_id>.45.png</code>	45x45 pixel png
<code><brand_id>.150.png</code>	150x150 pixel png

Install the new brand

Do the following:

1. Open a terminal and log in using the username "afa" and the related password.
2. Create a new directory `/usr/share/fa/data/plugins/brand_name` where *brand_name* is the name of the new brand.
3. Place the `brand_config.xml` file and all the icon files into the new directory.

4. Run the following command:

```
/usr/share/fa/bin/fa_install_plugin<full path to brand_config.xml>
```

For example: **/usr/share/fa/bin/fa_install_plugin**

```
/usr/share/fa/data/plugins/BrandX/brand_config.xml
```

5. If you are logged into the ASMS web interface, logout and then log back in.

Note: This is necessary because configuration is loaded only upon login. If changes are made to a `brand_config.xml` file while logged into the web interface, they will take affect only after logging out and logging back in.

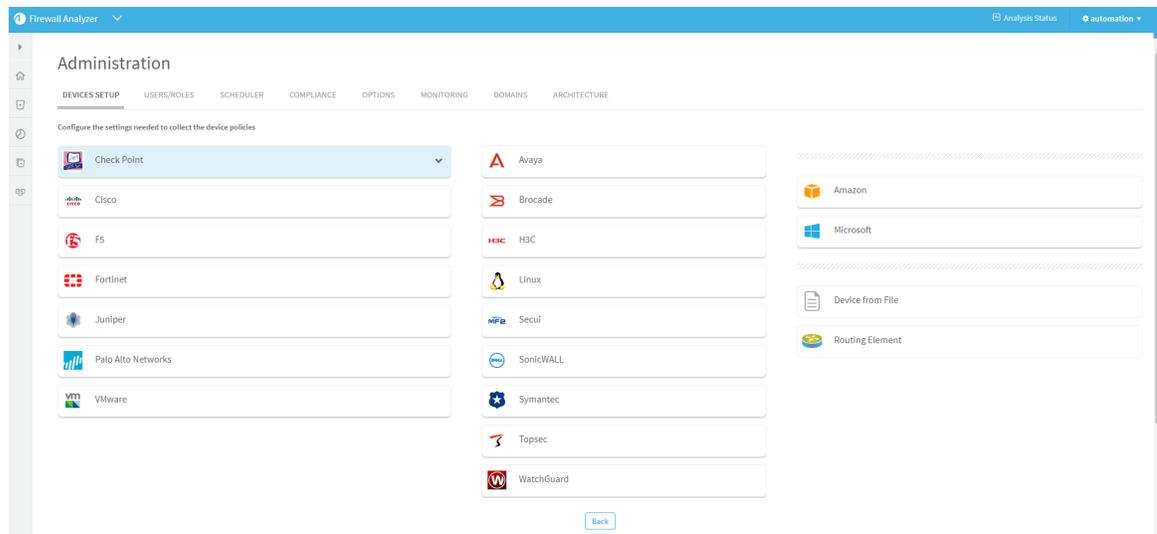
The new device will now appear as an option in the web interface when adding a new device to AFA.

Add the device to AFA

Do the following:

1. Log into the AFA web interface.
2. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
3. Click **New**, and then click **Devices**.

The vendor device selection page appears.



4. In the vendor's list, choose the new device type.
5. Complete the fields with the device's information.
6. Click **Finish**.

The new device is added to the device tree.

7. If you selected **Set user permissions**, the **Edit users** dialog box appears.



8. Set which users will have access to the reports produced by the device, by doing the following:
 - a. Select the users to have access.

To select multiple users, hold down the **Ctrl** key while clicking on the desired users.

- b. Click **OK**.

A success message appears.

9. Click **OK**.

Collect routing information via SNMP

You can use SNMP to retrieve the routing table for devices. The procedure below describes the tags you must add to the `config_brand.xml` file to enable this option for a device.

Note: SNMP versions 3 and 2c are supported.

Do the following:

1. Open the device's `brand_config.xml` file.
2. Under the `<DEVICE>` tag, add the following tag:

```
<FORM_FIELD id="snmp" title="SNMP" type="fieldset"/>
```

3. Under the `<FEATURES>` tag, add the following tag:

```
<FEATURE name="topology" script="snmp2urt"/>
```

4. Save your changes.

For an example, see [Configuration file example with routing](#).

Configuration file example

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<DEVICE id="netfilter" name="iptables" title="Linux netfilter - iptables">
<FORM_FIELD id="root_psw" title="root password" type="password" />
<DATA_COLLECTION prompt="\] \s*[\#\$] \s*$" more_prompt="^\s*-+\s*[Mm]ore
\s*-+\s*$">
<COMMANDS_SEQUENCE>
```

```

<CMD id="1" command="su -" save_output="no" condition="root_psw"
prompt="sword:\s*$" />
<CMD id="2" command="%root_psw%" save_output="no" condition="root_psw"
prompt="\]\s*#\s*$" />
<CMD id="3" command="route" save_output="yes" />
<CMD id="4" command="iptables -L" save_output="yes" />
</COMMANDS_SEQUENCE>
<EXIT_COMMAND command="exit" />
</DATA_COLLECTION>
<DIFF context_lines="5" />
<EXCLUDE regex="no exclusions defined" />
</DEVICE>

```

Configuration file example with routing

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<DEVICE id="edev" name="Elad Dev" title="Elad security dev">
<FORM_FIELD id="snmp" title="SNMP" type="fieldset"/>
<CONNECTION_CMD id="ssh" command="ssh -l %user_name% %host_name% "
title="SSH-cmd"/>
<DATA_COLLECTION prompt="^ASig1000-&gt;" more_prompt="^\s*---\s*more
\s*---\s*$">
<COMMANDS_SEQUENCE>
<CMD id="1" command="get conf" save_output="yes" />
</COMMANDS_SEQUENCE>
<EXIT_COMMAND command="\x04"/>
</DATA_COLLECTION>
<DIFF context_lines="5"/>
<FEATURES>
<FEATURE name="topology" script="snmp2urt"/>
</FEATURES>
</DEVICE>

```

Monitoring support tag reference

This reference describes the use of each tag in the configuration file. The tags are listed in the same order as they appear in the configuration file.

Tag syntax

Tag syntax is presented as follows:

- All parameters are presented in *italics*.
- All optional elements of the tag appear in square brackets [].

For a comprehensive example, see [Configuration file example](#), or refer to other examples under `/usr/share/fa/data/plugins/`.

DEVICE

Syntax

```
DEVICE -[id="id"] [name="name"] [title="title"]
```

Description

This is the main tag for the device, and it identifies the device.

Parameters

Id	String. The ID of the device brand.
Name	String. The name of the device brand. The name will appear throughout the Web interface (for example, in the Overview and Changes tabs).
Title	String. The full name of the device brand. The title represents the device in the list of device types in the Devices tab of the Administration pages.

Subtags

- [FORM_FIELD](#)
- [CONNECTION_CMD](#)
- [DATA_COLLECTION](#)
- [DIFF](#)
- [EXCLUDE](#)
- [ROUTING](#)
- [FEATURES](#)

Example

In the following example, the device name FortiGate will appear throughout the Web interface, while the title Fortinet - FortiGate will appear in the list of device types only.

```
DEVICE id="fortigate" name="FortiGate" title="Fortinet - FortiGate"
```

FORM_FIELD

Syntax

```
FORM_FIELD id="id" title="title" [type="type"]
```

Description

By default, when adding or modifying a device in the Web interface, AFA provides fields for host name, user name, and password. This tag specifies additional fields that should appear for the new device.

This tag is optional.

Parameters

id	String. The ID of the field. It can include only the following characters: a-z , _ , - The ID is used as a tag in the file <code>firewall_data.xml</code> .
title	String. The label representing the field in the Web interface.
type	String. The field's type. This can have the following values: <ul style="list-style-type: none"> <code>text</code>. The user must input free text in this field. <code>password</code>. The user must input a password in this field. The default value is <code>text</code> .

Subtags

None.

Example

In the following example, a field called "Virtual Domain" was added for the device. The field type was not specified and is therefore "text".

```
FORM_FIELD id="vdom" title="Virtual Domain"
```

CONNECTION_CMD

Syntax

```
CONNECTION_CMD id="id" command="command" title="title"
```

Description

By default, when adding or modifying a device in the Web interface, the **Remote Management Capabilities** area includes the following connection options: SSH and Telnet. You can use this tag to add additional options.

This tag is optional.

Parameters

id	String. The ID of the connection option. It can include only the following characters: a-z, A-Z, 0-9, @, _, !, +, ., :, -,), (The ID is used as a tag in the file <code>firewall_data.xml</code> .
command	String. The connection command. This may include the following parameters from the file <code>firewall_data.xml</code> : <ul style="list-style-type: none"> • <code>%attribute%</code>. An attribute, where <i>attribute</i> represents the name of any attribute defined in the <code>FORM_FIELD</code> tag. <code>%password%</code> <code>%user_name%</code> <code>%host_name%</code>
title	String. The label representing the connection option in the Web interface.

Subtags

None.

Example

In the following example, the connection option SSH is defined.

```
CONNECTION_CMD id="ssh" command="ssh %user_name%@%host_name%" title="SSH"
```

DATA_COLLECTION

Syntax

```
DATA_COLLECTION prompt="prompt" [more_prompt="more_prompt"]
```

Description

This tag specifies device prompts that AFA will encounter when connecting to the device.

Parameters

prompt	String. The basic device prompt that appears when the AFA automatic data collection client connects to the device. This is a regular expression.
more_prompt	String. The device prompt that appears when there is additional data that is not currently displayed. This is a regular expression. This parameter is optional.

Subtags

- [LOGIN_PROMPT](#)
- [POST_LOGIN_PROMPT](#)
- [COMMANDS_SEQUENCE](#)
- [DATA_COLLECTION](#)

Example

```
DATA_COLLECTION prompt="#\s*$" more_prompt="^\s*--\s*[Mm]ore\s*--\s*$"
```

LOGIN_PROMPT

Syntax

```
LOGIN_PROMPT prompt="prompt" response="response" try_again="try_again"
```

Description

This tag specifies the device prompt that AFA will encounter after successfully connecting to the device. Usually, this prompt relates to logging in to the device, for example a request for a password.

This tag is optional.

Parameters

prompt	String. A regular expression that describes the device prompt that appears after the AFA automatic data collection client has connected to the device. This regular expression should match the device prompt (e.g. "user1@device1 #") as tightly as possible.
response	String. The command or string that the AFA automatic data collection client should send after receiving the prompt.
try_again	String. Indicates whether after receiving the device prompt specified by the <code>prompt</code> parameter, the AFA automatic data collection client should attempt to log in again, or continue to wait for the basic login prompt. This can have the following values: <ul style="list-style-type: none"> <code>yes</code>. Attempt to log in again. <code>no</code>. Do not attempt to log in again. Instead, wait for the device prompt specified by the <code>prompt</code> parameter.

Subtags

None.

Example

In the following example, upon receiving the "yes/no?" prompt, the AFA automatic data collection client will send the response "yes" and then attempt to log in again.

```
LOGIN_PROMPT prompt="(yes/no)?\s+$" response="yes" try_again="yes"
```

POST_LOGIN_PROMPT

Syntax

```
POST_LOGIN_PROMPT prompt="prompt" response="response"
```

Description

This tag specifies device prompts that AFA will encounter after successfully logging in to the device.

This tag is optional.

Parameters

prompt	String. The device prompt that appears after the AFA automatic data collection client has logged in to the device. This is a regular expression.
response	String. The command or string that the AFA automatic data collection client should send after receiving the prompt.

Subtags

None.

Example

```
POST_LOGIN_PROMPT prompt="Terminal type\?.*$" response="xterm"
```

COMMANDS_SEQUENCE

Syntax

COMMANDS_SEQUENCE

Description

This tag specifies the sequence of commands that AFA should use during data collection.

Parameters

None.

Subtags

- [CMD](#)
- [CMD_VIRT](#)

CMD

Syntax

```
CMD id="id" command="command" save_output="save_output"
[condition="condition"] [prompt="prompt"]
```

Description

This tag specifies a command that AFA should use during data collection.

Parameters

id	Integer. The command's ID and order number. Commands are implemented in numerical order.
command	String. The connection command that the AFA automatic data collection client should send to the device. This may include the following parameters from the file <code>firewall_data.xml</code> : <ul style="list-style-type: none"> • <code>%attribute%</code>. An attribute, where <i>attribute</i> represents the attribute's name. <code>%password%</code> <code>%user_name%</code> <code>%host_name%</code>
save_output	String. Indicates whether the result of the command should be added to output device configuration file. This can have the following values: <ul style="list-style-type: none"> • <code>yes</code>. Add the result of the command to the output device configuration file. • <code>no</code>. Do not add the result of the command to the output device configuration file.

id	Integer. The command's ID and order number. Commands are implemented in numerical order.
condition	String. The name of an attribute defined in the <code>FORM_FIELD</code> tag, which if assigned a value (i.e., the parameter is not empty), should cause the AFA automatic data collection client to send this command. This can have the following values: <ul style="list-style-type: none"> • The name of any attribute added in the <code>FORM_FIELD</code> tag • FW_VIRT. Run the command only if the device has a virtual system.
prompt	String. The device prompt that will appear after the AFA automatic data collection client has sent this command. This is a regular expression and may include the following parameters from the file <code>firewall_data.xml</code> : <ul style="list-style-type: none"> • <code>%attribute%</code>. An attribute, where <i>attribute</i> represents the attribute's name. <code>%password%</code> <code>%user_name%</code> <code>%host_name%</code> <p>Note: By default, the AFA automatic data collection client will expect to receive the last defined prompt, (which was specified in the preceding <code>DEVICE</code>, <code>CMD</code> or <code>LOGIN</code> tag).</p>

Subtags

None.

Example

In the following example, the **enable** command will run only if the device configuration file includes an **enable** attribute that is not empty. The result of the command will not be saved.

```
CMD id="1" command="enable" save_output="no" condition="enable"
prompt="sword:\s*$"
```

CMD_VIRT

Syntax

```
CMD_VIRT id="id" command="command" save_output="save_output"
[condition="condition"] [prompt="prompt"]
```

Description

This tag specifies a command that AFA should use during data collection on a virtual system.

This tag is optional.

Parameters

id	Integer. The command's ID and order number. Commands are implemented in numerical order.
command	String. The connection command that the AFA automatic data collection client should send to the device. This may include the following parameters from the file <code>firewall_data.xml</code> : <ul style="list-style-type: none"> • <code>%attribute%</code>. An attribute, where <i>attribute</i> represents the attribute's name. <code>%password%</code> <code>%user_name%</code> <code>%host_name%</code>
save_output	String. Indicated whether the result of the command should be added to output device configuration file. This can have the following values: <ul style="list-style-type: none"> • <code>yes</code>. Add the result of the command to the output device configuration file. • <code>no</code>. Do not add the result of the command to the output device configuration file.

id	Integer. The command's ID and order number. Commands are implemented in numerical order.
condition	String. The name of an attribute defined in the <code>FORM_FIELD</code> tag, which if assigned a value (i.e., the parameter is not empty), should cause the AFA automatic data collection client to send this command. This can have the following values: <ul style="list-style-type: none"> • The name of any attribute added in the <code>FORM_FIELD</code> tag. • FW_VIRT. Run the command only if the device has a virtual system.
prompt	String. The device prompt that will appear after the AFA automatic data collection client has sent this command. This is a regular expression and may include the following parameters from the file <code>firewall_data.xml</code> : <ul style="list-style-type: none"> • <code>%attribute%</code>. An attribute, where <i>attribute</i> represents the attribute's name. <code>%password%</code> <code>%user_name%</code> <code>%host_name%</code> <p>Note: By default, the AFA automatic data collection client will expect to receive the last defined prompt, (which was specified in the preceding <code>DEVICE</code>, <code>CMD</code> or <code>LOGIN</code> tag).</p>

Subtags

None.

Example

In the following example, the **end** command will run only if the device configuration file includes a **vdom** attribute that is not empty. The result of the command will not be saved.

```
CMD_VIRT id="4" command="end" save_output="no" prompt="#\s*$"
condition="vdom"
```

DATA_COLLECTION

Syntax

```
EXIT_COMMAND command="command"
```

Description

This tag specifies the command that AFA should use to end the connection to the device.

Parameters

command	String. The command that the AFA automatic data collection client should send, in order to end the connection.
----------------	--

Subtags

None.

Example

In the following example, the command is "exit".

```
EXIT_COMMAND command="exit"
```

DIFF

Syntax

```
DIFF context_lines="contextLines"
```

Description

When real-time monitoring and alerting is enabled, specified users receive e-mails upon changes to monitored devices, and the changes are displayed in the Web interface's **Changes** tab. This tag specifies the number of lines before and after a change to display in e-mails and in the Web interface's **Changes** tab. The lines surrounding a change represent the change's context.

This tag is optional.

Parameters

contextLines	Integer. The number of lines to show before and after a change. The default value is 3.
---------------------	---

Subtags

None.

Example

In the following example, the 5 lines before and after a change will be displayed.

```
DIFF context_lines="5"
```

EXCLUDE

Syntax

```
EXCLUDE regex="regex" [lines_before="lines_before"]  
[lines_after="lines_after"] [inline="inline"]
```

Description

When real-time monitoring is enabled, AFA periodically checks whether the device configuration has changed. You can use this tag to exclude certain lines in the device configuration from monitoring.

For example, the current date and other counters frequently change, yet do not represent an actual change to the device configuration. In order to prevent changes to such lines from repeatedly being interpreted as a device configuration changes and reported via e-mail and the Web interface's **Changes** tab, you can exclude these lines from monitoring.

This tag is optional.

Parameters

regex	String. A regular expression, describing a string in the device configuration file that should be ignored by AFA when checking for changes to the device configuration.
line_ before	Integer. The number of lines preceding the string specified in <code>regex</code> , including the line in which the string appears, that should be excluded from monitoring.
lines_ after	Integer. The number of lines following the string specified in <code>regex</code> , including the line in which the string appears, that should be excluded from monitoring.
inline	String. Indicates whether the whole line (or any whole lines before or after) or only the part of the line that matches the regular expression is excluded. This can have the following values: <ul style="list-style-type: none"> <code>yes</code>. Exclude only the part of the line that matches the regular expression. <code>no</code>. Exclude the whole line (or any lines before or after).

Subtags

None.

Example

In the following example, when checking the device configuration for changes, AFA will exclude 30 lines starting from the string "set private-key".

```
EXCLUDE regex="set private-key" lines_after="30"
```

ROUTING

Syntax

```
ROUTING script="script"
```

Description

This tag specifies a script that should be used to analyze the device's routing table.

This tag is optional.

Parameters

script	String. The name of the script to use for creating a routing table.
---------------	---

Subtags

None.

Example

In the following example, the script `forti2urt.pl` is specified.

```
ROUTING script="forti2urt.pl"
```

FEATURES

Syntax

```
FEATURES
```

Description

This tag specifies features that are supported for the device.

Note: By default, only real-time monitoring is supported for the device. To add more features, contact AlgoSec.

This tag is optional.

Parameters

None.

Subtags

- [FEATURE](#)

FEATURE

Syntax

```
FEATURE name="name" [script="script"]
```

Description

This tag specifies a feature that is supported for the device.

Parameters

name	String. The name of the feature.
script	String. The name of the script to use to run the feature.

Subtags

None.

Example

In the following example, the topology feature is supported for the device.

```
FEATURE name="topology" script="snmp2urt"
```

Early availability features

This topic describes how to enable ASMS's Early Availability features.

ASMS's Early Availability features enable you to access new functionality and support earlier than general availability in hopes that customers provide feedback on the design and implementation. Early Availability features have shorter QA cycles and therefore are disabled by default.

Warning: We recommend that you do not keep Early Availability features in use in production. Either enable only in testing systems, or disable them in production systems when returning to general use.

- [Cisco ISE devices in AFA](#)
- [Arista devices in ASMS](#)
- [Enable / Disable map support for Azure](#)
- [Enable /Disable ActiveChange for Azure](#)
- [Enable support for Check Point R80 layers](#)

Cisco ISE devices in AFA

Support for Cisco ISE is available as an early availability (EA) feature. ASMS supports Cisco ISE devices as follows:

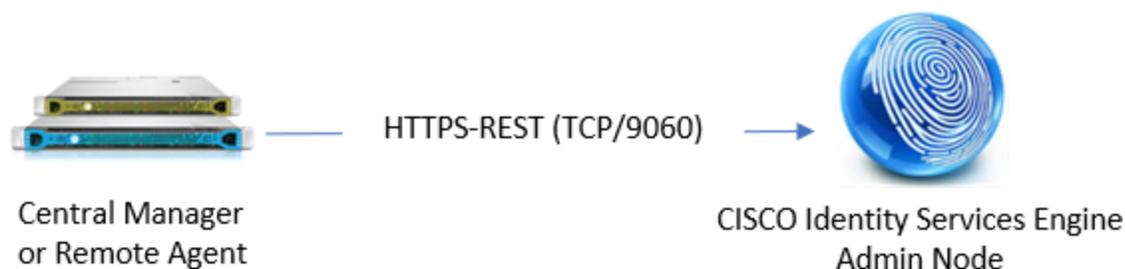
- Support includes FireFlow, but without ActiveChange
- Support does *not* include any AppViz features that rely on FireFlow
- Support does *not* include using a Geographic Distribution Remote Agent to manage Cisco ISE devices.

The following sections describe ASMS's connection to CISCO ISE devices:

- [Network connectivity](#)
- [Device permissions](#)
- [Enable / disable early availability support for Cisco ISE](#)
- [Add a Cisco ISE device to AFA](#)

Network connectivity

The following diagram shows an ASMS Central Manager or Remote Agent connecting to a Cisco ISE device.



Device permissions

ASMS connects to Cisco ISE devices via the Admin Node, using the ERS API.

To do so, ASMS requires an Administrator user with **Read/Write** permissions and the **ERS-Operator** group assignment.

Additionally, ASMS requires:

- A REST connection over port 9060
- Cisco ISE TrustSec SXP feature enabled for the device

Enable / disable early availability support for Cisco ISE

Do the following:

1. In the AFA Administration area, navigate to the **Options > Advanced Configuration** tab.
2. Click **Add** to add a new configuration parameter, and enter the following details:

Name	AlgoSec_EA_CISCOISE
Value	Enter one of the following: <ul style="list-style-type: none"> • Yes = enable advanced map support • No (default)= disable advanced support

3. Click **OK**.

Add a Cisco ISE device to AFA

This procedure describes how to add a Cisco ISE device to AFA.

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. In the vendor and device selection page, select **Cisco > CISCO ISE**.

3. Complete the fields as needed.

Access Information

Enter details for accessing your device.

Host	Enter the device's host name or IP address.
User Name	Enter the username to use for device access.
Password	Enter the password to use for device access.

Geographic Distribution

Select the remote agent that should perform data collection for the device.

To specify that the device is managed locally, select **Central Manager**.

This field is relevant when a Geographic Distribution architecture is configured.

Options

Select the following as needed:

Real-time change monitoring	Select this option to enable real-time change monitoring. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

4. Click **Finish**. The new device is added to the device tree.
5. If you selected **Set user permissions**, the **Edit users** dialog box appears.
 In the list of users displayed, select one or more users to provide access to reports for this account.
 To select multiple users, press the **CTRL** button while selecting.
 Click **OK** to close the dialog.

A success message appears to confirm that the device is added.

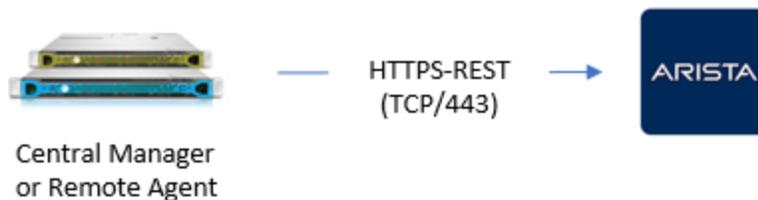
Arista devices in ASMS

This section describes the ASMS Early Availability support for Arista devices:

- [Network connectivity](#)
- [Device permissions](#)
- [Enable / Disable support for Arista](#)
- [Add an Arista device to AFA](#)

Network connectivity

The following image shows an ASMS Central Manager or Remote Agent connected to an Arista device over HTTPS-REST.



Device permissions

To analyze Arista devices, ASMS connects to Arista EOS devices using the REST-based eAPI, ensuring high performance and efficient data collection.

ASMS requires a user with **Read** permissions, and a REST connection over port **443**.

The user must also have permissions are required to run the following commands via API Explorer:

- **show version**
- **show interfaces**
- **show ip interfaces**
- **show ip route vrf (all | <vrf-name>)**
- **show ip access lists"**
- **show ip access-lists summary**

If the REST eAPI is not yet enabled, run the following using the Arista CLI:

```
Arista(config)#management api http-commands
Arista(config-mgmt-api-http-cmds)#no shut
```

Enable / Disable support for Arista

This procedure describes how to enable or disable support for Arista devices in ASMS.

Do the following:

1. In AFA, click your username, and select **Administration > Advanced Configuration**.
2. Click **Add** to add a new configuration parameter.
3. Define your parameter values as follows:

Name	ALGOSEC_EA_ARISTA
Value	One of the following: <ul style="list-style-type: none"> • yes = Enable Arista device support • no = Disable Arista device support

For more details, see [Advanced Configuration](#). Continue with [Add an Arista device to AFA](#).

Add an Arista device to AFA

This procedure describes how to add an Arista EOS device to AFA.

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#)
2. In the vendor device selection page, click **Arista > Arista EOS**.
3. Complete the following fields:

Host	Enter the host name of the Arista device. This is the name that will be displayed in the devices tree.
User Name	Enter the username to use when accessing the device.
Password	Enter the password to use when accessing the device.
Enable Password	Enter the enable password to use when accessing the device.

Note: In the **Geographic Distribution** area, you must select **Central Manager**.
Arista devices cannot be managed by Remote Agents.

- Click **Next**, and then select the managed devices you want to add to AFA.
- Select the following as needed:

Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see Configure real-time monitoring .
Set user permissions	Select this option to set user permissions for this device.

- Click **Finish**. The new device is added to the device tree.
- If you selected **Set user permissions**, the **Edit users** dialog box appears.
In the list of users displayed, select one or more users to provide access to reports for this account.
To select multiple users, press the **CTRL** button while selecting.
Click **OK** to close the dialog.
A success message appears to confirm that the device is added.

Enable / Disable map support for Azure

By default, no icon appears in the graphic network map for Azure subscriptions, and traffic simulation queries involving VMs from Azure subscriptions do not benefit from

internal routing information. Advanced graphic network map support for Azure devices is available as an early availability feature. Early availability features may be limited in their scope and have undergone a shortened testing cycle. They are disabled by default.

When advanced graphic network map support for Azure devices is enabled, the internal routing information is available to traffic simulation queries and the following network elements appear in the graphic network map: VNet routers, VNet peerings, and internet gateways. The subnets coming off the VNet routers include the containers.

Note: VPN gateways are not supported.

Note: AFA does not currently support the use of a Geographical Distribution Remote Agent to manage this device.

To enable/disable early availability map support for Azure:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Advanced Configuration** tab.

The **Advanced Configuration** page appears.

4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

5. In the **Name** field, type `AlgoSec_EA_Azure_Topology`.

6. In the **Value** field, type one of the following:

- Type `yes` to enable advanced map support.
- Type `no` to disable advanced map support. This is the default setting.

7. Click **OK**.

Enable /Disable ActiveChange for Azure

ActiveChange for Microsoft Azure is available as an early availability feature. Early availability features may be limited in their scope and have undergone a shortened testing cycle. They are disabled by default.

When ActiveChange for Azure is enabled, you can add and remove rules from the policy directly from FireFlow. Note that you cannot create new objects; you are limited to using existing objects. The work order will never recommend creating new objects regardless of whether ActiveChange is enabled.

Note: The following procedure enables ActiveChange for Azure in the ASMS, but does not automatically enable ActiveChange for specific Azure subscriptions. In order to enable ActiveChange for a specific Azure subscription, you must select the **Enable ActiveChange** checkbox when defining the Azure in AFA.

Note: AFA does not currently support the use of a Geographical Distribution Remote Agent to manage this device.

To enable/disable early availability ActiveChange for Azure:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Advanced Configuration** tab.

The **Advanced Configuration** page appears.

4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

5. In the **Name** field, type `AlgoSec_EA_Azure_ActiveChange`.6. In the **Value** field, type one of the following:

- Type `yes` to enable advanced map support.
- Type `no` to disable advanced map support. This is the default setting.

7. Click **OK**.

Enable support for Check Point R80 layers

Enabling this feature expands AFA support to include inline layers and ordered layers (global and domain-level). AFA supports these layers in the policy tab (including searching and exporting) and in change monitoring (in the **Changes** tab directly in the UI and in reports). Additionally, relevant AFA API responses will include layer information.

AFA represents layers with layer specific columns and action values. In the policy tab, each layer is grouped by headings.

No.	Name	Layer Type	Layer Name	Global	Status	Source	Destination	VPN	Services & Applications	Content	Action	Track
Global1 Network - Pre (Ordered Layer # 1)												
2		Ordered	Global1 Network	Pre	Disabled	Any	DMZZone	Any	Any	Any	Drop	Log
3	Parent rule for Domain's policy	Ordered	Global1 Network	Pre	Enabled	Any	Any	Any	Any	Any	CaramelVSX_VSX Network	None
CaramelVSX_VSX Network - Domain (Ordered Layer # 1)												
3.1		Ordered	CaramelVSX_VSX Network	Domain	Enabled	Any	host11	Any	Any	Any	Accept	Log

Before enabling this feature, AFA supports only the global policy layer and the domain-level first ordered layer. Inline layers and rules in a second (or more) domain-level ordered layer are ignored, and rules with an action that calls an inline layer are treated as allow rules. All early availability features are disabled by default.

Note: Additional layer support is not extended to policy optimization, risk analysis, or traffic simulation queries. For these functionalities, rules in a second (or more) domain-level ordered layers are ignored, and rules with an action that calls an inline layer are treated as allow rules.

When early availability support is enabled, FireFlow and AppViz are not supported for Check Point R80 devices with policies with inline layer rules or rules implied from the 2nd and beyond ordered layers.

Warning: After enabling, this feature cannot be disabled again. Additionally, ActiveChange will not be supported after enabling layers support, on any layer.

If you are using ActiveChange for Check Point devices, we recommend that you do not enable this feature on your production environment.

Enable early availability support for Check Point R80 Layers

Do the following:

1. In the toolbar, click your username and select **Administration** to access the AFA Administration area.
2. Click the **Advanced Configuration** tab.
3. On the **Advanced Configuration** page, click **Add**.
4. In the **Add New Configuration Parameter** dialog, enter the following:

Name	AlgoSec_EA_CKP_R80_Layers
Value	This parameter is set to no by default. Define the value as yes to enable it. Once enabled, this feature cannot be disabled again.

5. Click **OK**.

Tip: If you add a Check Point R80 device from a configuration file based on a recent report to an AFA system with this flag enabled, make sure that the configuration file is also generated from an AFA system with this flag enabled.

For more details, see [Add other devices and routing elements](#).

Manage groups

This section describes how to configure device groups in AFA.

About groups in AFA

A *group* is a set of devices, in which *no* information about the relationships between the member devices is provided, or when the devices are not connected in a tiered network. AFA allows you to quickly define a group and configure parameters for analyzing the member devices. You can then do the following:

- Schedule an analysis of all the devices in a group at once.
- Produce an additional high-level report that aggregates the reports of all the member devices, so that you have a bird's-eye view of your group-wide risk exposure.

For information on defining sets of devices, in which information about the relationships between the member devices *is* provided, see [Managing Matrices](#) (see [Manage matrices](#)).

In addition to user-defined groups, AFA includes a built-in group called ALL_FIREWALLS. This group consists of all devices in the system, and you can generate reports for it. You cannot edit or delete this group.

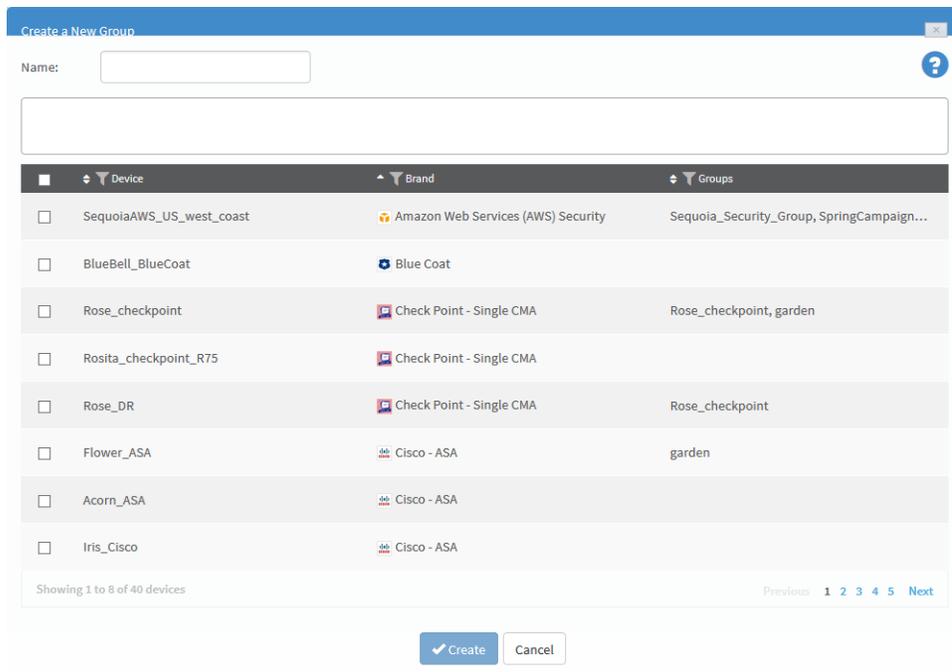
Note: In a Geographic Distribution architecture, groups may contain devices that are managed by different remote agents.

Add groups

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Click **New**, then click **Group**.

The **Create a New Group** dialog box appears.



3. In the **Name** field, type the name of the new group.
4. Select the devices that you want to add to the group.

You can search for devices by typing the full or partial name of a device into the box.

You can browse the list by clicking **Previous** or **Next** below the list. Additionally, you can see more devices on the same page by expanding the size of the dialog box by pulling the bottom corner. You can filter the devices by Device, Brand and Group by clicking  beside the column title.

The devices appear in the members box.

5. To remove members from the group, clear the device's check box.

The device is removed from the members box.

Note: A group must include at least two members.

6. Click **Create**.

A success message appears.

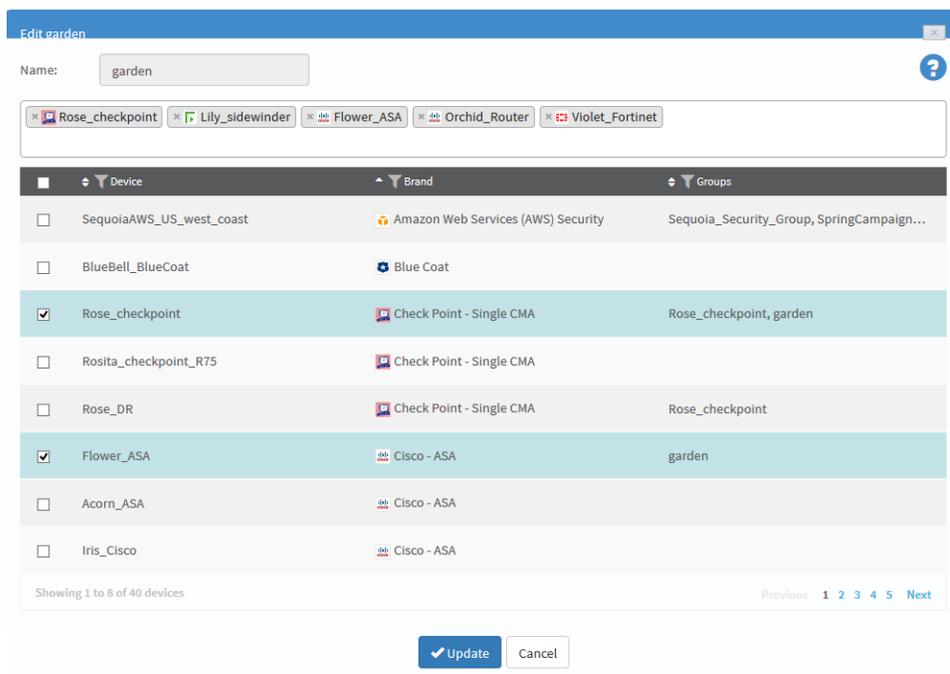
7. Click **OK**.

Edit groups

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired group and click **Edit**.

The **Edit Groups** dialog box appears.



3. To add a member to the group, select the desired device.

You can search for devices by typing the full or partial name of a device into the box.

You can browse the list by clicking **Previous** or **Next** below the list. Additionally, you can see more devices on the same page by expanding the size of the dialog

box by pulling the bottom corner. You can filter the devices by Device, Brand and Group by clicking  beside the column title.

The devices appear in the members box.

4. To remove members from the group, clear the device's check box.

The device is removed from the members box.

Note: A group must include at least two members.

5. Click **Update**.

A success message appears.

6. Click **OK**.

Rename groups

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired group from the tree and click **Rename**.

The **Rename group** dialog box appears.



3. In the **Group name** field, change the group name.
4. Click **OK**.

A success message appears.

5. Click **OK**.

Delete groups

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired group and click **Delete**.
A confirmation message appears.
3. Click **OK**.
A success message appears.
4. Click **OK**.

The group is deleted.

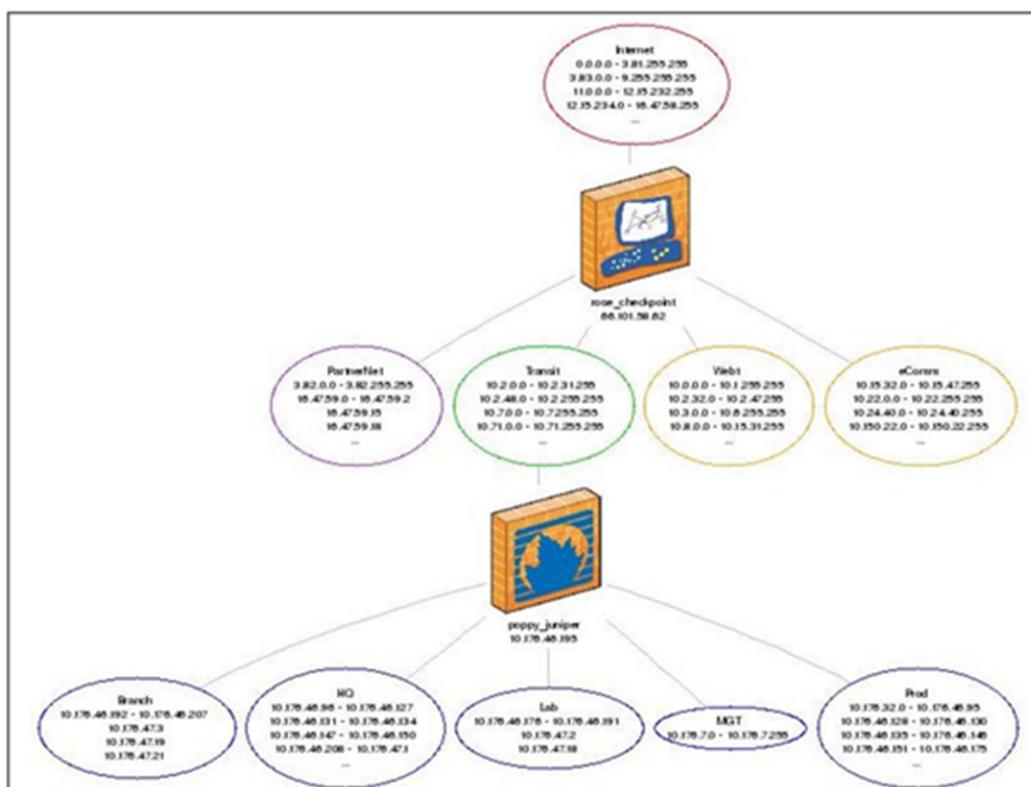
Manage matrices

This section describes how to configure matrices in AFA.

About AFA matrices

A *matrix* is a set of devices, in which information about each device member's position in the network hierarchy is provided.

When you create a matrix, AFA uses a special algorithm to calculate the relationships between the members. If desired, you can override the results and edit the topology information.



Note: In a Geographic Distribution architecture, matrices may contain devices that are managed by different remote agents.

When a report is generated for the matrix, AFA analyzes the devices' multi-tiered network topology and enables you to do the following:

- View a network diagram of the device members' topology, including the connections between them.
- View risks associated with traffic that is allowed across *all* devices in the matrix.
- Run a traffic simulation query on the generated matrix analysis report.

Add matrices

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Click **New**, then click **Matrix**.

The **Create a New Matrix** dialog box appears.

Device	Brand	Groups
<input type="checkbox"/> SequoiaAWS_US_west_coast	Amazon Web Services (AWS) Security	Sequoia_Security_Group, SpringCampaign...
<input type="checkbox"/> BlueBell_BlueCoat	Blue Coat	
<input type="checkbox"/> Rose_checkpoint	Check Point - Single CMA	Rose_checkpoint, garden
<input type="checkbox"/> Rosita_checkpoint_R75	Check Point - Single CMA	
<input type="checkbox"/> Rose_DR	Check Point - Single CMA	Rose_checkpoint
<input type="checkbox"/> Flower_ASA	Cisco - ASA	garden
<input type="checkbox"/> Acorn_ASA	Cisco - ASA	
<input type="checkbox"/> Iris_Cisco	Cisco - ASA	

3. In the **Name** field, type the name of the new matrix.
4. Select the devices that you want to add to the matrix.

You can search for devices by typing the full or partial name of a device into the box.

You can browse the list by clicking **Previous** or **Next** below the list. Additionally, you can see more devices on the same page by expanding the size of the dialog box by pulling the bottom corner. You can filter the devices by Device, Brand and Group by clicking  beside the column title.

The devices appear in the members box.

- To remove members from the matrix, clear the device's check box.

The device is removed from the members box.

Note: A matrix must include 2-4 members.

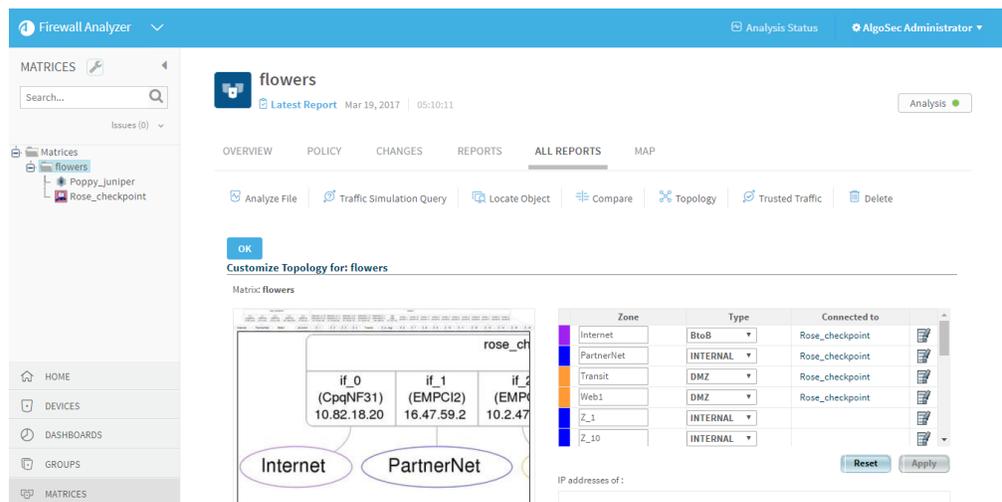
- Click **Create**.

A message box appears asking whether you want to customize the matrix settings.

- Do one of the following:

- To customize the matrix's topology at a later time, click **No**.
- To customize the matrix's topology now, do the following:
 - Click **Yes**.

The **Customize Matrix Topology** page appears, enabling you to edit all zones in the matrix's multi-tiered topology.



The screenshot shows the 'Customize Topology for: flowers' dialog box in the Firewall Analyzer. The dialog is titled 'Matrix: flowers' and contains a network topology diagram on the left and a configuration table on the right.

The topology diagram shows a central box labeled 'rose_ch' with three interfaces: 'if_0 (CpqNF31) 10.82.18.20', 'if_1 (EMPCI2) 16.47.59.2', and 'if_2 (EMPI2) 10.2.47'. Below the diagram are two ovals labeled 'Internet' and 'PartnerNet'.

The configuration table on the right has the following data:

Zone	Type	Connected to
Internet	BtoB	Rose_checkpoint
PartnerNet	INTERNAL	Rose_checkpoint
Transit	DMZ	Rose_checkpoint
Web1	DMZ	Rose_checkpoint
Z_1	INTERNAL	
Z_10	INTERNAL	

At the bottom of the dialog, there are 'Reset' and 'Apply' buttons, and a field for 'IP addresses of:'.

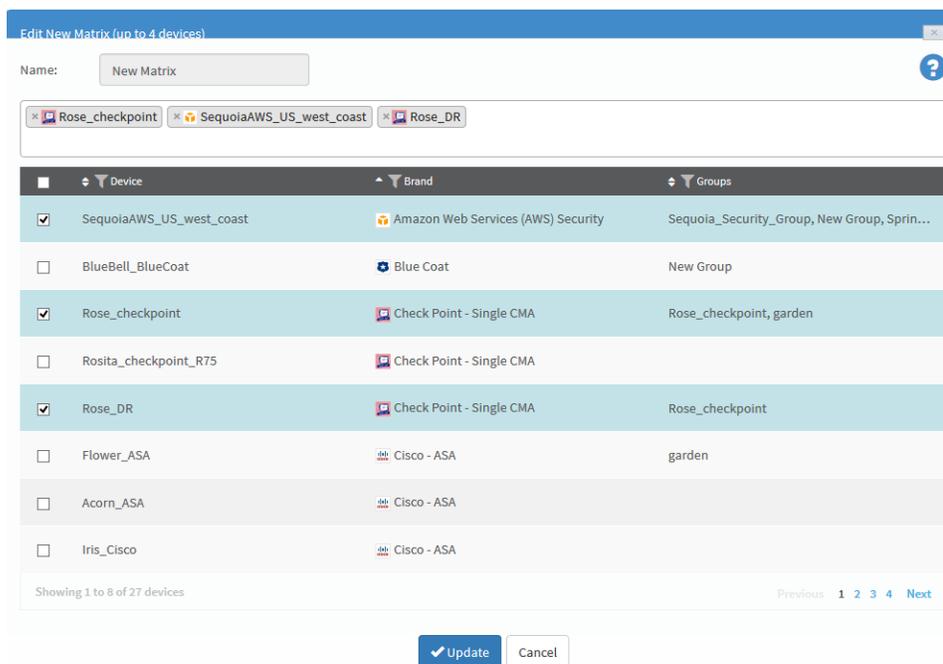
- b. Customize the matrix topology.
- c. Click **OK**.

Edit matrices

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired matrix and click **Edit**.

The **Edit Matrix** dialog box appears.



3. To add a member to the matrix, select to desired device.

You can search for devices by typing the full or partial name of a device into the box.

You can browse the list by clicking **Previous** or **Next** below the list. Additionally, you can see more devices on the same page by expanding the size of the dialog

box by pulling the bottom corner. You can filter the devices by Device, Brand and Group by clicking  beside the column title.

The devices appear in the members box.

4. To remove members from the matrix, clear the device's check box.

The device is removed from the members box.

Note: A matrix must include 2-4 members.

5. Click **Update**.

A success message appears.

6. Click **OK**.

A message box appears asking whether you want to customize the matrix settings.

7. Do one of the following:

- To customize the matrix's topology at a later time, click **No**.
- To customize the matrix's topology now, do the following:

- a. Click **Yes**.

The **Customize Matrix Topology** page appears, enabling you to edit all zones in the matrix's multi-tiered topology.

- b. Customize the matrix topology.

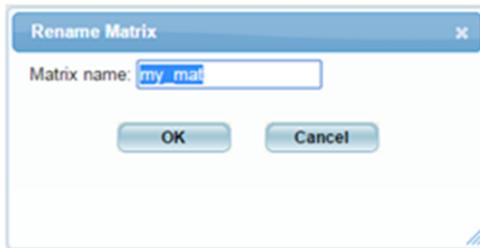
- c. Click **OK**.

Rename matrices

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired matrix and click **Rename**.

The **Rename Matrix** dialog box appears.



3. In the **Matrix name** field, modify the matrix name as desired.
4. Click **OK**.
A success message appears.
5. Click **OK**.

Delete matrices

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired matrix and click **Delete**.
A confirmation message appears.
3. Click **OK**.
A success message appears.
4. Click **OK**.

The matrix is deleted.

Manage DR sets

AFA provides the ability to define pairs (or groups) of Disaster Recovery (DR) sets. Whenever one of the devices in the set is found in the path of a traffic simulation query, the other devices will automatically be tested against the same traffic, ensuring they allow it as well. This capability significantly eases troubleshooting and change management for DR device sets that do not share the same policy.

This section describes how to configure disaster recovery (DR) sets in AFA.

Add DR sets

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Click **New**, then click **DR Set**.

The **Create a New DR Set** dialog box appears.

Device	Brand	Groups
<input type="checkbox"/> SequoiaAWS_US_west_coast	Amazon Web Services (AWS) Security	Sequoia_Security_Group, New Group, Sprin...
<input type="checkbox"/> Rose_checkpoint	Check Point - Single CMA	Rose_checkpoint, garden
<input type="checkbox"/> Rosita_checkpoint_R75	Check Point - Single CMA	
<input type="checkbox"/> Rose_DR	Check Point - Single CMA	Rose_checkpoint
<input type="checkbox"/> Flower_ASA	Cisco - ASA	garden
<input type="checkbox"/> Acorn_ASA	Cisco - ASA	
<input type="checkbox"/> Iris_Cisco	Cisco - ASA	
<input type="checkbox"/> DC_42_root	Cisco - Router	

3. In the **Name** field, type the name of the new DR set.

4. Select the devices that you want to add to the DR set.

You can search for devices by typing the full or partial name of a device into the box.

You can browse the list by clicking **Previous** or **Next** below the list. Additionally, you can see more devices on the same page by expanding the size of the dialog box by pulling the bottom corner. You can filter the devices by Device, Brand and Group by clicking  beside the column title.

The devices appear in the members box.

5. To remove members from the DR set, clear the device's check box.

The device is removed from the members box.

Note: A DR set must include at least two members.

6. Click **Create**.

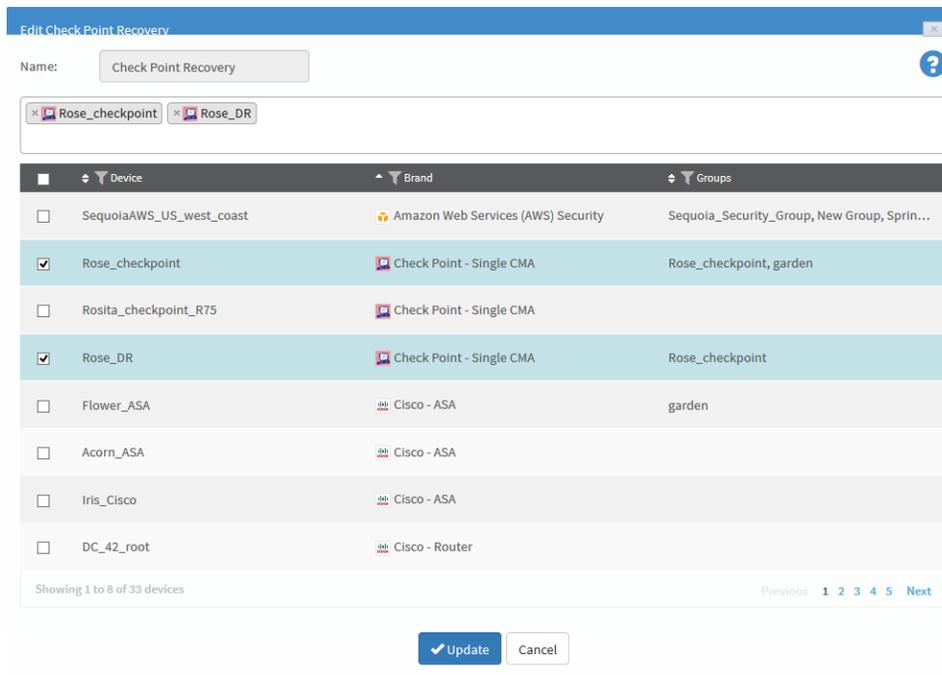
A success message appears.

7. Click **OK**.

Edit DR sets

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired DR set and click **Edit**.

The **Edit DR** set dialog box appears.



- To add a member to the DR set, select the desired device.

You can search for devices by typing the full or partial name of a device into the box.

You can browse the list by clicking **Previous** or **Next** below the list. Additionally, you can see more devices on the same page by expanding the size of the dialog box by pulling the bottom corner. You can filter the devices by Device, Brand and Group by clicking  beside the column title.

The devices appear in the members box.

- To remove members from the DR set, clear the device's check box.

The device is removed from the members box.

Note: A DR set must include at least two members.

- Click **Update**.

A success message appears.

6. Click **OK**.

Rename DR sets

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired DR set from the tree and click **Rename**.

The **Rename Dr Set** dialog box appears.



3. In the **DR Set name** field, modify the DR set name as desired.
4. Click **OK**.

A success message appears.

5. Click **OK**.

Delete DR sets

Do the following:

1. Access the **Devices Setup** page. For details, see [Access the DEVICES SETUP page](#).
2. Select the desired DR set from the tree and click **Delete**.

A confirmation message appears.

3. Click **OK**.

A success message appears.

4. Click **OK**.

The DR set is deleted.

Manage the map

This section describes advanced support options for improving the accuracy of the graphic network map and the operations which depend on it.

For details, see:

- [Complete the map](#)
- [Complete the map \(CLI\)](#)
- [Troubleshoot traffic simulation queries](#)
- [Edit IP ranges in clouds](#)
- [Remove devices](#)
- [Restore device interfaces](#)
- [Specify routing data manually](#)

Complete the map

AFA creates the graphic network map using all the routing information it collects from the devices defined in AFA. Whenever a device's routing table implies the existence of a device that is not defined in AFA, the device is represented in the map as a generic router. Because AFA has only limited information about these routers, they cause holes in the network map which AFA can only represent as a cloud. Some of these routers have a large impact on the paths within the network, and the fact that they are not defined in AFA deprives the map (and AFA) of the significant routing information they could provide.

Completed map contents

A complete map will include:

- A direct connection between every internal subnet in the network (without passing through any clouds).
- A direct connection between every internal subnet and all permitted external IP addresses that ends in the relevant cloud (without passing through any clouds).

AFA provides a completeness score for your map and enables you to complete your map by providing a prioritized list of generic routers in the map that should be defined as devices AFA. The routers which would complete the most paths are given the highest priority. AFA automatically performs a DNS lookup to help identify which of your devices correspond to which IP address. To further assist in identifying the device names, you can optionally provide the network's SNMP credentials.

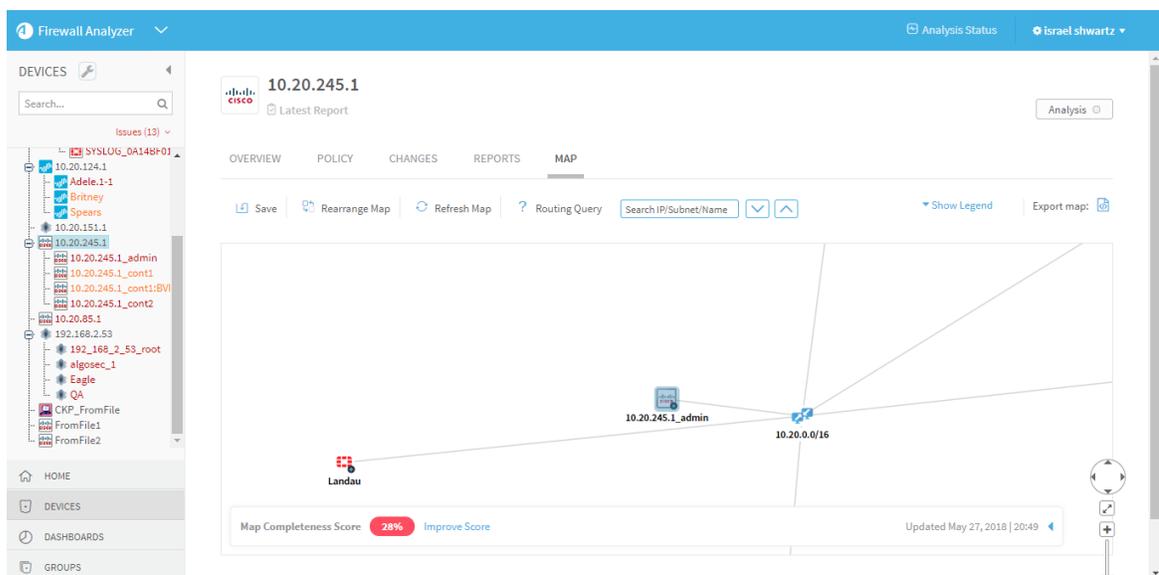
Tip: Alternately, complete the map via CLI instead. For more details, see [Complete the map \(CLI\)](#).

Identify routers to define in AFA

Do the following:

1. View the graphic network map.

The **Map** appears in the workspace.



The screenshot shows the Firewall Analyzer interface. On the left is a 'DEVICES' sidebar with a search bar and a tree view of network devices. The main workspace displays a network map for IP address '10.20.245.1'. The map shows a central node '10.20.0/16' connected to '10.20.245.1_admin' and 'Landau'. At the bottom of the workspace, a 'Map Completeness Score' is shown as 28% with an 'Improve Score' button. The interface also includes a top navigation bar with 'Analysis Status' and a user profile 'Israel Schwartz'.

The map completeness score appears at the bottom of the workspace.

Note: The map completeness score and the routers that AFA recommends

defining are calculated by simulating routes between internal subnets and between each internal subnet and external IP. By default, the maximum number of paths that will be simulated is 400, and the external IP addresses used in the calculation is 8.8.8.8. If a custom risk profile spreadsheet is being used in AFA, the networks in the spreadsheet are used as the default internal networks. If no such spreadsheet is being used, RFC 1918 is used to provide the default internal networks.

2. Next to the map completeness score, click the **Improve Score** link.

The **Improve Map Connectivity** page appears.

The list on the left is a prioritized list of routers to define in AFA. The routers which would complete the most paths are given the highest priority, and therefore appear at the top of the list. The name of the router appears when the DNS lookup was successful ; otherwise, the IP address of the router appears.

Each router appears in the list with its IP address as a link. Clicking on the link will focus the map on that router.

The device name to the left of the router's name is the device defined in AFA which is closest to the router. When multiple devices are close to the router, a link to a list of the devices appears.

3. To filter the list of routers, type a search in the search box.

The search results include results for router names, router IP addresses, or names of the closest device defined in AFA.

4. To define a router in AFA, hover over the router in the list and click  .

The administration area for defining new devices appears, enabling you to define the device in AFA. For more details, see [Add devices to AFA](#).

5. To merge routers in the map into a single router, do the following:

6. Select the routers in the list that you want to merge.

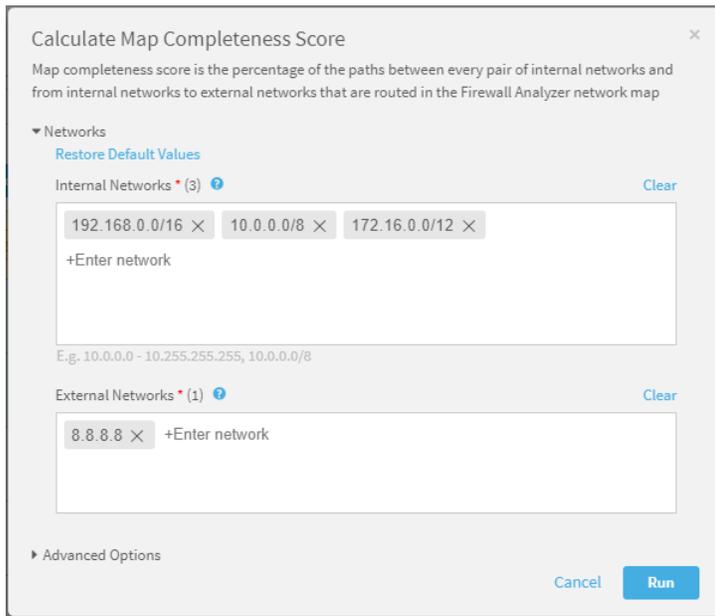
The **Merge Selected** button at the top of the list becomes enabled when two or more routers are selected.

7. Click .

The routers are merged into one router in the map. The new router is represented with the merged routers icon.

8. To re-run the map completeness calculation with custom values, do the following:
9. Click on the map completeness score icon.

The **Calculate Map Completeness Score** window appears.



Calculate Map Completeness Score

Map completeness score is the percentage of the paths between every pair of internal networks and from internal networks to external networks that are routed in the Firewall Analyzer network map

▼ Networks

[Restore Default Values](#)

Internal Networks * (3) [Clear](#)

192.168.0.0/16 × 10.0.0.0/8 × 172.16.0.0/12 ×

+Enter network

E.g. 10.0.0.0 - 10.255.255.255, 10.0.0.0/8

External Networks * (1) [Clear](#)

8.8.8.8 × +Enter network

► Advanced Options

[Cancel](#) [Run](#)

10. Edit the internal or external networks in the fields.

The map completeness score and the routers that AFA recommends defining are calculated by simulating routes between internal subnets and between each internal subnet and external IP.

11. To restore the default network values, click the **Restore Default Values** link.
12. To customize the maximum number of paths that will be simulated and/or to

provide SNMP credentials for the sake of identifying router names, do the following:

- a. Click **Advanced Options**.
- b. Complete the additional fields.

Note: When SNMP is provided, the only information being fetched via SNMP is the name of the devices.

13. Click **Run**.

Complete the map (CLI)

AlgoSec provides a CLI tool to help complete the map.

Note: Using the AFA web interface is the preferred method to complete the map. See [Complete the map](#). When you chose to use the CLI tool, the results will not appear in the UI.

Map completeness CLI tool scope

The CLI tool provides:

- A connectivity score for the map.
- A prioritized list of generic routers in the map that should be defined as devices AFA. The routers which would complete the most paths are given the highest priority.

In order to identify which device corresponds to which IP address, the tool automatically performs a DNS lookup. To further assist the tool in identifying the device names, you can optionally provide the network's SNMP credentials.

- A list of mis-matched routes in the map (the route was complete in one direction, but not the other).

Identify routers to define in AFA

Do the following:

1. Set the map to prefer paths where the source is a subnet (and not a cloud) and disable this preference for destinations. For details, see the [PrioritizeFIPDestination](#) parameter.

Note: Make sure to revert these parameters to the settings required for your environment after you finish running the CLI tool.

2. Prepare the following input files:

- **A .txt file with all the *internal subnets* within the network.** The subnets should all be connected without going through the internet.

Each subnet in the file must be in CIDR format and on a new line ("line break" is the delimiter).

Example:

```
10.0.0.0/8  
192.168.0.0/16
```

- **A .txt file with all the *external IP addresses* that should be reachable from each internal subnet.**

Each IP address must be on a new line ("line break" is the delimiter).

Example:

```
8.8.8.8  
82.102.187.174
```

- **(Optional) A .txt file with the network's SNMP credentials.** Providing this information helps the CLI tool determine the names of the devices in the prioritized list (not just the IP addresses) when the DNS lookup does not provide the name.

- For SNMP version 2, the file must include the following (with the community string value inserted):

```
version: 2community:
```

- For SNMP version 3, the file must include the following (with all the values inserted):

```
version: 3username: authprotocol:authpassword:privprotocol:
privpassword:
```

Note: When SNMP is provided, the only information being fetched via SNMP is the name of the devices.

3. Open a terminal and log in using the username "afa" and the related password.
4. Run the following command with any desired optional parameters:

```
map_completeness -i <internal_nets.txt> -e <external_IPs.txt>
```

For details, see [Map completeness parameters](#).

5. The tool simulates the routes between each internal subnet and between each internal subnet and external IP.

For example:

```
Running internal queries:Simulating 950 paths of 8556 possible paths.
100% ProcessedRunning external queries:Simulating 372 paths of 372
possible paths.100% Processed-----
```

Where:

Summary	Description...
Internal networks: 2	Number of internal subnets in the input file.
External IPs: 2	Number of external IPs in the input file.

Summary	Description...
Internal subnets in the map database: 93	Number of subnets in the current map that are included in the internal subnets in the input file.
3 Unique missing router addresses	Number of routers in the current map that are not defined in AFA.
294 Mismatches were found	Number of paths that are complete in one direction, but not the other.
Map is 16.28% Complete	The completeness score for the current map. This is the percentage of possible paths that are complete.

Note: Routes with NAT will be identified as mis-matched even though they do not predict a hole in the map.

The two output files are created and given the names you specified in the command parameters or the default names *missing_routers.txt* and *routing_mismatches.txt*.

The missing routers output file provides a list of devices to add to AFA. The file includes the number of paths that are incomplete because of each missing device. The devices are listed in descending priority, where devices that would complete more paths are given higher priority. If the tool was not able to determine the name of a device using a DNS lookup or SNMP, only the IP address appears.

```

=====
                          Missing Routers
=====
Device Name                Device IPs                Missing paths
-----
10.186.4.5                  10.186.4.5                192
10.20.0.1                   10.20.0.1                 154
10.132.0.1                  10.132.0.1                30

```

Map completeness parameters

Parameters	Mandatory?	Description
-i <internal_nets.txt>	Yes	Passes the internal networks input file. The value is the relative path to the file.

Parameters	Mandatory?	Description
-e <external_IPs.txt>	Yes	Passes the external IPs input file. The value is the relative path to the file.
-s <snmp_credentials.txt>	No	Passes the SNMP credentials input file. The value is the relative path to the file.
-r <missing_routers.txt>	No	Enables you to provide the name of the output file with the prioritized list of routers. By default, the files name will be <i>missing_routers.txt</i> .
-m <routing_mismatches.txt>	No	Enables you to provide the name of the output file with the routing mismatches. By default, the files name will be <i>routing_mismatches.txt</i> .
-n <max_queries>	No	Enables you to specify the maximum number of routes to simulate. The value is the maximum number of routes (where each route is simulated in both directions). The internal subnets are permitted this number of routes and the external IPs are permitted this number of routes (individually). The default value is 1000 routes. In other words, 1000 for internal subnets and 1000 for external IPs, where each route is simulated in both directions. Note: This CLI tool does not simulate every possible route, but a sampling. This parameter specifies the size of the sample.
-v	No	Enables verbose mode. The output files will contain additional information which may be useful for debugging. By default, verbose mode is disabled.
-p	No	Specifies the output files should be printed in human-readable format. The default is CSV format.
-h	No	Prints help. Help will also print if the command is run with invalid syntax.

Troubleshoot traffic simulation queries

All traffic simulation queries in AFA are based on information provided by the graphic network map. AFA enables you to use the map to view network issues and determine how to improve traffic simulation query results.

If you ran a group device query and received unexpected results, you can troubleshoot those results by providing the expected results. AFA will make a recommendation to help you make the traffic traverse correctly.

Note: The traffic simulation query troubleshooting feature is for AFA administrators only.

Note: This feature is not relevant for single device queries.

Do the following:

1. Run the group Traffic Simulation Query.

A new window opens displaying the traffic simulation results.

Traffic Simulation Results

Partially allowed Nov 25, 2018 12:41:00 Export

Rescue

Requested Traffic

SOURCE	DESTINATION	APPLICATION	SERVICE
10.30.73.53	10.176.57.0/24		tcp/80
10.47.71.62	10.123.40.0/24		

Devices in Path (10)

Parts of the requested traffic are not routed. The routed parts are partially allowed

VIEW BY: Path

REQUESTED TRAFFIC

- PATH 1
 - DC_A2
 - Violet_Fortinet
 - DC_B2
 - Shaw_WebEndpoint
 - DePod1_SRX
 - Development_SG/FullStack
- PATH 2
 - Peon_Neliskio
 - Poppy_Jumper
 - Development_SG/FullStack

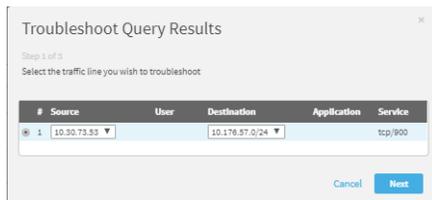
Expected a different path?

100%

The path detected by the query appears on both the left side pane and the map.
The devices appear in the same order as the path detected in the query.

2. Click **Expected a different path?**.

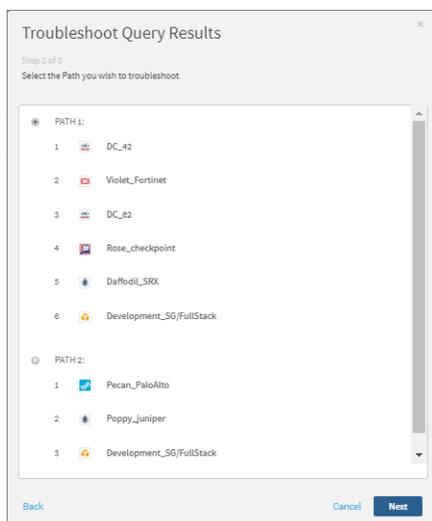
The Troubleshooting Query Results wizard appears.



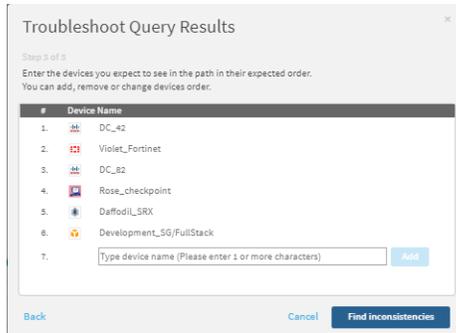
Note: If the query has more than one traffic line with unexpected results, you can only troubleshoot one path at a time from one of those traffic lines.

3. If the query involves multiple traffic lines or a single traffic line with multiple sources and/or multiple destinations, select the traffic line and click **Next**.

The Troubleshooting Query Results wizard appears.



4. Select the path you wish to troubleshoot and click **Next**.



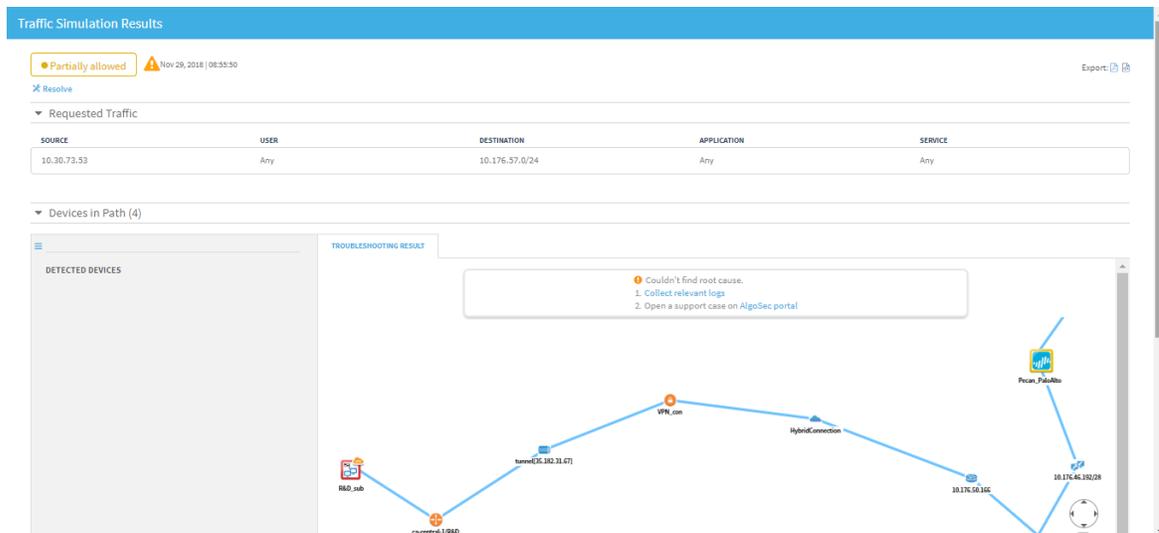
- Specify the expected path for the query. You can optionally add new devices, change the order of the devices, and/or delete devices.

Note: You can only add devices to the path that are currently defined in AFA.

- Click **Find inconsistencies**.

The new route is simulated.

If the query does not detect the expected path, the result appears displaying the identified problems and suggested solutions.



- Do one of the following:

<p>For any of the following cases:</p> <ul style="list-style-type: none"> • Identified problem is an issue with a device • Root cause could not be detected • Too many paths were found 	<p>Do the following:</p> <ol style="list-style-type: none"> a. Collect the relevant logs. b. Open a support case on the AlgoSec portal.
<p>If there is a missing device</p>	<ol style="list-style-type: none"> a. Define the device in AFA. b. Run analysis on the device c. Run the query again.

Note: If the identified problem is that the traffic is not routed in the network, no troubleshooting can be performed.

Note: If there is no problem and the path is exactly as expected, no further troubleshooting is needed.

Edit IP ranges in clouds

You can add or remove the automatically generated IP ranges in clouds. Once implemented, any edits will remain for future map calculations. Additionally, you can display a list of all current cloud edit entries and disable edits that are no longer relevant.

Note: AFA supports adding or removing ranges from clouds, but not removing clouds.

Do the following:

1. Open a terminal and log in using the username "afa" and the related password.
2. To add a range to a cloud, enter the following command:

```
fa_map -add CIDR -stub stub_router_IP [-comment comment]
```

where, *CIDR* is the CIDR you want to include, *stub_router_IP* is the IP address of the adjacent router, and *comment* is a comment for the cloud edit entry (in quotations).

The comment parameter is optional.

Note: The input range must be in CIDR format.

The range is added to the cloud.

3. To remove a range from cloud(s), do one of the following:

Remove a range from all clouds except for specific clouds

Enter the following command:

```
fa_map -remove_from_all CIDR -except_stub stub_router_IP  
[-comment comment]
```

where, *CIDR* is the CIDR you want to exclude, *stub_router_IP* is the IP address of the adjacent router for which you want to keep the CIDR, and *comment* is a comment for the cloud edit entry (in quotations).

You can use the **except_stub** parameter multiple times to include the CIDR in multiple clouds, as in the following example:

```
fa_map -remove_from_all 10.0.10.0/24 -except_stub 192.168.1.20  
-except_stub 10.155.102.250 -comment "10.0.10.0/24 is only  
behind 192.168.1.20 and 10.155.102.250"
```

Remove a range from a specific cloud

Enter the following command:

```
fa_map -remove CIDR -stub stub_router_IP[-comment comment]
```

where, *CIDR* is the CIDR you want to exclude, *stub_router_IP* is the IP address of the adjacent router, and *comment* is a comment for the cloud edit entry (in quotations).

Note: The **comment** parameter is optional.

Note: The input range must be in CIDR format.

The range is removed from the cloud.

4. To display a list of all currently configured cloud edit entries, enter the following command:

```
fa_map -list -stub stub_router_IP
```

where, *stub_router_IP* is the IP address of the router for which you would like to see all cloud edit entries.

Note: The **stub** parameter is optional. When a router is not specified, all entries in the database are displayed.

The list of all cloud edit entries in the database is displayed.

5. To disable a cloud edit, enter the following command:

```
fa_map -del-entry CIDR -stub stub_router_IP -action exclude
```

where, *CIDR* is the CIDR of the entry you want to delete and *stub_router_IP* is the IP address of the router for the entry you want to delete.

Note: The input CIDR and router IP address must be exactly as they are in the cloud edit entry. It is recommended to display the entries (see above) and verify these inputs before running this command.

The following prompt appears:

```
Are you sure you want to delete entry [Y/n]
```

Press **Enter**.

The cloud is recalculated without the edit.

Remove devices

You can remove devices from the graphic network map. You can remove devices from the current map calculation and/or from all future map calculations. If you only remove the device from current map, the device will appear in the map again once a new report is generated.

Note: A removed device will not appear in traffic simulation query results.

Do the following:

1. Open a terminal and log in using the username "afa" and the related password.
2. To remove devices from the current map, do the following:
3. Enter the following command:

```
fa_map -d DeviceID
```

where, *DeviceID* is the name of the device you wish to remove from the current graphic network map.

4. To cause devices to be omitted from all future map updates, do the following:
5. Open `/home/afa/.fa/config`.
6. On a new line, add the configuration item `MAP_BLACK_LIST`, and set the configuration item's value to a semi-colon separated list of devices that you wish to remove from the graphic network map.

For example, the following removes the devices `rose_checkpoint` and `flower_asa` from the graphic network map, for all future maps.

```
MAP_BLACK_LIST=rose_checkpoint;flower_asa
```

7. Save the file.

Restore device interfaces

You can specify that certain device interfaces be ignored directly from the graphic network map. The procedure below describes how to restore interfaces you ignored and view a list of all ignored interfaces.

Do the following:

1. Open a terminal and log in using the username "afa" and the related password.
2. Enter the following command:

```
fa_map -restore_ignored_interface InterfaceName -n DeviceName
```

where, *InterfaceName* is the name of the interface you wish to ignore, and *DeviceName* is the name of the interface's device.

3. To view a list of all the ignored interfaces for a specific device, enter the following command:

```
fa_map -list_ignored_interfaces -n DeviceName
```

where, *DeviceName* is the name of the interface's device.

4. To view a list of all the ignored interfaces for all devices, enter the following command:

```
fa_map -list_ignored_interfaces
```

Specify routing data manually

Administrators can manually specify routing information for a device, instead of using the automatically generated routing information that AFA compiles with each analysis. For more information, see [Specify routing data manually](#).

Do the following:

1. View the graphic network map.

The **Map** appears in the workspace.

2. Right-click the desired device ,and select **Routing Information**.

The **Routing Information** dialog box appears, displaying the current URT file.

3. Select **Static Routing Table (URT)**.

New fields appear.

4. Click the **Download current URT file** link or the **Download Sample file** link.

The file downloads to your computer.

5. Edit the file with the routing information you want to import.

For information about URT file syntax, see [How to manually specify routing information for Cisco Layer 2 devices](#) in AlgoPedia.

6. Click **Upload new file**, and select the new URT file.

The file is validated and uploaded. If there is an error in syntax or content, an error message appears.

7. Click **OK**.

The new routing table will take affect after the next device analysis.

Schedule analysis

This section describes how to schedule analyses for devices, groups and matrices.

AFA can run multiple reports in parallel, and the maximum number of reports that can be generated simultaneously depends on your AFA system configuration and power. In order to change this value, contact AlgoSec support.

Note: If a manual report process is running on a specific device, the current monitoring cycle for that device is skipped. AFA will attempt to run the next monitoring cycle as scheduled. If a monitoring cycle is already running on a specific device when a manual report is requested, AFA waits for the monitoring process to complete before generating the report.

Note: It is recommended to only run 'All Firewalls' analyses at night, in order to avoid a high strain on your system during normal operating hours.

 [Schedule Analysis](#): Watch to learn how to schedule analysis to suit your business needs.

Add and edit analysis jobs

To add or edit an analysis job:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Scheduler** tab.

The **Scheduler** tab appears.

Firewall Analyzer Analysis Status AlgoSec Administrator

Administration

DEVICES SETUP USERS/ROLES **SCHEDULER** COMPLIANCE OPTIONS MONITORING DOMAINS ARCHITECTURE

Schedule Recurring Analysis

Job	Name	Timing	Device / Group	Risk Profile	Edit	
<input type="checkbox"/>	1	Job 1	Daily at 19:30	Rose_checkpoint	Default	

Delete New

Schedule Dashboard E-Mail

Job	Name	Timing	Dashboard	Edit	
<input type="checkbox"/>	2	Dash 2	Daily at 19:30	Compliance Dashboard	

Delete New

4. Do one of the following:

- To schedule a new analysis job, in the **Schedule Recurring Analysis** area, click **New**.
- To edit an existing analysis job, click on the Edit icon next to the desired job.

New fields appear.

The screenshot shows the 'Administration' page in the Firewall Analyzer interface. The 'SCHEDULER' tab is active, and the 'Schedule Recurring Analysis' dialog is open. The dialog contains the following sections:

- Job Details:**
 - Job name: Job 3
 - Base group reports on existing device reports.
 - Select risk profile: Standard
 - Run device analysis: Default (Always (slow))
- Select a device/group:**
 - Schedule job for the device / group: Please select a device or a group
 - Select device / group button
- Recurrence:**
 - Daily
 - Weekly
 - Monthly
 - Quarterly
 - Yearly
 - Upon policy install
- Recurrence Pattern:**
 - Set time: 19:30

Buttons for 'Cancel' and 'OK' are located at the bottom right of the dialog.

5. In the **Job name** field, type a name for the job.
6. (Optional) To aggregate a group/matrix members' existing reports into a group/matrix report, (instead of generating new reports for each member and using those reports to generate a group/matrix report), select the **Base group reports on existing device reports** check box.

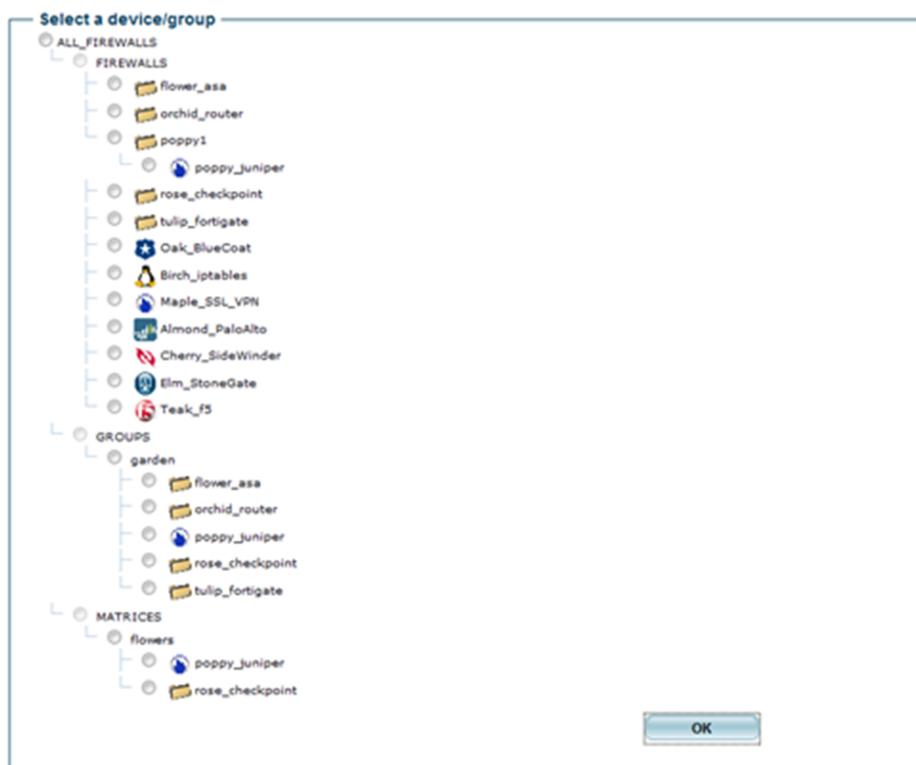
This field is relevant only when generating group reports and matrix reports.
7. To select a risk profile, select the **Select risk profile** check box, and select a risk profile from the drop-down menu.
8. Select one of the following settings in the **Run device analysis** drop-down menu:

- **Only if the policy/topology changed** - if a policy is detected as unchanged during a scheduled analysis, then AFA should not run a full report, but instead create an unchanged report that links to the last report for the policy.
- **Always (slow)** - AFA will always run a full analysis, regardless of whether the policy has changed or not.

Note: Selecting this option will result in longer analysis time and requires more disk space.

9. Specify the device, group, or matrix for which you want to schedule an automatic analysis, by doing the following in the **Select a device/group** area:
10. Click **Select device/group**.

A tree of all the devices, groups, and matrices appears.



11. Choose the desired device, group, or matrix.

Note: When you select a "parent" tier device, all the devices beneath it are automatically analyzed with each analysis.

12. Click **OK**.

13. In the **Recurrence** area, specify how often the analysis job should run.

You can select either a daily, weekly, monthly, quarterly, or yearly analysis, or configure the analysis to occur when a policy is installed on the device(s).

Note: You can only select **Upon policy install**, if real-time change monitoring is enabled for this device.

The fields in the **Recurrence Pattern** area change according to your selection.

14. In the **Recurrence Pattern** area, configure the desired pattern of recurrence.

Note: If you want to see the scheduled job run during the current schedule cycle, schedule your analysis at least five minutes later than the current time.

15. Click **OK**.

Delete scheduled jobs

Use this procedure to delete a scheduled analysis or dashboard email.

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Scheduler** tab.

The **Scheduler Setup** tab is appears with a list of scheduled analysis and dashboard e-mail jobs.

4. Select the check box next to the desired job.
5. Click **Delete**.

A confirmation message appears.

6. Click **Yes**.

The job is deleted.

Configure real-time monitoring

AFA provides the option to monitor devices for changes in real-time (as opposed to waiting for a full analysis).

This option must be activated for the ASMS environment and then enabled per device. AFA will periodically check devices' policies for changes, and detected changes will be displayed in the AFA Web interface.

Additionally, a syslog message will be logged in `/var/log/messages`.

Note: You can configure AFA to send e-mail notifications to selected users whenever changes are detected. For more details, see [Configure event-triggered notifications](#).

Activate real-time monitoring

Note: In addition to activating real-time monitoring with this procedure, real-time monitoring must be enabled on each device you want to monitor. When you add a device to AFA, this is enabled by default. This option is controlled by the **real-time change monitoring** check box in the **Devices Setup** page for each device.

Do the following

1. In the toolbar, click your username.

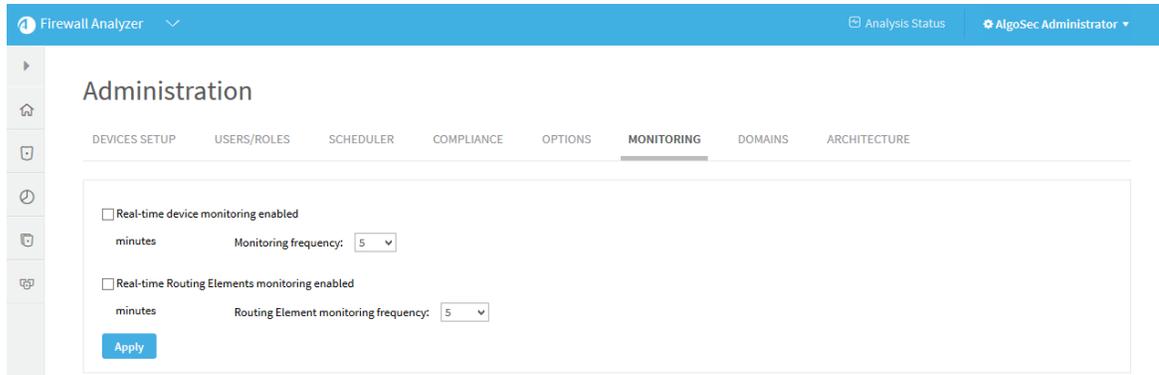
A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Monitoring** tab.

The **Monitoring** page appears.



The screenshot shows the 'Administration' page in the Firewall Analyzer interface. The 'MONITORING' tab is selected. The page contains two sections for configuring real-time monitoring:

- Real-time device monitoring enabled
minutes Monitoring frequency: 5
- Real-time Routing Elements monitoring enabled
minutes Routing Element monitoring frequency: 5

An 'Apply' button is located at the bottom of the configuration area.

4. To activate real time monitoring for devices, do the following:
 1. Select the **Real-time device monitoring enabled** option.
 2. Set the **Monitoring frequency** to the interval of time in minutes at which AFA should monitor devices.
5. To activate real-time monitoring for routing elements, do the following:
 1. Select the **Real-time Routing Elements monitoring enabled** option.
 2. Set the **Routing Element monitoring frequency** to the interval of time in minutes at which AFA should monitor routing elements.
6. Click **Apply**.

AFA users and roles

This section describes the users, roles, permissions, and authentication supported in AFA, and how AFA administrators can manage AFA users and roles.

AFA users and roles provide the basis for authentication across both AFA and FireFlow.

AFA authentication

ASMS supports authentication via an LDAP or RADIUS authentication server, Single Sign On (SSO), or the local AFA database.

Configuring an authentication server or SSO provides additional functionality, such as associating each AFA role with a specific LDAP group. In such cases, users are automatically assigned roles according to their LDAP group membership.

Note: When an authentication server or SSO is configured, user credentials and roles are managed on the external server. In such cases, any changes made directly in AFA are overwritten the next time the user logs in.

For more details, see:

- [Configure user authentication](#). Describes how to configure an authentication server or SSO.
- [Manage users and roles in AFA](#). Describes how to manage users and roles directly in AFA.

AFA user types and permissions

AFA supports the following types of users:

Administrators	<p>Can perform any task.</p> <p>For example, in addition to the tasks that non-administrative users can perform, administrators can also:</p> <ul style="list-style-type: none"> • Manage other users • Define and edit monitored devices • Configure AFA general settings and preferences • Schedule AFA analyses.
Non-administrator privileged users	<p>Can run analyses, generate reports, view policies and reports, view network map and monitoring changes, and run traffic simulation queries.</p>

Each user is assigned one of the following access levels as part of their *default permission profile*:

Standard Access	<p>Enables users to view existing reports, run traffic simulation queries, initiate new device analyses, and use the customization features such as customizing the topology.</p>
ReadOnly Access	<p>Enables users to view existing reports and run traffic simulation queries on these reports.</p>
None	<p>Prevents users from having any access at all to reports.</p> <p>This access level is automatically applied to all devices that the user is authorized to view; however, you can override the default access level on a per-device basis. Permissions and access levels can additionally be managed using AFA <i>roles</i>. All users assigned a role inherit the permissions and access levels specified for the role.</p>

For more details, see [Manage users and roles in AFA](#).

Configure user authentication

This topic describes how to configure ASMS user authentication, including single sign-on, authentication servers, and LDAP forests.

Best practice: Whenever possible, leverage LDAP/LDAPS for authentication. This

enables all ASMS users to log in easily, including change requestors, application owners, auditors, and so on.

Configuring LDAP/LDAPS for ASMS also enables auto-provisioning, which means that users are automatically created and assigned to their appropriate roles based on their LDAP group membership, without any additional configuration.

 [Configure LDAP in AFA](#): Watch to learn how to sync AFA with your organization's LDAP server.

Single Sign On (SSO) and ASMS

ASMS supports a SAML 2.0-based Single Sign On (SSO) solution, enabling you to integrate user logins with your SSO Provider.

SSO solutions have the following elements:

A service provider (SP)	In our case, AlgoSec is a service provider that provides ASMS.
An identity provider (IdP)	In our case, your SSO Provider provides user identity verification as the identity provider.

When SSO is enabled:

- ASMS directs users to authenticate against your SSO Provider as the IdP, and then redirects the user back to ASMS.
- Users already logged in to the SSO Provider are directed directly to ASMS.
- The **Logout** button no longer appears in ASMS. Log out by logging out of your SSO Provider only.

For more details, see:

- [SSO Provider requirements](#)
- [Configure Single Sign On](#)

Note: ASMS provides service provider metadata at the following URL:

https://<Algosec URL>/AFA/php/module.php/saml/sp/metadata.php/<SP Identifier>

SSO Provider requirements

As your IdP, your SSO Provider must be aware of the following ASMS services:

Assertion Consumer Service, or the Single Sign On URL	Informs the IdP where ASMS redirects the user for Single Sign On (login) requests. Configured as: https://<ASMS URL>/simplesaml/module.php/saml/sp/saml2-ac.php/<SP Identifier>
Single Logout Service	May not be required in all situations. Informs the IdP where ASMS redirects the user for Single Sign Out (logout) requests. Configured as: https://<ASMS URL>/simplesaml/module.php/saml/sp/saml2-logout.php/<SP Identifier>

The SSO Provider must inform ASMS about the user performing the authentication. The following data is passed with the returned attributes, post-authentication:

Attribute	Content	Example
UID	Username	laura
email	Email address	lauras@email.com
displayName	Name displayed in the user interface	Laura Sanchez

Tip: If your SSO Provider cannot be configured to provide the required data in this format, configure a customized UID parser.

For details, see [Configure a customized UID parser](#).

Configure Single Sign On

To configure Single Sign on in ASMS, do the following:

1. In the AFA Administration area, browse to the **OPTIONS > Authentication** tab.
2. Under **User Authentication**, select **Single Sign On**, and complete the following fields as needed:

Service Provider identifier	The identifier of the AlgoSec SP. This identifier must be unique, and it must be added to the list of known SPs in your identity provider's configuration.
Identity Provider identifier	The identifier of your installed IdP.
IdP's Single Sign On service URL	The URL of the IdP's Login page.
IdP's Single Sign Out service URL	The URL of the IdP's Logout page.

3. **Optional:** To fetch user data, select the **Fetch User Data** checkbox and do one of the following:

Fetch user data from an LDAP server

Do the following:

- a. Select **LDAP**, and complete the fields as needed:
 - [LDAP Server Credentials fields](#)
 - [Attribute Mapping fields](#)
 - [Fields Mapping fields](#)
 - [FireFlow specific fields](#)

- b. Click **Test connectivity** for the specific server to test connectivity. A message informs you whether AFA connected to the server successfully.
- c. To configure one or more secondary LDAP servers, select **Use Secondary Servers**, and complete the additional fields as needed. For details, see [LDAP Server Credentials fields](#).
- d. Continue with [step 4](#).

LDAP Server Credentials fields

Server	Type the IP address of the LDAP server's host computer.
LDAP Version	Select the version of LDAP used on the LDAP server.
Port	Type the port number on the LDAP server's host computer.
Timeout	Use the arrow buttons to select the maximum amount of time in seconds to wait for the LDAP server's reply.
Secure Connection	Select this option to secure connections with the LDAP server, then choose the method to use for securing the connection: LDAPS or StartTLS . The default method is LDAPS . The value of the Port field changes according to the method selected.
Verify Server Certificate	Select this option to specify that AFA should check the LDAP server's certificate against a locally stored certificate. AFA will only connect to the LDAP server if the certificates are identical. The CA Certificate field appears.
CA Certificate	Select the locally stored certificate against which AFA should compare the LDAP server's certificate. The certificate must be stored under <code>/home/afa/.fa/ca_certs</code> in order to appear in the drop-down list.

Bind Type	<p>Select the bind type to use:</p> <ul style="list-style-type: none"> • Simple. AFA sends the entered username and password to the LDAP server. If the entered username exists in the LDAP server, and the password matches the username, then the user is logged in. • Regular. AFA logs in to the LDAP server using a user DN and password, and then checks the entered username and password against the LDAP server. If the entered username exists in the LDAP server, the password matches the username, <i>and</i> any additional criteria are met, then the user is logged in. • Anonymous. AFA accesses the LDAP server anonymously, and then checks the entered username and password against the LDAP server. If the entered username exists in the LDAP server, the password matches the username, <i>and</i> any additional criteria are met, then the user is logged in. <p>If you chose Regular or Anonymous, additional fields appear. The default value is Regular.</p>
User DN	<p>Type the user DN that AFA should use to log in to the LDAP server. This field appears only for Regular bind type.</p>
Password	<p>Type the password that AFA should use to log in to the LDAP server. This field appears only for Regular bind type.</p>

Attribute Mapping fields

Name	<p>Type the attribute that contains a user's name, in user objects in the database. The default value is <code>sAMAccountName</code>.</p>
Group Membership	<p>Type the attribute that contains a user's groups, in user objects in the database. The default value is <code>member</code>.</p>

Fields Mapping fields

Associated Roles	Select this option to import user group information from the LDAP server. Selecting this option enables assigning user roles via a specified correspondence between LDAP groups and AFA, FireFlow, or AppViz roles. To manage roles from within the AlgoSec Suite (not the LDAP), do not select this option.
Full Name	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Full Name field.
Email	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Email field.
Notes	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Notes field.

FireFlow specific fields

Organization	Type the name of the LDAP server user field from which you want to import data to the FireFlow Organization field.
Address	Type the name of the LDAP server user field from which you want to import data to the FireFlow Address field.
City	Type the name of the LDAP server user field from which you want to import data to the FireFlow City field.
State	Type the name of the LDAP server user field from which you want to import data to the FireFlow State field.
Zip Code	Type the name of the LDAP server user field from which you want to import data to the FireFlow Zip Code field.
Country	Type the name of the LDAP server user field from which you want to import data to the FireFlow Country field.
Home Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Home Phone field.

Work Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Work Phone field.
Mobile Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Mobile Phone field.
Pager	Type the name of the LDAP server user field from which you want to import data to the FireFlow Pager field.

Fetch user data from the SSO Provider (the IdP)

Select **IDP** and complete the fields as needed. For details, see:

- [Fields Mapping fields](#)
- [FireFlow specific fields](#)

When complete, continue with [step 4](#).

Fields Mapping fields

Full Name	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Full Name field.
Email	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Email field.
Notes	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Notes field.

FireFlow specific fields

Organization	Type the name of the LDAP server user field from which you want to import data to the FireFlow Organization field.
Address	Type the name of the LDAP server user field from which you want to import data to the FireFlow Address field.
City	Type the name of the LDAP server user field from which you want to import data to the FireFlow City field.

State	Type the name of the LDAP server user field from which you want to import data to the FireFlow State field.
Zip Code	Type the name of the LDAP server user field from which you want to import data to the FireFlow Zip Code field.
Country	Type the name of the LDAP server user field from which you want to import data to the FireFlow Country field.
Home Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Home Phone field.
Work Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Work Phone field.
Mobile Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Mobile Phone field.
Pager	Type the name of the LDAP server user field from which you want to import data to the FireFlow Pager field.

4. To set a default mail domain, select **Default Mail Domain**, and enter the URL.

When this option is configured, AFA automatically generates an email address for users by attaching the specified email suffix to its username (when an email address is not provided).

5. At the bottom of the page, click **OK**. Changes to user authentication settings immediately take effect.

Optionally, do any of the following:

Encrypt communication between ASMS and your SSO Provider

If you must encrypt communication between ASMS and your IdP (the SSO Provider), have the IdP create a certificate for ASMS to use. This is the default behavior for most IdPs.

Do the following:

1. Open a terminal and log in as user **afa**.
2. Save the IdP's certificate in a Base-64 encoded PEM format to **/usr/share/fa/simplesaml/cert/**.

Tip: The default filename is **server.crt**. We recommend that you use a different filename, as this default file is overwritten during upgrades.

3. If you saved the file under a name other than **server.crt**, configure the name of the IdP certificate file.

Do the following:

- a. Navigate to the **/home/afa/.fa/config** configuration file, and open it for editing.
- b. Add the **SSOSAML_IdP_Certificate** parameter, and define its value as the name of the IdP certificate file.

For example:

```
SSOSAML_IdP_Certificate=MyIdPCert.cr
```

Configure IdP-initiated, or unsolicited, SSO

By default, ASMS uses **SP-initiated**, or **solicited SSO**, in which the SP signs the Assertion Certificate passed between the two systems. This is the recommended usage.

ASMS also supports **IdP-initiated**, or **unsolicited SSO**, in which the IdP signs the Assertion Certificate instead.

While both scenarios have users access ASMS using the ASMS URL, the method used may affect parameter values in the system configuration.

Do the following:

1. In the AFA Administration area, navigate to the **Options > Advanced Configuration** tab.
2. Add the following parameters and their values, one at a time:

SSOSAML_IdP_Unsolicited_SSO	Yes/No. Specifies whether to use the IdP method first.
SSOSAML_IdP_Unsolicited_SSO_URL	The IdP's URL.
SSOSAML_IdP_Unsolicited_SSO_SP_ID_KEY	The parameter name for the SP unique identifier.

For more details, see [Advanced Configuration](#).

Configure a customized UID parser

Various IdPs have different response formats, and yours may not match the format expected by ASMS.

If you cannot configure the response format to match ASMS's expectation, define a customer UID parser to translate the responses.

Do the following:

1. View the response format being sent to ASMS:
 - a. Switch to **Debug** mode.
 - b. Log in to ASMS again, and navigate to the **public_html/algosec/.ht-fa-history** log file.
 - c. Search for the debug log and find the user attributes received, including the object returned and its structure.
2. Create the customer UID parser as follows:
 - a. On the ASMS server, create the following new directory:
/usr/share/fa/php/site

- b. Copy the original parser from `/usr/share/fa/php/SampleUIDParser.php` to `/usr/share/fa/php/site/<parser name>.php`, giving it a meaningful name.
- c. Open the `/usr/share/fa/php/site/<parser name>.php` file for editing, and modify the file so that the `parseUID` function returns the value you expect. By default the function returns `"$userAttributes['UID'][0]"`.
- d. Change your parser permissions by running:

```
-rw-r----- root apache
```

3. Set PHP to include files from the `/usr/share/fa/php/site/` directory. Do the following:

- a. Browse to and open the `/etc/php.ini` file for editing.
- b. Change the PHP include path directive to include the new directory:

```
include_path =  
"./usr/share/fa/phplib:/usr/share/fa/php:/usr/share/fa/php/inc:/usr/share/fa/php/site"
```

- c. Configure AFA to use the new UID parser. In the `~afa/.fa/config` configuration file, add the following attribute:

```
UID_PARSER_NAME=<parser name>
```

- d. Restart Apache server. Run:

```
/etc/init.d/httpd restart
```

Force local authentication

ASMS enables users to log in directly to ASMS, without using SSO, even when SSO is configured. For example, this may be helpful if your IdP is down, or if there are configuration errors.

Note: Forcing local authentication uses direct ASMS logins, and requires that users

are defined locally in ASMS.

Do the following:

Navigate to ASMS, with the additional `ForceLocalAuth=1` string added on to the end of the URL.

For example: `https://<Algosec Server>/algosec/suite/login.html?ForceLocalAuth=1`

The local ASMS login page appears, and users can log in using ASMS credentials.

Troubleshoot SSO configuration

If an SSO error occurs, the browser displays an error page instead of ASMS.

Error messages often show as `SimpleSAML_Error_Error` errors, and contain a UUID that can be used to locate the event in the `.ht-fa-history` log file. There, following the instructions indicated as **ACTION REQUIRED**.

Common errors include:

<p>Time assertion failures, such as:</p> <ul style="list-style-type: none"> • <code>[message:protected] => Received an assertion that is valid in the future. Check clock synchronization on IdP and SP.</code> • <code>[message:protected] => Received an assertion that is valid in the future. Check clock synchronization on IdP and SP.</code> 	<p>Check the clock configurations on the ASMS machine and the SSO Provider. Both of these clocks must be synchronized, including timezone.</p>
<p>Lost sessions and STATE-related errors</p>	<p>Verify that the SSO Provider directs the user to ASMS using the same hostname as accessed by the user.</p>

<p>cause:SimpleSAML_Error_ Exception:private] => SimpleSAML_Error_UnserializableException Object</p>	<p>The message cannot be parsed. It may have been encrypted, and the SSO Provider certificate not defined.</p> <p>Place the SSO Provider certificate in the following directory, and define it's name in the AFA configuration file: /usr/share/fa/simplesaml/cert/</p>
<p>[message:protected] => saml20-idp-remote/'Test': Could not find PEM encoded certificate in "/usr/share/fa/simplesaml/cert/server.crt".</p>	<p>The certificate may have an incorrect format.</p> <p>Ensure that the certificate format is PEM.</p>
<p>Users are able to connect from expired sessions</p>	<p>If a user is able to log in to ASMS, even if the ASMS session timeout period has passed, verify whether the ASMS timeout and the SSO Provider timeout are configured correctly.</p> <p>The ASMS session timeout must be set to a time limit equal or greater than the SSO Provider's session timeout.</p>

Disable SSO configuration

If your SSO configuration behaves unexpectedly, you may want to disable it while you troubleshoot the issues.

Do the following:

1. Log in to the ASMS server or Central Manager as user **root**.
2. Navigate to the **/home/afa/.fa/config** file, and open it for editing.
3. Set the **Use_SSO** value to **no**.

SSO is disabled. Log in to ASMS using a user defined in ASMS directly.

User authentication via authentication servers

The AlgoSec Security Management Suite (ASMS) supports authenticating users via an authentication server in the following ways:

Local user database	<p>The AlgoSec Security Management Suite maintains a local user database that is composed of the usernames and passwords of users you have added. When a user attempts to log in, the AlgoSec Suite compares the entered username and password to the local user database. If the entered username exists in the database, and the password matches the username, then the user is logged in.</p>
LDAP server	<p>If your company uses an LDAP (Lightweight Directory Access Protocol) server for authenticating network users (for example, Microsoft Active Directory), you can configure the AlgoSec Suite to authenticate users against the LDAP server. When a user attempts to log in (using the login credentials defined for them on the LDAP server), the AlgoSec Suite sends the entered username and password to the LDAP server. If the entered username exists in the LDAP server, and the password matches the username, then the user is logged in. The user will automatically be added to ASMS, allowing you to manage the user in the ASMS web interface.</p> <p>If desired, you can configure additional criteria for authentication. For example, you can specify that the LDAP server should only search certain parts of its database for the entered username and password, or that users must belong to a certain LDAP user group.</p> <p>The AlgoSec Suite additionally supports importing user data, such as permissions and roles, from an LDAP Server. When this is configured, each user is automatically assigned roles based on their LDAP groups.</p> <p>Note: It is possible to use multiple LDAP servers to authenticate users. For more details, see Import user data from an LDAP server.</p>

RADIUS server	<p>Some companies use a RADIUS (Remote Authentication Dial In User Service) server for authenticating network users. The AlgoSec Security Suite can be configured to use the corporate RADIUS server to authenticate users. When a user attempts to log in (using the login credentials defined on the RADIUS server), ASMS sends the entered username and password to the RADIUS server. If the entered username exists in the RADIUS database, and the password matches the username, then the user is logged in. The user will automatically be added to ASMS, allowing you to manage the user in the ASMS web interface.</p> <p>The AlgoSec Suite additionally supports importing data from an LDAP server for RADIUS authenticated users. See Import user data from an LDAP server.</p> <p>Note: Microsoft Active Directory can be configured as a RADIUS server. For information on configuring Active Directory, refer to Microsoft documentation.</p>
----------------------	--

By default, the AlgoSec Security Suite uses the local user database to authenticate users. If you want to use a RADIUS server and/or an LDAP server in addition to local authentication, you must configure the desired user authentication method using the following procedure.

Note: When more than one user authentication method is enabled, you can choose which method to use on a per-user basis.

If importing user data from an LDAP server is not configured, you must manually define privileged users in AFA.

Configure user authentication via an authentication server

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select Administration.

The **Administration** page appears, displaying the **Options** tab.

3. In the Options tab, click the Authentication sub-tab.

The **Authentication** page appears.

The screenshot shows the Firewall Analyzer interface. The top navigation bar includes "Firewall Analyzer", "Analysis Status", and "AlgoSec Administrator". The main content area is titled "Administration" and has several tabs: "DEVICES SETUP", "USERS/ROLES", "SCHEDULER", "COMPLIANCE", "OPTIONS", "MONITORING", "DOMAINS", and "ARCHITECTURE". The "OPTIONS" tab is selected, and within it, the "Authentication" sub-tab is active. The "Authentication" sub-tab contains the following sections:

- User Authentication**
 - Authentication Server
 - Local RADIUS LDAP
 - The Authentication server is case-sensitive
 - Single Sign On
- Radius Authentication**
 - Server:
 - Secret key:
 - Port:
 - Timeout:
 -
 - Fetch user data from LDAP (?)
 - Use Secondary Servers
- Default for new users:**
 - Local
 - Radius
 - LDAP
- Default Mail Domain:**
 -
 - For example: "Algosec.com"
- CyberArk**
 - Allow to setup devices with CyberArk credentials management (?)
 - 
 - Default values (Optional):**
 - Platform (Policy ID):
 - Safe:
 - Folder:

At the bottom of the form, there are "Cancel" and "OK" buttons.

4. Choose Authentication Server.

Note: The **Local** check box is selected by default and cannot be cleared.

5. To enable user authentication using a corporate RADIUS server:

a. Select the **RADIUS** check box.

Radius Authentication fields appear.

The screenshot shows the 'Administration' console for 'Firewall Analyzer'. The 'Options' tab is active, and the 'Authentication' sub-tab is selected. Under 'User Authentication', the 'Authentication Server' section has 'Local' checked and 'RADIUS' selected. The 'Radius Authentication' section includes input fields for 'Server', 'Secret key', 'Port' (set to 1812), and 'Timeout' (set to 3), with a 'Test connectivity' button. Below these are checkboxes for 'Fetch user data from LDAP' and 'Use Secondary Servers'. The 'Default for new users' section has 'Local' selected, and the 'Default Mail Domain' section has an empty text field. 'Cancel' and 'OK' buttons are at the bottom.

b. Complete the fields as needed. If you selected the **Use Secondary Servers** check box, additional fields appear.

For details, see [RADIUS authentication fields](#).

6. To enable user authentication against an LDAP server:

a. Select the **LDAP** check box.

New fields appear.

LDAP Authentication

LDAP Server Credentials

Server:

LDAP Version:

Port:

Timeout:

Secure Connection

Bind Type:

User DN (?):

Password:

Attribute Mapping

Name:

Group Membership:

Permitted Users

Users Under Base DN (?):

Members of Group DN (?):

Extra Filtering:

Fetch user data from LDAP

Use Secondary Servers

- b. Complete the fields using the information in LDAP Authentication Fields (see [LDAP authentication fields](#)).

If you selected the **Use Secondary Servers** or **Fetch user data from LDAP** check boxes, additional fields appear.

Continue completing the fields using the information in LDAP Authentication Fields (see [LDAP authentication fields](#)).

7. To test connectivity for a defined RADIUS or LDAP server, click **Test connectivity** for

the specific server.

A message informs you whether AFA connected to the server successfully.

8. In the **Default for new users** area, choose the default authentication method for new users.

Note: You can override the default authentication method to use on a per-user basis.

9. To set a default mail domain, select **Default Mail Domain**, and type the URL.

When this option is configured, AFA automatically generates an email address for users by attaching the specified email suffix to its username (when an email address is not provided).

10. Click **OK**.

Changes to user authentication settings immediately take effect.

RADIUS authentication fields

In this field...	Do this...
Server	Type the IP address of the RADIUS server's host computer.
Secret key	Type the secret key to use for authenticating to the RADIUS server.
Port	Type the port number on the RADIUS server's host computer.
Timeout	Use the arrow buttons to select the maximum amount of time in seconds to wait for the RADIUS server's reply.

In this field...	Do this...
Fetch user data from LDAP	<p>Select this option to fetch user data from an LDAP server.</p> <p>AFA will perform authentication (check passwords) against the defined RADIUS server, but will also access the specified LDAP server to obtain user information and optionally assign roles.</p> <p>Important: When this option is selected, you must additionally define the LDAP server and configure the import with the Fetch user data from LDAP check box.</p> <p>For more information, see Importing User Data from an LDAP Server (see Import user data from an LDAP server).</p>
Use Secondary Servers	<p>Select this option to configure one or more secondary RADIUS servers.</p> <p>You must complete the fields in the Secondary Radius Servers area.</p>

LDAP authentication fields

In this field...	Do this...
LDAP Server Credentials	
Server	Type the IP address of the LDAP server's host computer.
LDAP Version	Select the version of LDAP used on the LDAP server.
Port	Type the port number on the LDAP server's host computer.
Timeout	Use the arrow buttons to select the maximum amount of time in seconds to wait for the LDAP server's reply.
Secure Connection	<p>Select this option to secure connections with the LDAP server, then choose the method to use for securing the connection: LDAPS or StartTLS.</p> <p>The default method is LDAPS.</p> <p>The value of the Port field changes according to the method selected.</p>

In this field...	Do this...
Verify Server Certificate	<p>Select this option to specify that AFA should check the LDAP server's certificate against a locally stored certificate. AFA will only connect to the LDAP server if the certificates are identical.</p> <p>The CA Certificate field appears.</p>
CA Certificate	<p>Select the locally stored certificate against which AFA should compare the LDAP server's certificate.</p> <p>The certificate must be stored under <code>/home/afa/.fa/ca_certs</code> in order to appear in the drop-down list.</p>
Bind Type	<p>Select the bind type to use:</p> <ul style="list-style-type: none"> • Simple. AFA sends the entered username and password to the LDAP server. If the entered username exists in the LDAP server, and the password matches the username, then the user is logged in. • Regular. AFA logs in to the LDAP server using a user DN and password, and then checks the entered username and password against the LDAP server. If the entered username exists in the LDAP server, the password matches the username, <i>and any additional criteria are met</i>, then the user is logged in. • Anonymous. AFA accesses the LDAP server anonymously, and then checks the entered username and password against the LDAP server. If the entered username exists in the LDAP server, the password matches the username, <i>and any additional criteria are met</i>, then the user is logged in. <p>If you chose Regular or Anonymous, additional fields appear.</p> <p>The default value is Regular.</p>
User DN	<p>Type the user DN that AFA should use to log in to the LDAP server.</p> <p>This field appears only for Regular bind type.</p>
Password	<p>Type the password that AFA should use to log in to the LDAP server.</p> <p>This field appears only for Regular bind type.</p>
Attribute Mapping	

In this field...	Do this...
Name	<p>Type the attribute that contains a user's name, in user objects in the database.</p> <p>The default value is <code>sAMAccountName</code>.</p>
Group Membership	<p>Type the attribute that contains a user's groups, in user objects in the database.</p> <p>The default value is <code>member</code>.</p>
Permitted Users	
Users Under Base DN	<p>Type the base DN.</p> <p>The baseDN is the highest level in the LDAP tree, where AFA should search. Any entries above this level will not be searched.</p>
Members of Group DN	<p>Type the DN of the LDAP group that includes all users who may log in to AFA and FireFlow.</p> <p>This field is optional. When it is filled in, users who are not members of this LDAP group will not be allowed to log in to AFA or FireFlow, even if they are members of other LDAP groups mapped to AFA or FireFlow roles.</p> <p>Note: This LDAP group includes all FireFlow requestors. When this field is filled in, only users who are members of this group are allowed to submit requests to FireFlow.</p>
Extra Filtering	<p>Type any additional criteria that users must meet in order to be authenticated.</p> <p>The default value is <code>(objectClass=*)</code>.</p>

In this field...	Do this...
Fetch user data from LDAP	<p>Select this option to import user data from the LDAP server upon each login. For example, when a user logs in, data such as the user's telephone number can be imported.</p> <p>You must complete the fields in the Fields Mapping area.</p> <p>Note: The default values for these fields are taken from Active Directory. If a different LDAP server is used, the names must be changed accordingly.</p> <p>Since data is imported only upon user login, the data stored for users who log in infrequently may be outdated.</p>
Fields Mapping	
Associated Roles	<p>Select this option to import user group information from the LDAP server. Selecting this option enables assigning user roles via a specified correspondence between LDAP groups and AFA, FireFlow, or AppVizroles.</p> <p>To manage roles from within the AlgoSec Suite (not the LDAP), do not select this option.</p>
Full Name	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Full Name field.
Email	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Email field.
Notes	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow Notes field.
FireFlow specific fields	
Organization	Type the name of the LDAP server user field from which you want to import data to the FireFlow Organization field.

In this field...	Do this...
Address	Type the name of the LDAP server user field from which you want to import data to the FireFlow Address field.
City	Type the name of the LDAP server user field from which you want to import data to the FireFlow City field.
State	Type the name of the LDAP server user field from which you want to import data to the FireFlow State field.
Zip Code	Type the name of the LDAP server user field from which you want to import data to the FireFlow Zip Code field.
Country	Type the name of the LDAP server user field from which you want to import data to the FireFlow Country field.
Home Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Home Phone field.
Work Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Work Phone field.
Mobile Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow Mobile Phone field.
Pager	Type the name of the LDAP server user field from which you want to import data to the FireFlow Pager field.
Use Secondary Servers	Select this option to configure one or more secondary LDAP servers. You must complete the fields in the Secondary LDAP Servers area. (See LDAP Server Credentials at top of this table.)

Import user data from an LDAP server

Whether you are authenticating users with an LDAP or RADIUS authentication server, you can configure ASMS to import user data from an LDAP server. Upon each login, ASMS will fetch the user's full name and email address, as well as roles and inherited permissions. All of this information will be updated for the users on the AlgoSec server.

Note: This procedure is only relevant when *authenticating* with an LDAP or RADIUS authentication server. If you want to fetch data from an LDAP, but authenticate with SSO, see [Configure user authentication](#).

Note: If the system is configured to import user information from an LDAP server, changes to user settings must be made only on the LDAP server (changes made in the AlgoSec Suite may be overridden the next time the user logs in).

Note: The data stored for users who log in infrequently may be outdated. Each user's information is fetched and updated upon login; in addition to name and email, this includes the list of roles the user is assigned, the list of permissions the user inherits, and the list of users assigned the fetched roles.

Do the following:

1. Configure LDAP or RADIUS user authentication. For details, see [User authentication via authentication servers](#).
 - When authenticating with an LDAP server, select the **Fetch user data from LDAP** check box and complete the fields in the **Fields Mapping** area.
 - When authenticating with a RADIUS server, do the following:
 - a. Select the **Fetch user data from LDAP** check box in the RADIUS Authentication fields area.
 - b. Additionally define the LDAP, select the **Fetch user data from LDAP** check box and complete the fields in the **Fields Mapping** area.

Note: Many fields in FireFlow appear as options for mapping data.

2. Click **OK**.
3. If you selected the **Associated Roles** option, indicate a correspondence between

LDAP groups and AlgoSec Suite roles doing the following:

4. Add/Edit the user role you want to link with an LDAP group. For details, see [Manage users and roles in AFA](#).
5. Type the LDAP group name that you want to link with the role in the **Role LDAP DN** field.

When users log in that are members of this LDAP group, they will automatically be granted the role.

Configure an LDAP forest

If you have multiple LDAP servers with different users defined on each one, you can configure an *LDAP forest* consisting of these servers. AFA and FireFlow will authenticate LDAP users against the correct LDAP server.

Complete this procedure for each LDAP server you want to include in the forest.

Do the following:

1. Choose a number to represent the LDAP server.

Number 1 represents the primary LDAP server, and numbers 2 and 3 represent possible backup servers. If you do not want those servers to be included in the forest, choose a number higher than 3.

2. In the toolbar, click your username.

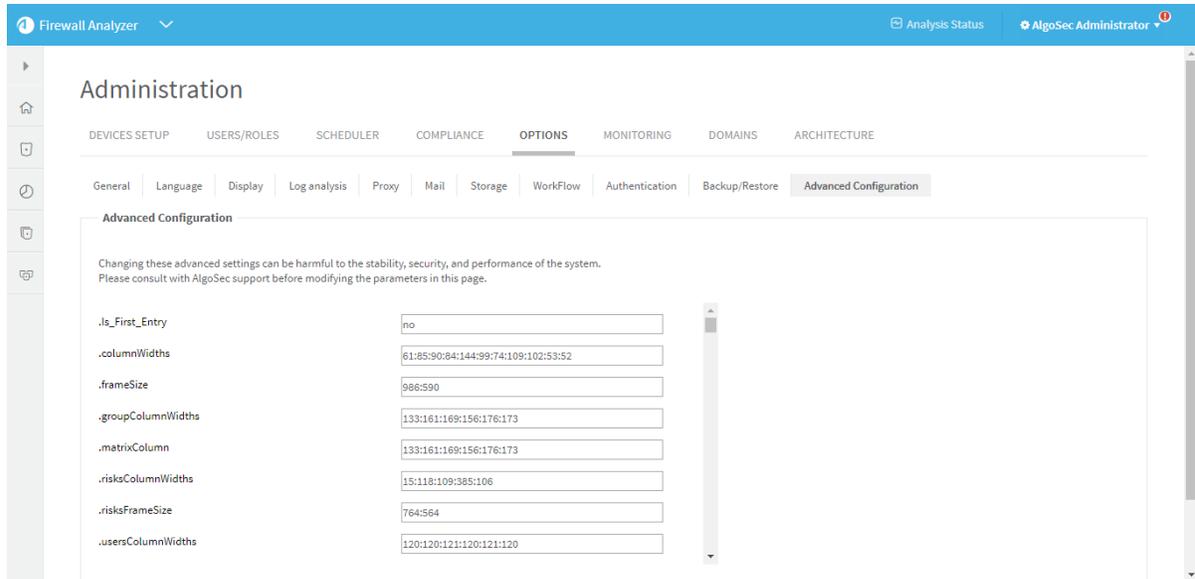
A drop-down menu appears.

3. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

4. In the **Options** tab, click the **Advanced Configuration** sub-tab.

The **Advanced Configuration** page appears.



5. Add the parameters specified in LDAP Parameters (see [LDAP parameters](#)), one at a time, by doing the following:

- a. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

- b. In the **Name** field, type `ParamNumber`

Where:

- `Param` is the parameter name.
- `Number` is the server number selected in the previous step.

For example, to specify the port number of LDAP server number 4, type `LDAP_Port4`.

- c. In the **Value** field, type the parameters value.
- d. Click **OK**.

- e. Repeat the above steps for each parameter.
- f. Click OK.

LDAP parameters

Set this parameter...	To this...
LDAP_Port	The port number on the LDAP server's host computer. This parameter is mandatory.
LDAP_Timeout	The maximum amount of time in seconds to wait for the LDAP server's reply. This parameter is mandatory.
LDAP_Version	The version of LDAP used on the LDAP server. This parameter is mandatory.
Ldap_Secured_Authentication_Method	The method to use for securing connections with the LDAP server. This can have the following values: <ul style="list-style-type: none"> • ldaps • starstls This parameter is mandatory.
LDAP_Server	The IP address of the LDAP server's host computer. This parameter is mandatory.
LDAP_UseSecured	Indicates whether to secure connections with the LDAP server. This can have the following values: <ul style="list-style-type: none"> • yes • no This parameter is mandatory.

Set this parameter...	To this...
LDAP_VerifyCert	<p>Indicates whether AFA should check the LDAP server's certificate against a locally stored certificate. AFA will only connect to the LDAP server if the certificates are identical.</p> <p>This can have the following values:</p> <ul style="list-style-type: none"> • yes • no <p>This parameter is mandatory.</p>
LDAP_Certificate	<p>The locally stored certificate against which AFA should compare the LDAP server's certificate.</p> <p>The certificate must be stored under <code>/home/afa/.fa/ca_certs</code>.</p> <p>This parameter is mandatory.</p>
LDAP_Domain	<p>The LDAP server's domain name.</p> <p>This parameter is mandatory.</p>
LDAP_Username	<p>The user DN that AFA should use to log in to the LDAP server.</p> <p>This parameter is optional.</p>
LDAP_Password	<p>The password that AFA should use to log in to the LDAP server.</p> <p>This parameter is optional.</p>

Set this parameter...	To this...
LDAP_Bind_Type	<p>The bind type to use. This can have the following values:</p> <ul style="list-style-type: none"> • <i>Simple</i>. AFA sends the entered username and password to the LDAP server. If the entered username exists in the LDAP server, and the password matches the username, then the user is logged in. • <i>Regular</i>. AFA logs in to the LDAP server using a user DN and password, and then checks the entered username and password against the LDAP server. If the entered username exists in the LDAP server, the password matches the username, <i>and</i> any additional criteria are met, then the user is logged in. • <i>Anonymous</i>. AFA accesses LDAP server anonymously, and then checks the entered username and password against the LDAP server. If the entered username exists in the LDAP server, the password matches the username, <i>and</i> any additional criteria are met, then the user is logged in. <p>This parameter is optional.</p>
LDAP_BaseDN	<p>The base DN.</p> <p>This parameter is optional.</p>
LDAP_ExtraFiltering	<p>Any additional criteria that users must meet in order to be authenticated.</p> <p>The default value is <code>(objectClass=*)</code>.</p> <p>This parameter is optional.</p>
LDAP_NameAttr	<p>The attribute that contains a user's name, in user objects in the database.</p> <p>This parameter is optional.</p>
LDAP_MemberAttr	<p>The attribute that contains a user's groups, in user objects in the database.</p> <p>This parameter is optional.</p>

Set this parameter...	To this...
LDAP_GroupDN	<p>The DN of the user group to which users must belong in order to be authenticated.</p> <p>This parameter is optional.</p>
LDAP_AttrEmail	<p>The name of the LDAP server user field from which you want to import data to AFA and FireFlow Email field.</p> <p>This parameter is optional.</p>
LDAP_AttrFullName	<p>The name of the LDAP server user field from which you want to import data to AFA and FireFlow Full Name field.</p> <p>This parameter is optional.</p>
LDAP_AttrNotes	<p>The name of the LDAP server user field from which you want to import data to AFA and FireFlow Notes field.</p> <p>This parameter is optional.</p>
LDAP_AttrOrganization	<p>The name of the LDAP server user field from which you want to import data to the FireFlow Organization field.</p> <p>This parameter is optional.</p>
LDAP_AttrAddress1	<p>The name of the LDAP server user field from which you want to import data to the FireFlow Address field.</p> <p>This parameter is optional.</p>
LDAP_AttrCity	<p>The name of the LDAP server user field from which you want to import data to the FireFlow City field.</p> <p>This parameter is optional.</p>
LDAP_AttrState	<p>The name of the LDAP server user field from which you want to import data to the FireFlow State field.</p> <p>This parameter is optional.</p>
LDAP_AttrZip	<p>The name of the LDAP server user field from which you want to import data to the FireFlow Zip Code field.</p> <p>This parameter is optional.</p>

Set this parameter...	To this...
LDAP_ AttrCountry	The name of the LDAP server user field from which you want to import data to the FireFlow Country field. This parameter is optional.
LDAP_ AttrHomePhone	The name of the LDAP server user field from which you want to import data to the FireFlow Home Phone field. This parameter is optional.
LDAP_ AttrWorkPhone	The name of the LDAP server user field from which you want to import data to the FireFlow Work Phone field. This parameter is optional.
LDAP_ AttrMobilePhone	The name of the LDAP server user field from which you want to import data to the FireFlow Mobile Phone field. This parameter is optional.
LDAP_ AttrPagerPhone	The name of the LDAP server user field from which you want to import data to the FireFlow Pager field. This parameter is optional.
LDAP_ AttrCustom	The name of a custom FireFlow attribute. This parameter is optional.

LDAP forest example

In the following example, LDAP server 4 is added to the forest:

```
LDAP_Port4=349
LDAP_Timeout4=120
LDAP_Version4=3
Ldap_Secured_Authentication_Method4=LDAPS
LDAP_Server4=192.164.2.43
LDAP_UseSecured4=no
LDAP_VerifyCert4=no
LDAP_Certificate4=Algosec_CA.pem
```

```
LDAP_Domain4=ldomain4
LDAP_Username4=CN=Bob,OU=Algosec,DC=algosec,DC=local
LDAP_Password4=$FOQABRER$27:A3:BD:F2:90:C7:21:5A:3A:F4:F4:AB:R8:20:6F:25
LDAP_Bind_Type4=Regular
LDAP_BaseDN4=dc=algosec,dc=local
LDAP_ExtraFiltering4=(objectClass=*)
DAP_NameAttr4=sAMAccountName
LDAP_MemberAttr4=memberOf
LDAP_GroupDN4=
LDAP_AttrEmail4=mail
LDAP_AttrFullName4=displayName
LDAP_AttrNotes4=description
LDAP_AttrOrganization4=company
LDAP_AttrAddress14=streetAddress
LDAP_AttrCity4=l
LDAP_AttrState4=st
LDAP_AttrZip4=postalCode
LDAP_AttrCountry4=co
LDAP_AttrHomePhone4=homePhone
LDAP_AttrWorkPhone4=telephoneNumber
LDAP_AttrMobilePhone4=mobile
LDAP_AttrPagerPhone4=pager
LDAP_AttrCustom4=group,primaryGroupID;allowDial,msNPAllowDialin;mark,
department
```

Log in when an LDAP forest is configured

Do the following:

1. In the AFA or FireFlow **Login** page, type the following in the **Username** field:

LdapDomain\userName

Where:

- `LdapDomain` is the domain name of the LDAP server on which they are defined.
- `userName` is the user's LDAP username.

For example, if Bob is defined on an LDAP server whose domain name is `Ldomain4`, then he must type "Ldomain4\Bob" in the **Username** field.

2. In the **Password** field, type your LDAP password.
3. Click **Login**.

Note: The backup servers will *not* be consulted, in the event that AFA/FireFlow did not locate the user in the specified LDAP domain.

Manage users and roles in AFA

This topic describes how to manage AFA users and roles in the AFA **Administration** area.

Note: If you have an authentication server or SSO configured, user credentials must be managed on your external server. If your user roles are assigned based on LDAP group membership, roles must be managed on the LDAP server. In these cases, any changes made directly in AFA are overwritten the next time the user logs in. For more details, see [Configure user authentication](#).

Tip: AFA users and roles provide the basis for authentication across both AFA and FireFlow. If you are an AFA administrator, but not a FireFlow administrator, you can also access FireFlow role and user management via the AFA **Administration** area.

Add or edit users

This procedure describes how to add and edit AFA users directly in the AFA database.

Tip: Alternately, manage users via an authentication server or SSO, or import users

via a CSV file. For details, see [Configure user authentication](#) or [Import users via CSV](#).

Do the following:

1. Click your username at the top-right to access the AFA **Administration** area.
2. Click the **USERS/ROLES** tab to display the user and role tables. For example:

The screenshot shows the 'Administration' section of the Firewall Analyzer interface. The 'USERS/ROLES' tab is selected. The page title is 'Administration'. Below the title are several tabs: DEVICES SETUP, **USERS/ROLES**, SCHEDULER, COMPLIANCE, OPTIONS, MONITORING, DOMAINS, and ARCHITECTURE. A sub-header reads 'Manage the users, roles, their permissions and configurations'. There are two tables:

	Fullname	Email	Notification	Username	Admin	FireFlow Admin	Notes	Edit
<input type="checkbox"/>	afademo	afademo@algosec.com	✓	afademo	✓			
<input type="checkbox"/>	AlgoSec Administrator	admin@company.com	✓	admin	✓			
<input type="checkbox"/>	FA	afademo@a.com	✓	A	✓	✓		
<input type="checkbox"/>	FireFlow	some_email_not_used@somewhere.org		FireFlow_batch				
<input type="checkbox"/>	harry helpdesk	harry@company.com		harry				
<input type="checkbox"/>	Ned NetOps	ned@company.com	✓	ned	✓	✓	Firewall Administrator	
<input type="checkbox"/>	Sue Security	sue@company.com	✓	sue			Information Security	

Below the table are 'Delete' and 'New' buttons. Below the table is another table for roles:

	Role Name	Role Description	Edit
<input type="checkbox"/>	Admins	AFA + FF Admins - full access	
<input type="checkbox"/>	helpdesk	For helpdesk staff - query only	

Below the role table are 'Delete' and 'New' buttons. At the bottom left, there are links: 'Manage FireFlow roles' and 'Manage FireFlow requestors'.

3. To add a new user, click the **New** button below the user table. To edit an existing user, click the edit button at the right side of the row you want to edit.

In the user form that appears, select and enter values as needed:

User details

Username	<p>Enter a username for the user.</p> <p>Usernames can contain any alpha-numeric character and the following special characters: "@", "_", ".", or "-". See ASMS username and password requirements.</p>
-----------------	--

Full name	Enter the user's full name.
E-Mail	Enter the user's e-mail address.
Notes	Enter any notes about the user.
Authentication	<p>Select how to authenticate this user:</p> <ul style="list-style-type: none"> • Local. Authenticate the user against the local ASMS user database. • RADIUS. Authenticate the user against a RADIUS server. • LDAP. Select this option to enable user authentication against an LDAP server. <p>For more details, see Configure user authentication.</p>
Landing Page	<p>Select Firewall Analyzer or FireFlow. Select Automatic to use the default landing page for the selected role.</p> <p>For more details, see Default landing pages per role.</p>

Password

New password	<p>Enter a password for the user.</p> <p>Passwords can contain any alpha-numeric character or any special character, excluding back ticks (`). See ASMS username and password requirements.</p>
Confirm password	Re-enter the password you entered in the New password field.

General Permissions

Select any of the following options for this user:

Administrator	Make the user an administrator.
FireFlow Administrator - Allow FireFlow Advanced Configuration	Make the user a FireFlow configuration administrator. This enables the user to perform advanced configuration tasks in FireFlow.

Enable Analysis from file	Allow the user to perform analyses from configuration files.
Enable Trusted Traffic -> global	Allow the user to view trusted traffic.

Roles

Select the user roles to assign to the user. The user is automatically granted permissions specified in the assigned roles.

Tip: If you assign additional permissions to this user, the user will have both the permissions inherited from their roles, as well as additional permissions assigned to the user.

Email Notifications

Define the scenarios in which this user receives notifications from AFA:

Changes in risks	The user is notified for each change detected in risks.
Changes in policy	The user is notified for each change detected in policies.
Every group report	The user is notified for each group report generated.
Every report	The user is notified for each report generated.
Every configuration change	The user is notified for each configuration change detected.

Rules and VPN Users about to expire	<p>The user is notified when device rules and/or VPN users are about to expire.</p> <p>Tip: To configure the number of days before rule or VPN user expiration that AFA should send a notification, complete the Days before expiration alerts field in the General sub-tab of the Options tab in the Administration area.</p> <p>For details, see Define AFA preferences.</p>
Error messages	<p>The user receives error messages from AFA, such as for low disk space and license expiration.</p> <p>This option is relevant for administrators only.</p>
Changes in customization	<p>The user is notified for each customization change detected, such as for topology, trusted traffic, and risk profile customizations.</p> <p>This option is relevant for administrators only.</p>
Hide change details	<p>User notification emails include only device names and a link to the AFA.</p> <p>Specific details about new reports and change alerts are omitted from emails to this user.</p> <p>Tip: Alternately, hide change details for all user notifications. For details, see the hide_change_details parameter.</p>

Authorized Views and Actions

Select the items this user can view or perform as follows:

Report	<p>Select the report pages/information that the user can view. Select Full Report to indicate that the user can view all report information.</p> <p>Pages that are not selected will be inaccessible to the user.</p> <p>Note: A user can only be given access to Configuration and Logs information if they have access to the Explore Policy page.</p>
---------------	--

Home Views	<p>Select the Home page elements that the user can view. Select All Home Views To indicate that the user can view all Home page elements.</p> <p>Pages that are not selected will be inaccessible to the user.</p>
Reporting Tool	<p>Select this option to allow the user to access the AlgoSec Reporting Tool (ART).</p> <p>Note: Non-administration users that open the Reporting Tool will only see data relevant to the user's allowed firewalls.</p>
Actions	<p>Select the actions that the user can perform in AFA. Select All Actions to indicate that the user can perform all actions.</p> <p>Controls used to perform actions that are not selected will be disabled.</p>

Authorized Devices

Select the user's default access level to devices. Do the following:

- a. Select a default permission profile to determine the permission level for the selected devices.
- b. Click **Select devices....** to select the devices you want to apply the selected permission level on.
The device tree appears.
- c. Select the checkboxes next to each relevant device and click **OK**.

A table appears with your selected devices and permissions.

For example:

Authorized Devices

Default permission profile: Standard ▼

Device/Group	Permission profile	Notification
Rose_checkpoint	Read only ▼	<input checked="" type="checkbox"/>
birch iptables	Read only ▼	<input checked="" type="checkbox"/>
Rose_DR	Standard ▼	<input checked="" type="checkbox"/>
Oak_Stonegate	Standard ▼	<input checked="" type="checkbox"/>

[Select devices...](#)

If needed, do either of the following:

- Select a different option from the **Permission profile** dropdown to change the profile for a specific device
- Clear or re-select the **Notification** checkbox to change notification settings for a specific device

7. Click **OK** to save your changes.

Default landing pages per role

ASMS is configured with specific landing pages per user or role. Change this default to display a different page as needed.

- Landing pages configured for specific users override any configuration for a user's role.
- Users with multiple roles, with different landing pages for each role, will see the landing page with the highest priority.

Landing pages are prioritized for FireFlow first, and then AFA.

If no landing page is defined for the user, or any of the user's roles, landing pages are defined as follows:

Permissions	Landing page
Administrators	AlgoSec Firewall Analyzer

Permissions	Landing page
AFA Users	First FireFlow, if licensed and activated, and then AFA.
Requestors (unprivileged users)	AlgoSec Firewall Analyzer

Add and edit user roles

This procedure describes how to add and edit user roles.

Tip: If you have an LDAP server configured, associate AFA user roles with specific LDAP user groups to have each user in the group automatically inherit the AFA role.

Do the following:

1. Click your username at the top-right to access the **AFA Administration** area.
2. Click the **USERS/ROLES** tab to display the user and role tables. For example:

The screenshot shows the 'Administration' page in the Firewall Analyzer interface. The 'USERS/ROLES' tab is selected, displaying two tables:

	Fullname	Email	Notification	Username	Admin	FireFlow Admin	Notes	Edit
<input type="checkbox"/>	afademo	afademo@algosec.com	✓	afademo	✓			
<input type="checkbox"/>	AlgoSec Administrator	admin@company.com	✓	admin	✓			
<input type="checkbox"/>	FA	afademo@a.com	✓	A	✓	✓		
<input type="checkbox"/>	FireFlow	some_email_not_used@somewhere.org		FireFlow_batch				
<input type="checkbox"/>	harry helpdesk	harry@company.com		harry				
<input type="checkbox"/>	Ned NetOps	ned@company.com	✓	ned	✓	✓	Firewall Administrator	
<input type="checkbox"/>	Sue Security	sue@company.com	✓	sue			Information Security	

Buttons: Delete, New

	Role Name	Role Description	Edit
<input type="checkbox"/>	Admins	AFA + FF Admins - full access	
<input type="checkbox"/>	helpdesk	For helpdesk staff - query only	

Buttons: Delete, New

Links: [Manage FireFlow roles](#), [Manage FireFlow requestors](#)

3. To add a new role, click the **New** button under the role table. To edit an existing role,

click the edit  button in the row for the role you want to edit.

In the user form that appears, select and enter values as needed:

Role details

Role name	Enter a name for the role.
Role description	Enter a description of the role.
Role LDAP DN	<p>Enter the DN of the LDAP group that corresponds to this role.</p> <p>When users who are members of this LDAP group log in, they will automatically be granted this role.</p> <p>For example: cn=network_users,ou=organization,o=mycompany,c=us</p> <p>Note: This field is enabled only if you have AFA configured to fetch user data from an LDAP server.</p> <p>To enable this field, select the Fetch user data from LDAP option on the OPTIONS > Authentication tab in the AFA Administration area. For details, see Import user data from an LDAP server.</p>
Landing Page	<p>Select Firewall Analyzer or FireFlow. Select Automatic to use the default landing page for the selected role.</p> <p>For more details, see Default landing pages per role.</p>

General Permissions

Administrator	Make all users with this role administrators.
FireFlow Administrator - Allow FireFlow Advanced Configuration	<p>Make all users with this role FireFlow configuration administrators.</p> <p>This enables these users to perform advanced configuration tasks in FireFlow.</p>
Enable Analysis from file	Allow all users with this role to perform analyses from configuration files.

Enable Trusted Traffic -> global	Allow all users with this role to view and edit trusted traffic settings.
--	---

Authorized Views and Actions

Report	<p>Select the report pages that users with this role can view.</p> <ul style="list-style-type: none"> • Select Full Report to indicate that users with this role can view all report pages. • Pages that are not selected will be inaccessible to users with this role.
Home Views	<p>Select the Home page elements that users with this role can view.</p> <ul style="list-style-type: none"> • Select All Home Views to indicate that users with this role can view all Home page elements. • Pages that are not selected will be inaccessible to users with this role.
Actions	<p>Select the actions that users with this role can perform in AFA.</p> <ul style="list-style-type: none"> • Select All Actions to indicate that users with this role can perform all actions. • Controls used to perform actions that are not selected will be disabled.

Authorized Devices

Select the default device access provided to all users with this role. Do the following:

- a. Select a default permission profile to determine the permission level for the selected devices.
- b. Click **Select devices....** to select the devices you want to apply the selected permission level on.

The device tree appears.

- c. Select the checkboxes next to each relevant device and click **OK**.

A table appears with your selected devices and permissions.

For example:

Authorized Devices

Default permission profile:

Device/Group	Permission profile	Notification
Rose_checkpoint	<input type="text" value="Read only"/>	<input checked="" type="checkbox"/>
birch_iptables	<input type="text" value="Read only"/>	<input checked="" type="checkbox"/>
Rose_DR	<input type="text" value="Standard"/>	<input checked="" type="checkbox"/>
Oak_Stonegate	<input type="text" value="Standard"/>	<input checked="" type="checkbox"/>

If needed, do either of the following:

- Select a different option from the **Permission profile** dropdown to change the profile for a specific device
- Clear or re-select the **Notification** checkbox to change notification settings for a specific device

4. Click **OK** to save your changes.

Delete AFA users or roles

This procedure describes how to delete users from the local AFA database, or delete user roles.

Tip: Alternately, manage users via an authentication server or SSO. For details, see [Configure user authentication](#).

Do the following:

1. Click your username at the top-right to access the AFA **Administration** area.
2. Click the **USERS/ROLES** tab to display the user and role tables. For example:

The screenshot shows the 'Administration' section of the Firewall Analyzer interface. The 'USERS/ROLES' tab is selected. The page contains two tables: a users table and a roles table. Both tables have checkboxes for selection and 'Delete' and 'New' buttons below them.

Users Table:

	Fullname	Email	Notification	Username	Admin	FireFlow Admin	Notes	Edit
<input type="checkbox"/>	afademo	afademo@algosec.com	✓	afademo	✓			
<input type="checkbox"/>	AlgoSec Administrator	admin@company.com	✓	admin	✓			
<input type="checkbox"/>	FA	afademo@a.com	✓	A	✓	✓		
<input type="checkbox"/>	FireFlow	some_email_not_used@somewhere.org		FireFlow_batch				
<input type="checkbox"/>	harry helpdesk	harry@company.com		harry				
<input type="checkbox"/>	Ned NetOps	ned@company.com	✓	ned	✓	✓	Firewall Administrator	
<input type="checkbox"/>	Sue Security	sue@company.com	✓	sue			Information Security	

Roles Table:

	Role Name	Role Description	Edit
<input type="checkbox"/>	Admins	AFA + FF Admins - full access	
<input type="checkbox"/>	helpdesk	For helpdesk staff - query only	

Links at the bottom: [Manage FireFlow roles](#), [Manage FireFlow requestors](#)

3. Select the check box next to the user or role you want to delete, and click **Delete**.

4. In the confirmation message that appears, click **OK**.

The selected user or role is deleted from AFA.

ASMS username and password requirements

ASMS user names can contain any alpha-numeric character and the following special characters:

- @ (at symbol)
- _ (underscore)
- . (period)
- - (hyphen)
- / (forward-slashes)

ASMS passwords can contain any alpha-numeric character or any special character, except for back-ticks (`)

Use the following regular expressions to confirm that your usernames and passwords meet ASMS requirements:

Value	Regular Expression
Username or username with LDAP domain	<code>^[a-zA-Z0-9@_.-V]*\$</code>
Password	<code>^[a-zA-Z0-9\x20-\x5F\x7B-\x7E]*\$</code>

Import users via CSV

You can import multiple local users into ASMS from a CSV file. This allows you to onboard large numbers of users without manually configuring each of them.

Prepare a users CSV file

Do the following:

1. Open a new text file.
2. In the first line of the file, type a list of column headers.

For a list of supported headers, refer to the following table. The headers must be separated by commas.

3. For each user you want to import, type a new line containing values that correspond to the column headers.

Refer to the following table for information about each header's possible values. The values must be separated by commas. If no value is specified, the default is used.

For example:

```
username,password,fullname,email,note,policy_change,administrator,
authentication_type,default_fw_profile,firewallsJohnS,JohnSPass,
John Smith,JohnSmith@mycompany.com,customersupport,yes,yes,,
readonly,(ECZ_ASA1;yes;Standard)(ISG1000_root:trust-vr;yes;Standard)
JaneB,,Jane Brown,JaneBrown@mycompany.com,sales,no,no,ldap
```

4. Save the file.

Supported column headers

Header Name	Description	Possible Values
username	The username to assign the user. This header is mandatory.	Any
fullname	The user's full name. This header is mandatory.	Any.
email	The user's email address. This header is mandatory.	An email address in standard email address format.
note	Notes about the user.	Any.
password	The password to assign the user.	Any
policy_change	Indicates whether the AFA system should send notifications to the user when changes are made to policies.	<ul style="list-style-type: none"> • yes • no (Default)
group_changes	Indicates whether the AFA system should send notifications to the user when a group report is generated.	<ul style="list-style-type: none"> • yes • no (Default)
all_changes	Indicates whether the AFA system should send notifications to the user when a report is generated.	<ul style="list-style-type: none"> • yes • no (Default)

Header Name	Description	Possible Values
configuration_changes	Indicates whether the AFA system should send notifications to the user when configuration changes are made.	<ul style="list-style-type: none"> • yes • no (Default)
object_expirations	Indicates whether the AFA system should send notifications to the user when device rules and/or VPN users are about to expire.	<ul style="list-style-type: none"> • yes • no (Default)
error	<p>Indicates whether the AFA system should send error messages to the user. These include low disk space and license expiration warnings.</p> <p>This header is only relevant for administrators.</p>	<ul style="list-style-type: none"> • yes • no (Default)
customizations	<p>Indicates whether the AFA system should send notifications to the user when customization changes are made. These include notifications about topology, trusted traffic, and risk profile customizations.</p> <p>This header is only relevant for administrators.</p>	<ul style="list-style-type: none"> • yes • no (Default)

Header Name	Description	Possible Values
authentication_type	<p>The type of authentication to use for this user.</p> <p>For information on configuring AFA to work with a RADIUS Server or an LDAP server, see Configure user authentication.</p>	<ul style="list-style-type: none"> • <code>local</code>. Authenticate the user against the local AFA user database. • <code>radius</code>. Authenticate the user against a RADIUS server. • <code>ldap</code>. Authenticate the user against an LDAP server.
administrator	Indicates whether to make the user an administrator.	<ul style="list-style-type: none"> • yes • no (Default)
run_file_analysis	Indicates whether to allow the user to perform analyses from configuration files.	<ul style="list-style-type: none"> • yes • no (Default)
global_customisation	Indicates whether to make the user a FireFlow configuration administrator. This enables the user to perform advanced configuration tasks in FireFlow.	<ul style="list-style-type: none"> • yes • no (Default)
fireflow_admin	Indicates whether the FireFlow user can perform advanced configuration tasks, such as using VisualFlow to edit workflows.	<ul style="list-style-type: none"> • yes • no (Default)
default_fw_profile	The user's default access level to devices.	<ul style="list-style-type: none"> • readonly • none • standard (Default)

Header Name	Description	Possible Values
firewalls	A list of devices for which the user should be granted permissions.	<p>Each device in the list must be in the following format: <code>(deviceName;notify;permissionProfile)</code></p> <p>where:</p> <ul style="list-style-type: none"> • <code>deviceName</code> is the device's name • <code>notify</code> indicates whether the user should receive notifications about the device (<code>yes/no</code>) • <code>permissionProfile</code> is the user's access level to the device (<code>readonly/none/standard</code>) <p>Multiple devices should not be separated by anything</p> <p>For example:</p> <div style="border: 1px solid #ccc; border-radius: 5px; padding: 5px; background-color: #f9f9f9; width: fit-content; margin: 10px auto;"> <code>(device) (device) (device) ...</code> </div>

Run the import users script

This procedure describes how to import users into AFA from an CSV file.

Do the following:

1. Open a terminal and log in using the username "afa" and the related password.
2. Enter the following command:

```
import_users -f CSVFile
```

For information on the command's flags, see the following table.

The `import_users` script runs and imports users from the file into both AFA and FireFlow.

Import users script flags

Flag	Description
-f <i>CSVFile</i>	<p>The name of the CSV file.</p> <p>Note: The file must be located in the current directory.</p>

Customize risk and compliance management

AFA supports many risk and compliance customizations, allowing you to define your organization's specific needs.

For details, see:

- **Create custom risk profiles** with built-in and custom risk items. For details, see:
 - [Customize risk profiles](#)
 - [Customize risk items](#)
- **Define new zone types**, in addition to the predefined Internal, External, and DMZ. For details, see [Customize zone types](#).
- **Add new host group definitions**. For details, see [Customize hostgroups](#).
- **Add new service definitions**. For details, see [Customize services](#).
- **Configure AFA to treat private IP addresses as non-threatening**. For details, see [Configure trusted private IP addresses](#).
- **Customize the security rating** and the way security rating information is displayed. For details, see [Configure security ratings](#).
- **Configure which regulatory compliance standards** are relevant to your environment. For details, see [Customize the regulatory compliance report](#).
- **Customize the configuration requirements for baseline compliance**. For details, see [Customize baseline configuration profiles](#).

Customize risk profiles

AFA analyzes device configuration and reports security risks using risk profiles, which define sets of security risk items and their security levels.

By default, AFA uses a Standard Risk Profile for all devices, which includes a set of standard risk items. Each risk item represents an XQL query that AFA performs on simulation results to detect risks.

Create custom risk profiles as needed, including different combinations of risk items, changing severity levels of each risk item, or creating custom risk items. Custom risk items enable you to define complex risks by composing your own XQL queries.

For more details, see:

- [View a risk profile](#)
- [Add a new risk profile](#)
- [Delete a custom risk profile](#)
- [Set a default risk profile](#)

Note: After making changes to risk profiles, you must run a new analysis before seeing any changes in AFA reports.

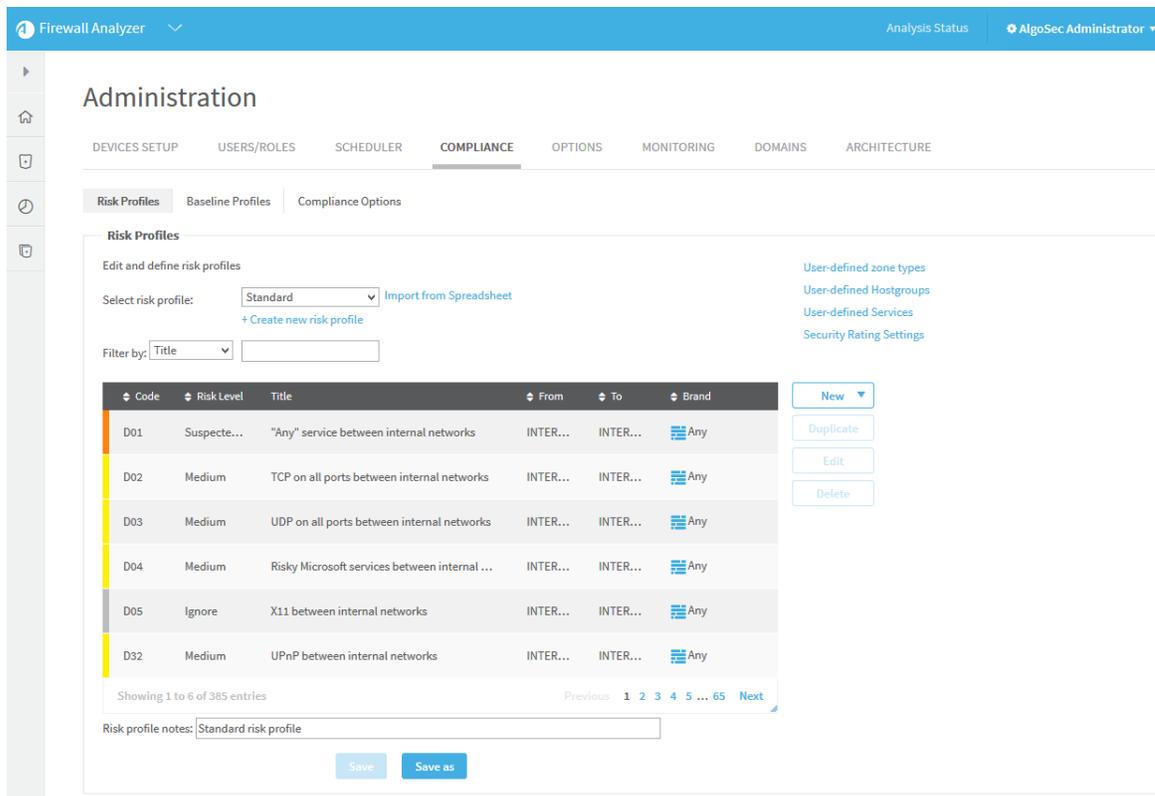
 **Edit a Risk Profile:** Watch to learn how to edit a risk profile to suit your network needs.

View a risk profile

This procedure describes how to view a specific risk profile in the AFA Administration area, as well as the details shown.

Do the following:

1. Access the AFA Administration area. Click your username in the toolbar and select **Administration**.
2. Click the **Compliance > Risk Profiles** tab, displaying the **Standard** risk profile with risk items displayed in a grid below.



The risk item grid includes the following data:

Code	The risk item code.
Risk Level	<p>The severity level applied to the risk level.</p> <p>The severity level is also indicated by the color bar on the left of the row, as follows:</p> <ul style="list-style-type: none"> • Brown = Low • Yellow = Medium • Orange = Suspected High • Red = High • Grey = Ignored <p>Note: Ignored risk items are listed in AFA reports towards the bottom of the Risk Assessment page, and not in the main page with other detected risks.</p>
Title	The risk item's title, or name.

From / To	The source and destination zone of connections specified by the risk item.
Brand	The relevant device brand for the risk item.

3. To load a different risk profile, select it from the **Select risk profile** dropdown menu above the grid. The page is updated with the selected risk profile.

Continue with any of the following:

- [Add a new risk profile](#)
- [Delete a custom risk profile](#)
- [Set a default risk profile](#)
- [Customize risk items](#)

Add a new risk profile

Add a new risk profile by creating one from scratch, modifying an existing profile and saving it under a new name, or importing a spreadsheet that specifies safe traffic.

Create a new risk profile from scratch

Create a new risk profile from scratch when you want to start with completely empty risk items.

Do the following:

1. Access the **Risk Profiles** tab in the AFA Administration area. For details, see [View a risk profile](#).
2. Click **+ Create new risk profile**, and enter a name for your new profile.
3. Customize your risk items as needed. For details, see [Customize risk items](#).
4. When you're done, click **Save** and then **OK** to confirm.

Your new risk profile is ready to use in your next AFA analysis.

Create a new risk profile from an existing one

Create a new profile by starting with an existing one when you want to use the existing one as a basis for your new profile.

Do the following:

1. View the specific risk profile you want to start with in the **Risk Profiles** tab in the AFA Administration area. For details, see [View a risk profile](#).
2. Customize your risk items as needed for your new profile. In the Risk profile notes field, enter a description for your new risk profile.
3. Click **Save As**, and enter a new name for your new profile.
4. Click **OK**, and then **OK** again to confirm.

Your new risk profile is ready to use in your next AFA analysis.

Tip: While the **Standard** risk profile is read-only, you can use it as the basis for a custom profile. Then, you can define your custom profile as the default risk profile for all future reports. For details, see [Set a default risk profile](#).

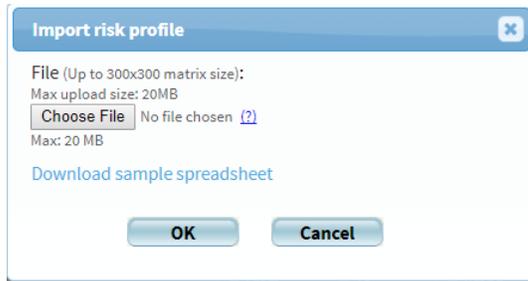
Create a new risk profile from a spreadsheet

Create a custom risk profile by uploading a spreadsheet that defines safe and risky traffic. When you upload this file, AFA creates a new risk profile. By default, any traffic not included in the spreadsheet is defined as a risk.

Use the template provided in the AFA Administration area to create this spreadsheet.

Do the following:

1. Open the **Risk Profiles** tab in the **AFA Administration** area. For details, see [View a risk profile](#).
2. Click **Import from spreadsheet**. In the **Import risk profile** dialog, **Download sample spreadsheet**.



3. Save the file locally using a meaningful name, and populate it with details about the traffic you want to allow or define as risky. For details, see [Spreadsheet requirements](#).
4. When your spreadsheet is ready, return to the **Import risk profile** dialog, and click **Choose File**. Browse to and select the file you edited, and then click **OK** to upload the file.

AFA generates your new risk profile, defining any traffic that is not specified in your uploaded file as a risk.

AFA optimizes your risks, and combines similar items to create the fewest number of new risk items possible.
5. Click **Save as** to save your new Risk Profile. Enter a meaningful name, and click **OK**.

Your new risk profile is ready to use in your next AFA analysis.

Note: When you upload a spreadsheet, AFA optimizes risk creation by combining traffic flows when possible. This may result in individual risks with wide definitions. In such cases risk descriptions specify the traffic or server that triggered the risk to help you understand why the risk was triggered.

Spreadsheet requirements

The spreadsheet uploaded to AFA to generate a custom risk profile must include the following sheets:

- **Traffic.** Defines the traffic you want to mark as allowed or risky by the generated risk profile.

Modify the number of rows or columns as needed to describe the traffic.

- **Networks.** Defines network objects used in the **Traffic** sheet.
- **Services.** Defines service objects used in the **Traffic** sheet.

Across all sheets in the spreadsheet:

- Object names are case-sensitive.
- Comments are supported in all sheets, only outside the data table, title rows or columns. Add **#** before the comment text.

For more details, see [Populate the Traffic sheet](#) and [Populate the Networks and Services sheets](#).

Note: To define conditional severities, include the **Conditional Severities** sheet as well.

Populate the Traffic sheet

You must populate every cell in the **Traffic** sheet data table, as follows:

Source / destinations	<p>List source network objects in the left column, and destination network objects across the top row.</p> <p>Destinations do not need to be the same as the sources, but must be network objects defined in the Networks tab, or the predefined Other object.</p> <p>The Other object includes all IP addresses that are not included in network objects listed on the Networks tab, and generally includes the public internet.</p>
------------------------------	---

Service objects	<p>Each cell that intersects a source and destination must contain one or more service objects, as follows:</p> <ul style="list-style-type: none"> • To define safe traffic, enter the name of a safe service object. • To define risky traffic, enter the name of a risky service object using the following syntax: not(<i>service_object</i>) or !service_object • To define multiple service objects in a single cell, enter each object name on a new line in the cell (ALT+ENTER). <p>Service object values must either be listed on the Services tab, or be one of the following predefined services:</p> <ul style="list-style-type: none"> • Any. All services • None. No services.
------------------------	---

Tip: Optionally, specify risk severity levels for risk traffic associated with a specific source or destination. For details, see [Specify risk severity in your spreadsheet](#).

Populate the Networks and Services sheets

Populate the **Networks** and **Services** sheets as follows:

Object names	List object names in the left column.
Object content	<p>List object content in the same row as the objects name.</p> <p>Assign multiple values to each object as needed, by specifying multiple values across the row, each value in it's own cell.</p>
Object names	Object names support lowercase and uppercase letters, digits, and underscores (_).
Network objects	Network objects support single IP addresses, subnets, or ranges.
Service objects	<p>Service objects support:</p> <ul style="list-style-type: none"> • Protocol/port format for TCP, UDP, and ICMP protocols • Other standard names such as SSH, FTP, and so on, including AlgoSec standard services

Specify risk severity in your spreadsheet

By default, all risks generated by uploading a spreadsheet are given a Medium severity.

To customize this, specify severity levels in the **Traffic** sheet for risks associated with specific traffic, sources, or destinations.

Do the following:

In the **Traffic** sheet, add the following characters to your cells to indicate severity levels:

- **H** = High
- **S** = Suspected high
- **M** = Medium
- **L** = Low
- Any conditional ID specified in a **Conditional Severities** sheet.

Add your severity notations to cells in your **Traffic** sheet as follows:

Specify severity for all traffic from a specific source	Indicate the severity level with the network object in the left column.
Specify severity for all traffic from a specific destination	Indicate the severity level with the network object in the header row.
Specify severity for all traffic from a specific source and to a specific destination	<p>Indicate the severity level with the service object in the intersecting cell.</p> <p>In such cases:</p> <ul style="list-style-type: none"> • By default, the generated risk will be relevant to all traffic between the services, via services other than those included in the service object. • If you specify severity for a risky service object, the generated risk will be relevant to all traffic between the servers via the specified service object.

<p>Specify multiple severity levels for traffic from a specific source to a specific destination</p>	<p>Further segregate traffic by defining a permitted service object and one or more negated service objects in the same intersecting cell, each with a specified severity.</p> <p>In such cases:</p> <ul style="list-style-type: none"> • Place each object on a new line in the cell (ALT+ENTER) • The first object in the cell can be safe or negated. All other objects must be negated.
---	---

Note: If a severity is specified for either the traffic, or for a specific source or destination, AFA assigns the specified severity to that risk.

If different severities are assigned to the source and destination, AFA uses the higher severity when generating the risk.

For more details, see [Populate the Traffic sheet](#).

The following table shows an example of a **Traffic** sheet with severities indicated:

To From	Net1	Net2	Net3	PartnerNet	PCIzone;S	Other
Net1	-	!(forbiddenSvc)	SecureSrvs ; C2	Any	SecureSrvs	Any
Net2	Any	-	Any	Any	SecureSrvs	Any
Net3	OnlySrv/X	!(OnlySrv/X)	-	Any	SecureSrvs	Any
PartnerNet	PartnerSrv	!PartnerSrv ; C1	!PartnerSrv ; C1	Any	SecureSrvs	Any
PCIzone;S	SecureSrvs ; M !forbiddenSvc ; H	SecureSrvs	SecureSrvs ; C2	SecureSrvs ; C3	-	None;H
Other	-	-	http_Services	-	None;H	Any

In this example, AFA will use the data in the highlighted cell to generate risks with the following severities:

High	Traffic from PCIZone to Net1 , via forbiddenSvc
Medium	Traffic from PCIZone to Net1 , via any services other than those defined in forbiddenSvc or SecureSrvs
Not risky	Traffic from PCIZone to Net1 , via SecureSrvs

Note that although the risk specified for all traffic from **PCIZone** is **Suspected high**, no traffic from **PCIZone** to **Net1** is specified as **Suspected high**, as the severities associated with each service object take precedence.

Delete a custom risk profile

Delete any unused risk profiles to declutter your system.

Do the following:

1. View the specific risk profile you want to delete in the **Risk Profiles** tab in the AFA Administration area. For details, see [View a risk profile](#).
2. Below the **Risk Profile** table, click  **Delete this profile**.
3. Click **OK** to confirm, and then **OK** again.

Set a default risk profile

By default, the risk profile used when running an analysis is always the Standard risk profile. Set a custom risk profile as the default, as needed.

Do the following;

1. Access the AFA Administration area. Click your username in the toolbar and select **Administration**.
2. Click the **Compliance > Compliance Options** tab.
3. In the **Default risk profile** dropdown, select the risk profile you want to set as default, and click **OK**.

For example:

The screenshot shows the Administration interface with the following structure:

- Top navigation: DEVICES SETUP, USERS/ROLES, SCHEDULER, COMPLIANCE (highlighted)
- Sub-navigation: Risk Profiles, Baseline Profiles, Compliance Options (highlighted)
- Section: Risk and Compliance Options
 - Default risk profile: RiskProfile_Demo.xml (dropdown menu)
 - Trust private IP addresses (10.*, 172.16.*:172.31.*, 192.168.*)
 - Regulatory compliance reports to be included in the device analysis

AFA uses the selected risk profile by default when running an analysis.

Customize risk items

In addition to creating a custom risk profile, you can customize individual risk items or add new ones from scratch.

Edit, duplicate, or add a custom risk item

Edit risk items, duplicate them to create new items based on existing risk items, or add a new custom risk item from scratch.

Do the following:

1. View the Risk Profile with the risk items you want to edit. For details, see [View a risk profile](#).
2. Do one of the following:

<p>Edit an existing risk item</p>	<p>Select the risk in the grid, and click Edit.</p> <p>The risk item is opened for editing. Make your changes as needed, and then click OK.</p>
--	---

<p>Duplicate an existing risk item</p>	<p>Select the risk in the grid, and click Duplicate.</p> <p>A new risk item is opened for editing, with the same values as the risk item you had originally selected.</p> <p>Make your changes as needed, especially giving the new risk item a new name, and click OK.</p>
<p>Create a new risk item</p>	<p>Click New, and then select one of the following options:</p> <ul style="list-style-type: none"> • Basic risk. Create a basic risk • Risk with destination threshold. Create a risk item with a specific destination threshold • Risk with source threshold. Create a risk with a specific source threshold • Risk with specific IP addresses. Create a risk with specific IP addresses, an IP address range, or a subnet • PCI risk. Create a risk that refers to PCI zones

3. Populate the fields as needed for your risk item type. For details, see:

- [Risk Info fields](#)
- [Risk Query fields](#)
- [Customize risk items](#)
- [Customize risk items](#)

4. When you're done, click **OK** to return to your risk profile.

Risk Info fields

All risk types include the following data in the **Risk Info** area:

- **Title.** Enter a name for your new risk.
- **Level.** Select a risk severity level.
- **Template.** Displays the type of risk item you're editing.
- **Code.** An automatically assigned code for this risk item. For example, user-defined items have a code that start with **U**.

Risk Query fields

Risk query fields will differ depending on the type of risk item you're editing.

Name	Description
From zone / To Zone	<p>Relevant for basic risks and risks with source or destination thresholds</p> <p>Select the zone types that represent where the traffic you want to analyze is coming from and going to.</p>
With service	<p>Relevant for all risk types</p> <p>Select a service you want to consider as risky in this risk item.</p> <p>Supported services include pre-defined services, user-defined services, or device-defined services.</p> <p>Note: Selecting a device-defined service imports the service from the device, and creates a new user-defined service with the same details. In such cases, the new service's name is the same as the device-defined service, with an additional prefix of algosec_.</p> <p>Tip: Alternately, create a new service group that consists of one or more services. To do this, click Create New. For more details, see Customize services.</p>
Source / Destination / PCI zone	<p>Relevant for: risks with specific IP addresses or PCI risks</p> <p>Enter one or more IP addresses or address ranges. Separate multiple addresses and address ranges with commas.</p> <p>Alternately, click Add to use a wizard. There, select a method to use to define your source or destination, including:</p> <ul style="list-style-type: none"> • An individual IP address • An IP address range • Host group defined on the device • AlgoSec Hostgroup, a host group defined by AlgoSec <p>Enter subsequent values to continue through the wizard, following on-screen instructions as needed.</p>

Name	Description
Trust VPN IP addresses	<p>Relevant for basic risks and risks with source or destination thresholds</p> <p>Select to determine that VPN traffic be excluded from this risk item, and not shown in the AFA report.</p> <p>Default = Enabled</p>
Threshold on Destination / Source IP address	<p>Relevant for risks with source or destination thresholds only</p> <p>Enter the threshold for the source or destination IP address, depending on the type of risk item you're editing.</p>
Advanced	<p>Relevant for all risk types</p> <p>Define an XQL query for the risk item.</p> <p>Click Advanced and enter your query in the Advanced Query Editor.</p> <p>Warning: Setting an invalid query format may cause analysis errors when creating future reports.</p> <p>Follow the guidelines needed for the risk type you're editing. For details, see Advanced risk editing.</p>

Tip: Click **Auto Fill** to load pre-defined values from a template in to the Risk details area below, based on the values you've selected. Any existing values are overwritten.

For more details, see [Customize risk items](#).

Risk Details fields

The Risk Details includes the following data for all risk types:

Assessment / Remedy	<p>Enter a description of the risk and risk remedy.</p> <p>These texts are displayed in the AFA report whenever this risk item is triggered.</p> <ul style="list-style-type: none"> • Both Assessment and Remedy values can be written in any language. • Optionally, include keywords that link the risk item's assessment or remedy to other parts of the AFA report. <p>Insert keywords by typing them directly or click Insert Field to select them from a list.</p> <p>For more details, see Assessment and remedy keywords.</p>
Description	<p>Enter a general description of the risk, using terms that are not tied to any particular device.</p> <p>This text appears in Group reports whenever a device in the group has triggered this risk item.</p>
Suppressed by	<p>Enter the codes of other risk items that should prevent the current risk item from appearing in AFA reports or click Select to select them from a list.</p> <p>Note: Configuring suppression for your risks helps to avoid clutter and double-reporting in your AFA reports. However, overall security rating scores do also consider suppressed risks.</p> <p>Additionally, risks are not suppressed unless the suppression resolves all cases of that risk.</p> <p>For more details, see Suppression in AFA.</p>

Suppression in AFA

In AFA reports, each specific risk may be suppressed by another risk.

For example, you may want to do this when you have a more general risk that also includes the specific risk.

The following sample device, rule, and risk configuration illustrates this concept:

If no suppression is configured:

If you have a device with the following rules ...

Rule	Source	Destination	Services
01	10.1.1.2	20.1.1.1	Any
02	10.2.1.2	20.2.1.1	Telnet

... and the risk profile for the device includes the following risks:

Code	Risk Level	Title	From	To	Brand
D01	Suspected High	Allows ANY service	INTERNAL	INTERNAL	Any
D02	Medium	Allows ANY TCP service	INTERNAL	INTERNAL	Any
D03	Medium	Allows TELNET service	INTERNAL	INTERNAL	Any

The **RISKS** report for your device might include the following risk and rule details:

Security Rating	High	Suspected High	Medium
<ul style="list-style-type: none"> 1 D01 Allows ANY service Triggered by 1 rule (01) 1 D02 Allows ANY TCP service Triggered by 1 rule (01) 2 D03 Allows TELNET service Triggered by 2 rules (01,02) 			

If suppression is configured:

If you've configured the device's risk profile to include suppression as follows:

- D02 is suppressed by D01:

The screenshot shows a web interface for configuring risk rules. It is divided into two main sections: "Risk Info" and "Risk details".

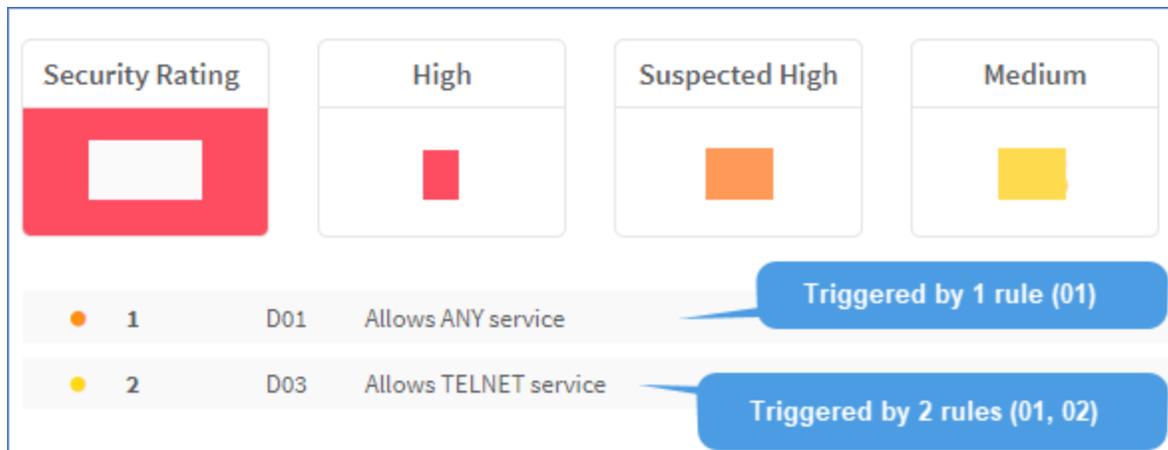
- Risk Info:** Contains a "Title:" field with the value "Allows ANY TCP service". Below the title are several colored bars (purple, brown, blue) representing different risk categories or severity levels.
- Risk details:** Contains a large brown rectangular area, likely for detailed configuration or description. Below this area is a "Suppressed by:" field with the value "D01 (Allows ANY service)" and a "Select" button.

- D03 is suppressed by D02:

The screenshot shows a web interface for configuring risk rules, similar to the previous one. It is divided into two main sections: "Risk Info" and "Risk details".

- Risk Info:** Contains a "Title:" field with the value "Allows TELNET service". Below the title are several colored bars (purple, brown, blue) representing different risk categories or severity levels.
- Risk details:** Contains a large brown rectangular area, likely for detailed configuration or description. Below this area is a "Suppressed by:" field with the value "D02 (Allows ANY TCP service)" and a "Select" button.

The **RISKS** report for the device shows the following:



In this report, **Risk D02** does not appear at all. This is because:

- Risk **D01** suppresses risk **D02**.
- The number of rules triggering **D02** = The number of rules triggering **D01**.

Also in this report, **D03** is shown because suppression is not in effect. This is because:

- While risk **D02** suppresses risk **D03**;
- The number of rules triggering risk **D02** \neq The number of rules triggering risk **D03**.

Delete a risk item

Delete custom risk items that you don't need anymore.

Warning: Do not delete risks with a prefix of **unnamed** or **AlgoSec**. Deleting these items may damage a risk profile.

Tip: While Standard risk items cannot be deleted, they can be disabled. For details, see [Disable a risk item](#).

Do the following:

1. View the risk profile with the risk item you want to delete. For details, see [View a risk profile](#).

2. In the grid, select the risk item you want to delete, and click **Delete**.
3. Click **OK** to confirm.

The risk item is deleted, and will no longer be included in future AFA reports.

Disable a risk item

Disable standard or custom risk items when you want to prevent them from being included in all AFA reports, but you don't want to remove them from the system.

Warning: Do not disable any risks with a prefix of **unnamed** or **AlgoSec**. Disabling these items may damage a risk profile.

Do the following:

1. View the risk profile with the risk item you want to disable. For details, see [View a risk profile](#).
2. In the grid, select the risk item you want to disable, and click **Edit**.
3. In the **Level** field, select **Ignore**, and then click **OK**.

The risk item is disabled, and will not be included in future AFA reports.

Customize zone types

Device and matrix topologies are defined in AFA using zone types. Each of the network's zones is assigned a zone type, and the zone is represented in the zone type's color in all AFA diagrams and reports.

If desired, you can define additional zone types. Configuring user-defined zone types enables you to tailor risk profiles to your exact network topology. Each user-defined zone type is based on one of AFA's built-in zone types.

Built-in zone types

Zone Type	Color	Description	Example
External	Red	Represents network zones that are directly connected to the Internet.	The "Outside" zone is assigned to this zone type.
Internal	Blue	Represents network zones that are not connected to the Internet.	The "Inside" zone is assigned to this zone type.
DMZ	Orange	Represents the DMZ (Demilitarized Zone).	The "DMZ" zone is assigned to this zone type.

Add and edit zone types

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

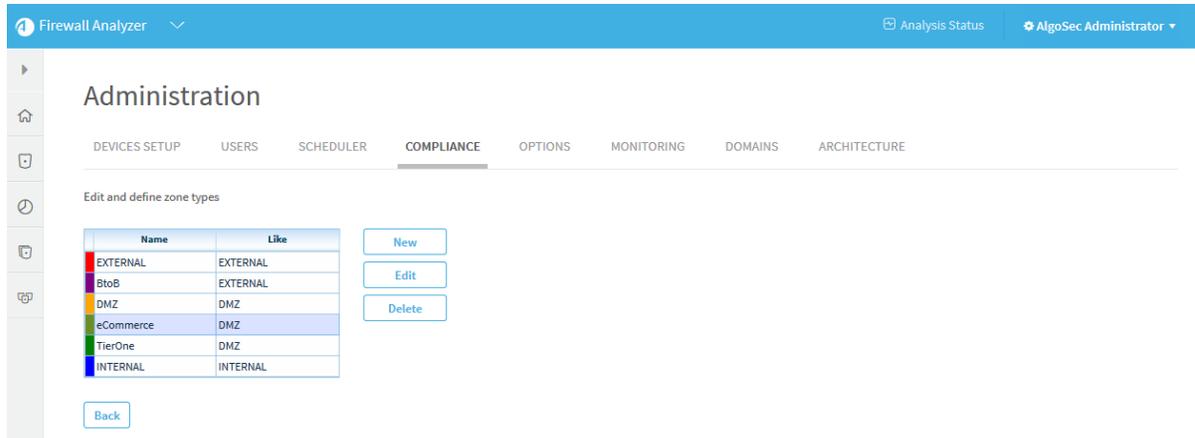
The **Administration** page appears, displaying the **Options** tab.

3. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

4. Click [User-defined zone types](#) .

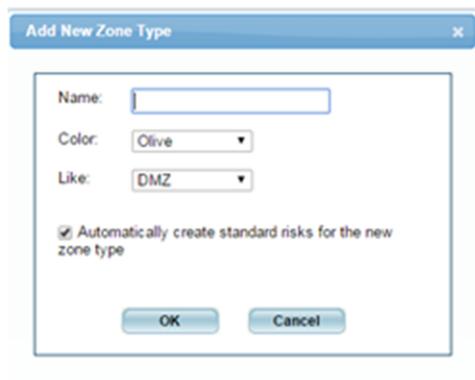
The **Edit and define zone types** page appears.



5. Do one of the following:

- To add a new zone type, click **New**.
- To edit an existing zone type, select the desired zone type and click **Edit**.

The **Add New Zone Type** or **Edit Zone Type** dialog box appears.



Note: You cannot edit the built-in zone types (EXTERNAL, INTERNAL, or DMZ).

6. Complete the fields using the information in the following table.

7. Click **OK**.

Zone Type Fields

In this field...	Do this...
Name	Type the zone type's name. This field is read-only when editing a zone.
Color	Select a color to represent the zone type.
Like	Select an existing zone type from which this zone type should inherit its settings. You can then override the inherited settings as desired. This field is read-only when editing a zone.
Automatically create standard risks for the new zone type	Select this option to automatically use the Standard Risk Profile for the zone. This field appears only when adding a new zone.

Delete zone types

Note: You cannot delete a zone type if it appears in a defined device's topology.

Note: You cannot delete the built-in zone types (EXTERNAL, INTERNAL, or DMZ).

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

4. Click [User-defined zone types](#).

The **Edit and define zone types** page appears.

5. Select the desired zone type and click **Delete**.

A confirmation message appears.

6. Click **OK**.

The zone type is deleted.

Customize hostgroups

You can define hostgroups to use when performing tasks such as running traffic simulation queries and/or configuring the trusted traffic you want to view.

Add and edit host groups

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

4. Click [User-defined Hostgroups](#).

The **Edit and define hostgroups** page appears.

The screenshot shows the 'Administration' page in the 'COMPLIANCE' tab. The page title is 'Administration' and the sub-header is 'Edit and define hostgroups'. The table below lists several host groups with their names and IP addresses. A 'New' button is located to the right of the table, along with 'Edit' and 'Delete' buttons. A 'Back' button is at the bottom left of the table area.

Name	IP Addresses
<input type="checkbox"/> AlgoSec_PCI_xml_other-from	10.120.46.16-10.176.49.255, 10.176.61.0-255.255.255.255, 10.25.4.0-10.50.63.255
<input type="checkbox"/> AlgoSec_PCI_xml_PartnerNet	10.120.46.0-10.120.46.15
<input type="checkbox"/> AlgoSec_PCI_xml_PCIZone	10.176.50.0-10.176.60.255
<input type="checkbox"/> AlgoSec_PCI_xml_Net3	10.3.64.0-10.3.64.255
<input type="checkbox"/> AlgoSec_PCI_xml_Net1	10.25.3.0-10.25.3.255, 10.21.0.0-10.21.0.255
<input type="checkbox"/> AlgoSec_PCI_xml_Net2	10.50.64.0-10.50.79.255
<input type="checkbox"/> AlgoSec_PCI_xml_other-to	10.120.46.16-10.176.49.255, 10.176.61.0-255.255.255.255, 10.25.4.0-10.50.63.255
<input type="checkbox"/> AlgoSec_AW0	2.2.2.2-2.2.2.3, 1.2.3.4, 4.4.4.4

5. Do one of the following:

- To add a new host group, click **New**.
- To edit an existing host group, select the check box next to the desired host group and then click **Edit**.

The **New Hostgroup** dialog box appears.

6. In the **Name** field, type a name for the host group.

7. In the **IP Addresses** field, type the IP address or IP address range that the host group represents.

8. Click **OK**.

The new host group appears in the list.

Delete hostgroups

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

4. Click [User-defined Hostgroups](#).

The **Edit and define hostgroups** page appears.

5. Select the check box next to the desired host group and then click **Delete**.

A confirmation message appears.

6. Click **OK**.

The host group is deleted.

Customize services

You can define service groups that contain one or more services to use when performing tasks such as running traffic simulation queries and/or configuring the trusted traffic you want to view.

Add and edit service groups

Note: To define a single custom service, add a service group that contains only the desired service.

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

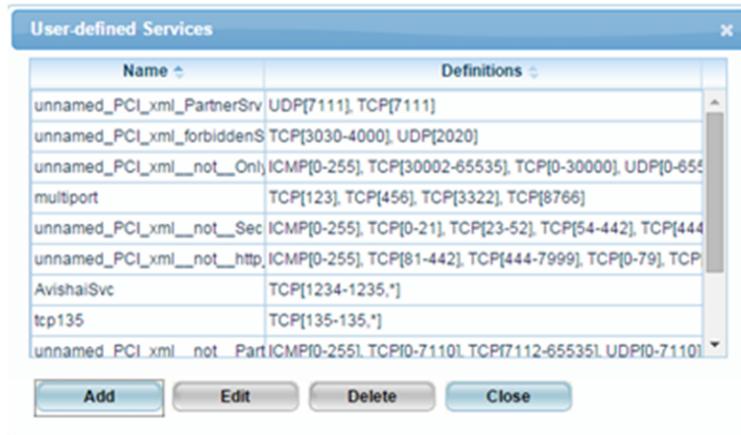
The **Administration** page appears, displaying the **Options** tab.

3. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

4. Click [User-defined Services](#).

The **User-defined Services** window appears.



5. Do one of the following:

- To add a new service, click **Add**.
- To edit an existing service, select the service and then click **Edit**.

The **New Service Group / Edit Service Group** dialog box appears.



6. In the **Service group name** field, type the service group's name.

7. To add a service to the group, do the following:

If this is not the first service to be added to the group, click **New Member**.

Complete the fields using the information in the following table.

In this field...	Do this...
Protocol	Select the service's protocol.
Destination port	Type the destination port range.
Source port	Type the source port range.

8. To remove a service from the group, select the service in the **Service group members** list box, then click **Remove**.
9. Click **Save**.
A success message appears.
10. Click **OK**.
11. Click **Close**.

Delete service groups

Do the following:

1. In the toolbar, click your username.
A drop-down menu appears.
2. Select **Administration**.
The **Administration** page appears, displaying the **Options** tab.
3. Click the **Compliance** tab.
The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.
4. Click [User-defined Services](#).
The **User-defined Services** window appears.
5. Select the desired service and click **Delete**.
A success message appears.
6. Click **OK**.

The service is deleted.

7. Click **Close**.

Configure trusted private IP addresses

By default AFA treats private IP addresses like 10.0.0.1 as non-threatening. Since these IP addresses are not routed on the public Internet, they typically represent machines that are owned by your corporation and are therefore not threatening. If desired, you can change this behavior.

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

3. The **Administration** page appears, displaying the **Options** tab.

4. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

5. Click the **Compliance Options** sub-tab.

6. Do one of the following:

- To treat private IP addresses as threatening, clear the **Trust private IP addresses** check box.
- To treat private IP addresses as non-threatening, select the **Trust private IP addresses** check box.

7. Click **OK**.

Note: This setting will only take effect in future reports that you generate.

Configure security ratings

AFA reports' **Home** and **Risks** pages display a security rating which indicates the device's degree of compliance with security standards.

Note: It is possible for a device with more risks to have a higher security rating than a device with fewer risks.

The Security Rating is calculated as the ratio of the number of risks detected vs. the number of risks searched for, and the total number of risks searched for differs per device.

If a device has multiple interfaces and some are configured as Internal, some as External, and some as DMZ, more risks will be searched for than on a device with only an Internal and External interface. Also, some risks are defined only for specific device vendors.

Security rating calculation

AFA calculates the security rating with the following formula:

$$\text{Security rating} = 100 \times (1 - (W_1X_1 + W_2X_2 + W_3X_3 + W_4X_4) / (W_1T_1 + W_2T_2 + W_3T_3 + W_4T_4))$$

where:

This variable...	Represents...
W_1	The weight of High risks. Default = 10.
W_2	The weight of Suspected High risks. Default = 4.
W_3	The weight of Medium risks. Default = 2.

This variable...	Represents...
W_4	The weight of Low risks. Default = 1.
X_1	The number of High risks detected in the current device policy.
X_2	The number of Suspected High risks detected in the current device policy.
X_3	The number of Medium risks detected in the current device policy.
X_4	The number of Low risks detected in the current device policy.
T_1	The maximum number of High risks possible for the device. This is determined by the device's brand and topology.
T_2	The maximum number of Suspected High risks possible for the device. This is determined by the device's brand and topology.
T_3	The maximum number of Medium risks possible for the device. This is determined by the device's brand and topology.
T_4	The maximum number of Low risks possible for the device. This is determined by the device's brand and topology.

Security rating calculation background

In ASMS's security rating calculation, risk is determined by the weakest link in the defense. This means that several well-configured devices do not mitigate the risk posed by a single, badly-configured device.

ASMS, therefore, cannot determine the security rating for a group of devices as a simple average of the security ratings of the group's members. Instead, ASMS looks at all possible risk items as a "whole", and deducts one "point" for every risk item flagged on at least one group member.

This approach may lead to scenarios where the security rating of a group is even lower than that of each group member.

For example, suppose the following:

- There are **100** possible risk items
- There are **100** devices in the group
- Each device is flagged for a single risk item.

In this case, the security rating of each device will be **99**, because 99 of the 100 possible risk items are not flagged.

The case may differ as follows:

If the same risk item is flagged on all 100 devices	The group security rating will also be 99 , since 99 of the 100 possible risk items are still not flagged.
If each device is flagged for a different risk item	The group security rating will be 0 , because 100 out of 100 possible risk items are flagged for at least one group member.

Customize security rating settings

You can customize the security rating by changing the weight assigned to each type of risk. In addition, you can customize the security rating bar's appearance in reports, and the number of days included in the **Security Rating Trend** graph in the **Risks** page of reports.

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

4. Click [Security Rating Settings](#).

The **Security Rating Settings** dialog box appears.

Security Rating Settings

Days in Trend Graph: 180

Low Breakpoint: 50 (default is 50) High Breakpoint: 85 (default is 85)

Formula Weights (2)

Risk Level	Weight	Defaults
High	10	10
Suspected High	4	4
Medium	2	2
Low	1	1

OK Cancel

5. Complete the fields using the information in the following table.

Days in Trend Graph	Type the number of days to include in the Security Rating Trend graph in the Risks page of reports. The default value is 180 days.
Low Breakpoint	Type a number representing the point on the security ratings bar where the bar should change from red to yellow, if the leftmost end of the bar is 0 and the rightmost end is 100. The default value is 50.
High Breakpoint	Type a number representing the point on the security ratings bar where the bar should change from yellow to green, if the leftmost end of the bar is 0 and the rightmost end is 100. The default value is 85.
Formula Weights	Enter the desired weight for each risk type.

6. Click **OK**.

Customize the regulatory compliance report

AFA provides regulatory compliance reports for a variety of regulatory compliance standards. These reports can be accessed from the **Regulatory Compliance** report page of each AFA report.

You can customize the **Regulatory Compliance** page in the following ways:

- [Remove and add compliance reports](#)
- [Customize the compliance score value](#)
- [Customize compliance score severity thresholds](#)

To add or remove reports in the CLI or to create a custom regulatory compliance report, see [Customize regulatory compliance report](#).

Remove and add compliance reports

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

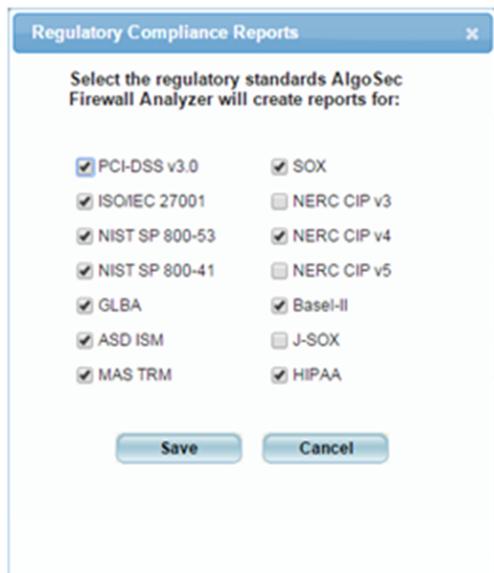
3. Click the **Compliance** tab.

The **Compliance** page appears, displaying the **Risk Profiles** sub-tab.

4. Click the **Compliance Options** sub-tab.

5. Next to **Regulatory compliance reports to be included in the device analysis**, click **Select**.

The **Regulatory Compliance Reports** dialog box appears.



For a description of each standard, see [Supported regulatory compliance reports](#).

6. To enable a report, select its check box.
7. To disable a report, clear its check box.
8. Click **Save**.

Note: When upgrading AFA, any newly supported reports are automatically enabled.

Supported regulatory compliance reports

Standard	Description
US Centric	
SOX	Required for publicly traded companies on US markets.
NERC CIP v3, v4, v5	Required for Power manufacturing and distribution, including Oil, Gas and Nuclear. The customer may choose to analyze against either v3, v4 or v5 of the NERC CIP standards, to evaluate readiness for future standard deadlines.
HIPAA	Required for protecting patient data in US healthcare companies.

Standard	Description
NIST SP 800-53	Required by US DoD. This report uses the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4 (April 2013).
NIST SP 800-41	Required by US DoD. This report uses the National Institute of Standards and Technology (NIST) Guidelines on Firewalls and Firewall Policy, Revision 1 (Sep 2009).
GLBA	Consumer identity safety requirements for US companies.
Europe Centric	
ISO/IEC 27001	ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks.
Basel-II	This addresses the Basel Committee on Banking Supervision's framework International Convergence of Capital Measurement and Capital Standards (June 2006).
Global	
PCI DSS 3.0	<p>The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data.</p> <p>You can optionally indicate which servers are in your PCI zone. Specifying these servers enables AFA and AppViz to provide you with more specific security information for PCI applications. See Configure the PCI zone.</p>
Australia Centric	
ASD-ISM	Firewall configuration guidelines from Australian Government.
Japan Centric	
J-SOX	Japanese version of SOX.

Standard	Description
Singapore Centric	
MAS-TRM	Guidelines for information security for Singapore operating banks, published by the government banking regulator.

Customize the compliance score value

AFA reports' **Regulatory Compliance** page displays a compliance score which indicates the device's degree of compliance with each compliance report. AFA calculates the compliance score with the following formula:

$$\text{Compliance score} = (X1 + WX2)/(X1 + X2 + X3)$$

Compliance Score Formula Variables

This variable...	Represents...
X1	The total number of requirements in the compliance report for which the device policy is compliant. Each of these requirements has a status of  .
X2	The total number of requirements in the compliance report for which additional information or manual verification is necessary for the device policy to meet the requirement. Each of these requirements has a status of  .
X3	The total number of requirements in the compliance report for which the device policy is not compliant. Each of these requirements has a status of  .
W	The weight of the number of requirements for which additional information or manual verification is necessary to meet the requirement. The default value is 0.5.

You can customize the compliance score value by changing the value of the "W" variable.

Do the following:

1. In the toolbar, click your username.

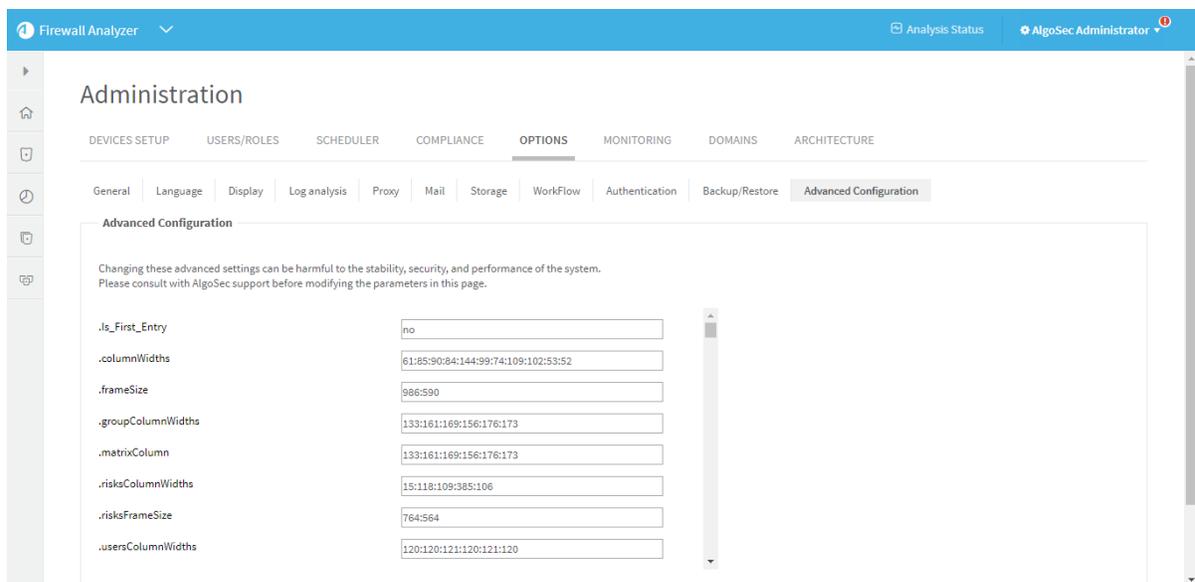
A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Advanced Configuration** tab.

The **Advanced Configuration** tab appears.



4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.



5. In the **Name** field, type `Compliance_Score_Star_Weight`.

6. In the **Value** field, type the value you wish to assign to the "W" variable.

7. Click **OK**.
8. Click **OK**.

Customize compliance score severity thresholds

AFA provides the ability to customize the compliance score severity thresholds.

By default, a bad score is 55% and below (red), a moderate score is between 55% and 70% (yellow), and a good score is 70% and above (green).

Do the following:

1. In the toolbar, click your username.

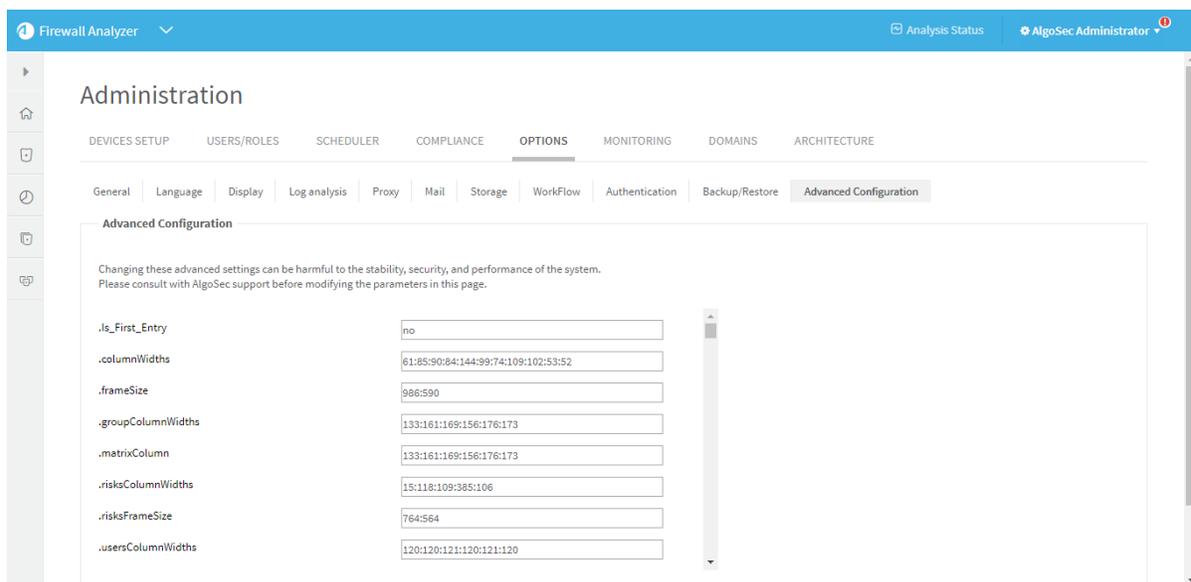
A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Advanced Configuration** tab.

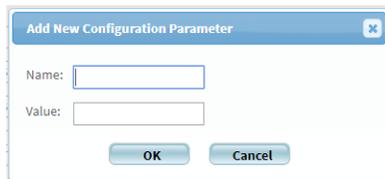
The **Advanced Configuration** tab appears.



4. To adjust the threshold for a bad score, do the following:

- a. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.



- b. In the **Name** field, type `Compliance_Score_Max_Red`.
- c. In the **Value** field, type the maximum value for a bad score.

For example, if you want a score of 60% and below to be a bad score, type 60.

- d. Click **OK**.

5. To adjust the threshold for a good score, do the following:

- a. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

- b. In the **Name** field, type `Compliance_Score_Min_Green`.
- c. In the **Value** field, type the minimum value for a good score.

For example, if you want a score of 80% and above to be a good score, type 80.

- d. Click **OK**.

6. Click **OK**.

Configure the PCI zone

Specifying the servers in the PCI zone enables AFA to specify the vulnerability of PCI applications in the PCI regulatory compliance report. Additionally, configuring these servers enables AppViz to tag which network objects intersect the PCI Zone and the applications that use these servers.

Note: This feature is only relevant when using AppViz.

AFA can only show the vulnerability of PCI applications in the PCI report when AppViz is integrated with a vulnerability scanner. When using AppViz without a vulnerability scanner, AppViz will still tag the network objects and applications that intersect the PCI zone with the PCI label.

Do the following:

1. In the toolbar, click your username.
A drop-down menu appears.
2. Select **Administration**.
3. The **Administration** page appears, displaying the **Options** tab.
4. Click the **Compliance** tab.
The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.
5. Click the **Compliance Options** sub-tab.
6. In the **Regulatory Compliance** area, in the **PCI zone** field, type an IP address, range, or CIDR.
7. To add another entry, click , and type the additional value in the field.
8. To remove a field, click .
9. In the **Vulnerability level threshold** field, select the threshold for acceptable vulnerability in the drop-down menu.

Applications with the selected vulnerability level (or lower) will be considered vulnerable in PCI reports. For example, selecting **Medium** will cause applications with medium or low security scores to be considered vulnerable.

Note: Specifying the vulnerability level threshold is only relevant when AppViz is integrated with a vulnerability scanner.

Customize baseline configuration profiles

A *baseline configuration compliance profile* contains a set of commands to be run on the device upon analysis and the desired output for the commands, allowing you to determine the device's compliance with a certain basic configuration. In order for a device's report to include a baseline configuration compliance report page, a baseline configuration compliance profile must be specified for the device when defining the device in AFA. See [Manage devices](#).

AFA includes a set of built-in baseline configuration compliance profiles suitable for all device brands which appear as options in the **Baseline Configuration Compliance Profile** drop-down list and in the `/usr/share/fa/data/baseline_profiles/` directory.

If desired, you can create custom baseline compliance profiles.

AFA provides the following options:

- [Access baseline profiles configuration](#)
- [Add a custom baseline configuration compliance profile](#)
- [Duplicate a baseline configuration compliance profile](#)
- [Delete a custom baseline configuration compliance profile](#)
- [Edit a baseline configuration compliance profile](#)
- [Example: Customize a baseline configuration compliance profile](#)

Access baseline profiles configuration

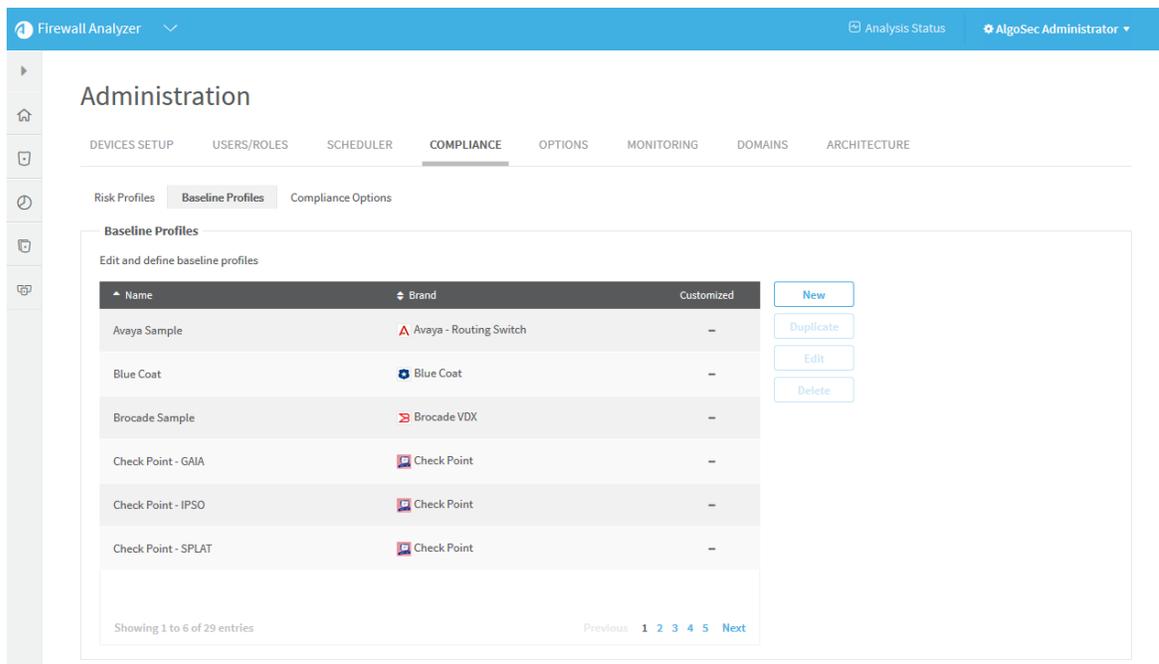
Do the following:

1. In the toolbar, click your username.
A drop-down menu appears.
2. Select **Administration**.
The **Administration** page appears, displaying the **Options** tab.
3. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

4. Click the **Baseline Profiles** sub-tab.

A list of baseline profiles appears.



The screenshot shows the Firewall Analyzer interface. The top navigation bar includes 'Firewall Analyzer', 'Analysis Status', and 'AlgoSec Administrator'. The main navigation menu has tabs for 'DEVICES SETUP', 'USERS/ROLES', 'SCHEDULER', 'COMPLIANCE', 'OPTIONS', 'MONITORING', 'DOMAINS', and 'ARCHITECTURE'. The 'COMPLIANCE' tab is active, and the 'Baseline Profiles' sub-tab is selected. The 'Baseline Profiles' section is titled 'Edit and define baseline profiles' and contains a table with the following data:

Name	Brand	Customized	
Avaya Sample	Avaya - Routing Switch	-	New, Duplicate, Edit, Delete
Blue Coat	Blue Coat	-	
Brocade Sample	Brocade VDX	-	
Check Point - GAIA	Check Point	-	
Check Point - IPSO	Check Point	-	
Check Point - SPLAT	Check Point	-	

At the bottom of the table, it says 'Showing 1 to 6 of 29 entries' and 'Previous 1 2 3 4 5 Next'.

Add a custom baseline configuration compliance profile

Do the following:

1. Access the Baseline Profile configuration area. For details, see [Access baseline profiles configuration](#).
2. Click **New**.

The baseline profile form appears.

4. Click **Save**.

The new custom baseline profile appears in the baseline profile table.

Note: A  appears in the **Customized** field of all custom baseline profiles.

Duplicate a baseline configuration compliance profile

You can create a custom baseline configuration compliance profile by duplicating an existing baseline profile and editing the duplicate.

Do the following:

1. Access the Baseline Profile configuration area. For details, see [Access baseline profiles configuration](#).
2. Select one of the baseline profiles.
3. Click **Duplicate**.

The baseline profile form appears with the values of the original profile.

The screenshot displays the 'Baseline Profiles' editor in the Firewall Analyzer. The interface is titled 'Administration' and has a navigation menu with 'COMPLIANCE' selected. Under 'COMPLIANCE', there are sub-menus for 'Risk Profiles', 'Baseline Profiles', and 'Compliance Options'. The 'Baseline Profiles' sub-menu is active, showing a form to edit a profile. The form is titled 'Baseline Profile' and has a 'Brand' dropdown set to 'bluecoat' and a 'Profile Name' field set to 'Blue Coat'. Below this, there is a 'Commands' section with a table of five commands:

Command ID (id)	Command Name (name)	Command Syntax (cmd)
1	Show Appliance Name	show appliance-name
2	Show Version	show version
3	Show Configuration	show configuration
4	Show SNMP Settings	show snmp
5	Show Security Settings	show security

On the right side of the editor, there is a sidebar with a 'Document is unchanged' status and a list of actions: 'Add Subelement', 'Add Attribute', and 'Add Attribute' (repeated multiple times).

4. Edit the fields, as desired, using [Example: Customize a baseline configuration compliance profile](#).

Note: To prevent the creation of two baseline profiles with the same display name, change the **Profile Name**.

5. Click **Save**.

The new custom baseline profile appears in the baseline profile table.

Note: A appears in the **Customized** field of all custom baseline profiles.

Edit a baseline configuration compliance profile

You can create a custom baseline configuration compliance profile by editing an existing baseline profile.

Note: The original baseline profile will not be over-written, but it will not be available to use unless you delete the new custom baseline profile.

Do the following:

1. Access the Baseline Profile configuration area. For details, see [Access baseline profiles configuration](#).
2. Select a baseline profile.
3. Click **Edit**.

The baseline profile form appears.

The screenshot displays the Firewall Analyzer Administration interface. The top navigation bar includes 'Firewall Analyzer', 'Analysis Status', and 'AlgoSec Administrator'. The main menu is 'Administration', with sub-menus for 'DEVICES SETUP', 'USERS/ROLES', 'SCHEDULER', 'COMPLIANCE', 'OPTIONS', 'MONITORING', 'DOMAINS', and 'ARCHITECTURE'. The 'COMPLIANCE' sub-menu is active, showing 'Risk Profiles', 'Baseline Profiles', and 'Compliance Options'. The 'Baseline Profiles' section is selected, and the 'Edit' button is highlighted. The form is titled 'Baseline Profile' and contains the following fields and sections:

- Brand (brand_id):** cma
- Profile Name (display_name):** Check Point - GAIA
- Commands (CommandsDef):** A table with three rows:

Command	Command Syntax (cmd)	Command Name (name)	Command ID (id)
	service dhcpd status	DHCP Server	1
	route -n grep D	Dynamic routing	2
	ifconfig	Unused Interface	3

On the right side, there is a 'Document is unchanged' status and a 'Save' button. Below this, there are several dropdown menus for 'Add Subelement', 'Add Attribute', and 'Add Nodes', each with a list of options.

4. Edit the fields using [Example: Customize a baseline configuration compliance profile](#).
5. Click **Save**.

The new custom baseline profile appears in the baseline profile table.

Note: A  appears in the **Customized** field of all custom baseline profiles.

Delete a custom baseline configuration compliance profile

Note: You can only delete custom baseline profiles. Custom baseline profiles are indicated with a  in the **Customized** field.

Do the following:

1. Access the Baseline Profile configuration area. For details, see [Access baseline profiles configuration](#).
2. Select one of the custom baseline profiles.
3. Click **Delete**.
4. Click **OK**.

Example: Customize a baseline configuration compliance profile

The following is an example of adding an additional command and baseline requirement to an existing Cisco baseline profile.

1. Access the Baseline Profile configuration area. For details, see [Access baseline profiles configuration](#).
2. Select a baseline profile.

In this example, we selected the **Cisco ACE Sample** profile. The profile is highlighted in blue.

The screenshot shows the 'Administration' page in the Firewall Analyzer interface. The 'COMPLIANCE' tab is selected, and the 'Baseline Profiles' sub-tab is active. A table lists various baseline profiles with columns for Name, Brand, and Customized status. The 'Cisco ACE Sample' profile is highlighted. Action buttons (New, Duplicate, Edit, Delete) are visible on the right side of the table.

Name	Brand	Customized
Cisco - ASA	Cisco Firewall	-
Cisco - Nexus Router	Cisco Nexus Router	-
Cisco ACE Sample	Cisco ACE	-
Cisco ACE Sample	Cisco ACE	✓
DELL SonicWALL Sample	DELL SonicWALL	-
FS BigIP	FS BigIP	-

3. Click **Edit**.

The baseline profile form appears.

The screenshot shows the 'Administration' page in the Firewall Analyzer, specifically the 'COMPLIANCE' section. The 'Baseline Profiles' tab is selected, and the 'Edit and define baseline profiles' area is active. The 'Commands (CommandDef)' section is highlighted in blue. The interface includes the following elements:

- Brand:** ace
- Profile Name:** Cisco ACE Sample
- Comment:** You can edit this sample baseline report to include more tests and requirements. To do that, please refer to the AlgoSec Firewall Analyzer User Guide or online help.
- Commands (CommandDef):**
 - Command 1:** Command ID (id) 1, Command Name (name) Show Route, Command Syntax (cmd) show ip route
 - Command 2:** Command ID (id) 2, Command Name (name) Show Config, Command Syntax (cmd) show running-config
- Baseline Requirement 1:**
 - Requirement Name (name):** Routing details
 - Requirement Description (description):** Routing settings.
 - Requirement ID (id):** 1
 - Command:** Command ID (id) 1
 - Criterion:** Criterion Type (type) Required Regexp
 - Line (item):** ((([0-9]{1,3})\.){3}([0-9]{1,3}))
- Baseline Requirement 2:**
 - Requirement Name (name):** Device details
 - Requirement Description (description):** General hardware settings.
 - Requirement ID (id):** 2
 - Command:** (empty)

4. To add a command to the profile:
 - a. Click **Commands (CommandDef)**.
The **Commands** area is highlighted in blue.

Baseline Profile

Brand (brand_id) ace Profile Name (display_name) Cisco ACE Sample

comment
You can edit this sample baseline report to include more tests and requirements.
To do that, please refer to the AlgoSec Firewall Analyzer User Guide or online help.

Commands (CommandsDef)

Command

Command ID (id) 1 Command Name (name) Show Route Command Syntax (cmd) show ip route

Command

Command ID (id) 2 Command Name (name) Show Config Command Syntax (cmd) show running-config

Command

Use the menu to add attributes.

Document is unchanged

Add Subelement

Command

Add Attribute

Add Nodes

Add CDATA

Add comment

Add Top Element

CommandsDef

BaselineRequirement

- b. In the **Add Subelement** menu on the right side of the workspace, click **Command**.

Add Subelement

Command

Add Attribute

Add Nodes

Add CDATA

Add comment

Add Top Element

CommandsDef

BaselineRequirement

An additional Command window appears in the profile.

Commands (CommandsDef)

Command

Command ID (id) 1 Command Name (name) Show Route Command Syntax (cmd) show ip route

Command

Command ID (id) 2 Command Name (name) Show Config Command Syntax (cmd) show running-config

Command

Use the menu to add attributes.

Note: You can click **X** at anytime to remove a Top Element, Subelement, or Attribute from the profile.

- In the **Add Attribute** menu on the right side of the workspace, click attributes to add to the command. Available options are **id** (Command ID), **name** (Command Name), and **cmd** (Command Syntax). For details, see [Command](#).
- Fill in attribute fields.

Note: The Command ID must be unique.

The screenshot shows a window titled 'Commands (CommandsDef)' containing three 'Command' sub-windows. Each sub-window has three input fields: 'Command ID (id)', 'Command Name (name)', and 'Command Syntax (cmd)'. The first entry has ID 1, Name 'Show Route', and Syntax 'show ip route'. The second entry has ID 2, Name 'Show Config', and Syntax 'show running-config'. The third entry has ID 3, Name 'Show Password Strength', and Syntax 'show password'.

- To add a baseline requirement to the profile:

In the **Add Top Element** menu on the right side of the workspace, click **BaselineRequirement**.

A additional **Baseline Requirement** window appears in the profile.

The screenshot shows a window titled 'Baseline Requirement' with a blue header. Below the header, there is a text area containing the instruction: 'Use the menu to add subelements and attributes.'

- In the **Add Subelement** menu on the right side of the workspace, you can add the following subelements in hierarchical order:

- Command
- Criterion
- Line (Item)

For more details, see [Tag Reference](#),

- Click **Add Attribute** to add attributes to the baseline requirement or any of the subelements.
- Fill in attribute fields.

Note: The Command ID must be unique.

11. Click **Save**.

Tag Reference

This reference describes the use of each tag in the baseline configuration compliance profile. The tags are listed in the same order as they appear in the file.

Tag syntax is presented as follows:

- All parameters are presented in *italics*.
- All optional elements of the tag appear in square brackets [].

BaselineProfile

Syntax

```
BaselineProfile brand_id="id" display_name="name"
```

Description

This is the main tag for the baseline compliance profile, and it identifies the profile.

Parameters

brand_id	<p>String. The brand ID of the device brand relevant to the baseline configuration compliance report.</p> <p>The <code>brand_id</code> for each device brand is configured in the brand's <code>brand_config.xml</code> file in <code>/usr/share/fa/data/plugins/<i>brand_name</i></code>. See the <code>Id</code> parameter in the <code>DEVICE</code> tag.</p>
display_name	<p>String. The name of the baseline configuration compliance profile.</p> <p>The name will appear at the head of the Baseline Configuration Compliance Report.</p>

Subtags

- [CommandsDef](#) (see [CommandsDef](#))
- [BaselineRequirement](#) (see [BaselineRequirement](#))

Example

The following example describes a baseline profile for a Cisco ASA device with the name "Cisco ASA".

```
BaselineProfile brand_id="asa" display_name="Cisco ASA"
```

CommandsDef

SyntaxCommandsDefDescription

This tag specifies the sequence of commands that AFA should run on the device during analysis.

Parameters

None.

Subtags

- [Command](#) (see [Command](#))

BaselineRequirement

Syntax

BaselineRequirement name="*name*" id="*id*"

Description

This tag specifies a requirement that the device must meet in order to be considered "in compliance". The requirement consists of a list of required outputs for the commands that AFA will run on the device, specified in the CommandsDef (see [CommandsDef](#)) tag.

Parameters

name	String. The requirement's name.
id	Integer. The requirement's ID and order number. Commands are displayed in numerical order in the Baseline Compliance Report.

Subtags

- Command (see [Command](#))

Example`BaselineRequirement name="First" id="1"`

Command

Syntax

Command id="*id*" [**name**="*name*"] **cmd**="*cmd*"

Description

This tag specifies a command that AFA should run on the device.

Parameters

id	Integer. The command's ID and order number. Commands are implemented in numerical order.
name	String. The command's name.
cmd	String. The command that AFA should run on the device.

Subtags

- Criterion (see [Criterion](#))

Example`Command id="1" name="Check Access" cmd="show access-list"`

Criterion

Syntax

Criterion type="type"

Description

This tag specifies a criterion that the command output must meet.

Parameters

type	<p>String. The criterion type. This can be any of the following:</p> <ul style="list-style-type: none"> • Required Line. The line specified in the <code>Item</code> sub-tag must be present in the command output. • Required Regexp. The regular expression specified in the <code>Item</code> sub-tag must be present in the command output. • Forbidden Line. The line specified in the <code>Item</code> sub-tag must <i>not</i> be present in the command output. • Forbidden Regexp. The regular expression specified in the <code>Item</code> sub-tag must <i>not</i> be present in the command output. • Custom Function. The custom function specified in the <code>Item</code> sub-tag must return <code>true</code> when run on the command output. • Manual Review. The regular expression or line specified in the <code>Item</code> sub-tag will be searched for in the command output.
------	---

Subtags

- Item (see [Item](#))

Example`Criterion type="Custom Function"`

Item

Syntax

Item [comments="*comments*"]

Description

This tag specifies information about a criterion that the command output must meet.

Parameters

comments	String. Comments about a criterion that the command output must meet.
----------	---

Contents

This tag contains further details about a criterion that the command output must meet.

Subtags

None.

Example

```
<Item comments="first required line for command 2">extended permit ip  
207.193.122.0 255.255.255.0</Item>
```

BaselineHeader

Syntax

BaselineHeader title="*title*"

Description

This tag specifies information about the header text of the Baseline Compliance Report.

Parameters

title	String. The title that should appear in the header section of the report page.
-------	--

Contents

This tag contains the header text that should appear in the Baseline Compliance Report.

Subtags

None.

Example`<BaselineHeader title="Introduction">Introduction to the report</BaselineHeader>`

BaselineFooter

Syntax

BaselineFooter title="*title*"

Description

This tag specifies information about the footer text of the Baseline Compliance Report.

Parameters

title	String. The title that should appear in the footer section of the report page.
-------	--

Contents

This tag contains the footer text that should appear in the Baseline Compliance Report.

Subtags

None.

Example`<BaselineFooter title="Summary">Summary of the report</BaselineFooter>`

Sample Baseline Configuration Compliance Profile

```
<BaselineProfile display_name="Custom Profile" brand_id="asa">
  <CommandsDef>
    <Command id="1" name="Check Access" cmd="show access-list" />
  </CommandsDef>
```

```

<BaselineRequirement name="First" description="This is first requirement."
id="1">
  <Command id="1">
    <Criterion type="Required Line">
      <Item comments="">extended permit ip 207.193.122.0 255.255.255.0</Item>
      <Item comments="">extended permit tcp object-group</Item>
    </Criterion>
    <Criterion type="Required Regexp">
      <Item>.*\.company\.com</Item>
    </Criterion>
    <Criterion type="Forbidden Line">
      <Item>extended deny ip host 100.77.20.9 192.168.52.0</Item>
    </Criterion>
    <Criterion type="Custom Function">
      <Item>perl /home/shira/.fa/check_resolv.pl</Item>
    </Criterion>
  </Command>
</BaselineRequirement>

<BaselineHeader title="Introduction">Introduction to the report - freetext
</BaselineHeader>

<BaselineFooter title="Summary">Summary of the report - freetext
</BaselineFooter></BaselineProfile>

```

Advanced risk editing

This section explains how to perform advanced editing of custom risk items. For information on custom risk items, see [Customize risk profiles](#).

Overview

You can customize Risk Profiles by defining *custom risk items*. Custom risk items allow you to define more complex risks by composing the XQL query of your choice. For example, you can define risks for the following types of allowed traffic:

- Group of several services from X to Y
- Insecure external access to device
- Over N machines can manage your device
- TCP on over M ports can enter your network
- "From A to B with service C" rules

All operators used in risk item XQL queries are standard XQL operators: `eq`, `ne`, `lt`, `gt`, `and`, `or`, `$match$` (checks against a regular expression, e.g. `'/abc[de]'`), `no_match`, `brackets()`.

Risk item types

AFA supports the following types of risk items:

Type	Description
Traffic	<p>Relates to risks regarding traffic allowed through the device.</p> <p>This type of risk item can be used to detect risky traffic allowed by the device.</p> <p>In standard risk items, this type is represented by the letters D,J,Z,K,I,S,O,M,E. In custom risk items, this type is represented by the letter U.</p>
Host Group	<p>Relates to risks regarding host group definitions.</p> <p>This type of risk item can be used to detect certain host groups defined on the device, according to specific criteria.</p> <p>In standard risk items, this type is represented by the letter H. In custom risk items, this type is represented by the letter U.</p>
Properties	<p>Relates to risks regarding device property definitions.</p> <p>This type of risk item can be used to detect the value of certain device properties.</p> <p>In standard risk items, this type is represented by the letter P. In custom risk items, this type is represented by the letter U.</p>

Type	Description
Rules	<p>Relates to risks regarding rule definitions.</p> <p>This type of risk item can be used to detect specific rules in the policy, for example rules with "Any" as their source and so on.</p> <p>In standard risk items, this type is represented by the letter R. In custom risk items, this type is represented by the letter U.</p>

Traffic risk item guidelines

Sample traffic risk item (Rule I08)

```

Queries/QIndex[@name="q_srv_Outside_Inside"]/QEntry[
  @srv $eq$ "http" $and$
  eval("256", "Number") $lt$ @n_dst_impact_ips
]/QRes[
  @n_risky_dst_ips $ne$ 0 $and$
  @n_risky_src_ips $ne$ 0 $and$
  @is_vpn $ne$ "yes"
]

```

QIndex

This section specifies the traffic source and destination zones, by indicating them in the name of the query results file.

Parameters

@name	<p>The query results file's name in the format:</p> <p><code>q_srv_srcZone_dstZone</code></p> <p>where <i>srcZone</i> is the source zone, and <i>dstZone</i> is the destination zone, as defined in the AFA's device topology.</p> <p>Available zones include <code>Outside</code>, <code>Inside</code>, <code>DMZs</code>, and any user-defined zone type</p> <p>For example:</p> <ul style="list-style-type: none"> • In the preceding example, the file name is <code>q_srv_Outside_Inside</code>. • For traffic going from <code>Inside</code> to <code>DMZs</code>, the relevant file name would be <code>q_srv_Inside_DMZs</code>. • For traffic between different Internal zones, the relevant file name would be <code>q_srv_Inside_Inside</code>. <p>For access to device itself, use the file name <code>q_fw_access</code>.</p>
-------	---

QEntry

This section describes the type of traffic between the source and destination zones (specified in QIndex) that will trigger the risk. In the preceding example, a traffic query issued to the device simulation engine will trigger this risk if the service is HTTP and the number of affected destination IP addresses is over 256.

Parameters

@srv	The service that was queried.
@action	<p>The action that occurred:</p> <ul style="list-style-type: none"> • <code>PASS</code>. Traffic was passed by the device. • <code>DROP</code>. Traffic was blocked by the device.
@is_external_src	<p>Indicates whether the source zone of the traffic is external or not:</p> <ul style="list-style-type: none"> • <code>yes</code>. The source zone is external. • <code>no</code>. The source zone is not external.
@n_src_impact_ips	The total number of source IP addresses detected as relevant for this query.

@srv	The service that was queried.
@n_dst_impact_ips	The total number of destination IP addresses detected as relevant for this query.
@n_TCP_dst_ports	The total number of destination TCP ports detected as relevant for this query.
@n_UDP_dst_ports	The total number of destination UDP ports detected as relevant for this query.

QRes

This section describes the type of traffic query results that will trigger the risk. In the preceding example, the traffic must be encrypted in order for this risk to be triggered.

Parameters

@is_vpn	Indicates whether encrypted traffic should trigger the risk or not: <ul style="list-style-type: none"> • <code>yes</code>. Encrypted traffic should trigger the risk. • <code>no</code>. Encrypted traffic should not trigger the risk.
@pass_rule	The name of the rule that is relevant for this traffic in AFA.

Host group risk item guidelines

Sample host group risk item (RiskH02)

```
Hosts
/Host[
@name $eq$ "Trusted_hosts" $and$
eval("20", "Number") $lt$ @n_Total
]
```

This query checks whether the pre-defined "Trusted_hosts" object (which represents servers that can manage this firewall) contains a certain number of IP addresses.

Parameters

@name	The host group's name. Only alphanumeric characters, '_', '.', and '-' can be used. Other characters are automatically replaced by '_'.
@n_Total	The number of IP addresses contained in the host group.
@internal	Indicates whether this host group contains internal IP addresses: <ul style="list-style-type: none"> • yes. This host group contains internal IP addresses. • no. This host group does not contain internal IP addresses.
@external	Indicates whether this host group contains external IP addresses: <ul style="list-style-type: none"> • yes. This host group contains external IP addresses. • no. This host group does not contain external IP addresses.
@zone_spanning	Indicates whether this host group spans multiple zones: <ul style="list-style-type: none"> • yes. This host group spans multiple zones. • no. This host group does not span multiple zones.

Property risk item guidelines

Property risk items are used to detect the value of certain firewall properties. These properties are extracted by AFA during analysis. For a full list of properties, refer to the `properties.xml` file in the relevant report directory.

Note: Properties will differ between firewall vendors. Parameters can be created for Check Point firewalls from the `asm.C` file.

Sample property risk item (risk P05)

```
Props[http_enforce_buffer_overflow[@value $ne$ "true"]]
```

Rule risk item guidelines

Sample rule risk item (risk R01)

```
Rules/Rulebase[@interface="%INTERFACE"]/Rule
```

```
[
@dst      =   "*"   $and$
@srv      =   "*"   $and$
@orig_rule $ne$ ""   $and$
@orig_rule $ne$ "0"  $and$
@vpn $ne$ "VPN_PERMIT" $and$
@vpn $ne$ "VPN" $and$
@action   =   "PASS"
]
```

This query detects all rules other than VPN rules, where both the destination and the service are "any", and the action is "PASS".

Parameters

@src	The source object of the rule.
@dst	The destination object of the rule.
@srv	The service object of the rule.
@src_xlt	The translated source hostgroup object.
@dst_xlt	The translated destination hostgroup object.
@ruleno	The expanded rule ID.
@action	The rule action: <ul style="list-style-type: none"> PASS. Pass the specified traffic. DROP. Drop the specified traffic.
@orig_rule	The original rule number (in vendor format).

@src	The source object of the rule.
@vpn	Indicates whether the rule is a VPN rule, as well as whether traffic is encrypted: <ul style="list-style-type: none"> • A number. The rule is a VPN rule, and the number indicates the relevant VPN rule's number. Traffic is not encrypted. • VPN or VPN_PERMIT. The rule is a VPN rule. Traffic is encrypted. • Empty (""). The rule is not a VPN rule.

Note: AFA performs these queries on its internal "Expanded rules". To see these rules in your device report, go to **Explore Policy -> Expanded Rules**.

Assessment and remedy keywords

The following keywords can be added to risk item assessments and remedies, for richer user-defined risk descriptions in the report. Keyword use is optional.

For more details, see [Customize risk items](#).

Traffic Risk Item Keywords

Keyword	Description
%AMOUNT	The number of rules that contributed to the risk.
%CUSTOMIZATION_NOTE	Standard text explaining how to eliminate this risk.
%FWNAME	A link to the device's host group.
%HGRP{ <i>hostgroup</i> }	A link to the specified host group, <i>hostgroup</i> . Can contain a zone name: <i>Inside</i> , <i>Outside</i> , <i>DMZs</i> , or a user-defined zone name.
%HREF{ <i>url</i> }	A link to an HTML file, <i>url</i> .
%N_DST_IMPACT_IPS	The number of destination IP addresses in the query output (without VPNs).

Keyword	Description
%N_DST_IMPACT_IPS_COUNT_VPN	The number of destination IP addresses in the query output (with VPNs).
%N_SRC_IMPACT_IPS	The number of source IP addresses in the query output (without VPNs).
%N_SRC_IMPACT_IPS_COUNT_VPN	The number of source IP addresses in the query output (with VPNs).
%N_TCP_DST_PORTS	The number of reachable destination TCP ports in the query output.
%N_UDP_DST_PORTS	The number of reachable destination UDP ports in the query output.
%PCIDS	The Payment Card Industry Data Security Standard risk level.
%QREF{ <i>QueryInputFile:service</i> }	A "Details" button linking to the query results for the specified traffic, where: <i>QueryInputFile</i> is the query input file, and <i>service</i> is the service, as defined in the AFA's device topology. For example: %QREF{q_srv_Inside_Outside:http}
%QSRC_LIST { <i>QueryInputFile</i> }	A list of source host groups that can access the device, as specified in the query input file, <i>QueryInputFile</i> .
%SRV{ <i>service</i> }	A link to the specified service, <i>service</i> . For example, %SRV{smtp} would be replaced by "smtp" and linked to the definition of this service, as defined on this device.
%SRV_LIST	A list of all the services in the query output.
%SRV_TABLE { <i>QueryInputFile</i> }	A "Details" button linking to a table of the services in the query results, where <i>QueryInputFile</i> is the query input file.

Host Group Risk Item Keywords

Keyword	Description
%AMOUNT	The number of rules that contributed to the risk.
%CUSTOMIZATION_NOTE	Standard text explaining how to eliminate this risk.
%HGRP{ <i>hostgroup</i> }	A link to the specified host group, <i>hostgroup</i> . Can contain a zone name: <i>Inside</i> , <i>Outside</i> , <i>DMZs</i> , or a user-defined zone name.
%HOST_TABLE	A list of relevant host groups.
%HREF{ <i>url</i> }	A link to an HTML file, <i>url</i> .
%N_OUTSIDE_IPS	The number of outside IP addresses in the query output.
%N_TOTAL	The total number of IP addresses in the query output.
%PCIDS	The Payment Card Industry Data Security Standard risk level.
%SRV{ <i>service</i> }	A link to the specified service, <i>service</i> . For example, %SRV{smtp} would be replaced by "smtp" and linked to the definition of this service, as defined on this device.

Property Risk Item Keywords

Keyword	Description
%CUSTOMIZATION_NOTE	Standard text explaining how to eliminate this risk.
%HGRP{ <i>hostgroup</i> }	A link to the specified host group, <i>hostgroup</i> . Can contain a zone name: <i>Inside</i> , <i>Outside</i> , <i>DMZs</i> , or a user-defined zone name.
%HREF{ <i>url</i> }	A link to an HTML file, <i>url</i> .
%META { <i>MetaDataParam</i> }	A link to a parameter, <i>MetaDataParam</i> , that was extracted during AFA analysis.

Keyword	Description
%PCIDS	The Payment Card Industry Data Security Standard risk level.
%PROPERTY { <i>propertyName</i> } { <i>displayName</i> }	A link to the specified device property, <i>propertyName</i> . The link anchor text is specified in the parameter <i>displayName</i> .
%SRV{ <i>service</i> }	A link to the specified service, <i>service</i> . For example, %SRV{smtp} would be replaced by "smtp" and linked to the definition of this service, as defined on this device.

Rule Risk Item Keywords

Keyword	Description
%AMOUNT	The number of rules that contributed to the risk.
%CUSTOMIZATION_ NOTE	Standard text explaining how to eliminate this risk.
%HGRP{ <i>hostgroup</i> }	A link to the specified host group, <i>hostgroup</i> . Can contain a zone name: <i>Inside</i> , <i>Outside</i> , <i>DMZs</i> , or a user-defined zone name.
%HOST_TABLE	A list of relevant host groups.
%HREF{ <i>url</i> }	A link to an HTML file, <i>url</i> .
%PCIDS	The Payment Card Industry Data Security Standard risk level.
%RULE	A link to the first rule in the query output.
%RULE_TABLE	A list of all the rules in the query output.
%SRV{ <i>service</i> }	A link to the specified service, <i>service</i> . For example, %SRV{smtp} would be replaced by "smtp" and linked to the definition of this service, as defined on this device.
%SRV_LIST	A list of all the services in the query output.

Configure notifications

This section describes how to configure the different types of automatic e-mail messages supported by AFA.

For details, see:

- [Schedule dashboard notifications](#)
- [Configure event-triggered notifications](#)
- [Configure device report page messages](#)

Schedule dashboard notifications

You can schedule dashboard e-mail notifications, by adding a dashboard e-mail job to the AFA Scheduler.

Add and edit dashboard e-mails

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Scheduler** tab.

The **Scheduler Setup** page appears with a list of scheduled analysis and dashboard e-mail jobs.

Firewall Analyzer | Analysis Status | AlgoSec Administrator

Administration

DEVICES SETUP | USERS/ROLES | **SCHEDULER** | COMPLIANCE | OPTIONS | MONITORING | DOMAINS | ARCHITECTURE

Schedule Recurring Analysis

Job	Name	Timing	Device / Group	Risk Profile	Edit	
<input type="checkbox"/>	1	Job 1	Daily at 19:30	Rose_checkpoint	Default	

Delete [New](#)

Schedule Dashboard E-Mail

Job	Name	Timing	Dashboard	Edit	
<input type="checkbox"/>	2	Dash 2	Daily at 19:30	Compliance Dashboard	

Delete [New](#)

4. Do one of the following:

- To schedule a new dashboard email job, in the **Schedule Dashboard E-mail** area, click **New**.
- To edit an existing dashboard email job, click on the Edit icon next to the desired job.

New fields appear.

The screenshot shows the 'Administration' section of the Firewall Analyzer interface, specifically the 'SCHEDULER' tab. The page title is 'Administration' and the sub-page is 'Schedule Dashboard E-Mail'. The interface is divided into several sections:

- Job Details:** Contains a 'Job name' text field with the value 'Dash 3' and a 'Select dashboard' dropdown menu showing 'Compliance Dashboard (11 charts)'.
- Email Details:** Contains a 'Recipients' text area with the value 'example@domain.net;someone@someplace.com', an 'Email Subject' text field, and an 'Email Body' text area.
- Recurrence:** Contains radio buttons for 'Daily' (selected), 'Weekly', 'Monthly', 'Quarterly', and 'Yearly'.
- Recurrence Pattern:** Contains a 'Set time' section with two dropdown menus showing '19' and '30'.

At the bottom right of the form, there are 'Cancel' and 'OK' buttons.

5. In the **Job name** field, type a name for the job.
6. In the **Select dashboard** drop-down list, choose a dashboard.
7. In the **Recipients** field, type an email address or a comma separated list of multiple email addresses to which to send the notifications.
8. (Optional) In the **Email Subject** field, type a subject for the email notifications.
The default subject is the dashboard's name.
9. (Optional) In the **Email Body** field, type a message to include in the body of the email notifications.
10. In the **Recurrence** area, specify how often the analysis job should run.

You can select either a daily, weekly, monthly, quarterly, or yearly analysis, or configure the analysis to occur when a policy is installed on the device(s).

The fields in the **Recurrence Pattern** area change according to your selection.

11. In the **Recurrence Pattern** area, configure the desired pattern of recurrence.
12. Click **OK**.

Deleting Scheduled Jobs

Use this procedure to delete a scheduled analysis or dashboard email.

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Scheduler** tab.

The **Scheduler Setup** tab is appears with a list of scheduled analysis and dashboard e-mail jobs.

4. Select the check box next to the desired job.

5. Click **Delete**.

A confirmation message appears.

6. Click **Yes**.

The job is deleted.

Configure event-triggered notifications

You can configure AFA to send e-mail notifications when certain events occur. All notifications are configured per user or role, and device related notifications are configured per device.

Supported notifications

Supported notifications include:

- When an analysis detects changes in the risks or policy of a device.
- When an analysis is completed.
- When real-time change monitoring detects configuration changes.
- When rules and VPN users are about to expire.
- When a system error or system customization occurs.

E-mail Notification Example 1: Analysis completed

Dear John Smith,

The Firewall Analyzer report for firewall checkpoint1 is ready.
You can view the report at
https://192.168.2.5/~demo/fa_reports/demo-12/index.html
Report summary:

Findings	
Risks Found: 2 medium risk, 2 low risk.	
Code	Risk Description
1. H03	External machines can manage your firewall (x3)
2. O03	Inside clients can connect to external IRC servers (x1 <i>all new</i>)
3. R02	Implicit Check Point Rules (DNS/TCP) (x1)
7. D02	TCP on all ports between internal networks (x1 <i>all new</i>)

E-mail Notification Example 2: Changes to policy and risks

Policy Changes since Last Analysis

Changes found between 2005-05-30 (demo-11) and 2005-06-01 (demo-12)

- **Changes In Risks**

ID	Risk Description
O03	Inside clients can connect to external IRC servers (x1 <i>all new</i>)
D02	TCP on all ports between internal networks (x1 <i>all new</i>)
H04	Zone-spanning object definitions (x1 1 less)

- **Changes In Rules**

Filtering rules

Changes	RULE	SOURCE	DESTINATION	SERVICE	ACTION	SOURCE NAT	DESTINATION NAT
4	X	1	zoonet	one__Valid_Address	http	PASS	-
5	X	1	zoonet	one__Valid_Address	https	PASS	-

The list of all your reports can be viewed at https://192.168.2.5/~demo/fa_reports/

Yours,
The Algorithmic Security Firewall Analyzer

Configure AFA to send event triggered e-mail notifications

1. Configure the mail server settings. For details, see [Configuring Mail Server Settings](#).
2. Enable the desired notifications for each user or role that should receive e-mail notifications. For details, see [Manage users and roles in AFA](#).

Configuring Mail Server Settings

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. In the **Options** tab, click the **Mail** sub-tab.

The **Mail** tab appears.

The screenshot shows the 'Administration' page in the Firewall Analyzer interface. The 'Mail' tab is selected under the 'OPTIONS' section. The configuration is divided into three main sections:

- SMTP server:** Includes fields for 'Server name', a checkbox for 'Use name and password', 'Username', 'Password', and a checkbox for 'Use SSL'.
- Email notification FROM address:** Includes an 'Email address' field with the value 'demo-fireflow@algosec.com' and a 'Test E-Mail message' button.
- Email greeting:** Includes a text area with the default greeting: 'Dear %NAME%,
[From the AlgoSec Firewall Analyzer demo server]' and a 'Default' button.

At the bottom of the form are 'Cancel' and 'OK' buttons.

4. Complete the fields as needed:

Server name	Type the SMTP server's name.
Use name and password	Select this option if the SMTP server requires a username and password.
Username	Type the username for the SMTP server.
Password	Type the password for the SMTP server.
Use SSL	Select this option to use SSL when authenticating with the SMTP server.
Email Notification FROM address	Type the "From" address of the notification. All e-mail notifications will appear as coming from this e-mail account.

Test E-Mail message	Click this button to send a test e-mail to all administrators.
Email greeting	Type an e-mail greeting to include in the body of the e-mail. (Optional)
Default	Click this button to reset the e-mail greeting to its default setting.

5. Click OK.

Configure device report page messages

You can configure AFA to send specific report pages to a user automatically, each time a report is generated for a certain device. AFA sends the specified user a single e-mail with the specified report pages attached as individually zipped PDF documents. The e-mail includes a list of the attached report pages, as well as a list of any report pages that could not be attached due to inadequate permissions or size limitations.

Note: The specified user must have permission to view the device and the specified report pages. E-mails will not be sent to users that do not have permission to view the device. Report pages for which the user does not have permissions will not be included in the e-mail. No e-mail notification options need to be enabled in the user's settings in order for the user to receive these e-mail messages.

Note: By default, each e-mail can be sent with up to 10 MB of attachments, only. Once the size limit has been reached, additional report pages will not be attached. It is possible to change the size limit, by opening `/home/afa/.fa/config` and adding the following line:

```
MaximumReportZipFileSize=sizeLimit
```

Where *sizeLimit* is the desired size limit in MB.

Note: It is possible to generate report page PDFs (including those that cannot be

sent to a user due to inadequate permissions or size limitations) for additional uses. For example, you could export the PDFs to a central repository in order to display them on an enterprise or MSSP portal. The desired usage should be implemented by a script that receives the path of the report's directory as a parameter, and which runs after generating report pages for all devices and users, but before removing all of the created files.

To configure AFA to use such a script, open `/home/afa/.fa/config` and add the following line:

```
PostPublishReportParts=command
```

Where *command* is the command to run.

To automatically send device report pages to users:

1. On the AFA server, under `/home/afa/.fa`, create a file called `publish_def.xml`.
2. Add the following lines to this file:

```
<ReportPartsPublish>
<DevicesDef>
<Device name="deviceName">
<User username="userName" parts="reportPages" />
</Device>
</DevicesDef>
</ReportPartsPublish>
```

Where:

- *deviceName* is the name of the device whose report pages should be sent. A list of all device names is available in the file `/home/afa/.fa/firewall_data.xml`.
- *userName* is the username of the user who should receive the report pages. A list of all usernames is available in the file `/home/afa/.fa/users_info.xml`.

- *reportPages* is a list of report page IDs separated by semicolons (;). A list of report pages and their IDs is available in the file `/usr/share/fa/data/publish_parts.xml`, where each report page is represented by a `Part` tag, and each page's ID number appears in the `Part` tag's `id` attribute.

An example is available under `/usr/share/fa/data`.

Note: Parts 1-14 are supported for group reports and single device reports. Parts 15 and up are only supported for single device reports.

3. Save the file.

Define AFA preferences

Use the following procedure to set preferences when domains are not enabled or when setting preferences in a specific domain.

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab and the **General** sub-tab.

3. Access the desired configuration options, by clicking the relevant sub-tab in the **Options Menu** area.

4. Set the desired preferences by completing the relevant fields:

- To set general analysis options, complete the fields using the information in General (see [General](#)).
- To set language options, click the **Language** sub-tab and complete the fields using the information in Language (see [Language](#)).
- To set Web interface options, click the **Display** sub-tab and complete the fields using the information in Display (see [Display](#)).
- To set log analysis options, click the **Log analysis** sub-tab and complete the fields using the information in Log Analysis (see [Log analysis](#)).
- To configure a proxy server, click the **Proxy** sub-tab and complete the fields using the information in Proxy (see [Define a device proxy](#)).
- To configure a mail server, click the **Mail** sub-tab and complete the fields using the information in Mail (see [Mail](#)).

- To set criteria for storing/deleting AFA reports, click the **Storage** sub-tab and complete the fields using the information in Storage (see [Storage](#)).
- To integrate AFA with a change management system, click the **Workflow** sub-tab and complete the fields using the information in Workflow (see [Workflow](#)).
- To configure how users are authenticated, click the **Authentication** sub-tab and complete the fields using the information in Authentication (see [Authentication](#)).
- To set backup and restore options (for all of ASMS), click the **Backup/Restore** sub-tab and complete the fields using the information in Backup/Restore (see [Backup/Restore](#)).

Note: If you are logged in to a specific domain in an ASMS environment with domains enabled, only the following options are available: General, Display, Authentication, Log Analysis, and Workflow.

5. To set advanced configuration parameters, click the **Advanced Configuration** sub-tab and complete the fields using the information in Advanced Configuration (see [Advanced Configuration](#)).
6. After changing a set of options, click **OK**.

Note: AFA preferences, as well as other information, are stored in the `.fa` directory in the user's home directory.

General

Use the **General** tab to set the following options.

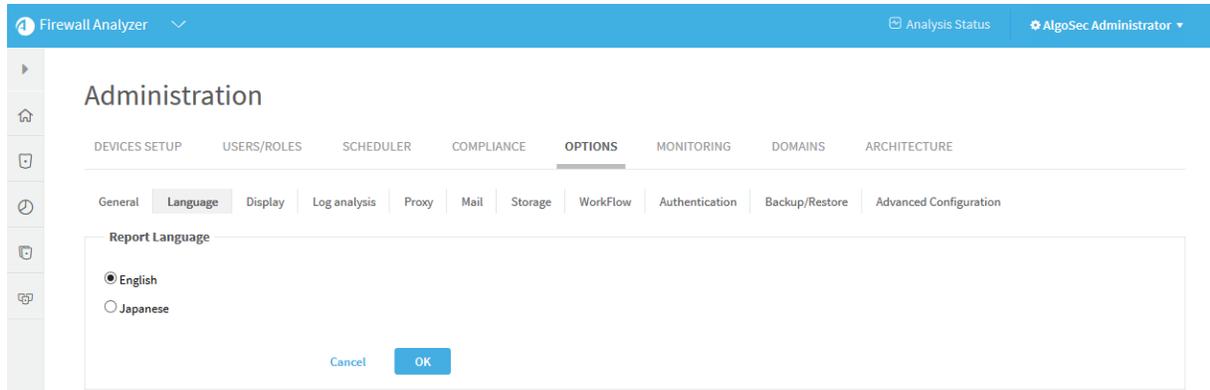
General Fields

In this field...	Do this...
Comprehensive mode - analyze every service defined on the device (slow)	<p>Select this option to specify that AFA should analyze all of the services defined on the device, and not only the ones relevant for risks.</p> <p>Selecting this option results in more comprehensive information in the reports' Policy tab, particularly when comparing different reports.</p> <p>Note: Checking this option will result in longer analysis time and will require more disk space.</p>
With IP address name lookups (slow)	<p>Select this option to add the DNS name next to any IP address shown in a report, if a DNS name exists. This functionality requires the AFA machine to be connected to the network and configured to use a name server.</p> <p>If you want analysis to run faster, clear this option.</p>
Include traffic changes analysis in Change History (slow)	<p>Select this option to specify that the Changes report page should include the calculated changes in allowed traffic (in addition to its regular content).</p> <p>If you want analysis to run faster, clear this option.</p>
Timed rules: only apply rules active at analysis time	<p>Select this option to specify that time-dependant rules should only be applied if they are active when AFA analysis is performed. This is relevant to policy optimization criteria.</p>
Use public key authentication in data collection	<p>Select this option to use public key authentication in SSH connections to a Check Point management, Juniper Netscreen devices, or NSMs.</p> <p>Note: When this option is enabled, the password defined for the device(s) in AFA must be the local private key passphrase.</p>
Simulation timeout (seconds)	<p>Type the maximum amount of time in seconds that a traffic simulation query can run.</p>

In this field...	Do this...
Data collection timeout (seconds)	Type the amount of time in seconds that the device analyzer should wait for the device's reaction before aborting communications. If you encounter timeout problems, increase this value.
Days before expiration alerts	Type the number of days before a device rule or VPN user expires that AFA should consider the rule/user as about to expire. This is relevant for policy optimization and for users who are configured to receive such notifications.
Report rules whose comment field...	Complete this field to indicate you want to find rules whose comments match a regular expression, or rules whose comments do not match a regular expression. Select the desired operator in the drop-down menu and type a regular expression describing the format for the rule comment. For example, if you select does not match , and then type a regular expression that defines the required format of a rule comment, you can detect non-compliant rule comments. Click on the Details button for more information and examples of regular expressions. If this field is left empty, rule comment detection will be disabled.
Run device analysis	Select Only if the policy/topology changed to specify that if a policy is detected as unchanged during a <i>scheduled</i> analysis, then AFA should <i>not</i> run a full report, but instead create an unchanged report that links to the last report for the policy. Select Always to specify that AFA will always run a full analysis, regardless of whether the policy has changed or not. Note: Selecting the Always option will result in longer analysis time and will require more disk space.

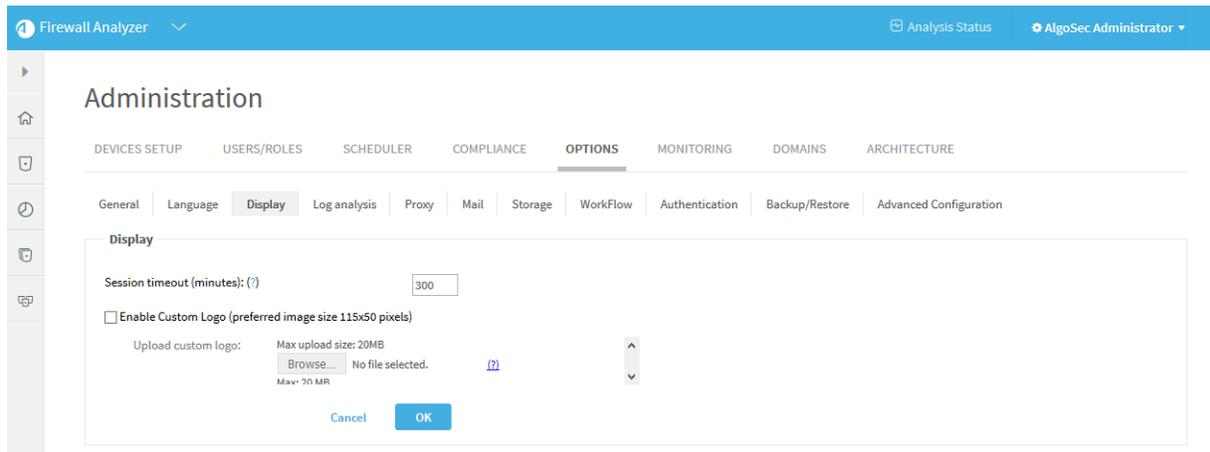
Language

In the **Language** tab, select the language for risk titles in reports. Currently only English and Japanese are supported.



Display

In the **Display** tab, set the display options described below.



Display Fields

In this field...	Do this...
Session timeout (minutes)	Enter the number of minutes of inactivity before a user is logged out of the Web interface.

In this field...	Do this...
Enable Custom Logo	<p>Select this option to upload a custom logo that will appear at the top right corner of every page of the AFA, FireFlow and AppViz Web Interfaces, as well as all future AFA reports.</p> <p>The logo file must be in GIF, JPG, or PNG format, and it must be 115 pixels in width and 50 pixels in height. It is important to use these exact dimensions, so that the logo image is not distorted.</p> <p>To remove a custom logo, clear this check box.</p>

Log analysis

In the **Log analysis** tab, set the log analysis options described below.

The screenshot shows the Firewall Analyzer Administration interface. The top navigation bar includes 'Firewall Analyzer', 'Analysis Status', and 'AlgoSec Administrator'. The main navigation menu includes 'DEVICES SETUP', 'USERS/ROLES', 'SCHEDULER', 'COMPLIANCE', 'OPTIONS', 'MONITORING', 'DOMAINS', and 'ARCHITECTURE'. The 'OPTIONS' tab is selected, and the 'Log analysis' sub-tab is active. The 'Log Analysis Options' section contains two input fields: 'Use log starting 500 days before the report date' and 'Timeout for log analysis is 900 minutes'. There are 'Cancel' and 'OK' buttons below these fields. The 'Syslog Collection for BusinessFlow Discovery' section has a 'Define' button.

Log analysis fields

In this field...	Do this...
Use log starting <i>n</i> days before the report date	<p>Type the number of days before a report date to specify how far back you want to use log data when generating AFA reports.</p> <p>For example, if you set this field to 180, AFA will use all logs generated between 180 days before the report date and the actual report date, when creating the report.</p>

In this field...	Do this...
Timeout for log analysis is <i>n</i> minutes	Type the maximum amount of time in minutes for log analyses to run.
Define log collection for selected devices	Click Define to define log collection for AppViz Discovery.

Define a device proxy

In the **Proxy** tab, set the proxy options described below.

Note: If you do not know the proxy settings in your organization, contact your local network administrator.

The screenshot shows the Firewall Analyzer Administration console. The top navigation bar includes "Firewall Analyzer" and "AlgoSec Administrator". The main navigation menu includes "DEVICES SETUP", "USERS/ROLES", "SCHEDULER", "COMPLIANCE", "OPTIONS", "MONITORING", "DOMAINS", and "ARCHITECTURE". The "OPTIONS" tab is selected, and the "Proxy" sub-tab is active. The "Proxy" configuration page contains the following elements:

- Use proxy server
- Proxy: Port:
- Use proxy authentication
- Username: Password:
- Buttons: Cancel, OK

Proxy fields

In this field...	Do this...
Use proxy server	<p>Select this option to specify that a proxy server is used to access the Internet. This is relevant for the following situations:</p> <ul style="list-style-type: none"> You want to connect to cloud devices defined in AFA (such as AWS or Azure) via a proxy server. You want to validate your AFA "Online" license via a proxy server. Defining the proxy server enables AFA to access the license server. <p>Note: This only applies if you received an "Online" license from AlgoSec.</p> <p>Note: Only one proxy server can be defined.</p>
Proxy	Type the proxy server's IP address.
Port	Type the port number used by the proxy server.
Use proxy authentication	<p>Select this option if the proxy server requires authentication.</p> <p>If you select this option, you must complete the Username and Password fields.</p>
Username	Type the username to use for authenticating to the proxy server.
Password	Type the password to use for authenticating to the proxy server.

Mail

In the **Mail** tab, configure a mail server for sending automatic e-mail notifications. For information about AFA e-mail notifications, see [Configure event-triggered notifications](#).

The screenshot shows the 'Administration' section of the Firewall Analyzer interface. The 'Mail' tab is selected under the 'OPTIONS' category. The configuration is divided into three sections:

- SMTP server:** Includes a 'Server name' text field, a checkbox for 'Use name and password', 'Username' and 'Password' text fields, and a checkbox for 'Use SSL'.
- Email notification FROM address:** Includes an 'Email address' text field containing 'demo-fireflow@algosec.com' and a 'Test E-Mail message' button.
- Email greeting:** Includes a text area containing 'Dear %NAME%,
[From the AlgoSec Firewall Analyzer demo server]' and a 'Default' button.

At the bottom of the form are 'Cancel' and 'OK' buttons.

Storage

Whenever AFA generates a report, the report is stored on the AFA server. Each AFA report may consume significant amounts of storage (about 75 MB* per report on average, though this can greatly vary). For example, if you have four devices whose policies are changed and analyzed daily, then AFA reports will consume about $4 \times 75 = 300$ MB per day, $7 \times 4 \times 75 = 2.1$ GB per week. Therefore, you would require an empty 150 GB disk in order to store 70 weeks worth of reports.

To enable you to efficiently manage your available disk space, and to prevent an overload of data on the AFA server, you can configure AFA to delete old reports, based on deletion criteria you define. You can configure clean-up to run automatically or trigger it manually, as needed.

Note: AFA checks the amount of local disk space remaining after running each report. If the remaining space is less than 10 GB, or if more than 95% of the disk is already used, AFA sends a warning e-mail to the users configured to receive error messages via e-mail notifications. See [Configuring Event-Triggered Notifications](#) (see [Configure event-triggered notifications](#)). In addition, AFA also sends notifications via the issues center and Syslog messages.

Note: AFA provides an option to only run a *scheduled* analysis if policy changes were detected since the previous analysis. This option ensures that full analyses will only run when the report will differ from the most recent report, saving both the CPU time needed to produce a report and the disk space needed to store it. To enable this option, select the **Run analysis only when policy is changed** check box, in the **General** sub-tab of the **Options** tab in the Administration area. For more details, see [Define AFA preferences](#).

Note: You can optionally save reports on your remote backup server by including reports in your ASMS backups. See the Backup/Restore (see [Backup/Restore](#)) tab.

Configure report cleanup

Do the following:

1. In the toolbar, click your username.
A drop-down menu appears.
2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

The screenshot shows the Firewall Analyzer Administration page with the Options tab selected. The page title is "Administration" and the sub-tab is "Options". The "Analysis Options" section contains the following settings:

- Comprehensive mode - analyze every service defined on the device (slow)
- With IP address name lookups (slow)
- Include traffic changes analysis in Change History (slow)
- Timed rules: only apply rules active at analysis time
- Use public key authentication in data collection
- Simulation timeout (seconds):
- Data collection timeout (seconds):
- Days before expiration alerts:
- Report rules whose comment field: [Details](#)

The "Default Scheduled Analysis Options" section contains:

- Run device analysis:

Buttons for "Cancel" and "OK" are located at the bottom of the form.

3. Click **Storage**.

The **Storage** tab appears.

The screenshot shows the Firewall Analyzer Administration page with the Storage tab selected. The page title is "Administration" and the sub-tab is "Storage". The "Automatic Report Deletion" section contains the following settings:

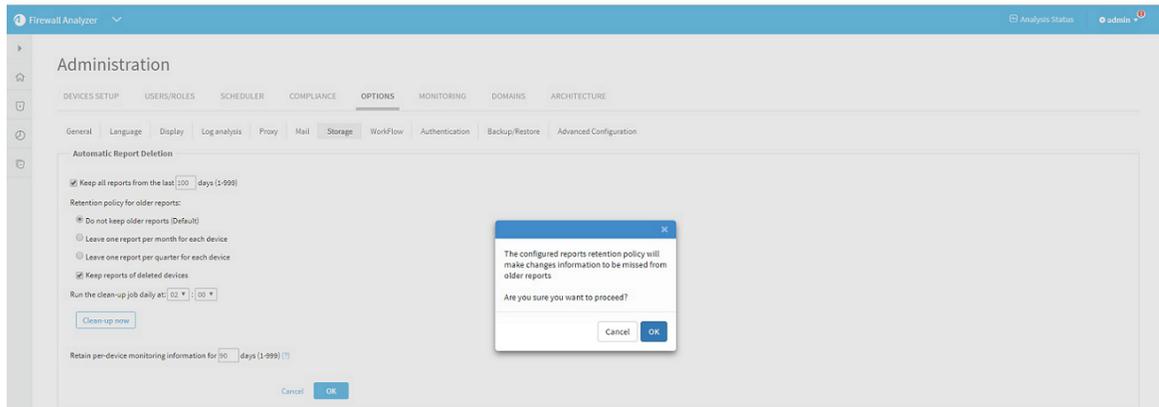
- Keep all reports from the last: days (1-999)
- Retention policy for older reports:
 - Do not keep older reports (Default)
 - Leave one report per month for each device
 - Leave one report per quarter for each device
 - Keep reports of deleted devices
- Run the clean-up job daily at: :
- [Clean-up now](#)
- Retain per-device monitoring information for days (1-999) (?)

Buttons for "Cancel" and "OK" are located at the bottom of the form.

4. Complete the fields using the information in Storage Fields (see [Storage Fields](#)).

5. Click **OK**.

If the number of days to retain reports is greater than the number of days to retain the monitoring information, a confirmation message appears.



Click **OK**.

The settings are changed.

6. To delete any reports that meet the deletion criteria immediately, rather than wait until the next scheduled clean-up time, do the following:

7. Click **Clean-up now**.

A success message appears.

8. Click **OK**.

Storage Fields

In this field...	Do this...
Keep all reports from the last <i>n</i> days	Select this option to enable automatic deletion of reports older than a specified number of days, then type the number of days after which reports should be deleted.
Do not keep older reports (Default)	Click this option to specify that AFA should delete all reports that have reached the age specified in the Keep all reports from the last <i>n</i> days field.
Leave one report per month for each device	Click this option to specify that each month AFA automatically deletes all reports, except for the most recent successful report for each device, for audit purposes.

In this field...	Do this...
Leave one report per quarter for each device	Click this option to specify that each quarter AFA automatically deletes all reports, except for the most recent successful report for each device, for audit purposes.
Keep reports of deleted devices	Select this option to specify AFA retain a device's reports when the device is removed from AFA.
Run the clean-up job daily at	Use the drop-down lists to specify the time at which AFA should perform automatic deletion each day.
Clean-up now	Click this button to delete any reports that meet the deletion criteria immediately, rather than wait until the next scheduled clean-up time. Important: If you made changes to the deletion criteria that you want to apply to the clean-up, click OK to save the changes before clicking this button.
Retain per-device monitoring information for <i>n</i> days	Type the number of days of change monitoring reports you want to retain for each device.

Workflow

In the **Workflow** tab, define the parameters for integration with an external corporate Change Management System (CMS). AFA supports integration with AlgoSec FireFlow, BMC Remedy, HP ServiceCenter (ServiceNow), or any other system supporting Web-based access.

When implementing a requested change in the device, many organizations choose to specify a CMS ticket ID in the relevant rule comment. AFA will automatically detect such CMS ticket IDs in rule comments. Wherever a rule is displayed in the AFA report, its comment will include a link to the CMS system, pointing at the relevant ticket. Clicking the link opens a browser window with the relevant CMS ticket open, allowing further examination of the change (who requested it, who authorized it and when, etc.).

Change request ID format

This option is relevant for all Workflow types. This option allows you to define a format to which the device rule comments must comply so AlgoSec recognizes them as containing a change request id. Only properly formatted rule comments will be linked to the CMS change request.

AFA will look for the following format in the rule comments:

```
<Before><Chang_Request_id><After>
```

Where **<Before>** and **<After>** are fixed strings, and **<Change _Request_id>** is a Perl regular expression (see note below).

For example:

Field	Input
Before	Change Request #
Change Request id	\d+
After	#

This comment will become a link: 'Change Request #1234#'. This comment will not become a link: 'Change Request 1234#' , because **<Before>** is not equal to 'Change Request #'.

Note: The required `Change_Request_id` format must be specified as a Perl regular expression. You can find tutorials on writing regular expressions on the Internet. Here are some examples of the type of things you can accomplish:

Note: `\d` represents a digit, `\s` represents a space, `\w` - an alphanumeric character.

Note: Examples:

`\d\d\d\d-\d\d-` comments must contain a change request number like 1234-56

\d\d-\d\d-\d\d\d\d\d- comments must contain a date like 01-01-2007

[A-Z]{2}\s*\d+- comments must contain two capital letters, then zero or more spaces, then one or more digits (e.g. "AK 123")

AlgoSec FireFlow

If you use AlgoSec FireFlow, select **AlgoSec Fireflow** in the **Workflow** tab to fill in FireFlow-specific parameters.

The screenshot shows the 'Administration' section of the Firewall Analyzer interface. The 'OPTIONS' tab is selected, and the 'Workflow' sub-tab is active. The 'Workflow' configuration area includes the following fields and buttons:

- Enable integration with external Change Management System
- AlgoSec FireFlow (dropdown menu)
- Server: [text input field]
- URL Template: /FireFlow/Ticket/Display.html?id=__REQUEST_ID__
- Change Request Id Format: Before: FireFlow #
- Change Request Id: Change Request Id: \d+
- After: [text input field]
- Buttons: Details, Show Full URL, Cancel, OK

- **Server:** Name of the AlgoSec FireFlow server to be accessed (usually the AFA server).
- **URL Template:** The structure of the URL that will be created for change request ID links in AFA reports. The following keywords will be replaced by the relevant values: `__SERVER_NAME__` and `__REQUEST_ID__`.
Click the **Show Full URL** button to see the resulting URL string.

BMC Remedy

If you use a BMC Remedy Change Management System, select **BMC Remedy** in the **Workflow** tab to fill in Remedy-specific parameters.

The screenshot shows the 'WorkFlow' configuration page in the Firewall Analyzer. The 'Enable integration with external Change Management System' checkbox is checked. The 'Server' field is empty, 'Mid Tier Server' is empty, and 'Form' is set to 'CHG:Infrastructure Change'. The 'URL Template' field contains the text 'http://_MID_TIER_SERVER_/arsys/servlet/ViewFormServlet?server'. There are also fields for 'Change Request Id Format' with 'Before' and 'After' sub-fields, and a 'Show Full URL' button.

Fill in the different fields, in order to allow AFA to create the correct links. The format of a typical URL to a Remedy change request is as follows:

```
<protocol>://<mid_tier_server>/arsys/servlet/ViewFormServlet?server=
<server_name>&form=<form_name>&qual=<query>
```

Where:

- `<protocol>`: may be either `http` or `https`
- `<mid_tier_server>`: (required) - the server name or IP where the Mid Tier is installed. May contain an optional port number, format: `192.168.2.60:8080`
- `<server_name>`: (required) - Name of the AR System server to be accessed.
- `<form>`: (required) - Name of the AR System form to be accessed.

Example:

If the parameters are:

- Mid Tier Server: `192.168.2.60:8080` (Host: `192.168.2.60`, Port: `8080`),
- Server: `remedy` (this is its DNS name)

- Form: Sample
- URL Template: kept at the AlgoSec default.

Then the fully formatted URL for change request id 12345 would look like this (all on one row):

```
http://192.168.2.60:8080/arsys/servlet/ViewFormServlet?server=remedy&form=Sample&qual=%27Change%20ID%2A%2B%27%3D%2212345%22
```

The URL template that AFA uses can be viewed and edited in the *URL Template* field. It contains the structure of the URL that will be created for change request ID links in AFA reports. You may change this field to specify the URL format explicitly (over-ride the defaults). The following keywords will be replaced by the relevant values: `__SERVER_NAME__`, `__MID_TIER_SERVER__`, `__FORM_NAME__`, `__REQUEST_ID__`.

Click **Show Full URL** to see the resulting URL string.

HP ServiceCenter (formerly Peregrine)

If you use a HP ServiceCenter (formerly Peregrine) Change Management System, select **HP ServiceCenter (Peregrine)** in the **Workflow** tab to fill in ServiceCenter-specific parameters.

The screenshot shows the 'Administration' section of the Firewall Analyzer interface. The 'WorkFlow' tab is selected under the 'OPTIONS' category. The 'Enable integration with external Change Management System' checkbox is checked. The configuration includes a dropdown menu for 'HP ServiceManager (Peregrine)', and input fields for 'Server', 'File', 'Query', and 'URL Template'. The 'URL Template' field contains the text 'http://__SERVER_NAME__/sc/index.do?ctx'. Below this, there are fields for 'Change Request Id Format' with 'Before' and 'After' sub-fields, and a 'Show Full URL' button. At the bottom, there are 'Cancel' and 'OK' buttons.

Fill in the different fields, in order to allow AFA to create the correct links. The format of a typical URL to an HP ServiceCenter change request is as follows:

```
protocol://<server>/sc/index.do?ctx=docEngine&file=<file>&query=
<query>&action=&title=Ticket%20Information
```

Where:

- `<protocol>`: may be either http or https
- `<server>`: The HP ServiceCenter (Peregrine) server (name or IP address)
- `<file>`: The table name
- `<query>`: Format of the actual query string, e.g. number="__REQUEST_ID__" or incident.id="__REQUEST_ID__"

The string "__REQUEST_ID__" must appear in the query, and will be replaced by the actual request ID in the final link URL.

The URL template that AFA uses can be viewed and edited in the *URL Template* field. It contains the structure of the URL that will be created for change request ID links in AFA reports. You may change this field to specify the URL format explicitly (over-ride the

defaults). The following keywords will be replaced by the relevant values: `__SERVER_NAME__`, `__FILE_NAME__`, `__QUERY__`.

Click **Show Full URL** to see the resulting URL string.

Note: Some versions of HP ServiceCenter may require the URL to contain a hash value in addition to the query itself. In order to integrate with AFA, this option should be disabled.

Note: In order to configure the Web application to ignore this hash value in ServiceCenter version 6.x and below, add the following lines to the Web application's `web.xml` file:

```
<init-param> <param-name>sc.querysecurity</param-name> <param-value>>false</param-value></init-param>
```

Note: In HP Service Manager version 9.2 and above, add the following lines to the Web application's `web.xml` file on the Service Manager server:

```
<init-param> <param-name>querySecurity</param-name> <param-value>>false</param-value></init-param>
```

Note: In addition, you must add the following line to the `sm.ini` file:

```
querysecurity:0
```

Other

If you use any other CMS system, which supports Web-access, choose **Other**.

- **Server:** Name of the HP ServiceCenter server to be accessed.
- **URL Template:** The structure of the URL that will be created for change request ID links in AFA reports. The following keywords will be replaced by the relevant values: `__SERVER_NAME__`, `__REQUEST_ID__`.
Click the **Show Full URL** button to see the resulting URL string.

Authentication

In the **Authentication** tab, configure the methods AFA uses for authenticating users and authenticating devices.

For more details, see [Configure user authentication](#) and [Integrate AFA and CyberArk](#).

The screenshot shows the 'Administration' section of the Firewall Analyzer interface. The 'Authentication' tab is selected under the 'OPTIONS' category. The configuration is divided into several sections:

- User Authentication:**
 - Authentication Server:** Radio buttons for Local (checked), RADIUS, and LDAP. A checkbox for 'The Authentication server is case-sensitive' is unchecked.
 - Single Sign On:** Radio button, currently unselected.
- Radius Authentication:**
 - Server: 192.168.2.137
 - Secret key: [masked]
 - Port: 1812
 - Timeout: 3
 - Buttons: 'Test connectivity' (blue), 'Fetch user data from LDAP (?)' (checkbox, unchecked), 'Use Secondary Servers' (checkbox, unchecked).
- Default for new users:**
 - Radio buttons for Local (checked), Radius, and LDAP.
- Default Mail Domain:**
 - Text input field (empty).
 - Example text: "For example : \"Algosec.com\""
- CyberArk:**
 - Checkbox: 'Allow to setup devices with CyberArk credentials management (?)' (unchecked).
 - Logo: CYBERARK
 - Default values (Optional):**
 - Platform (Policy ID): [input field]
 - Safe: [input field]
 - Folder: Root

At the bottom of the configuration area, there are 'Cancel' and 'OK' buttons.

Backup/Restore

This section describes how to back up and restore your AlgoSec Firewall Analyzer from AFA using both automatic scheduling and manual processes.

Backup files include ASMS users, devices, and other configurations and optional content, and can be saved locally or on a remote server. Only one backup or restore process can run at a single time.

Backup and restore prerequisites

Note the following before starting your backup or restore procedure:

User roles	You must be an administrator to perform the backup or restore.
Version	<p>You can only restore ASMS to the same major version from which the backup was taken.</p> <p>If you have upgrades to perform, upgrade your system only before the backup or after the restore. Do not attempt to upgrade your system between backup and restore processes.</p>
System processes	<p>Restoring your system requires some downtime. Disable any jobs scheduled to run during the restore process, such as ASMS monitoring or analysis.</p> <p>Reinstate the scheduling once the restore is complete.</p>
System requirements	We recommend always restoring to an appliance with the same number of cores as the appliance from which the backup was taken.

For more details, see:

- [Backup and restore on distributed architectures](#)
- [Define backup options](#)
- [Back up your system](#)
- [Restore your system](#)

Backup and restore on distributed architectures

Backup and restore handles data on a single appliance. Performing a restore overwrites the settings and device definitions on each target node with the data from the source node.

Additionally:

- **In geographic distributions**, the target appliance for the restore must have the same number of Remote Agents, with the same names, as the appliance on which the backup was performed.

- In load distributions, restoring to an environment with fewer Load Units than existed on the backup environment will impact performance.

Note: We recommend running your backup and restore on the Central Manager or Master Appliance only.

Define backup options

In the AFA Administration area, browse to the **Options > Backup / Restore** tab, and define the [Backup Scheduler options](#) and [Backup Server options](#).

The screenshot shows the 'Backup/Restore' configuration page in the Firewall Analyzer Administration interface. The page is titled 'Administration' and has a navigation menu with tabs: DEVICES SETUP, USERS/ROLES, SCHEDULER, COMPLIANCE, OPTIONS, MONITORING, DOMAINS, ARCHITECTURE. The 'OPTIONS' tab is selected, and the 'Backup/Restore' sub-tab is active. The main content area is divided into three sections: 'Backup/Restore' with 'Back up now...' and 'Restore now...' buttons; 'Backup Scheduler' with a 'Schedule backup' checkbox and options for 'Include traffic logs', 'Include reports', and 'Encrypt backup files'; and 'Backup Server' with fields for 'Back up via:' (FTP, SFTP, Local), 'Backup Server name:', 'Username:', 'Password:', and 'Path:'.

Backup Scheduler options

Define the following options to schedule a regular system backup:

Schedule backup	<p>Select to schedule a regular backup process.</p> <p>Define the daily, weekly, or monthly backup schedule in the Scheduling Options area that appears below.</p>
------------------------	---

Backup options	<p>Select either of the following:</p> <ul style="list-style-type: none"> • Include traffic logs. Includes traffic logs in the backup. • Include reports. Includes AFA reports in the backup. This option includes all reports created since the last scheduled backup.
Additional options	<p>Select Encrypt backup files to configure encryption for the backup file. In the Password and Retype password fields that appear, enter and confirm the password you want to use to secure the backup file.</p>

Backup Server options

Define the following options to define your backup server:

Back up via	<p>Select one of the following to determine how backup files are sent to the backup server:</p> <ul style="list-style-type: none"> • FTP • SFTP • Local
Backup server name	<p>Enter the name of the backup server. This field is not relevant for local backups.</p>
Username / Password	<p>Enter the credentials used to access the backup server. These fields are not relevant for local backups. Note: Public key authentication is supported for SFTP. In such cases, enter the private key's passphrase in the Password field.</p>

Path	<p>Enter the path where you want to store the backup files. The afa user must have permissions to access the specified path.</p> <p>If the directory does not exist, AFA will attempt to create the folder automatically, as follows:</p> <ul style="list-style-type: none"> • Local paths. When testing the connection • Remote paths. Only when performing a backup, either manual or automatic. <p>Note: If an error appears stating that there are connection problems, the user may not have the permissions required to create the directory.</p> <p>In such cases, either manually change the permissions or have an admin user create the directory.</p>
-------------	--

Back up your system

This procedure describes how to perform an immediate ASMS backup, in addition to any backup process you may have scheduled.

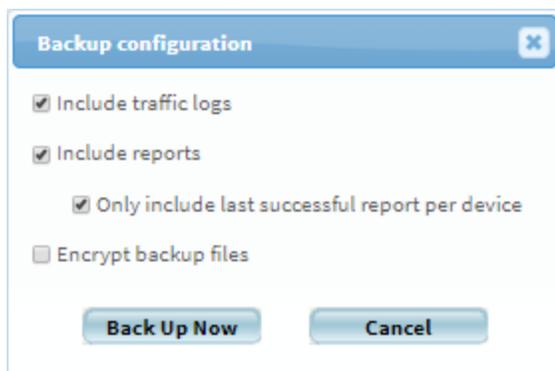
Do the following:

1. In the AFA Administration area, browse to the **Options > Backup / Restore** tab.
2. Click **Back up now...**
3. In the **Backup configuration** dialog that appears, select any of the following options as needed:

Include traffic logs	Include traffic logs. Includes traffic logs in the backup
-----------------------------	--

Include reports	Includes AFA reports in the backup. By default, this includes all reports created since the last scheduled backup. Tip: To save disk space, select Only include last successful report per device . Including all existing reports may require a significant amount of disk space
Encrypt backup files	Select to configure encryption specifically for this backup file. In the Password and Retype password fields that appear, enter and confirm the password you want to use to secure the backup file.

4. In the **Backup configuration** dialog, click **Back Up Now** to start the backup.



Backup files are created in the path configured, including several directories containing your backup files. Each directory contains a single backup, where the folder name is the epoch timestamp of when the backup was generated.

Restore your system

This procedure describes how to restore your ASMS system from a saved backup file. Restoring ASMS replaces all existing users, devices, and configurations with those specified in the selected backup file.

Do the following:

1. If you are working with HA/DR clusters, break your cluster before starting your restore.

2. In the AFA Administration area, browse to the **Options > Backup / Restore** tab.
3. Click **Restore now...**
4. In the **Backup configuration** dialog that appears, enter the following values:

File name	Enter the filename of the backup file you want to use.
Backup file requires password	Select if the backup file is encrypted. Enter the required password in the Password field that appears. Note: Entering an incorrect or old password restores only those reports that were not encrypted, or those encrypted with the password entered. In such cases, the restore process does not fail, but error messages in the log indicate the names of the reports that failed to restore.

The restore process begins.

Note: ASMS is unresponsive for the duration of the restore process.

To view details during the process, see the log file at `/data/algosec-ms/logs/ms-backuprestore.log`.

5. After the restore is complete, run a report on **All Firewalls** to ensure a valid network map.

Advanced Configuration

This topic describes how to add and modify advanced AFA configuration parameters, as well as a reference of parameters available.

Add a new AFA configuration parameter and value

This procedure describes how to add a new advanced configuration parameter to AFA. Use this procedure to override various system defaults or implement hotfix updates.

Do the following:

1. In the toolbar, click your username and select **Administration** to access the AFAAdministration area.
2. Navigate to **Options > Advanced Configuration**.
3. Click **Add**, and enter the name and value of your configuration parameter.
4. Click **OK** to close the dialog, and then **OK** again to save your changes.

Advanced AFA configuration parameter reference

The following tables list commonly used AFA configuration parameters and their possible values.

Use the alphabetical links below to jump between tables.

[A-B](#) | [C](#) | [D](#) | [E-I](#) | [L](#) | [M](#) | [N-R](#) | [S-W](#)

A-B

Parameter	Description
Active_Change_Backups_Number	CLI only. Define the number of backup files stored by AFA for Cisco firewalls, Juniper SRX devices, or Panorama devices. Default: 50
AddOnlyChildren	Determines whether the add_device_to_group and create_device_group SOAP APIs add both the parent and children devices to the group. Possible values: <ul style="list-style-type: none"> • 0: Both parents and children are added. (Default) • 1: Only children are added.
ALGOSEC_EA_ARISTA	Determines whether AFA administrators can add Arista devices to AFA. Default: FALSE

Parameter	Description
AlgoSec_EA_Azure_ActiveChange	Determines whether AFA administrators can define ActiveChange options for Azure devices. Default: FALSE
AlgoSec_EA_Cisco_ACI_ActiveChange	Determines whether AFA administrators can define ActiveChange options for Cisco ACI devices. Default: FALSE
ALGOSEC_EA_CISCOISE	Determines whether AFA administrators can add Cisco ISE devices to AFA. Default: FALSE
analyze_only_changed_reports	Determines whether analysis is always run, even if the configuration has not changed. Possible values: <ul style="list-style-type: none"> • yes: Analysis is run only if the configuration has changed • no: Analysis is always run
Backup_Firewall_History	Determines whether backup files include change history. Possible values: <ul style="list-style-type: none"> • yes. Change history is included • no. Change history is not included in backups
BUSINESSFLOW_ADDRESS	Determines the IP address of the BusinessFlow host, if not local.

C

Parameter	Description
CHANGE_HISTORY_DAYS	Determines the number of days that legacy changes are kept in report change histories. Default: 90

Parameter	Description
Chart_Threshold_Val	<p>Defines the chart threshold value for all condition type charts, including the built-in compliance charts.</p> <p>Possible value: Integer</p> <p>Default: 23</p>
Checkpoint_Adtlog_Exclude_Fields	<p>Defines a pipe-separated list of Check Point audit log fields that are ignored.</p> <p>For example:</p> <p>CKP_Adtlog_Exclude_Fields=CLCStatus threshold_event_uint</p> <p>Note: Regular expressions are supported.</p>
CKP_optimizations_per_policy	<p>Determines whether policy optimization items are shown for all rules in the policy, and not only those installed on the analyzed module.</p> <p>Default: yes</p>
CKP_REST_RULEBASE_BATCH_SIZE	<p>Defines the maximum size for each batch data collection for Check Point devices.</p> <p>For very large policies, set this parameter to a large value, such as 1000, to shorten the data collection time.</p> <p>Possible value: Integer</p> <p>Default: null</p>
CKP_turbo_log_collection	<p>Determines whether a dummy environment is used to speed up log collection on Check Point devices.</p> <p>Default: no</p>
CLUSTER_USE_VIP	<p>Determines whether a VIP is shown instead of a MIP in Check Point cluster topologies.</p> <p>Default: yes</p>

Parameter	Description
CollapseDevicesTreeOnLogin	<p>Determines whether the device tree is collapsed by default.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • true. Collapsed (Default) • false. Expanded
CollapseDevicesTreeOnLogin	<p>Determines whether the device tree appears fully collapsed or expanded by default.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • True (default). Sets the tree to display collapsed by default. • False. Sets the tree to display expanded by default.
Comments_Regex_Match	<p>Determines whether comments match or do not match the regular expression defined in Comments_Regex.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • 0: Does not match • 1: Matches
comprehensive_mode	<p>Determines whether comprehensive mode is enabled, where AFA queries all services that appear in any rule in the policy.</p> <p>Default: yes</p>
CONSIDER_MULTIPLE_NHG	<p>Determines whether all multiple routes for each range are saved and used for FIP.</p> <p>Supported only for IOS.</p> <p>Default: yes</p>
covered_exclude_services	<p>Defines a colon-separated list of values. Rules that contain any of the listed values as services are not listed as covering rules.</p> <p>Default: null (no exclusions)</p>

D

Days_To_Consider_Rules_As_New	<p>Determines the number of days before which rules are considered as unused.</p> <p>Additionally, if defined, rules with no rule creation time are considered to be older than the set value.</p> <p>For example, if this parameter is set to 30, rules that are less than 30 days old are never defined as unused.</p> <p>0 = Disable this feature, and instead use the value defined in Log_Analysis_Days_Before instead.</p>
Days_Without_Logs_Percentage_Threshold	<p>Determines the threshold at which warnings are sent for missing log days, in log data-based parts of the policy optimization.</p> <p>Possible values: Integers, 0-100</p> <p>0 disables the warning altogether</p> <p>Default: 50</p>
DB_host	<p>Defines the database host.</p> <p>Default: localhost</p>
DB_name	<p>Defines the database name.</p> <p>Default: afa</p>
DB_user	<p>Defines the database username.</p> <p>Default: afa</p>
default_dashboard	<p>Defines the default AFA dashboard shown.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • optimizations.xml (default) • compliance.xml • none - do not load a dashboard at login

Disable_IPT_Recommendations	<p>Determines whether to include Intelligent Policy Optimization recommendations on the Policy Optimization report page.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes: Disable IPT recommendations. Recommended if IPT recommendations are causing the report generation to take too long. • no: Enable IPT recommendations (Default) <p>Note: To determine the amount of time consumed by the generation of rule replacement recommendations, view the AFA log. The start of this task is marked IPT recommendations generation - Starting, and the end of this task is marked IPT recommendations generation - Finished.</p>
Disable_IPT_Time_Checking	<p>Defines the database username.</p> <p>Default: afa</p>
Disable_Monitoring	<p>Determines whether global monitoring is disabled.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes: Monitoring is disabled for all firewalls. • no: Monitoring is enabled. (Default)
Disable_Routing_Element_Monitoring	<p>Determines whether to disable monitoring for routing element devices.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes: Monitoring on routing element devices is disabled. • no: Monitoring on routing element devices are enabled. (Default)

E-I

Enable_Ms_Traffic_Logs_Processing	<p>Determines whether traffic log collection is enabled using the ms_trafficlogmanager service.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes. Enabled (Default) • no. Disabled
--	---

Export_Policy_Tab_With_Objects_Content	<p>Determines whether the exported PDF report's Policy page shows the network object content as well as the network object names.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes. Network object content and names shown • no. Network object names shown only (Default)
EXPECT_TIMEOUT	<p>Defines the timeout, in seconds, for processing a single command in the Expect data collection.</p> <p>Default: 120</p>
FailCLIOnMissingUIDs	<p>Determines whether the CLI is generated even in case of missing UIDs in Cisco PIX devices.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes: CLI generation fails in case of missing UID (Default) • no: CLI is generated even if there are missing UIDs
FIP_MAX_DEVICES_SEARCH_PATHS_FOR_DESTINATION_ANY	<p>Defines a maximum number of devices for which to run a query with a FIP destination of any.</p> <p>Default: 100</p>
FireFlowXmlEncoding	<p>Determines whether FireFlow XML change files are encoded as UTF-8 or ISO-8859-1.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • UTF-8 (Default) • ISO-8859-1. Supports Latin characters
FWFiles_Directory	<p>Defines the path of the Analyze from file firewalls.</p> <p>Default: \$HOME/algosec/fwfiles</p>

hide_change_details	<p>Determines whether to omit change details from emails about new reports and change alerts, for all users.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes: Hides change details for all users. Emails about new reports and change alerts include only the device name and a link to AFA. • no. Change details are displayed for all users. <p>Change this setting per user with the Hide change details checkbox. For details, see Manage users and roles in AFA.</p>
IPT_Density_Action_Limit	<p>The maximum density of a sparse object. When this limit is exceeded, the object is considered semi-dense.</p> <p>Default: 50</p>
IPT_Recommendation_Max_Ranges	<p>Defines the maximum number of CIDR blocks into which IPT will recommend splitting a host object, if the original object contains more IP addresses/ranges than defined in IPT_Recommendation_Max_Subnets_Per_Range.</p> <p>Default: 20</p>
IPT_Recommendation_Max_Services	<p>The maximum number of services or applications from which IPT will recommend composing a new object.</p> <p>Default: 20</p>
IPT_Recommendation_Max_Subnets_Per_Range	<p>Defines the maximum number of CIDR blocks into which IPT will recommend splitting a host object.</p> <p>IPT recommends creating a new object only when the number of used IP addresses/ranges is smaller than the defined number.</p> <p>Default: 4</p>

L

Locate_in_rules_include_any	<p>Determines whether rule search results include rules that contain the searched IP only in Any source or destination.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes: Rules results include rules where the searched IP address is found in Any source or destination • no: Rule results do not include rules where the searched IP address is found in Any source or destination (Default)
LOCK_WAIT_FREQUENCY	<p>Defines how often the Check Point and IOS data collection lock file is sampled, in seconds.</p> <p>The value of this parameter, multiplied by the value of the MAX_LOCK_WAIT parameter equal the total wait time for IOS devices.</p> <p>Default: 10</p>
Log_Analysis_Days_Before	<p>Defines the analysis log lookup, in days.</p> <p>Default: 60</p>
Log_Analysis_Months_Before	<p>Defines the time period for which traffic database is retained, in months. Traffic logs older than the defined value are deleted.</p> <p>Default: 12</p>
Log_Time_Interval_Minutes_Before_Error	<p>Defines the time period, in minutes, before which a device's log collection status is set to failure, in case log collection finds no new logs for a specific server for one of the following reasons:</p> <ul style="list-style-type: none"> • No logs have arrived to the log server. This may be an issue in the customer environment. • No logs were found for the target devices. This may be an AFA misconfiguration or error. <p>Default: 180</p>
Log_Timeout_Minutes	<p>Defines the timeout for the entire log collection process, in minutes.</p> <p>Default: 900 (15 hours)</p>

M

mailSuffix	<p>Defines an email address to use as a default if a new or edited user email address is left empty.</p> <p>Default: null</p>
MAP_BLACK_LIST	<p>Determines whether to ignore defined devices in AFA when creating the map.</p> <p>Default: null</p>
MAX_LOCK_WAIT	<p>Defines a time to wait for the Check Point, IOS, or NSM data collection lock file, in seconds.</p> <p>Default: 7200 (2 hours)</p>
MAX_LOCK_WAIT_NSC	<p>Defines a time to wait for the NSC data collection file, in seconds.</p> <p>Default: 7200 (2 hours)</p>
Max_Parallel_Analyses	<p>Determines the maximum number of analyses that are allowed to run in parallel.</p> <p>Default: The number of CPUs on the machine.</p>
Max_Parallel_Logcollect	<p>Determines the maximum number of log collections running in parallel.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Positive integers • 0: unlimited
Max_Rows_To_Sort	<p>Determines whether sorting and filtering in AFA report tables is enabled, and if so, for how many rows.</p> <p>Sorting and filtering large tables may take a long time.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Integer, 1 or greater. Defines the maximum number of rows for which sorting and filtering can be performed. • 0: Sorting and filtering is disabled. <p>Default: 10,000</p>

MGMT_ ROUTING_ FREQUENCY	Defines the frequency of routing information collection for management devices, such as Panorama, in minutes. Default: 60
Monitor_ exclude_PIX	Defines a single regular expression, including a simple string, to exclude from comparisons during monitoring. Tip: Even though this supports a single regular expression only, define multiple matches using an OR pipe (). For example: (log\s+in log\s+out)
Monitor_Force_ Data_Coll_ Ckp_Min	Defines how often data collection runs on Check Point devices, in minutes, even if no new logs are found. Default: 720
Monitor_Force_ Data_Coll_ Cycles_Num	Defines how often a full monitoring cycle is run on Check Point devices, in minutes, even if no new audit logs are found. Default: 720

monitor_ frequency	<p>Defines how often the monitoring process runs, in hours.</p> <p>Default: 5</p> <p>If MONITOR_USE_FREQUENCY_AS_HOUR_OF_DAY is set to no, or does not exist, defines the hour of the day at which the monitoring process runs. In such cases, supported hours include the hours between 2:00-24:00, skipping 1:00.</p> <p>Possible values: Integer, multiple of 60.</p> <p>For example:</p> <ul style="list-style-type: none"> • 60x2 = 120. 120 runs monitoring at 02:00 and 14:00. • 60x4 = 240. 240 runs monitoring at 04:00 and 16:00. • 60x12 = 720. 720 runs monitoring at 00:00 and 12:00. <p>Sample procedure: Configure monitoring to run once a day</p> <ol style="list-style-type: none"> 1. Set the new MONITOR_USE_FREQUENCY_AS_HOUR_OF_DAY configuration parameter value to no, or delete this parameter. 2. Set the monitor_frequency parameter value to 60x<x>, where <x> is the hour of the day at which you want monitoring to run. <p>For example, 60x14 = 840. 840 runs monitoring at 14:00.</p>
Monitor_ Frequency	<p>Defines a general monitoring frequency for all devices, in minutes.</p> <p>Default: 5</p>
MONITOR_ USE_ FREQUENCY_ AS_HOUR_ OF_DAY	<p>Determines whether monitoring processes are defined by setting frequency to the hour of the day.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • no: Monitoring processes run as scheduled. • yes: Monitoring processes runs as defined in the monitor_frequency parameter.
MONITORING_ HISTORY_ DAYS	<p>Defines the number of days to retain monitoring changes.</p> <p>Default: 90</p>

N-R

NSM_optimizations_per_policy	<p>Determines whether to show policy optimization items for all the rules in a policy, and not only for those that have the analyzed device in their target.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Yes: Optimizations shown for all rules in policy • No: Optimizations shown only for rules that have the analyzed device in their target. (Default)
PrioritizeFIPDestination	<p>Determines if routing queries and traffic simulation queries prioritize paths that begin and end with a subnet (and not a cloud) for destinations.</p> <p>The default setting is yes.</p> <ul style="list-style-type: none"> • yes. Enables the preference for subnets in destinations. • no. Disables the preference for subnets in destinations.
PrioritizeFIPSources	<p>Determines if routing queries and traffic simulation queries prioritize paths that begin and end with a subnet (and not a cloud) for sources.</p> <p>The default setting is yes.</p> <ul style="list-style-type: none"> • yes. Enables the preference for subnets in sources. • no. Disables the preference for subnets in sources.
PrioritizeFIPSources	<p>Determines whether subnets are prioritized for sources in routing and traffic simulation queries.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes. Subnets are prioritized for sources. (Default) • no. Subnets are not prioritized for sources.
Query_Timeout	<p>Defines the timeout for a single query, in seconds.</p> <p>Default: 15</p>

QueryByPolicy	<p>Determines whether traffic simulation group query results include all devices in device groups, or are grouped by policy with a single representative device for each policy.</p> <p>Note: This setting affects group traffic simulation query results and batch traffic simulation query results. It also affects initial plan query results in FireFlow.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes. Display group query results by policy. • no. Do not group query results by policy (Default)
RADIUS_FetchData	<p>Determines whether to fetch data and groups from LDAP for users authenticated by a Radius server.</p> <p>Default: no</p>
REMOVE_DELETED_DEVICE_REPORTS	<p>Determines whether to remove reports for all deleted devices.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Yes: Remove reports for deleted devices • No: Keep reports for deleted devices
Routing_Element_Monitor_Frequency	<p>Determines the frequency for which to run monitoring on routing elements, in minutes.</p> <p>Default: 5</p>
Rule_Selection_Limit	<p>Defines the maximum number of rules allowed to be selected for a single FireFlow change request.</p> <p>Tip: Avoid using large numbers to prevent performance issues in FireFlow.</p> <p>Default: 50</p>

S-W

Parameter name	Description
SHOW_ONLY_NODES_IN_PATH	<p>Determines whether the network map shown in query results shows only the nodes in the network path, without surrounding devices and objects.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes: Shows only the nodes in the network path queried, including stub routers, clouds, subnets, and so on. • no: Shows the nodes in the network path queried, and also surrounding devices and objects. (Default)
syslog_dump_interval	<p>Defines the maximum amount of time between syslog collection and memory dump to files, in minutes.</p>
TarFormat	<p>Determines support file download attributes.</p> <ul style="list-style-type: none"> • zip: AFA creates zip files for download. • tar: AFA creates tar files for download. • tgz: AFA creates tgz files for download. (Default) • extended_tgz: AFA creates an extended tgz file for download. Use this option when you have devices with names that are longer than 100 characters.
trust_rfc1918	<p>Determines that risk calculation is skipped for private networks. This means that most Z## risks will not be triggered.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Yes: Skipped for private networks. (Default) • No: Private networks are included in risk calculation.

Parameter name	Description
Use_Custom_Report	<p>Determines whether custom report pages are enabled.</p> <p>For more details, see Custom report pages.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes. Enable custom reports. (Default, when a custom report has been created and installed) • no. Disable custom reports, preventing any custom reports from appearing in AFA reports.
Use_Nexus_Wildcards	<p>Determines whether Traffic Simulation Query results on Cisco Nexus devices use wildcard IP ranges.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • yes: Wildcard IP ranges are included. • no: Wildcard IP ranges are not included. (Default)
WEBGUI_SESSION_LENGTH	<p>Defines the maximum length of a UI session that is not active, in minutes. Any session that goes on for longer than the defined setting is automatically ended.</p> <p>Default: 300</p>

Customize AFA

This section describes the following types of AFA customizations:

- [Custom report pages](#)
- [Custom documentation fields](#)
- [Custom dashboards and charts](#)
- [Customize regulatory compliance report](#)

Custom report pages

AFA enables you to create custom pages in your reports.

Create a custom report page

You can create a custom report page that will be included as a separate tab in each new device, group, or matrix report.

Note: Only one custom report page is supported.

Note: The custom report page cannot be exported to HTML or PDF.

To create a custom report page:

1. Create an XML file called `custom_report.xml`, containing all of the execution commands in the following format:

```
<Custom_Report>
<Report name="report_name">
<device command="device_script_execution_command" output=
"device_output_file"></device>
<group command="group_script_execution_command" output=
"group_output_file"></group>
<matrix command="matrix_script_execution_command" output=
"group_output_file"></matrix>
```

```
</Report>
</Custom_Report>
```

For more details, see [Custom report configuration file parameters](#).

The `<device>`, `<group>`, and `<matrix>` lines are optional. If you include the `<device>` line but do not include the `<group>` or `<matrix>` lines, the custom report page in the group or matrix report will display a concatenation of custom device pages.

2. Create a folder called `custom_report`, containing all of the scripts that must be executed.
3. Create a sub-folder called `additional_files` under the `custom_report` folder, containing additional files that are required for generating the custom report, for example data files, `.css` files, and so forth.
4. Add the file `custom_report.xml` and the folder `custom_report` (along with all its contents, including the subfolder `additional_files`) to a single `.zip` file.
5. Enter the following command:

```
extract_custom_report -f zip_file [-d domain_number] [-u user_name]
```

For more details, see [Extract custom report script flags](#).

The `extract_custom_report` script extracts the `.zip` file.

The next time a report is generated, it will include the custom page.

Note: If desired, you can disable the custom report page. For details, see the [Use Custom_Report](#) parameter.

Custom report configuration file parameters

Parameter	Description
<code>report_name</code>	The name of the report page.

Parameter	Description
device_script_execution_command	The script execution command for the custom device report page, including input parameters. For example: <code>sh device_script.sh</code>
device_output_file	The name of the HTML output file for the custom device report page. For example: <code>custom_device.html</code>
group_script_execution_command	The script execution command for the custom group report page, including input parameters. For example: <code>sh group_script.sh</code>
group_output_file	The name of the HTML output file for the custom device report page. For example: <code>custom_group.html</code>
matrix_script_execution_command	The script execution command for the custom matrix report page, including input parameters. For example: <code>sh matrix_script.sh</code>
matrix_output_file	The name of the HTML output file for the custom device report page. For example: <code>custom_matrix.html</code>

Extract custom report script flags

Flag	Description
-f <i>zip_file</i>	The name of the <code>.zip</code> file. Note: The file must be located in the current directory.
-d <i>domain_number</i>	The number of the domain in the <code>.fa</code> directory, where the <code>.zip</code> file should be extracted. This flag is optional.
-u <i>user_name</i>	The user to use when installing the contents of the <code>.zip</code> file. This user will be granted permissions for the <code>.zip</code> file's contents. This flag is optional. If it is not included, the contents of the <code>.zip</code> file will be installed using the "afa" user.

Custom documentation fields

By default, AFA adds a field called *Documentation* to each device policy, which you can use to add comments and other information to a rule. See [Adding/Removing AFA Rule Comments](#).

If desired, you can disable or enable the *Documentation* field or add more such fields.

Add documentation fields

Each documentation field appears as a column at the far-right side of the device policy.

Note: Documentation fields cannot be deleted, only disabled. For details, see [Enable/Disable documentation fields](#).

To add a documentation field:

1. Open a terminal and log in using the username "afa" and the related password.
2. Enter the following command:

```
update_document_fields ADD "field_name" "field_type"  
"field_default_value"
```

Where:

- *field_name* is the name of the field, for example "My Doc".
- *field_type* is the field's type. This can have the following values: `Text`, `Number`, `Bool`, **OR** `List`.
- *field_default_value* is the field's default value, for example "Good rule!"

The field is added to all device policies in AFA.

Enable/Disable documentation fields

To enable a documentation field:

1. Open a terminal and log in using the username "afa" and the related password.
2. Enter the following command:

```
update_document_fields ENABLE "field_name"
```

Where *field_name* is the name of the field.

The field is enabled for all device policies in AFA.

Note: When re-enabling a documentation field, all data that was entered in this field before it was disabled, will appear once again in the device policies.

To disable a documentation field:

1. Open a terminal and log in using the username "afa" and the related password.
2. Enter the following command:

```
update_document_fields DISABLE "field_name"
```

Where *field_name* is the name of the field.

The field is disabled for all device policies in AFA.

Custom dashboards and charts

You can create custom dashboards in AFA that include built-in charts, custom charts, or both, by defining them directly in XML.

Configure custom charts

When creating a dashboard with custom charts, you must configure the custom charts before you configure the dashboard itself.

- You specify the title of the chart.
- You specify the type of chart.
- You specify the variable for which the chart displays data.
- You specify the Y-axis values the chart displays.
- For bar charts, you also specify the following:
 - The number of devices displayed in the chart.
 - Whether the chart starts with displaying the devices with the most of the variable or the least of the variable.
 - The direction of the chart.
- For trend charts, you also specify how many days back the chart displays.

Add a custom chart

1. Open a terminal and log in using the username "afa" and the related password.
2. Create a new file in `/home/afa/.fa/charts`.
3. Name the file `chart_name.xml`, where `chart_name` is the name you choose for the chart.
4. Add the `CHART` tag to the file, using the information in Chart Tag Reference (see [Chart tag reference](#)). For an example, see Chart Example (see [Chart Example](#)).
5. Save the file.

Chart tag reference

This reference describes the use of the `chart` tag and its sub-tags.

Tag syntax is presented as follows:

- All parameters and content are presented in *italics*.
- All optional elements of the tag appear in square brackets `[]`.

Note: All tags, parameters, and content are case sensitive, and must be in lower

```
case.
```

chart

Syntax

```
chart
```

Description

This is the main tag for the chart. It specifies all the information included in the chart.

Parameters

None.

Subtags

- title (see [title](#))
- variable_name (see [variable_name](#))
- statistics_type (see [statistics_type](#))
- type (see [type](#))
- limit (see [limit](#))
- order_dir (see [order_dir](#))
- direction (see [direction](#))
- ymin (see [order_dir](#))
- ymax (see [ymax](#))
- days_back (see [days_back](#))

title

Syntax

```
<title>title</title>
```

Description

This tag specifies the title of the chart.

Parameters

None.

Subtags

None.

Content

<code>title</code>	<p>String. The name that you choose for the title of the chart. You can include the following variable in the title:</p> <ul style="list-style-type: none"> • <code>__GROUP_NAME__</code>. The name of the device group that is analyzed by the chart (as defined in the dashboard XML file). • <code>__THRESHOLD__</code>. The value set as the "Chart_Threshold_Val" configuration item. • <code>__COUNT__</code>. The number of devices the chart displays.
--------------------	---

Example

In the following example, if the number of devices in the chart is 8, and the chart analyzes the group "ALL_FIREWALLS", the title of the chart is "8 Devices with lowest security rating in group ALL_FIREWALLS".

```
<title>__COUNT__ Devices with lowest security rating in group __GROUP_NAME__
</title>
```

variable_name

Syntax

```
<variable_name [color="color"] [value_condition="value_condition"] [bar_name="bar_name"]>variable_name</variable_name>
```

Description

This tag specifies the variable that the chart displays.

Parameters

color	<p>String. The color of the bar or series of the variable, expressed in #RGB.</p> <p>This parameter is for <code>count</code> type and <code>trend_count_group</code> type charts, and the default chart type only.</p> <p>This parameter is optional.</p>
value_condition	<p>String. A condition, such that, only devices with a variable value that passes the condition will be counted.</p> <p>This parameter is for <code>count</code> type and <code>trend_count_group</code> type charts only. For <code>trend_count_group</code> type charts, only equality is supported, and the value is stated without the operator.</p> <p>Note: For <code>trend_count_group</code> type charts, this variable is an integer.</p> <p>This parameter is optional.</p>
bar_name	<p>String. The label of the bar.</p> <p>This parameter is for <code>count</code> type charts only.</p> <p>This parameter is optional.</p>
function	<p>String. An aggregate function used to compile the chart data. All aggregate SQL functions are supported (for example: "avg", "min", and "max").</p> <p>This parameter is for <code>trend_value</code> type charts only.</p> <p>This parameter is optional. The default function is the average function, which compiles the average of the data over the group.</p>
legend	<p>String. The label of the variable in the legend.</p> <p>This parameter is for <code>trend_value</code> type charts only.</p> <p>This parameter is optional.</p>
sum	<p>String. The sum of the statistic type.</p> <p>This parameter is for <code>sum_over_time</code> and <code>trend_sum_over_time</code> type charts only.</p> <p>This parameter is optional.</p>

Subtags

None.

Content

Variable Content Options	Available Statistic Type.	Specifies this...
rules	simple_count	The number of rules for each device.
covered_rules	simple_count	The number of covered rules for each device.
special_case_rules	simple_count	The number of special case rules for each device.
unused_rules	simple_count	The number of unused rules for each device.
security_rating	simple_count	The security rating for each device.
highest	risk_level	The highest risk level of each device.
PCI	compliance_pass	Whether a device meets PCI compliance.
high	risks_per_risk_level	The number of high risks for each device.
suspected_high	risks_per_risk_level	The number of suspected high risks for each device.
medium	risks_per_risk_level	The number of medium risks for each device.
low	risks_per_risk_level	The number of low risks for each device.

Example

In the following example, the color of the bars for this variable will be #cb3333, only devices with a variable value of 3 will be counted, and the label of the bars for this variable will be "high".

```
<variable_name color="#cb3333" value_condition="=3" bar_name="high">highest</variable_name>
```

statistics_type

Syntax

`<statistics_type>statistics_type</statistics_type>`

Description

This tag specifies the type of statistic that the chart displays.

Parameters

None.

Subtags

None.

Content

Content Options	Specifies this...
<code>simple_count</code>	<p>The count of the variable for each device. This statistic type is available for the following variables: <code>rules</code>, <code>covered_rules</code>, <code>special_case_rules</code>, <code>unused_rules</code>, and <code>security_rating</code>. For example, if the statistic type is <code>simple_count</code>, and the variable is <code>rules</code>, the chart will display the number of rules for each device.</p> <p>Note: When the <code>simple_count</code> statistic type is used with the <code>security_rating</code> variable, the security rating for each device is displayed.</p>
<code>risk_level</code>	<p>The risk level of each device. This statistic type is available for the <code>highest</code> variable. When this statistic type/variable combination is used, the chart will display the number of devices whose highest risk is high, suspected high, medium, and low.</p>
<code>compliance_score</code>	<p>The compliance score of each device. This statistics type is available for the following variables: <code>HIPAA</code>, <code>BASEL</code>, <code>NIST_800-41</code>, <code>NIST_800-53</code>, <code>ISO27001</code>, <code>NERC4</code>, <code>GLBA</code>, <code>TRM</code>, <code>DSD</code>, <code>SOX</code>, <code>PCI</code>.</p>
<code>compliance_color</code>	<p>The compliance color of each device. This statistics type is available for the following variables: <code>HIPAA</code>, <code>BASEL</code>, <code>NIST_800-41</code>, <code>NIST_800-53</code>, <code>ISO27001</code>, <code>NERC4</code>, <code>GLBA</code>, <code>TRM</code>, <code>DSD</code>, <code>SOX</code>, <code>PCI</code>.</p>

Content Options	Specifies this...
baseline_score	The baseline compliance score of each device (the score is the percentage of met requirements). This statistics type is available for the <code>baseline</code> variable.
risks_per_risk_level	The number of risks for a specific risk level for each device. This statistic type is available for the following variables: <code>high</code> , <code>suspected_high</code> , <code>medium</code> , and <code>low</code> . For example, if the statistic type is <code>risks_per_risk_level</code> , and the variable is <code>high</code> , the chart will display the number of high risk rules for each device.
total_changes	The number of changes on each device. This statistic type is available for the <code>sum</code> variable. When this statistic type/variable combination is used, the chart will display the total number of changes on each device.

Example

In the following example, the chart will display a simple count of the specified variable.

```
<statistics_type>simple_count</statistics_type>
```

type

Syntax

```
<type>[type]</type>
```

Description

This tag specifies the type of chart.

Parameters

None.

Subtags

None.

Content

Content Options	Specifies this...
count	A bar chart that specifies the count of devices for each variable.
condition	A bar chart that displays the number of devices whose variable value is greater than the <code>Chart_Threshold_Val</code> configuration item, and the number of devices whose variable value is not, for all devices in the group. For details, see the Chart_Threshold_Val parameter.
trend_value	A trend chart that displays a calculation (defined by the function parameter of <code>variable_name</code>) of the variable values over all devices in the group, over time.
trend_condition	A trend chart that displays the number of devices whose variable value is greater than the <code>Chart_Threshold_Val</code> configuration item, and the number of devices whose variable value is not, for all devices in the group, over time. For details, see the Chart_Threshold_Val parameter.
trend_count_group	A trend chart that displays the total count of the variable for all devices in the group, over time.
sum_over_time	A bar chart that displays the accumulation of the statistic for each device in the group.
trend_sum_over_time	A trend chart that displays the accumulation of the statistic, over time.
empty (default)	A bar chart that displays the count of the variable for each device in the group. There can be multiple variables per device.

Example

In the following example, the chart will be a bar chart that displays the total count of the variable for each device in the group. For example, if the chosen variable is `unused_rules`, the chart will display a bar chart with the count of unused rules per device.

```
<type>count</type>
```

limit

Syntax

```
<limit>[[limit]</limit>
```

Description

This tag specifies the number of devices the chart displays. This tag is only for bar charts.

Parameters

None.

Subtags

None.

Content

Integer. The number of devices the chart will display. If left empty, the `LIMIT` tag defaults to 25.

Example

In the following example, the chart will display 6 devices.

```
<limit>6</limit>
```

order_dir

Syntax

```
<order_dir>[order_dir]</order_dir>
```

Description

This tag specifies whether the chart starts with displaying the devices with the most of the variable or the least of the variable. This tag is only for bar charts.

Parameters

None.

Subtags

None.

Content

Content Options	Specifies this...
ASC	The bar chart will start with displaying devices with the least of the variable. For example, if the <code>LIMIT</code> tag is set to 6, this will produce a chart with the bottom 6 devices.
DESC	The bar chart will start with displaying devices with the most of the variable. For example, if the <code>LIMIT</code> tag is set to 6, this will produce a chart with the top 6 devices.
empty	The <code>ORDER_DIR</code> tag defaults to <code>DESC</code> .

Example

In the following example, the chart will start with displaying devices with the least of the variable.

```
<order_dir>ASC</order_dir>
```

direction

Syntax

```
<direction>[direction]</direction>
```

Description

This tag specifies the direction the chart displays. This tag is only for bar charts.

Parameters

None.

Subtags

None.

Content

Content Options	Specifies this...
horizontal	The bar chart will display horizontally.
vertical	The bar chart will display vertically.
empty	The <code>DIRECTION</code> tag defaults to <code>vertical</code> .

Example

In the following example, the chart will display vertically.

```
<direction>vertical</direction>
```

order_dir

Syntax

```
<ymin>[ymin]</ymin>
```

Description

This tag specifies the minimum y-axis value displayed in the chart. This tag is optional.

Parameters

None.

Subtags

None.

Content

Integer. The minimum y-axis value displayed in the chart. If left empty, the value is computed to fit the data.

Example

In the following example, the minimum y-axis value displayed in the chart is 0.

```
<ymin>0</ymin>
```

ymin

Syntax

`<ymax>[ymax]</ymax>`

Description

This tag specifies the maximum y-axis value displayed in the chart. This tag is optional.

Parameters

None.

Subtags

None.

Content

Integer. The maximum y-axis value displayed in the chart. If left empty, the value is computed to fit the data.

Example

In the following example, the maximum y-axis value displayed in the chart is 100.

```
<ymax>100</ymax>
```

days_back

Syntax

`<days_back>[days_back]</days_back>`

Description

This tag specifies the number of days back displayed in the chart. This tag is optional, and is only for trend charts.

Parameters

None.

Subtags

None.

Content

Integer. The number of days back displayed in the chart. If left empty, the value defaults to 100 days.

Example

In the following example, the trend chart will display data for the last 200 days.

```
<days_back>200</days_back>
```

Chart Example

<!-- This is an AFA dashboard chart configuration file. Each dashboard chart is configured by one such file. The user defined files should be in '<AFA home dir>/fa/dashboards/charts', or if domains are enabled, in '<AFA home dir>/fa/algosec_domains/<domain>/dashboards/charts'.

Note: The tags and properties in this file are case sensitive. A chart is configured by the 'CHART' tag. -->

```
<CHART>
```

<!-- The 'title' tag determines the title that will be displayed at the top of the chart. The title can contain several parameters which will be replaced by the appropriate values: `__GROUP_NAME__` - The AFA devices group whose data will be compiled in this chart (as defined in the dashboard XML) `__THRESHOLD__` - The threshold stated in the "Chart_Threshold_Val" configuration Item `__COUNT__` - The number of devices compiled for the charts. -->

```
<title>Number of devices by leading risk severity in group __GROUP__</title>
```

<!-- The 'type' tag determines the chart type. The default type (if no value is specified) will cause each variable (there may be several, representing different series) value to be plotted for each group member. Available types are: `count` - Count each variable over all group members `condition` - Count values greater than the "Chart_Threshold_Val" configuration item `trend_value` - For each time frame, calculate the property over the group members defined by the function property of `variable_name` (the default is average) `trend_condition` - For each time frame, count values greater than the "Chart_Threshold_

Val" configuration item trend_count_group - For each time frame, count the variable over all group members -->

```
<type>count</type>
```

<!-- 'statistics_type' - The type of the statistics. Allowed values are: simple_count, risk_level, compliance_pass, and risks_per_risk_level -->

```
<statistics_type>risk_level</statistics_type>
```

<!-- The 'variable_name' depends on 'statistics_type' value as follows: simple_count - covered_rules, security_rating, special_case_rules, unused_rules risk_level - highest compliance_pass - PCI risks_per_risk_level - high, suspected_high, medium, low For the default type and the count type, there may be multiple variables, which will be expressed as multiple series. The variable name has the following optional attributes: 'color' - The color of the bar/line (in count types) or series (in the default type), expressed in #RGB 'value_condition' - The condition to apply on statistics value to count (for example: ">3", "=2" ...). For count type charts only. For trend_count_group type chart the condition is strictly equality and the value is stated without the operator (for example: "3", "2" ...). Only values passing the condition will be counted. 'bar_name' - The label for the bar. For count type only. If not present than the condition will be taken. 'function' - An aggregate function to use when compiling the data on trend_value type charts. The default is 'avg', which averages the data over all devices. All aggregate SQL functions are supported (for example: 'min', 'max') 'legend' - The label of the variable in the legend. Relevant for trend_value chart type only. -->

```
<variable_name bar_name="high" value_condition="=3"
color="#cb3333">highest</variable_name><variable_name bar_name="suspected
high" value_condition="=2" color="#ff8213">highest</variable_name><variable_
name bar_name="medium" value_condition="=1"
color="#fcf00a">highest</variable_name><variable_name bar_name="low" value_
condition="=0" color="#e4c67e">highest</variable_name>
```

<!-- A chart may have several additional configurable properties, specified by the following tags: 'order_dir' - The ordering of the results: asc (ascending) or desc (descending). The default is descending. For default type bar charts only. In case of

multiple variables (multi-series chart), the sort is based on the first variable. 'limit' - How many results to show, combined with 'order_dir' creates a top-X/bottom-X charts. Default is 20. Relevant for the default type only. 'direction' - The direction of the chart: horizontal or vertical. The default is vertical. Relevant for bar charts only. 'ymin' - The minimum value of the Y axis. The default is auto computed to fit the data. 'ymax' - The maximum value of the Y axis. The default is auto computed to fit the data. 'days_back' - The number of days back to show in a trend chart. -->

</CHART>

Configure a custom dashboard

Configure a custom dashboard by specifying the charts that the dashboard includes, the relevant device group, and the number of charts that appear in a row.

Do the following:

1. Open a terminal and log in as user **afa**.
2. Create a new file in **/home/afa/.fa/dashboards**.
3. Name the file **<dashboard_name>.xml**, where **<dashboard_name>** is the name you choose for the dashboard.
4. Add the [DASHBOARD](#) tag to the file, with the additional [CHARTS](#) and [CHART](#) sub-tags.

For more details, see [Dashboard tag reference](#) and [Dashboard configuration example](#).

Dashboard tag reference

The following table describes the **DASHBOARD** tag and its subtags.

Tag name	Description
DASHBOARD	<p>Identifies the dashboard and specifies how charts are oriented. Includes the CHARTS sub-tag.</p> <p>Parameters include:</p> <ul style="list-style-type: none"> • name. String. The dashboard name. This name appears at the top of the dashboard. • columns. The number of charts that appear in each row of the dashboard. <p>The charts will be filled in order of appearance, from left to right and top to bottom.</p>
CHARTS	<p>Defines all the charts that appear in the dashboard. Includes several CHART sub-tags.</p>
CHART	<p>Defines the type of data in the chart, and which device group's data appears in the chart.</p> <p>Parameters include:</p> <ul style="list-style-type: none"> • group. String. The name of the AFA device group that is analyzed in the chart. • definition_file. String. The name of the chart XML file. <p>Specify a custom chart that you created and saved in the <AFA home dir>/fa/dashboards/charts directory, or a built-in chart.</p> <p>For more details, see Custom dashboards and charts.</p>

Dashboard configuration example

The following code shows an AFA dashboard configuration file, including a [DASHBOARD](#) tag and [CHARTS](#) and [CHART](#) sub-tags.

```
<DASHBOARD columns="2" name="Summary">
<CHARTS>
  <CHART definition_file="total_risks_per_type_per_fw.xml" group="ALL_
FIREWALLS"/>

  <CHART definition_file="security_rating_trend.xml" group="ALL_
FIREWALLS"/>
```

```
<CHART definition_file="rules_per_fw.xml" group="ALL_FIREWALLS"/>

<CHART definition_file="covered_rules_per_fw.xml" group="ALL_
FIREWALLS"/>

</CHARTS>

</DASHBOARD>
```

Customize regulatory compliance report

AFA provides the ability to customize the **Regulatory Compliance** page for each AFA report in the CLI. The CLI supports the following actions:

- Adding or removing compliance reports.
- Creating custom reports by modifying existing reports.

For descriptions of all built-in regulatory compliance reports, see [Supported regulatory compliance reports](#).

Note: To remove or add compliance reports in the Web Interface, customize the compliance score value, or customize the compliance score severity threshold, see [Customize the regulatory compliance report](#).

Note: To create a completely custom regulatory compliance report for your organization, contact AlgoSec support.

Add, remove or customize compliance reports

Do the following:

1. Open a terminal and log in using the username "afa" and the related password.
2. Create a new directory `/home/afa/.fa/compliance_reports/`. This is the override directory.

3. Copy `/usr/share/fa/data/compliance_reports/compliance_reports.xml` to `/home/afa/.fa/compliance_reports/`.

4. To create a custom report by modifying an existing report (and add it to the regulatory compliance page), do the following:

5. Create new templates for the report, by doing the following:

a. Find the report template(s) you want to modify in the override directory.

Report templates follow the following naming convention:

- For individual device reports: **compliance_rep_tmpl_*reportname*.html**
- For group device reports: **compliance_rep_tmpl_group_*reportname*.html**
- For matrix device reports: **compliance_rep_tmpl_matrix_*reportname*.html**

where *reportname* is the name of the compliance report.

b. Copy the report templates you want to modify, and save the copy (in the override directory). Use the above naming convention, with a new name for your new report.

c. Modify your template copies as you desire.

d. Save the files.

6. Open `/home/afa/.fa/compliance_reports/compliance_reports.xml`.

Add a new `report` tag as a sub-tag to the `compliance_reports` tag. The following table describes the `report` tag attributes:

Attribute	Description
id	Internal key necessary for report creation.

Attribute	Description
title	Title of the report. This title will appear as a link on the Regulatory Compliance page of the device report. The link leads to the compliance report.
template_file	HTML template file for a single device. This template will be used to create a single device compliance report.
template_file_group	HTML template file for a device group. This template will be used to create a device group compliance report.
template_matrix	HTML template file for a device matrix. This template will be used to create a device matrix compliance report.
active	Indicates whether the report is generated when a device is analyzed. This attribute can take the following values: yes. Include the report on the Regulatory Compliance page of the device report. no. Exclude the report.
sub_title	The sub-title for the report. This appears below the title of the report.

Example

```
<report title="Payment Card Industry Data Security Standard (PCI-DSS) version 2"
active="yes" template_file_matrix="compliance_rep_tmpl_matrix_pci2.html"
template_file_group="compliance_rep_tmpl_group_pci2.html" template_
file="compliance_rep_tmpl_pci2.html" sub_title="test sub-title" id="pci2"/>
```

1. Save the file
2. To add a built-in report to the regulatory compliance page, do the following:
3. Open `/home/afa/.fa/compliance_reports/compliance_reports.xml`.
4. Set the `active` attribute of the report you wish to enable to `yes`.
5. Save the file.
6. To remove a built-in report from the regulatory compliance page, do the following:

- a. **Open** `/home/afa/.fa/compliance_reports/compliance_reports.xml`.
- b. **Set the** `active` **attribute of the report you wish to remove to** `no`.
- c. **Save the file.**

Troubleshooting

This topic describes common procedures used when troubleshooting AFA.

Tip: To view a training video that follows an Information Security Officer troubleshooting common issues that may be preventing him from monitoring and analyzing several types of security devices, see [Performing Basic AFA Troubleshooting](#).

Troubleshooting and maintenance permissions

Troubleshooting and day-to-day system maintenance may require permissions to perform the following steps or access the following directories:

Stop/Start/Restart services

Users may need to stop/start/restart the following services:

- `algosec-ms`
- `apache-tomcat`
- `crond`
- `httpd`
- `iptables`
- `syslog-ng`
- `algosec-ms`

Files and folders

Users may need to copy files from various locations (For example, `/tmp`, `mv`, `rm`, `mkdir`) and run `chmod`, `chown`, and `chattr` on the following paths:

- `/usr/share/fa/*` (all sub-tree)
- `/home/afa/algosec/syslog_processor/*`
- `/home/afa`

- `/home/afa/.fa`
- `/home/afa/.fa/firewalls/*`

Run various commands

Users may be required to run the following commands:

- `crontab -e -u afa`
- `vi /etc/ntp.conf`
- `vi /etc/hosts`
- `vi /etc/security/limits.conf`
- `kill -9 / pkill -9`
- `screen`
- `strace`

In addition, they may be required to modify the **iptables** configuration on the AlgoSec appliance/VM.

Sync AFA and FireFlow DB passwords

Some support cases may require performing a sync between the Firewall Analyzer and FireFlow DB passwords.

To do this, run the following commands from the root user SSH CLI:

```
FA_USER='afa'
FA_CONF_FILE="/home/$FA_USER/.fa/config"
FIREFLOW_SITE_CONFIG='/usr/share/fireflow/local/etc/site/
FireFlow_SiteConfig.pm'
DB_ENC_PASS=`awk -F"'"' '/FireFlowDatabasePasswordEncrypted/
{print $2;exit}' $FIREFLOW_SITE_CONFIG`
export PGPASSWORD=`/usr/bin/sudo -H -u $FA_USER /usr/share/
fa/bin/fa_password -decrypt $DB_ENC_PASS 2>/dev/null`
psql -U postgres -c "alter user $FA_USER with password
'${PGPASSWORD}';"
```

```
sed -i 's/^DB_password=.* /DB_password='$DB_ENC_PASS' / '
$FA_CONF_FILE
```

Entering and exiting debug mode

AlgoSec Support may request that you enter **Debug** mode.

Enter Debug mode	Click your username in the toolbar and then click Info . In the Info dialog, click Enter Debug Mode .
Exit Debug mode	Click your username in the toolbar and then click Info . In the Info dialog, click Exit Debug Mode .

Contact technical support

Contact AlgoSec support to open a new case or update an existing case.

Open a new case from the [AlgoSec Portal > Support > Submit a Support Case](#).

You may be requested to send one of the following sets of files:

GUI-related issues	<p>algosec-support-gui.zip</p> <p>For details, see Download general log files</p> <p>If the algosec-support-gui.zip file is unavailable, send the following files instead:</p> <ul style="list-style-type: none"> • .fa-history • fa-install.log • .ht-fa-history <p>For more details, see Access log and configuration files.</p>
---------------------------	--

All other issues	algosec-support.zip For details, see Download report log files If the algosec-support.zip file is unavailable, send the following files instead: <ul style="list-style-type: none">• fa-install.log• .fa-history• log.html• index.html• .ht-fa-history For more details, see Access log and configuration files .
-------------------------	--

For more details, see the [AlgoSec Portal > Support > Support Home](#).

Access log and configuration files

Note: Accessing the device configuration and log files requires configuration and logs privileges.

The following table lists log and configuration files useful when troubleshooting AFA.

File Name	Description	Location
algosec-support.zip	<p>An archive file that includes the following report and general log files:</p> <ul style="list-style-type: none"> • fa-history • fa-install.log • ht-fa-history • log.html • fwa_monitor.history <p>Note: The fwa_monitor.history file may be missing if the file report has a status of FAILED, or if you encounter problems during the installation or licensing stages.</p>	<p>\$HOME/algosec/firewalls/<job-name>/</p> <p>Where <job-name> is the Job Name of the report.</p> <p>The Job Name consists of the user login name followed by a hyphen and an integer.</p> <p>Example: afa-3</p>
algosec-support-gui.zip	<p>An archive file that includes:</p> <ul style="list-style-type: none"> • fa-history • fa-install.log • ht-fa-history • map.sqlite • dump_nat_data 	<p>Download from AFA.</p> <p>For details, see Download general log files.</p>
log.html	<p>The report log file.</p> <p>Note: This file may be missing if the file report has a status of FAILED.</p>	<p>\$HOME/algosec/firewalls/<job-name>/</p> <p>For details, see:</p> <ul style="list-style-type: none"> • View report log files • Download report log files
algosec-support-full-ENTITY_NAME.zip	<p>Full support data files which include:</p> <ul style="list-style-type: none"> • report log files • full firewall configuration 	<p>Download from the device report.</p> <p>For details, see Download full support files.</p>

File Name	Description	Location
algosec-support-full-ENTITY_NAME-withlogs.zip	Full support data files which include: <ul style="list-style-type: none"> • report log files • full firewall configuration • traffic logs 	Download from the device report. For details, see Download full support files .
messages	All syslog messages.	/var/log/
fa-install.log	The AFA installation log	/var/log/
fa-history	The AFA application's history file.	\$HOME/ This file is hidden by default. To view, run: ls -a \$HOME/.fa-history
ht-fa-history	The Web interface's log file.	\$HOME/public_html/algosec/ This file is hidden by default. To view, run: ls -a \$HOME/public_html/algosec/.ht-fa-history
map.sqlite	The database of the map.	\$HOME/.fa/map.sqlite
dump_nat_data	Dump of NAT related tables.	
index.html	The report main index file. This serves as the log file if analysis failed.	\$HOME/algosec/firewalls/<job-name>/

Note: You'll need to access the log files directly if the ASMS web interface isn't available, or if the **algosec-support.zip** archive is missing. This may happen if a report has failed, or if you've encountered issues during installation or licensing.

For more details, see:

- [View report log files](#)
- [Download report log files](#)
- [Download full support files](#)
- [Download general log files](#)

View report log files

Report log files are accessed from a specific AFA report.

Do the following:

1. View the report.
2. In the report menu, click **Policy**.
3. In the **Report Information** area, click the **Log File** link.

The log file appears. All messages are prefixed with one of the following **severity** tags:

Severity Level	Description
Info	Normal information messages and notification of events. No user action is required.
Warning	AFA took corrective action to remedy a problem that was encountered. Usually, no user action is required unless the report failed to generate, in which case the log file should be sent to AlgoSec Technical Support. For more details, see Contact technical support .
Error	A problem that prevented the report from being generated occurred. Contact AlgoSec Technical Support. For more details, see Contact technical support .
Fatal	A severe error condition required an immediate halt to the report generation process. Contact AlgoSec Technical Support. For more details, see Contact technical support .

Download report log files

Report log files are accessed from a specific AFA report.

Do the following:

1. View the report.
2. In the report menu, click **Policy**.
3. In the **Report Information** area, click **AlgoSec Support File**.

The zip file is downloaded to your computer.

Download full support files

Full support files are accessed from a specific AFA report.

Do the following:

1. View the report.
2. In the report menu, click **Policy**.
3. In the **Report Information** area, click one of the following:
 - **Full Support Data with traffic logs (Large)**
 - **Full Support Data**

The zip file is downloaded to your computer.

Download general log files

General log files are useful for troubleshooting interface-related issues.

Do the following:

1. In the toolbar, click your username, and select **Info**.
2. In the **Info** dialog, click **Download Support Files**.
3. Click **Download Support Files**.

The **algotsec-support-gui.zip** file downloaded to your computer. It contains the following files:

- **catalina.out**
- **configuration_access_log.<date>.txt**
- **dump_nat_data**
- **fa-history**
- **fa-install.log**
- **fa/map.sqlite**
- **fwa_monitor.history**
- **ha-logs.tgz**
- **ht-fa-history**
- **localhost_access_log.<date>.txt**
- **log.html**
- **ms-backuprestore.log**
- **ms-batch-application.log**
- **ms-configuration.log**
- **ms-devicemanager.log**
- **ms-mapDiagnostics.log**
- **ms-watchdog.log**

Send us feedback

Let us know how we can improve your experience with the Administration Guide.

Email us at: techdocs@algosec.com

Note: For more details not included in this guide, see the online [ASMS Tech Docs](#).