



# AlgoSec Firewall Analyzer

Software Version: A30.00

## Administration Guide

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

**Document Release Date:** 5 June, 2020 | **Software Release Date:** August 2019

# Legal Notices

Copyright © 2003-2019 AlgoSec Systems Ltd. All rights reserved.

AlgoSec, FireFlow, and BusinessFlow 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

---

<b>AFA administration</b>	<b>16</b>
Access the AFA Administration area	16
Quickstart - Configure AFA to analyze devices	17
<b>Logins and other basics</b>	<b>19</b>
Supported browsers	19
Log in to ASMS	19
Customize your landing page	22
View ASMS product details	23
Log out of ASMS	24
<b>Manage devices</b>	<b>26</b>
AFA communication protocols	26
Device procedure reference	26
Device icons	27
Add devices to AFA	29
Add device prerequisites	29
Access the DEVICES SETUP page	29
Add cloud devices	32
AWS (Amazon Web Service) accounts in AFA	32
Microsoft Azure subscriptions in AFA	38
Add Check Point devices	42
Check Point network connections	43
Check Point device permissions	43
Add a Check Point Provider-1 device	45
Set user permissions	49
Add a Check Point SmartCenter/Gateway	50
Set user permissions	53
Add a Check Point CMA	53
Check Point fields and options	57
Enable data collection for Check Point devices	62
Enable data collection via SSH	63

---

Enable data collection via OPSEC .....	66
Enable data collection via REST .....	82
Add Cisco devices .....	84
Add a CSM-managed Cisco device .....	84
Add a Cisco IOS router .....	90
Cisco Nexus routers in AFA .....	95
Add a Cisco ASA firewall .....	100
Add a Cisco Application Centric Infrastructure (ACI) .....	108
Add a Cisco FirePower .....	112
Add F5 devices .....	115
Add an F5 BIG-IP LTM Only .....	115
Add an F5 BIG-IP LTM and AFM .....	119
Add Fortinet devices .....	125
Fortinet network connections .....	125
FortiManager device permissions .....	126
FortiGate device permissions .....	128
Add a Fortinet FortiManager device to AFA .....	129
Add a Fortinet FortiGate device to AFA .....	135
Add Juniper devices .....	138
Add a Juniper NSM .....	138
Add a Junos Space Security Director .....	148
Juniper SRX devices in AFA .....	152
Add a Juniper Netscreen .....	159
Add a Juniper M/E router .....	166
Add Palo Alto Networks devices .....	169
Palo Alto network connection .....	169
Panorama device permissions .....	169
Palo Alto Networks Firewall device permissions .....	170
Add a Palo Alto Networks Panorama .....	171
Add a Palo Alto Networks firewall .....	176
Add a Symantec Blue Coat .....	180

---

Add a VMware NSX .....	184
Required device permissions .....	187
Baseline configuration compliance .....	187
Device requirements reference by brand .....	187
Check Point device requirements .....	188
Cisco device requirements .....	188
Arista device requirements .....	189
Juniper device requirements .....	190
Fortinet device requirements .....	194
Palo Alto device requirements .....	194
F5 device requirements .....	194
Symantec BlueCoat SGOS device requirements .....	195
WatchGuard device requirements .....	195
TopSec device requirements .....	195
VMware NSX device requirements .....	195
AWS requirements .....	196
Azure requirements .....	196
Add other devices and routing elements .....	197
Add monitoring and routing devices .....	197
Add routing elements .....	201
Add/update multiple devices in bulk .....	203
Prepare your CSV file .....	204
Import your CSV file (UI) .....	205
Import your CSV file (CLI) .....	206
Bulk import support scope .....	207
CSV import file format .....	209
Basic device description headers .....	210
Access information headers .....	211
Cisco-related headers .....	212
CyberArk-related headers .....	213
Advanced headers .....	214

---

Remote management headers .....	215
Log and monitoring headers .....	216
Additional headers .....	218
SNMP polling headers .....	220
Maintain devices .....	221
Edit a device's configuration .....	221
Rename a device .....	222
Add additional device identifiers for sub-systems .....	222
Delete a device .....	223
Update a password for multiple devices .....	223
Specify routing data manually .....	225
Specify routing data manually for primary devices .....	225
Specify routing data manually for sub-systems .....	226
Specify routing data from the map .....	227
Integrate AFA and CyberArk .....	228
Supported devices for CyberArk integration .....	228
Configure CyberArk integration .....	229
<b>Alternate data collection methods .....</b>	<b>231</b>
When to use these procedures .....	231
Recommended device data collection per device type .....	231
Add a static file device to AFA (UI) .....	233
Add a static file device to AFA (CLI) .....	235
Semi-automatic data collection scripts .....	236
Check Point devices (manual) .....	237
Check Point SmartCenter on Solaris/Nokia/Secure Platform/Linux .....	237
Check Point Provider-1 .....	238
Check Point SmartCenter on Microsoft Windows .....	240
Alternative Methods for Obtaining the Routing Table .....	241
Check Point FireWall-1 devices (semi-automatic) .....	245
Sun/Nokia/SecurePlatform/Alteon/Linux Platforms .....	245
Check Point FireWall-1 with a Separate SmartCenter Server and Filter Module .....	245

---

Check Point Provider-1 .....	249
Check Point FireWall-1 with an Integrated Management and Filter Module .....	253
Using Saved Profiles .....	255
Windows Platform .....	256
Check Point FireWall-1 with Separate SmartCenter Server and Filter Module .....	256
Check Point FireWall-1 with Integrated SmartCenter Server and Filter Module .....	258
Cisco routers and devices .....	258
Collect data semi-automatically from Cisco IOS or Nexus routers .....	258
Collect data manually from Cisco IOS routers .....	261
Collect data manually from Cisco IOS-XR routers .....	263
Collect data manually from Cisco Nexus routers .....	264
Collect data manually from Cisco ASA devices .....	266
Tips for copying command line output .....	267
Juniper devices .....	267
Collect device data semi-automatically from Juniper Netscreen devices ..	267
Collect data manually from Juniper Netscreen devices .....	269
Collect data manually from Juniper M/MX routers .....	270
Collect data manually from Juniper SRX devices .....	271
Fortinet Fortigate (manual) .....	273
Palo Alto Networks (manual) .....	275
McAfee Firewall Enterprise (Sidewinder) (manual) .....	277
Symantec Blue Coat (manual) .....	279
<b>Extend device support .....</b>	<b>282</b>
Static configuration file support .....	282
Live monitoring support .....	282
Static support for generic devices .....	283
Supported device types .....	283
Adding Support for a File Device .....	283
Creating the JSON File .....	284

---

Tag Reference .....	285
config_type .....	286
device .....	286
hosts .....	286
hosts_groups .....	287
interfaces .....	287
services .....	288
services_groups .....	288
policies .....	288
rules_groups .....	289
nat_rules .....	290
zones .....	291
routes .....	291
schedules .....	291
Generic Device JSON File Examples .....	292
JSON File Example for a Policy-Based Device .....	292
JSON File Example for an Interface-Based Device .....	303
JSON File Example for a Zone-Based Device .....	311
Static support troubleshooting .....	414
Troubleshooting Files and Folders .....	414
Problem: Analysis Failed .....	415
Example .....	415
Generic device monitoring .....	416
Enable live monitoring support .....	417
Create data collection files for a generic device .....	417
Install the new brand .....	418
Add the device to AFA .....	418
Collect routing information via SNMP .....	420
Configuration file example .....	420
Configuration file example with routing .....	421
Monitoring support tag reference .....	422

---

Tag syntax .....	422
DEVICE .....	422
FORM_FIELD .....	423
CONNECTION_CMD .....	424
DATA_COLLECTION .....	425
LOGIN_PROMPT .....	426
POST_LOGIN_PROMPT .....	427
COMMANDS_SEQUENCE .....	428
CMD .....	429
CMD_VIRT .....	431
DATA_COLLECTION .....	433
DIFF .....	433
EXCLUDE .....	434
ROUTING .....	435
FEATURES .....	436
FEATURE .....	437
Early availability features .....	437
Enable / Disable support for Cisco ISE .....	438
Enable /Disable support for Arista .....	439
Enable / Disable map support for Azure .....	440
Enable /Disable ActiveChange for Azure .....	441
Enable support for Check Point R80 layers .....	442
<b>Manage groups .....</b>	<b>445</b>
About groups in AFA .....	445
Add groups .....	445
Edit groups .....	447
Rename groups .....	448
Delete groups .....	449
<b>Manage matrices .....</b>	<b>450</b>
About AFA matrices .....	450
Add matrices .....	451

---

Edit matrices .....	453
Rename matrices .....	454
Delete matrices .....	455
<b>Manage DR sets .....</b>	<b>456</b>
Add DR sets .....	456
Edit DR sets .....	457
Rename DR sets .....	459
Delete DR sets .....	459
<b>Manage the map .....</b>	<b>461</b>
Complete the map .....	461
Completed map contents .....	461
Identify routers to define in AFA .....	462
Complete the map (CLI) .....	465
Map completeness CLI tool scope .....	465
Identify routers to define in AFA .....	466
Map completeness parameters .....	469
Troubleshoot traffic simulation queries .....	470
Edit IP ranges in clouds .....	473
Remove devices .....	476
Restore device interfaces .....	477
Specify routing data manually .....	478
<b>Schedule analysis .....</b>	<b>480</b>
Add and edit analysis jobs .....	480
Delete scheduled jobs .....	484
<b>Configure real-time monitoring .....</b>	<b>486</b>
Activate real-time monitoring .....	486
<b>Manage users and roles .....</b>	<b>488</b>
AFA authentication .....	488
AFA permissions .....	488
Configure user authentication .....	489
Single Sign On (SSO) and ASMS .....	489

---

User authentication via authentication servers .....	502
Import user data from an LDAP server .....	513
Configure an LDAP forest .....	515
Log in when an LDAP forest is configured .....	522
Manage users and roles in AFA .....	523
Add and edit users .....	523
Delete users .....	532
Add and edit user roles .....	533
Delete user roles .....	537
ASMS username and password requirements .....	537
Import users via CSV .....	538
Prepare a users CSV file .....	538
Run the import users script .....	543
<b>Customize risk and compliance management .....</b>	<b>544</b>
Customize risk profiles .....	544
View a risk profile .....	545
Add a new risk profile .....	547
Delete a custom risk profile .....	554
Set a default risk profile .....	554
Customize risk items .....	555
Edit, duplicate, or add a custom risk item .....	555
Risk Info fields .....	556
Risk Query fields .....	556
Risk Details fields .....	558
Delete a risk item .....	562
Disable a risk item .....	563
Customize zone types .....	563
Built-in zone types .....	564
Add and edit zone types .....	564
Delete zone types .....	566
Customize hostgroups .....	567

---

Add and edit host groups .....	567
Delete hostgroups .....	568
Customize services .....	569
Add and edit service groups .....	569
Delete service groups .....	571
Configure trusted private IP addresses .....	572
Configure security ratings .....	573
Security rating calculation .....	573
Security rating calculation background .....	574
Customize security rating settings .....	575
Customize the regulatory compliance report .....	576
Remove and add compliance reports .....	577
Supported regulatory compliance reports .....	578
Customize the compliance score value .....	580
Customize compliance score severity thresholds .....	582
Configure the PCI zone .....	583
Customize baseline configuration profiles .....	585
Access baseline profiles configuration .....	585
Add a custom baseline configuration compliance profile .....	586
Duplicate a baseline configuration compliance profile .....	588
Edit a baseline configuration compliance profile .....	590
Delete a custom baseline configuration compliance profile .....	591
Example: Customize a baseline configuration compliance profile .....	591
Sample Baseline Configuration Compliance Profile .....	601
Advanced risk editing .....	602
Overview .....	602
Risk item types .....	603
Traffic risk item guidelines .....	604
Host group risk item guidelines .....	606
Property risk item guidelines .....	607
Rule risk item guidelines .....	607

---

Assessment and remedy keywords .....	609
<b>Configure notifications .....</b>	<b>613</b>
Schedule dashboard notifications .....	613
Add and edit dashboard e-mails .....	613
Deleting Scheduled Jobs .....	616
Configure event-triggered notifications .....	616
Supported notifications .....	617
E-mail Notification Example 1: Analysis completed .....	617
E-mail Notification Example 2: Changes to policy and risks .....	617
Configure AFA to send event triggered e-mail notifications .....	618
Configure device report page messages .....	620
<b>Define AFA preferences .....</b>	<b>623</b>
General .....	624
General Fields .....	625
Language .....	626
Display .....	627
Display Fields .....	627
Log analysis .....	628
Log analysis fields .....	628
Define a device proxy .....	629
Proxy fields .....	630
Mail .....	630
Storage .....	631
Configure report cleanup .....	632
Workflow .....	635
Change request ID format .....	636
AlgoSec FireFlow .....	637
BMC Remedy .....	637
HP ServiceCenter (formerly Peregrine) .....	639
Other .....	641
Authentication .....	642

---

Backup/Restore .....	643
Backup and restore prerequisites .....	644
Backup and restore on distributed architectures .....	644
Define backup options .....	645
Back up your system .....	647
Restore your system .....	648
Special Considerations for Distributed Architecture Environments .....	649
Advanced Configuration .....	650
<b>Override AFA system defaults .....</b>	<b>652</b>
Configure the device tree view .....	652
Configure group traffic query results .....	653
Enable IPT rule recommendations .....	654
Configure IPT rule recommendations .....	655
Disable sort/filters in tables .....	658
Configure change detail display .....	659
Enable custom report pages .....	660
Define chart threshold .....	661
Define default dashboard .....	662
Configure subnet prioritization .....	664
<b>Customize AFA .....</b>	<b>666</b>
Custom report pages .....	666
Create a custom report page .....	666
Custom report configuration file parameters .....	667
Extract custom report script flags .....	668
Custom documentation fields .....	669
Add documentation fields .....	669
Enable/Disable documentation fields .....	670
Custom dashboards and charts .....	670
Configure custom charts .....	670
Add a custom chart .....	671
Chart tag reference .....	671

---

Configure a custom dashboard .....	685
Dashboard tag reference .....	685
Dashboard configuration example .....	686
Customize regulatory compliance report .....	687
Add, remove or customize compliance reports .....	687
<b>Troubleshooting .....</b>	<b>690</b>
Troubleshooting and maintenance permissions .....	690
Entering and exiting debug mode .....	691
Contact technical support .....	692
Access log and configuration files .....	693
<b>Send us feedback .....</b>	<b>699</b>

# 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.

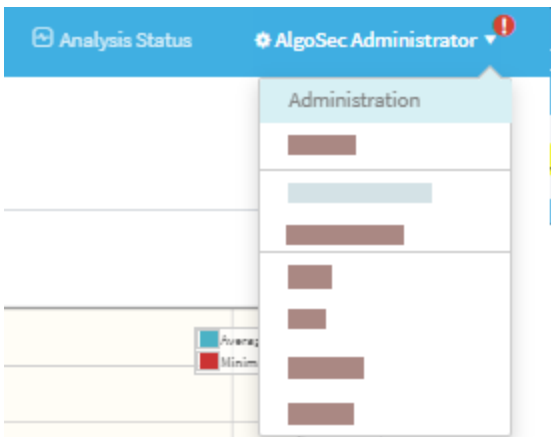
**Note:** For details about logging in or out of AFA, see [Logins and other basics](#).

## 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"><li>• <a href="#">Manage devices</a></li><li>• <a href="#">Manage groups</a></li><li>• <a href="#">Manage matrices</a></li></ul>
USERS/ROLES	Manage AFA users and user roles. For details, see <a href="#">Manage users and roles</a> .

<b>SCHEDULER</b>	Schedule analysis and notifications. For details, see <a href="#">Schedule analysis</a> .
<b>COMPLIANCE</b>	Manage risk profiles, baseline profiles, and compliance options. For details, see <a href="#">Customize risk and compliance management</a> .
<b>OPTIONS</b>	Configure AFA preferences including report storage options, user authentication options, backup options, and more. For details, see <a href="#">Define AFA preferences</a> .
<b>MONITORING</b>	Configure real-time monitoring. For details, see <a href="#">Configure real-time monitoring</a> .
<b>ARCHITECTURE</b>	Manage slaves 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 [Manage 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.

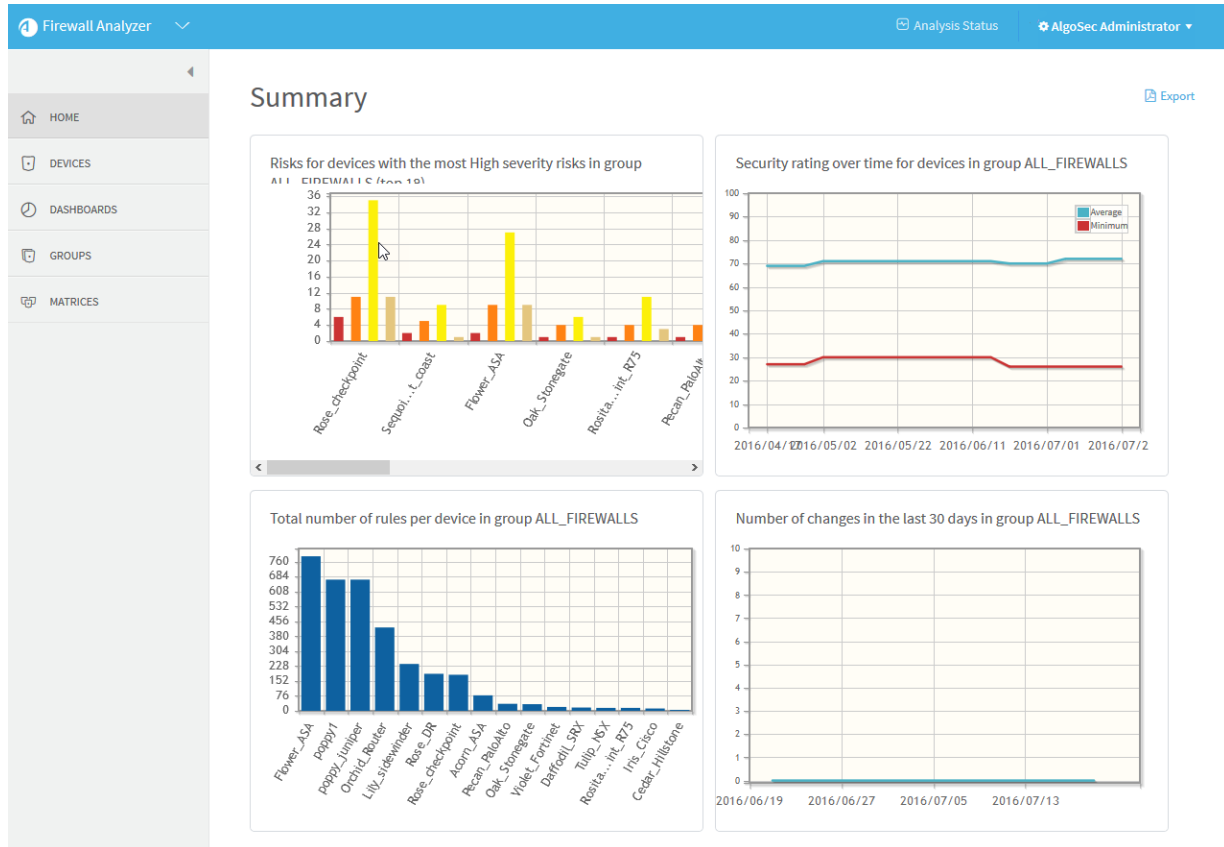


The screenshot shows the login interface for the algosec Security Management Suite. At the top right is a link labeled "About". The algosec logo is centered at the top. Below the logo, the text "Security Management Suite" is displayed. There are two input fields: "User Name" and "Password". Below these 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.

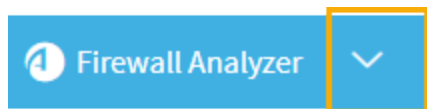
For example:



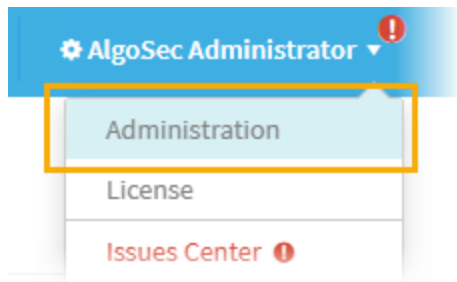
**Tip:** If you have multiple AlgoSec products and want to change your default landing page, see [Customize your landing page](#).

## Switch ASMS products

If you are a user in multiple ASMS products, such as AFA, FireFlow, and BusinessFlow, 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:



## 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.

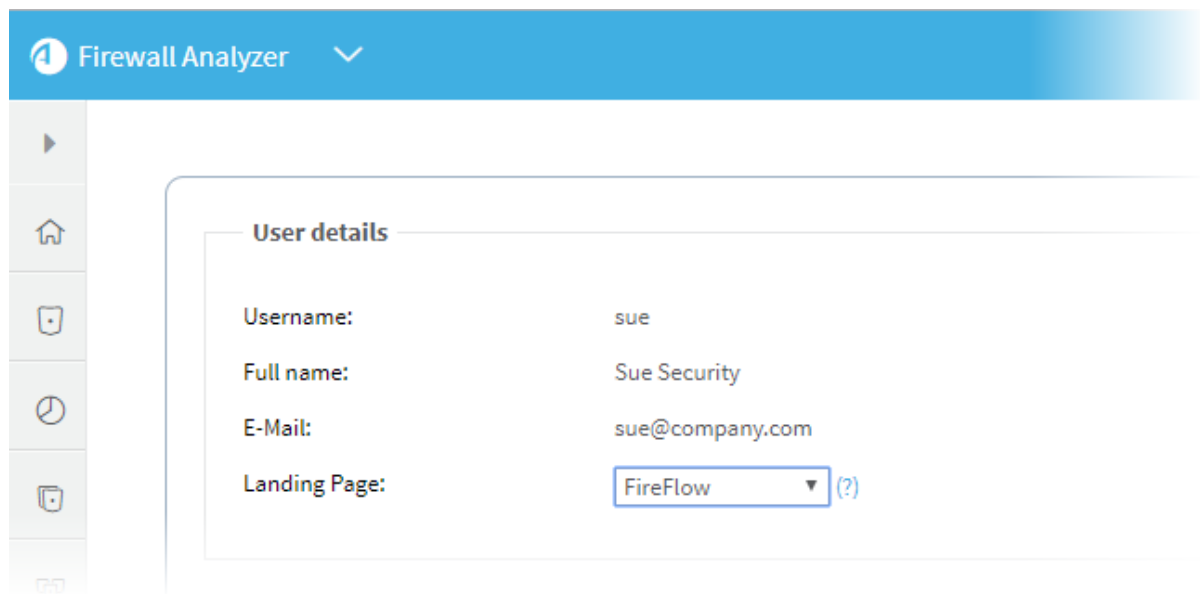
## Customize your landing page

The following procedure describes how ASMS users can define their own landing page.

Do the following:

1. Click your username in the toolbar and select **User Settings**.
2. In the **User details** area > **Landing page** drop-down, select the landing page you want to see when you first log in.

For example:



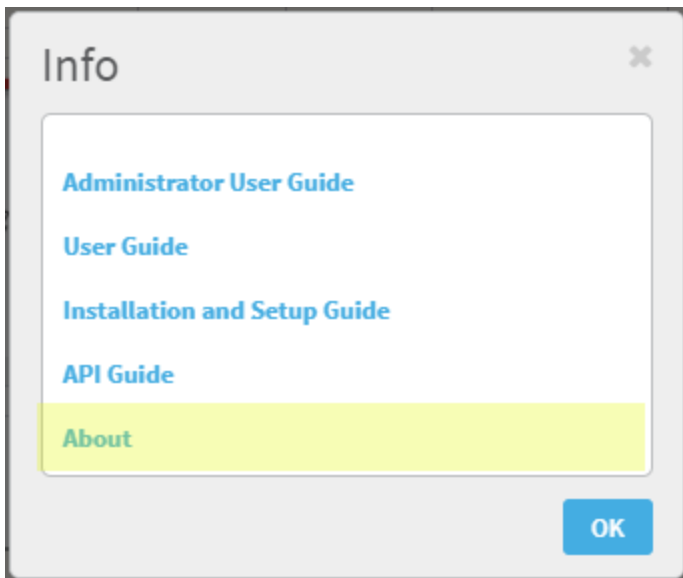
Log and out and log in again to view the change.

## View ASMS product details

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

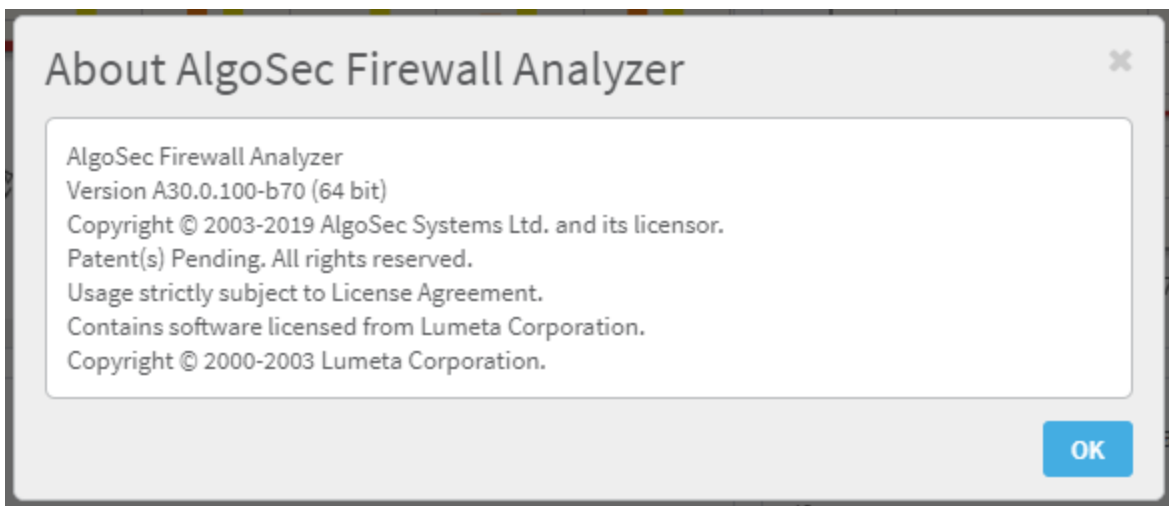
Do the following:

1. In the toolbar, click your username and then select **About** or **Info**.
2. 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-secure128 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:













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

<b>Device-specific procedures</b>	<ul style="list-style-type: none"> <li>• <a href="#">Add cloud devices</a></li> <li>• <a href="#">Add Check Point devices</a></li> <li>• <a href="#">Add Cisco devices</a></li> <li>• <a href="#">Add F5 devices</a></li> <li>• <a href="#">Add Fortinet devices</a></li> <li>• <a href="#">Add Juniper devices</a></li> <li>• <a href="#">Add Palo Alto Networks devices</a></li> <li>• <a href="#">Add a Symantec Blue Coat</a></li> <li>• <a href="#">Add a VMware NSX</a></li> </ul>
-----------------------------------	--

## 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/ACI, IOS Router, or Nexus Router device or security context
	Check Point Provider-1, 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 <b>Note:</b> Supported only if the device had been added in an ASMS version earlier than A30.00. For details, see <a href="#">Deprecated devices</a> .
	Topsec Firewall device
	WatchGuard device
	Hillstone Networks device <b>Note:</b> Supported only if the device had been added in an ASMS version earlier than A30.00. For details, see <a href="#">Deprecated devices</a> .
	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 <a href="#">Extend device support</a> .

### 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. 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.

<b>Manage ports</b>	<p><b>Note:</b> 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><b>Note:</b> In the case of a distributed architecture, open the port between the device and the specific remote agent or slave managing each device.</p>
<b>Device permissions</b>	<p>You may need to configure device user permissions to enable AFA to collect data from your device.</p> <p>For details, see <a href="#">Required device permissions</a>.</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](#)

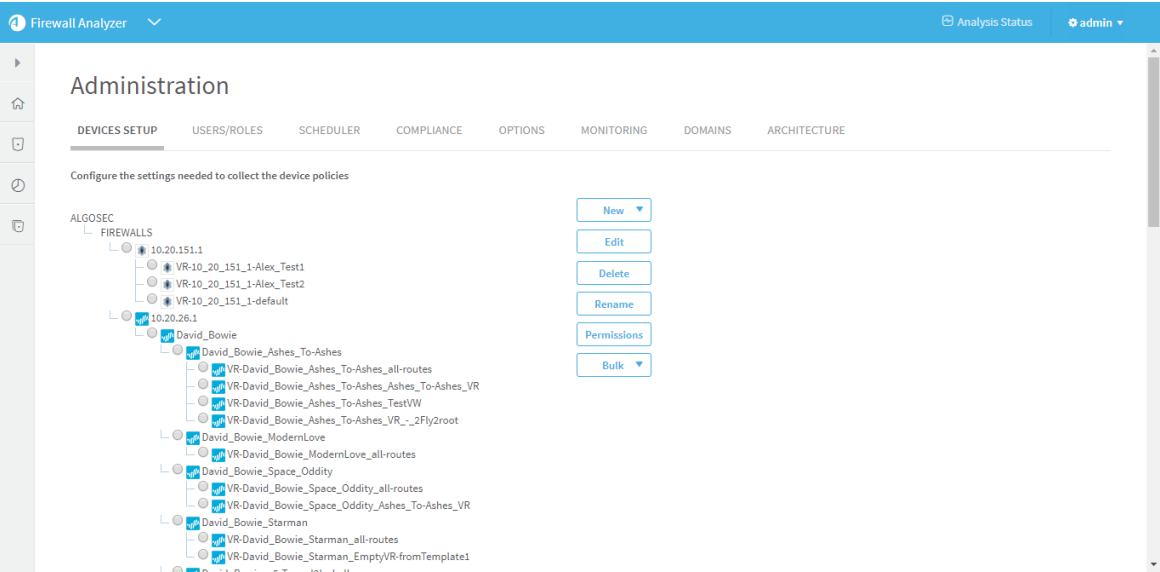
[prerequisites.](#)

Do the following:

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

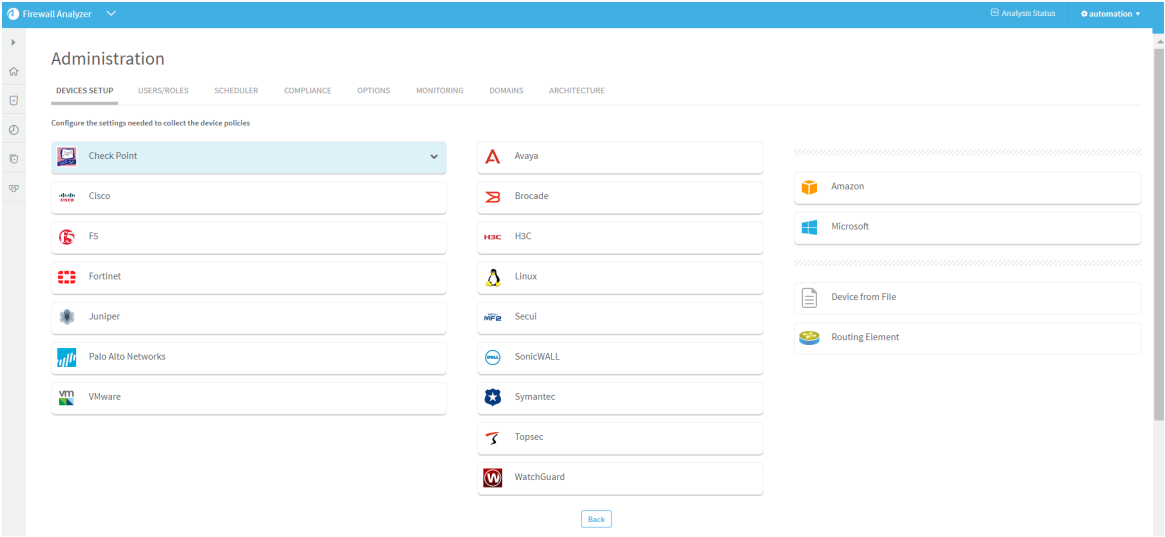
<b>From the main menu on the left</b>	Click <b>Devices, Groups, or Matrics</b> , and then click the  <b>Configure ..</b> button.  <b>Note:</b> This button is visible to AFA administrators only.
<b>From the Administration area</b>	In the toolbar, click your username, and select <b>Administration</b> .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

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



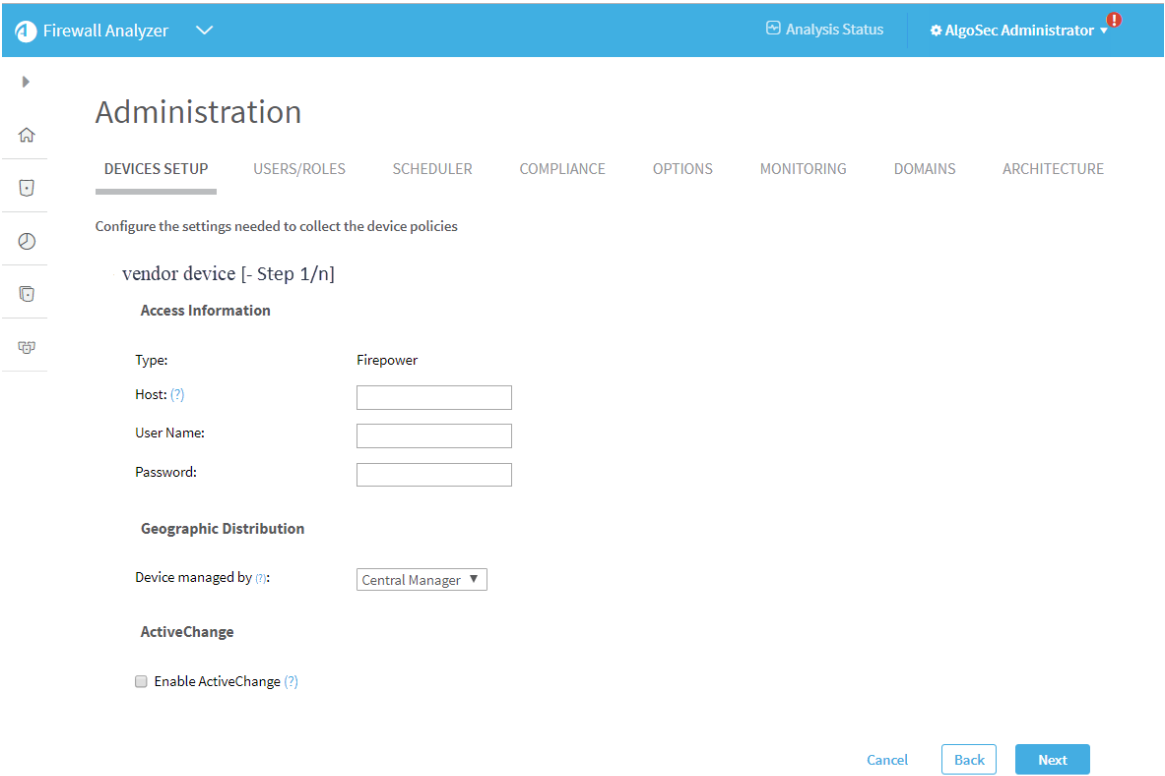
2. Click **New ▼** and select **Devices**.

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:



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

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

### ➔ 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:

Filter: Policy Type <input type="text" value="AmazonEC2"/>					
		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](#)

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

## 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

<b>Access Information</b>	<p>The device type is automatically defined.</p> <p>In the <b>Name</b> field, enter the name that you want to appear in the device tree for this account.</p> <div><b>Tip:</b> Use the account's host or route name.</div>
---------------------------	--

<b>Additional Information</b>	<p>Enter the following details to define access to your AWS account:</p> <ul style="list-style-type: none"> <li>• <b>AWS Access Key ID.</b> Enter your access key, supplied by Amazon.</li> <li>• <b>AWS Secret Key ID.</b> Enter your secret key, supplied by Amazon.</li> <li>• <b>Regions.</b> Select one of the following to define your region: <ul style="list-style-type: none"> <li>◦ All</li> <li>◦ China (Beijing)</li> <li>◦ GovCloud</li> </ul> </li> <li>• <b>Assume Role for a Different Account.</b> Select to define this AWS account with the credentials of another AWS account that is already defined in AFA. When selected, also define the <b>Target Account Role ARN</b> (the Amazon Resource Name (ARN) of the role to assume.)</li> </ul> <p>For more details, see <a href="#">Device access requirements for AWS</a>.</p>
<b>Route Collection</b>	<p>Select one of the following to determine how AFA should acquire the device's routing data.</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> Automatically generate routing data upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> Take the device's routing data from a static file that you provide.</li> </ul> <p>For details, see <a href="#">Specify routing data manually</a>.</p>
<b>Proxy</b>	<p>Click <b>Set Proxy Server</b> to configure a proxy server to connect all cloud devices defined in AFA, including both AWS and Azure.</p> <p>For more details, see <a href="#">Define a device proxy</a>.</p>
<b>ActiveChange</b>	<p>Select <b>Enable ActiveChange</b> for this device.</p>

<b>Options</b>	<p>Select the following options for your AWS account as needed:</p> <ul style="list-style-type: none"><li>• <b>Real-time change monitoring.</b> Select this option to enable real-time alerting upon configuration changes. For more details, see <a href="#">Configure real-time monitoring</a>.</li><li>• <b>Set user permissions.</b> Select this option to set user permissions for this device.</li></ul>
----------------	--

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.

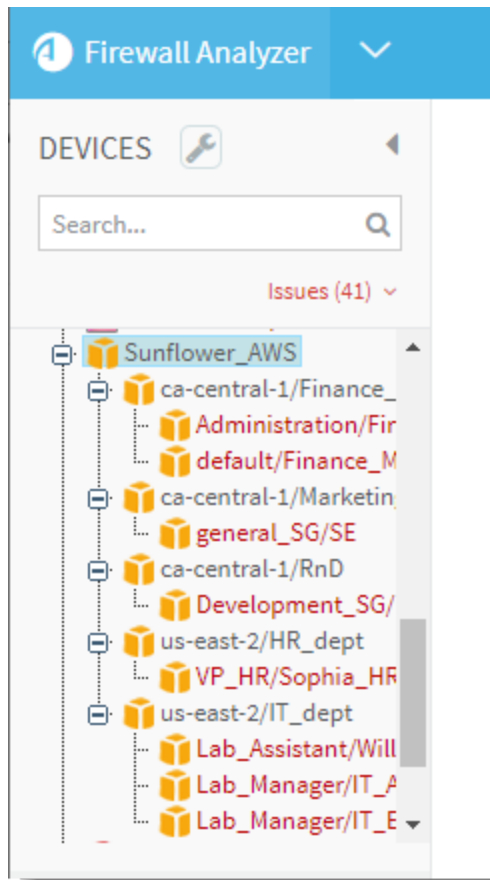
To select multiple users, press the **CTRL** button while selecting.

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.

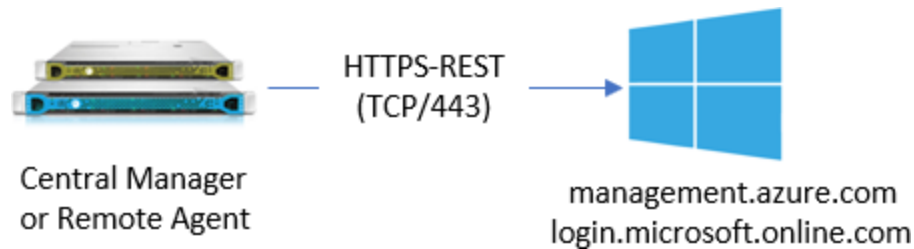
AFA separates the instances into groups called **security sets**. Each Azure security set is a group of VMS with the same security group and subnet security groups, as well as network policies. VMs with no security groups are assigned to a security set called **Unprotected VMs**. To enable accurate traffic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

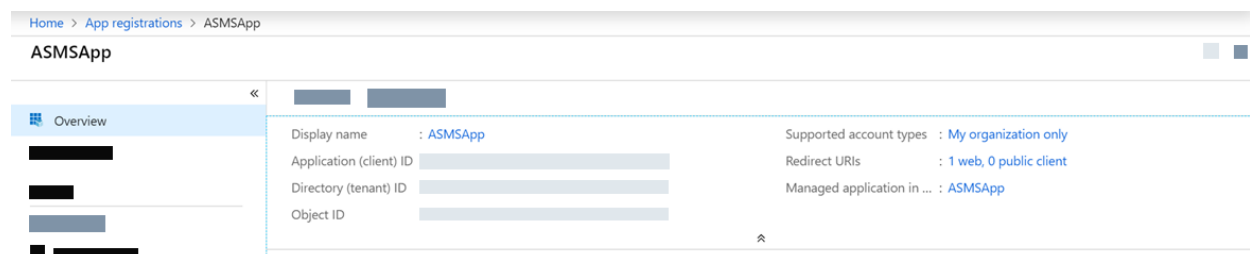
ASMS requires the following permissions for your Azure subscriptions:

### Device analysis

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

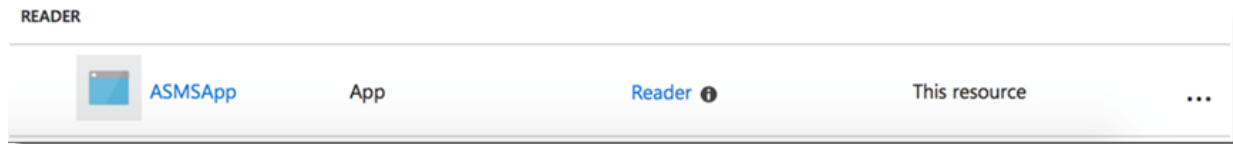
We recommend creating an App Registration with specific permissions instead of sharing an account with other applications.

For example:



The IAM permissions should be **Reader**.

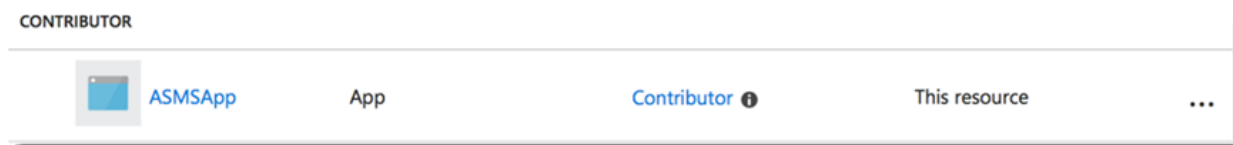
For example:



## 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

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

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.

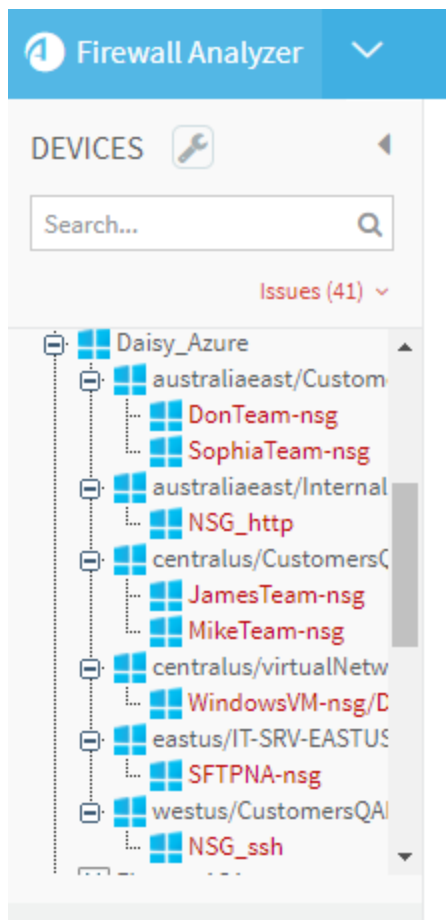
To select multiple users, press the **CTRL** button while selecting.

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

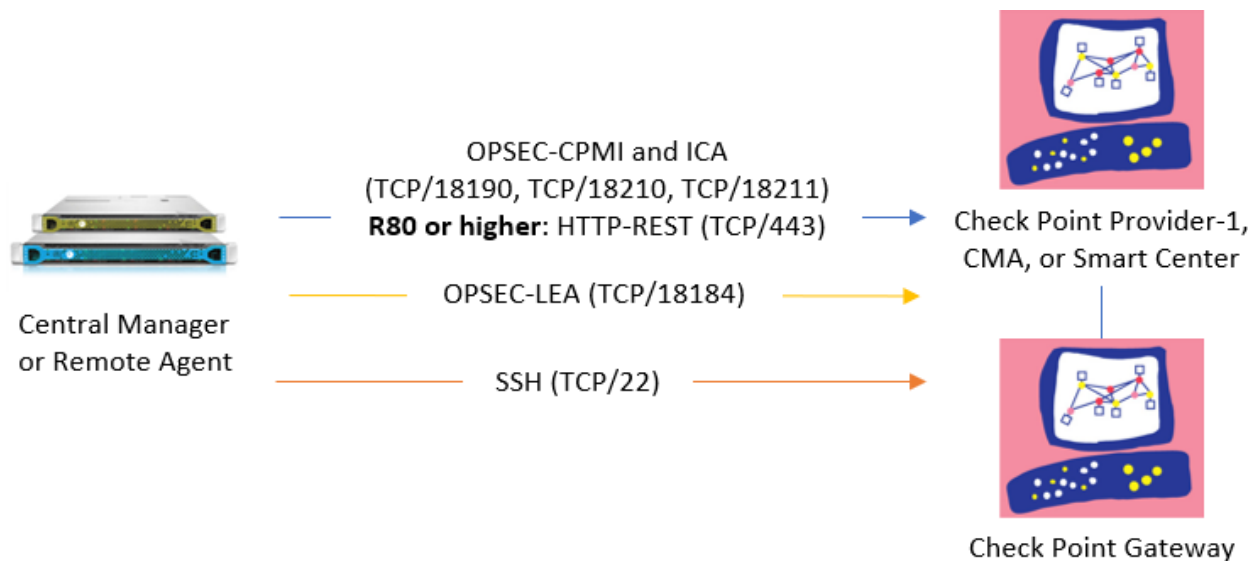
This topic describes how to add Check Point Provider-1, SmartCenter / Gateway, or CMA devices, as well as fields and options shared by all of these device types.

**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 Provider-1, 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:

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

**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:

<b>Read</b>	AFA requires read permissions on the domain folders, such as <b>\$FWDIR/conf</b> or <b>\$FWDIR/log</b> .
<b>Write</b>	AFA writes a package containing the required configuration in the <b>/tmp</b> or <b>/var/tmp</b> directory, based on the device platform, such as SP or Solaris. AFA also requires write permissions in the <b>\$FWDIR/conf</b> directory for temporary log files.
<b>Execute</b>	AFA runs several commands on the management device, including <b>fwm logexport</b> for logs and <b>cpstat</b> 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 Provider-1 device

Check Point Provider-1 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 Provider-1 server.

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:

<b>OPSEC</b>	Recommended.  Enter the IP address of the CMA that manages the devices you wish to analyze.
<b>SSH</b>	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 Provider-1, including standalone devices and virtual systems.

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

system.

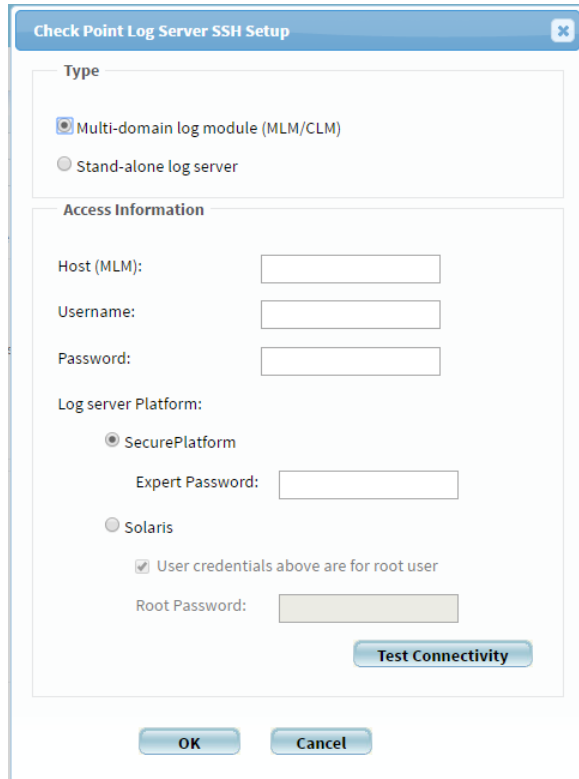
**Tip:** This enables AFA to detect certain policy optimization information, such as unused rules.

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**.



The image shows a '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'. In the 'Type' section, there are two radio buttons: 'Multi-domain log module (MLM/CLM)' which is selected, and 'Stand-alone log server'. The 'Access Information' section contains several fields: 'Host (MLM):', 'Username:', and 'Password:' each followed by a text input box. Below these is the 'Log server Platform:' section with two radio buttons: 'SecurePlatform' (selected) and 'Solaris'. Under 'SecurePlatform', there is an 'Expert Password:' field. Below the 'Solaris' option, there is a checked checkbox labeled 'User credentials above are for root user' and a 'Root Password:' field. At the bottom of the 'Access Information' section is a 'Test Connectivity' button. At the very 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**.

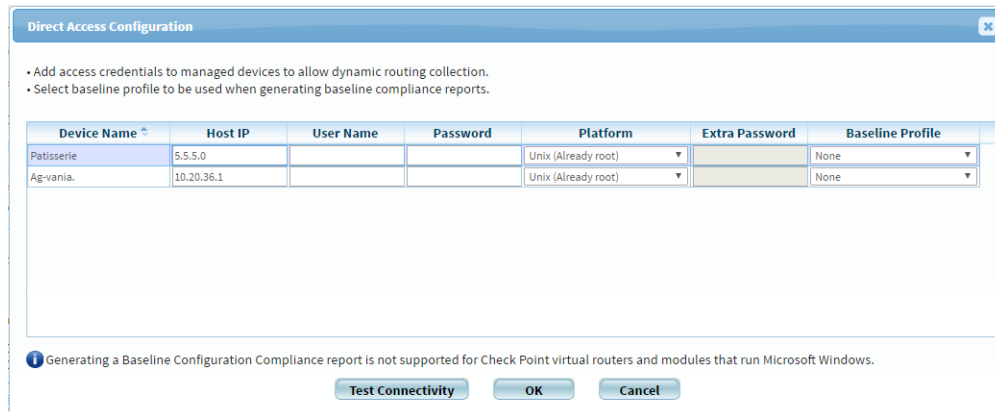
A message informs you whether AFA connected to the log server successfully.

- f. Click **OK**.

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.



**Direct Access Configuration**

- 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.

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.

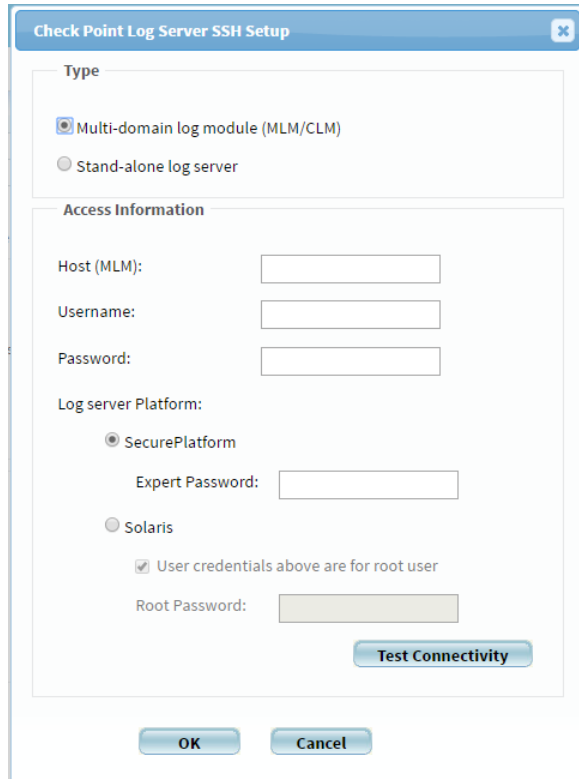
**Tip:** This enables AFA to detect certain policy optimization information, such as unused rules.

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**.



The image shows a dialog box titled "Check Point Log Server SSH Setup". It has 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 button labeled "Test Connectivity". At the bottom of the dialog box are two buttons: "OK" and "Cancel".

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**.

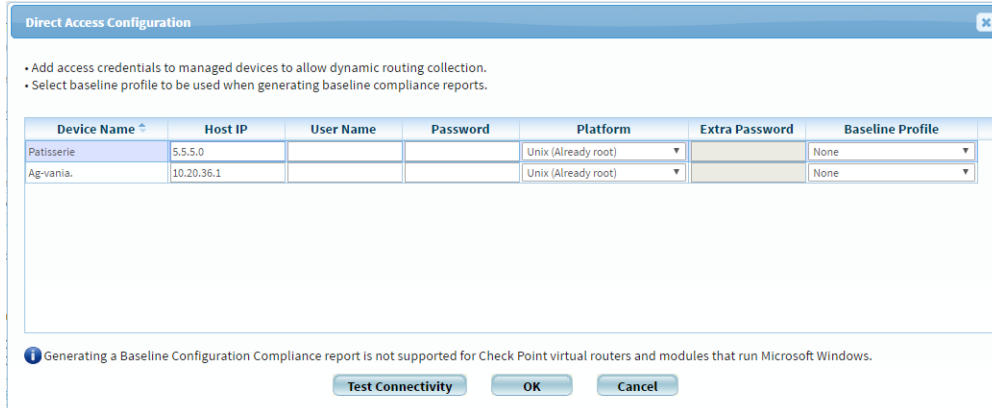
A message informs you whether AFA connected to the log server successfully.

- 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.



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

- 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

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 Provider-1. 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.

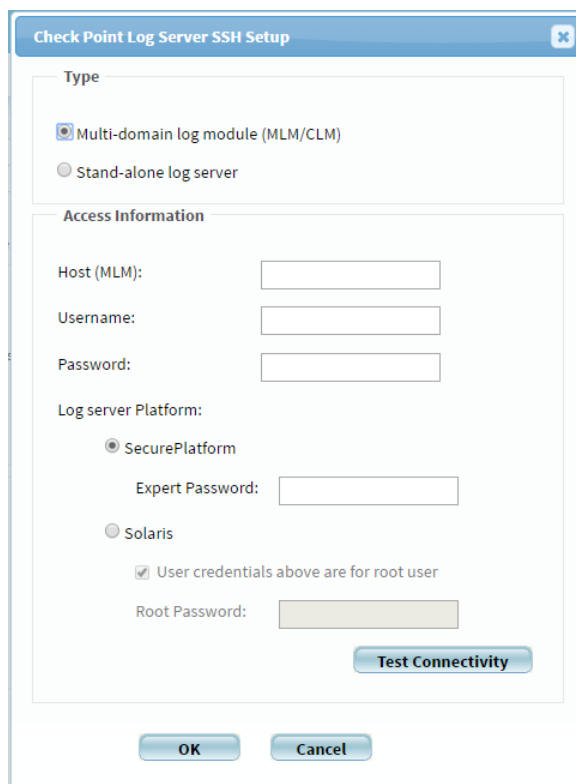
**Tip:** This enables AFA to detect certain policy optimization information, such as unused rules.

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**.



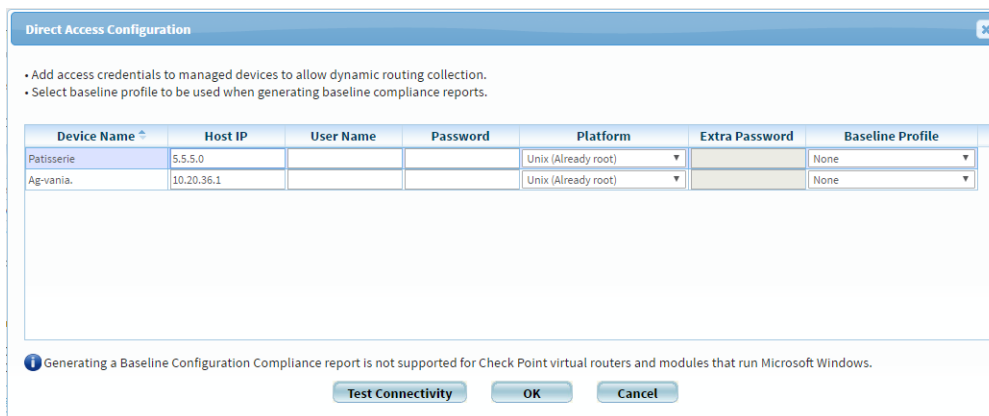
The image shows the 'Check Point Log Server SSH Setup' dialog box. It has a title bar with a close button. The dialog is divided into two main sections: 'Type' and 'Access Information'. In the 'Type' section, there are two radio buttons: 'Multi-domain log module (MLM/CLM)' (which is selected) and 'Stand-alone log server'. The 'Access Information' section contains several fields: 'Host (MLM):', 'Username:', and 'Password:', each with a text input box. Below these is a 'Log server Platform:' section with two radio buttons: 'SecurePlatform' (selected) and 'Solaris'. Under 'SecurePlatform', there is an 'Expert Password:' field. Below the 'Solaris' option, there is a checked checkbox labeled 'User credentials above are for root user' and a 'Root Password:' field. At the bottom right of the 'Access Information' section is a 'Test Connectivity' button. At the very 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.



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

- 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**

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

<b>Host</b>	Enter the host name or IP address of the device.
<b>R80 or higher</b>	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 <a href="#">Enable data collection via REST</a> ).

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

<b>Solaris / RedHat Linux</b>	<p>Choose this option to specify that the device is installed on a Solaris or RedHat Linux operating system.</p> <p>This field only appears if you selected <b>SSH</b> in the <b>Connect via</b> area.</p>
<b>User credentials above are for root user</b>	<p>Select this option to specify that the user name and password entered in the <b>User Name</b> and <b>Password</b> fields are the credentials for the Solaris root user.</p> <p>If you clear this option, you must complete the <b>Root Password</b> field.</p> <p>This field only appears if you selected <b>SSH</b> in the <b>Connect via</b> area.</p>
<b>Root Password</b>	<p>Type the root password for Solaris.</p> <p>This field only appears if you selected <b>SSH</b> in the <b>Connect via</b> area.</p>
<b>High Availability</b>	<p>Select this option to configure High Availability for CMAs.</p> <p><b>Important:</b> 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.</p> <p>This field only appears if you selected <b>OPSEC</b> in the <b>Connect via</b> area. It is not relevant for Check Point Provider-1.</p>
<b>Secondary Security Management (SmartCenter)</b>	<p>Type the secondary CMA.</p> <p>This field only appears if you selected <b>OPSEC</b> in the <b>Connect via</b> area. It is not relevant for Check Point Provider-1.</p>

### 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:

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

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

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

<b>Baseline Profile</b>	<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 <a href="#">Customizing Baseline Configuration Compliance Profiles</a> (see <a href="#">Customize baseline configuration profiles</a>).</p> <p>To disable Baseline Compliance Report generation for this device, select <b>None</b>.</p>
<b>Test Connectivity</b>	<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:

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

## 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 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](#).

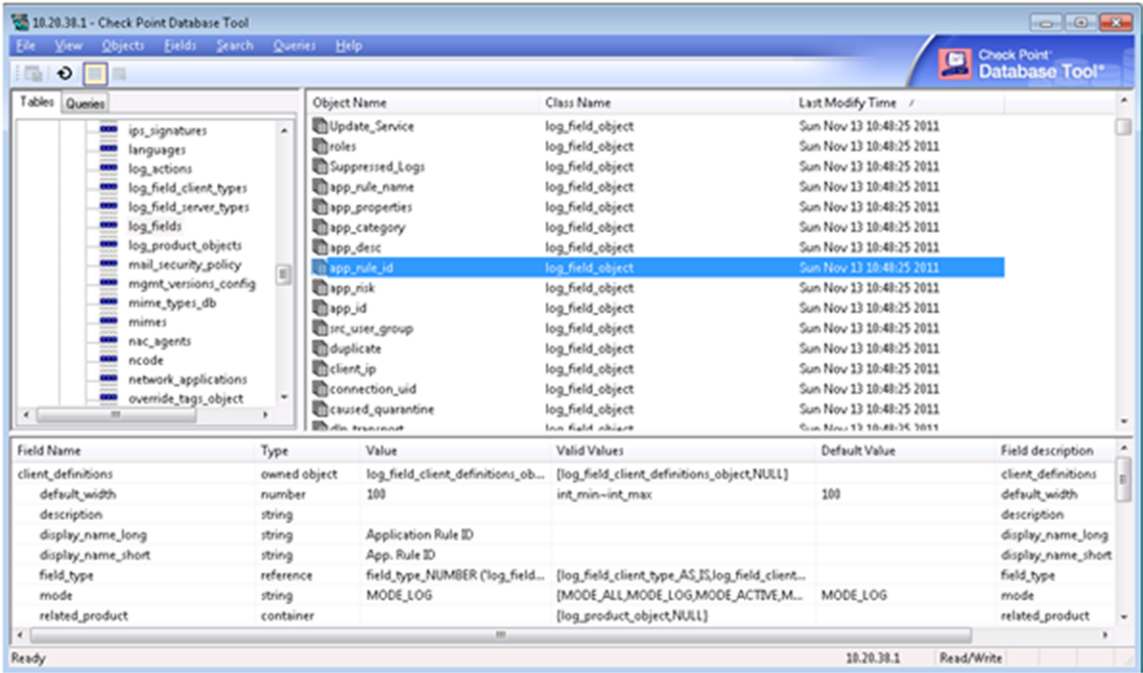
Do the following:

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

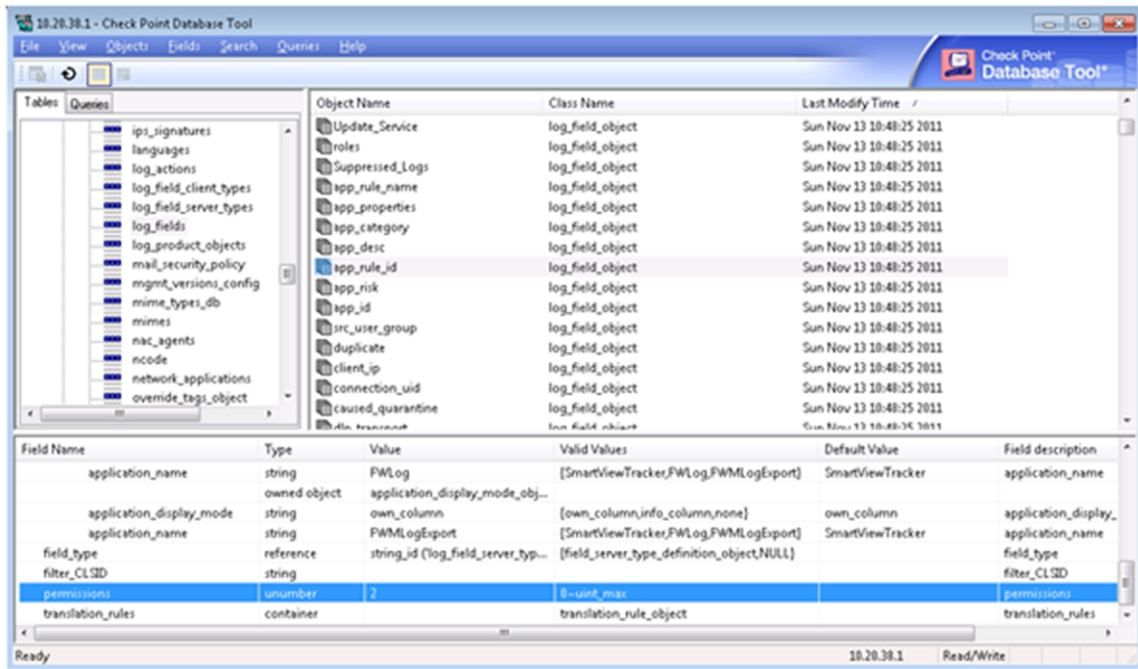
The management station is typically located at **C:\Program Files (x86)\CheckPoint\SmartConsole\RXX\PROGRAM** where **RXX** is the version number.

- 2. In the left pane, navigate to **Other > log\_fields**.
- 3. In the right pane, click on **app\_rule\_id**.

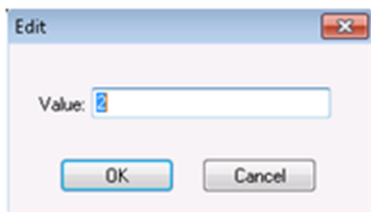
The bottom pane displays the fields that are displayed for **app\_rule\_id**.



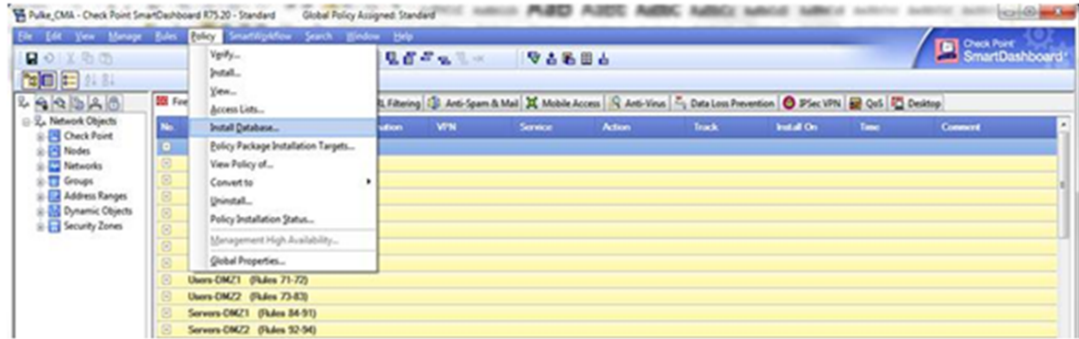
- 4. In the bottom pane, double-click on the **permissions** field.



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 - 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 PV-1 \(R80 and Higher\)](#)
  - [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.

**Retrieve a new OPSEC certificate**

After the certificate is ready, please fill the following and click "OK":

OPSEC Application Name:

One Time Password:

[How do I create a Check Point OPSEC certificate?](#)

▼ **Advanced**

CPMI Authorization Type:

CPMI Port:

LEA Authorization Type:

LEA Port:

**OK** **Cancel**

3. Complete the fields as follows:

<b>OPSEC Application Name</b>	Type the OPSEC application name, as specified in the OPSEC certificate. The default value is "AlgoSec".
<b>One Time Password</b>	Type the one-time password, as specified in the OPSEC certificate.
<b>Advanced</b>	Click to display advanced fields. The <b>CPMI Authorization Type</b> , <b>CPMI Port</b> , <b>LEA Authorization Type</b> , and <b>LEA Port</b> fields appear.
<b>CPMI Authorization Type</b>	Select the CPMI authorization type.
<b>CPMI Port</b>	Type the CPMI port number. The default value is 18190.
<b>LEA Authorization Type</b>	Select the LEA authorization type.
<b>LEA Port</b>	Type the LEA port number. The default value is 18184.

4. Click **OK** to retrieve the certificate from the Check Point SmartCenter, CMA or

Provider-1 server.

Once the certificate is installed, a confirmation window appears.

5. Click **OK**.

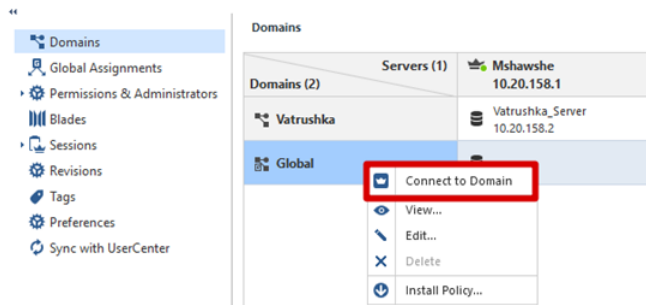
The **OPSEC Setup** area displays the certificate date and time of creation.

### Create a Check Point OPSEC Certificate for a PV-1 (R80 and Higher)

In order for AFA to collect data from a CheckPoint Provider 1 (PV-1) 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:

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

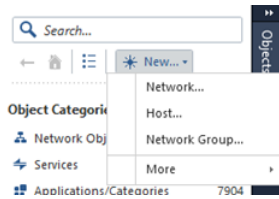


3. Create a network object for the host that will run AFA

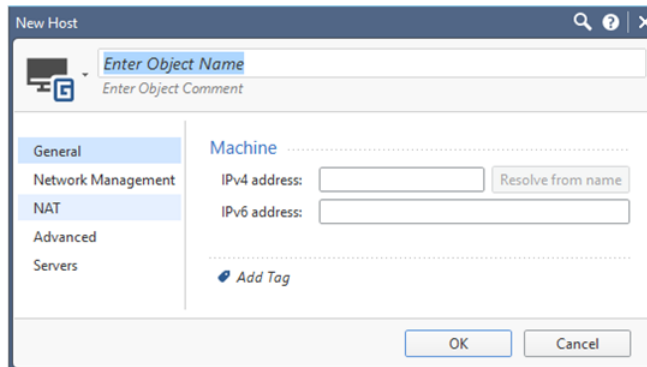
**Note:** If a network object for the host is already defined, you can skip this step.

Do the following:

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



The **New Host** window appears.

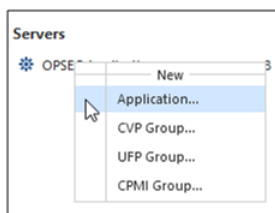


- b. Complete the **Object Name** and **IPv4 Address** fields with the name and address of the host that will run AFA.
  - c. Click **OK**.
4. Create an OPSEC application object for this network object.

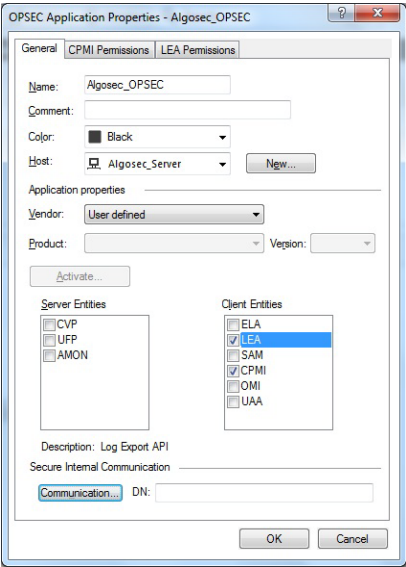
**Note:** If an OPSEC application object is already defined, you can skip this step.

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:

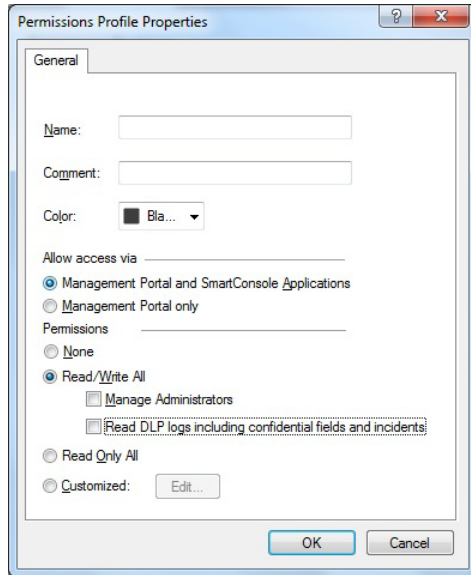
<b>Name</b>	Enter the OPSEC application name. <b>Note:</b> Record the name you entered here. You'll need to specify this name in AFA when you retrieve the certificate.
<b>Host</b>	Select the host to run AFA.
<b>Object Entities</b>	Select the <b>LEA</b> and <b>CPMI</b> items.

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.

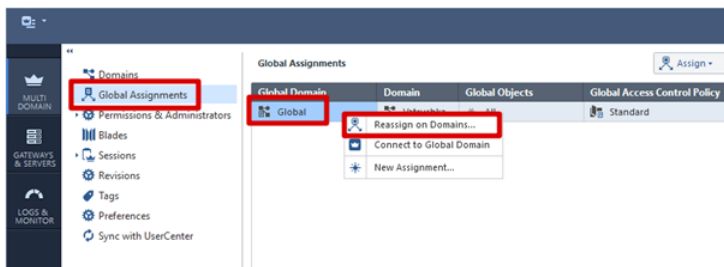
**Note:** Record the password you entered here. You'll need to specify this name in AFA when you retrieve the certificate.

- 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.

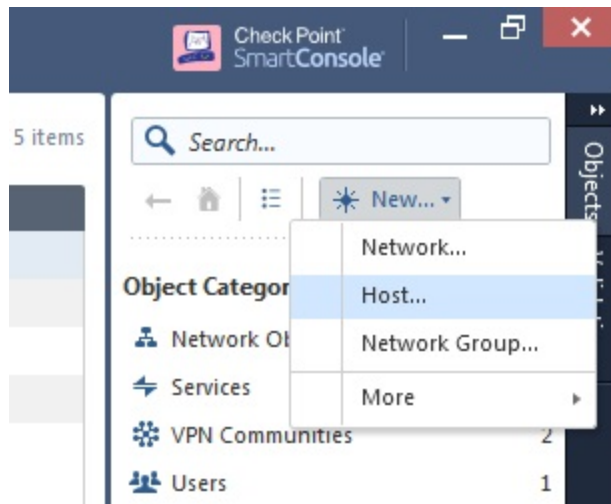
**Do the following:**

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

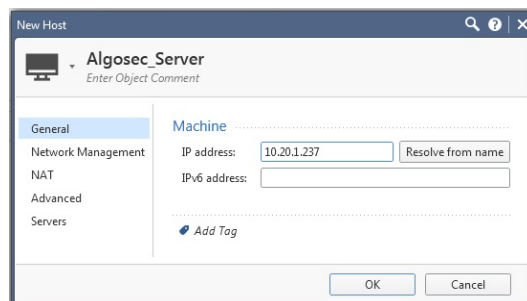
**Note:** If a network object for the host is already defined, you can skip this step.

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**.

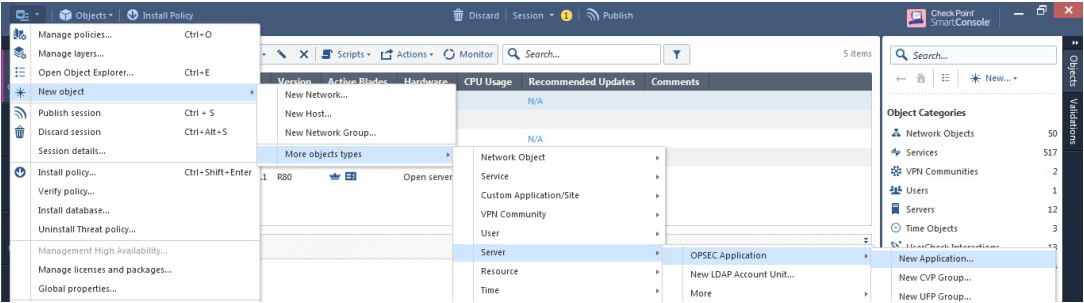


3. Create an OPSEC application object for this network object.

**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:

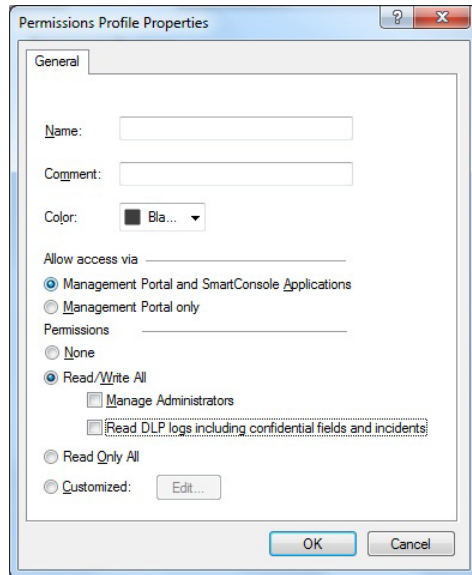
<b>Name</b>	Enter the OPSEC application name. <b>Note:</b> Record the name you entered here. You'll need to specify this name in AFA when you retrieve the certificate.
<b>Host</b>	Select the host to run AFA.
<b>Object Entities</b>	Select the <b>LEA</b> and <b>CPMI</b> items.

- 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 Provider-1 server, using Check Point's **Global SmartDashboard** utility.

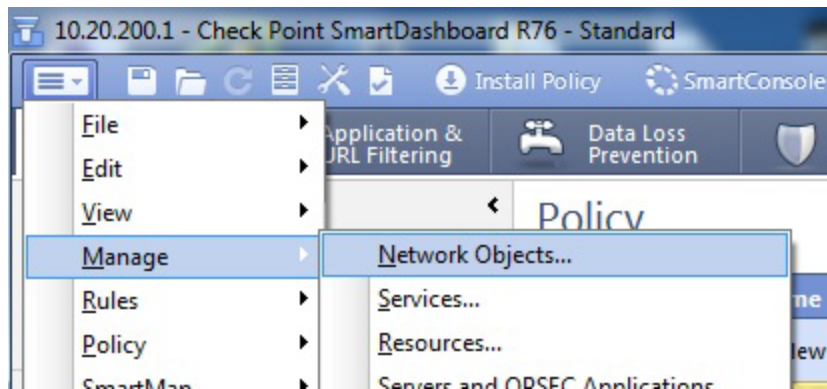
Do the following:

1. Create a network object for the host.

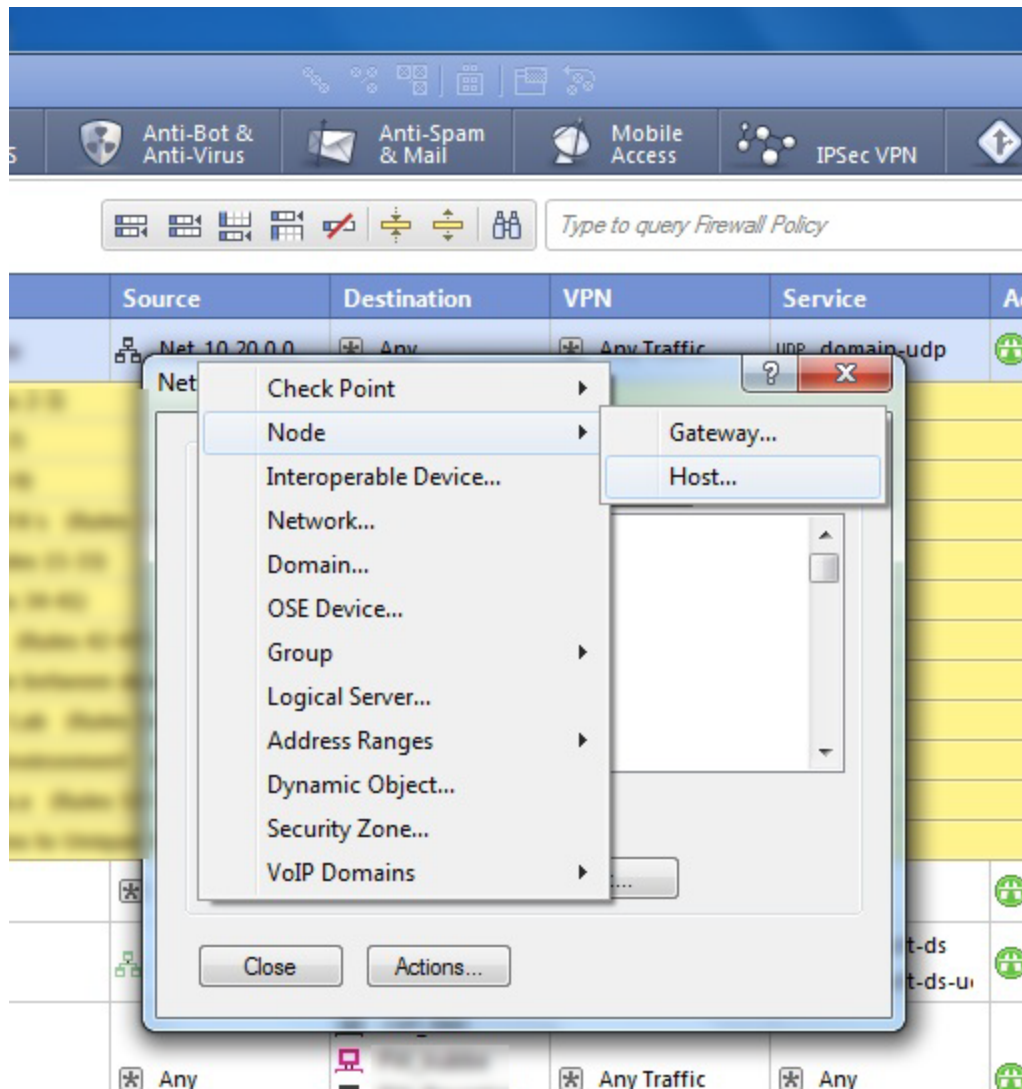
**Note:** If a network object for the host running AFA is already defined, you can skip this step.

Do the following:

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



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

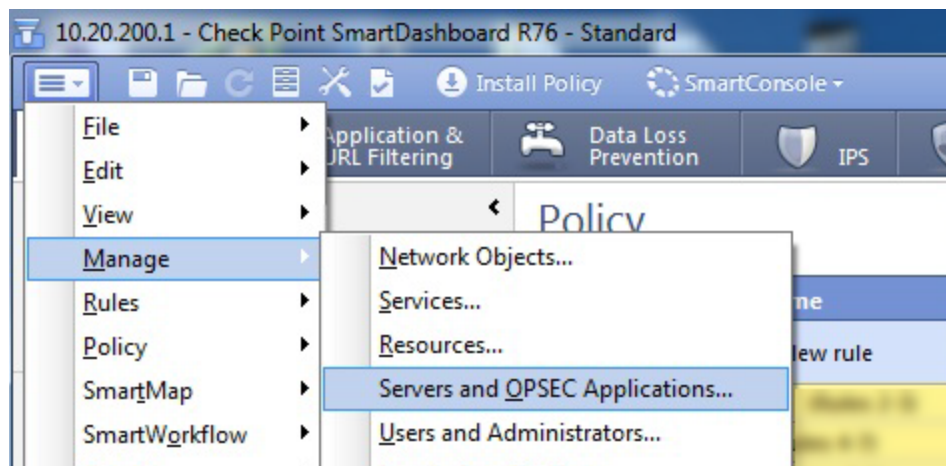


- c. In the **Host Node** dialog, enter the **Name** and **IP address** of the host that will run AFA, and then click **OK**.
2. Create an OPSEC application object for this network object.

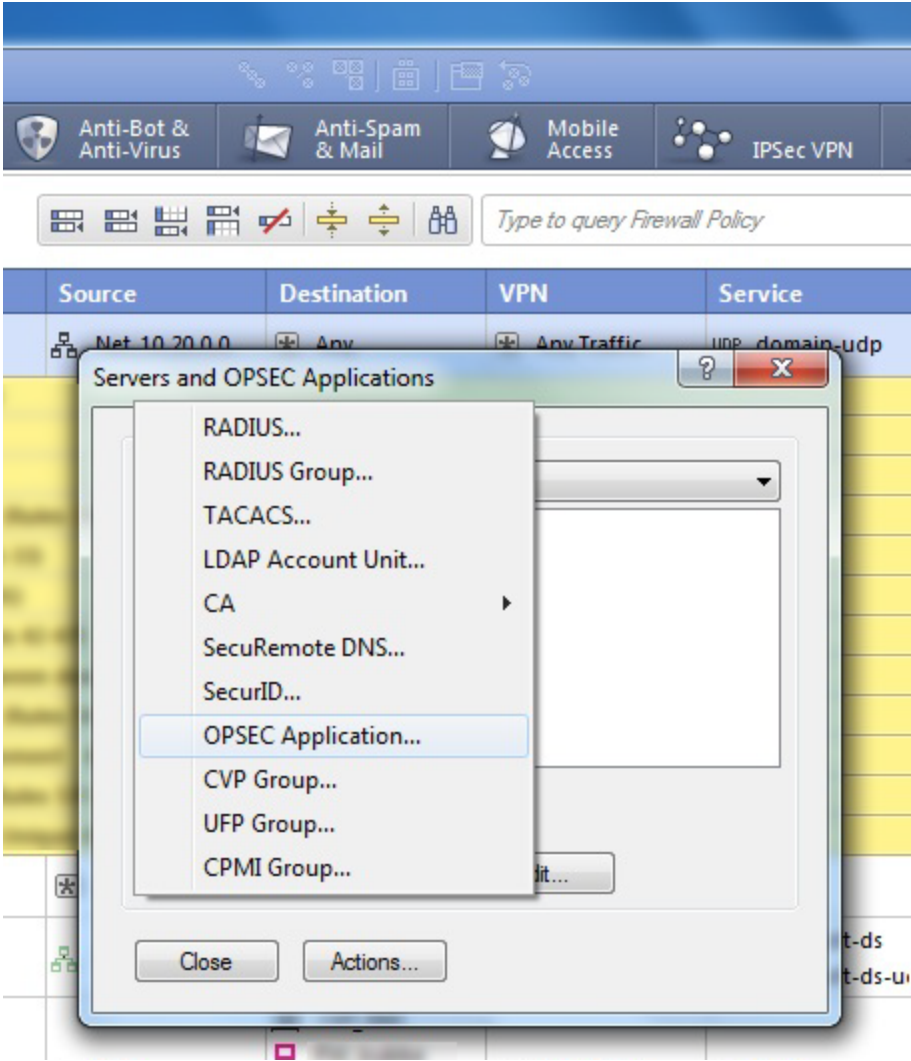
**Note:** If an OPSEC application object is already defined, you can skip this step.

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:

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

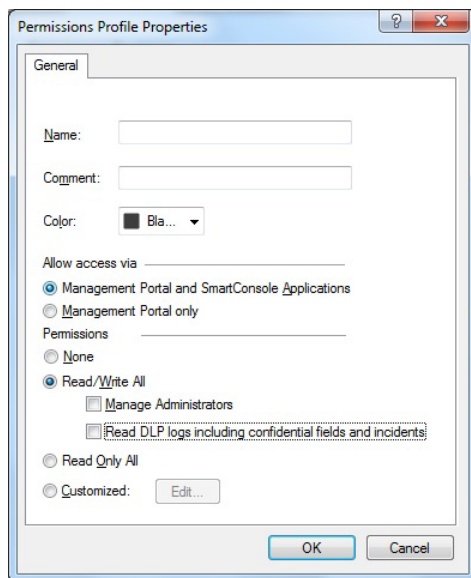
d. In the **CPI Permissions** tab, select **Permissions Profile**, and then do one of

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.

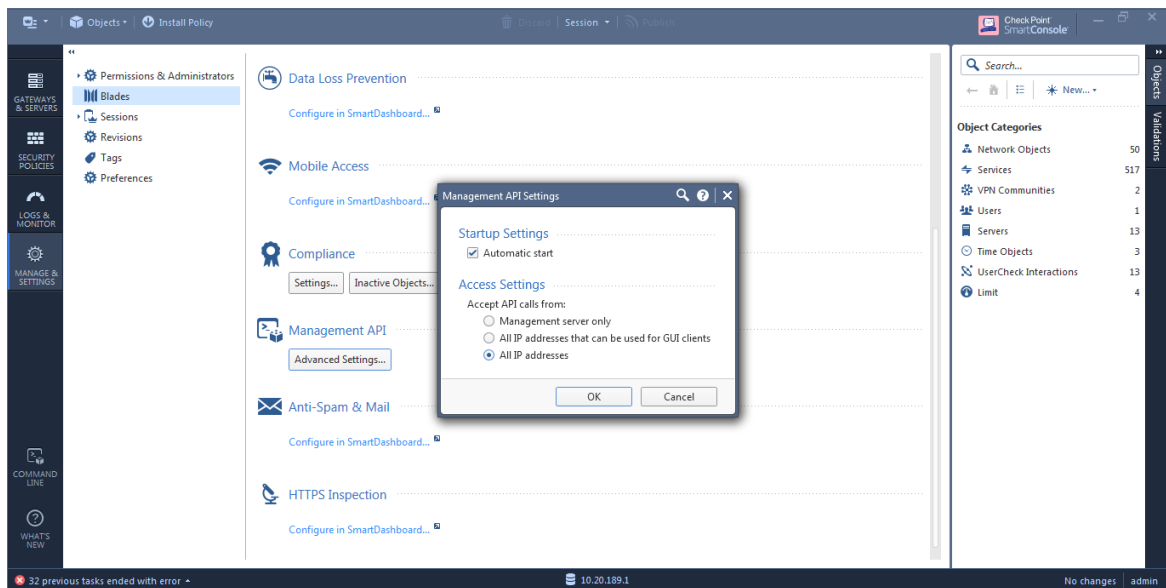
**Note:** For versions R80 and above, AFA collects data via REST, along with either SSH or OPSEC. In addition to enabling REST, you must also enable SSH or OPSEC as needed.

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.

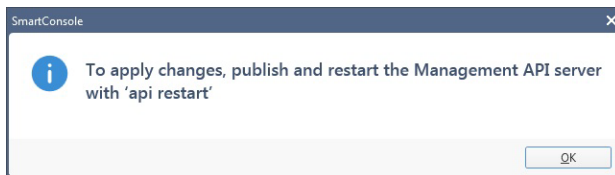


3. To automatically start the API server at Security Management Server startup, select the **Automatic Start** check box.
4. Select which IP addresses from which the API server accepts requests:

<b>All IP addresses that can be used for GUI clients</b>	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.
<b>All IP addresses</b>	The API server will accept scripts and web-service requests from any device

- Click **OK**.

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



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

#### Cisco CSM fields

In this field...	Do this...
<b>Access Information</b>	
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.
<b>Geographic Distribution</b>	
Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p>This field is relevant when a Geographic Distribution architecture is configured.</p>
<b>Baseline Configuration Compliance</b>	

In this field...	Do this...
Baseline Configuration Compliance Profile	<p>Select the baseline compliance profile to use, in order to enable generation of Baseline Compliance Reports for this device.</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 <a href="#">Customize baseline configuration profiles</a></p> <p>Select <b>None</b> to disable Baseline Compliance Report generation for this device.</p>
Route Collection	<p>Specify how AFA should acquire the device's routing information:</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA will automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA will take the device's routing information from a static file you provide. For more information, see <a href="#">Specify routing data manually</a>.</li> </ul>
Rules view	<p>Specify how rules should be displayed in device reports:</p> <ul style="list-style-type: none"> <li>• <b>ASDM:</b> Display rules in the Cisco Adaptive Security Device Manager (ASDM) graphical interface.</li> <li>• <b>CLI:</b> Display rules in command line format.</li> </ul> <p>The default value is <b>ADSM</b>.</p> <p><b>Note:</b> Intelligent Policy Tuner and the "Unused objects within rules" list are available only with ADSM.</p>
Log Collection and Monitoring	

In this field...	Do this...
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"> <li>• <b>Hit-counters:</b> Only use hit-counter data. The <b>Change History</b> report page will be based on "last modified" timestamps, and Intelligent Policy Tuner is disabled.</li> <li>• <b>Standard:</b> Use hit-counter data for rule usage, and Syslog data for the <b>Change History</b> report page. Intelligent Policy Tuner is disabled.</li> <li>• <b>Extensive:</b> Combine data from both hit-counters and Syslog. Intelligent Policy Tuner is enabled.</li> </ul> <p>The default value is <b>Extensive</b>.</p> <p><b>Note:</b> The <b>Extensive</b> method is only available when the <b>ADSM</b> is selected in the <b>Rules view</b> area.</p>
Syslog-ng server	<p>If you selected <b>Standard</b> or <b>Extensive</b> in the <b>Log collection method</b> field, you must specify the syslog-ng server. See <a href="#">Specify a Syslog-ng server</a>.</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><b>Note:</b> 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 <a href="#">Add additional device identifiers for sub-systems</a>.</p>
Log collection frequency (minutes)	<p>Type the interval of time in minutes, at which AFA should collect logs for the device.</p>

In this field...	Do this...
<b>Options</b>	
Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a> .
Set user permissions	Select this option to set user permissions for this device.

### Specify a Syslog-ng server

Do one of the following:

<b>Select a syslog-ng server</b>	<p>Select the syslog-ng server from the list of those already defined in AFA.</p> <p>Select <b>localhost</b> to use the built-in syslog-ng server. No credentials are required for this server.</p> <p><b>Note:</b> The <b>localhost</b> 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.</p>
----------------------------------	--

<b>Add a new syslog-ng server</b>	<p>To add a new syslog-ng server, such as if you had one existing before installing AFA, do the following:</p> <ol style="list-style-type: none"> <li>1. Click <b>New</b> and enter the following details: <ul style="list-style-type: none"> <li>• <b>Syslog-ng host.</b> The syslog-ng server's host name or IP address.</li> <li>• <b>User Name / SSH User Name.</b> The user name for connecting to the syslog-ng server.</li> </ul> <div data-bbox="613 562 1382 720" style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p><b>Note:</b> 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.</p> </div> <ul style="list-style-type: none"> <li>• <b>Password / SSH Password.</b> The password for connecting to the syslog-ng server.</li> </ul> </li> <li>2. Click <b>Test Connectivity</b> to test connectivity to the defined syslog-ng server.</li> </ol> <p>A message informs you whether AFA connected to the syslog-ng server successfully, and the new syslog-ng server is automatically selected in the <b>Syslog-ng server</b> drop-down list.</p> <p><b>Tip:</b> Save the device configuration to make this syslog-ng server available for other devices as well.</p>
<b>Edit an existing device</b>	<p>To edit an existing syslog-ng server, do the following:</p> <ol style="list-style-type: none"> <li>1. Select the syslog-ng server that you want to edit, and click <b>Edit</b>.</li> <li>2. Edit the properties as needed, and click <b>OK</b>.</li> <li>3. Click <b>Test Connectivity</b> to test connectivity to the defined syslog-ng server.</li> </ol> <p>A message informs you whether AFA connected to the syslog-ng server successfully.</p>

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 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.

### Cisco IOS Router Properties Fields

In this field...	Do this...
<b>Access Information</b>	
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. For Cisco IOS devices enabled for CyberArk, the <b>Password</b> and <b>Enable User Password</b> must be the same.
Enable User Name	Type the enable user name to use. Completing this field is mandatory.

In this field...	Do this...
Enable User Password	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>Type the enable user password to use.</li> <li>To specify an empty enable password, type "AlgoSec_no_passwd".</li> <li>If you do not want AFA to enter the enable mode, type "noenable".</li> </ul> <p>For Cisco IOS devices enabled for CyberArk, the <b>Password</b> and <b>Enable User Password</b> must be the same.</p> <p>Completing this field is mandatory.</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 AlgoSec server.</p> <p><b>Note:</b> This option only appears when CyberArk is configured in AFA. See Configuring CyberArk Integration (see <a href="#">Integrate AFA and CyberArk</a>).</p>
Platform (Policy ID)	<p>Type the Platform for this device which will be authenticated via CyberArk.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
Safe	<p>Type the safe for this device which will be authenticated via CyberArk.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
Folder	<p>Type the folder for this device which will be authenticated via CyberArk.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>

In this field...	Do this...
Object	Type this device's CyberArk Object.  This field is only relevant when retrieving credentials for this device from a CyberArk vault.
Geographic Distribution	
Device managed by	Select the remote agent that should perform data collection for the device.  To specify that the device is managed locally, select <b>Central Manager</b> .  This field is relevant when a Geographic Distribution architecture is configured.
Baseline Configuration Compliance	
Baseline Configuration Compliance Profile	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 <a href="#">Customize baseline configuration profiles</a> ).  To disable Baseline Compliance Report generation for this device, select <b>None</b> .  <b>Note:</b> If this router is divided into VRF modules, Baseline Compliance Reports will only be generated for the root/default VRF.
Advanced	

In this field...	Do this...
Include risk analysis and policy optimization	<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><b>Note:</b> Selecting this option will increase the analysis time for this router significantly and might result in performance degradation.</p>
Automatically add/remove VRF instances upon detection (Applies for all Cisco Routers)	<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	<p>Choose the method of data transmission: SSH or Telnet.</p> <p><b>Note:</b> Telnet is the less secure method.</p>
Custom Port	<p>To specify a custom port, select this option and type the port.</p> <p>This option is only relevant when SSH is selected.</p>
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>

In this field...	Do this...
<b>Route Collection</b>	<p>Specify how AFA should acquire the device's routing information:</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA will automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA will take the device's routing information from a static file you provide. For more information, see <a href="#">Manually Specifying Routing Information</a> (see <a href="#">Specify routing data manually</a>).</li> </ul>
<b>ActiveChange</b>	
Enable ActiveChange for all supported Cisco IOS routers	<p>Select this option to enable FireFlow to generate CLI recommendations and push them to the device.</p> <p>Checking this box will enable ActiveChange for all the supported Cisco firewalls, Cisco IOS routers, and Juniper SRX firewalls (not only for this device).</p>
<b>Options</b>	
Real-time change monitoring	Select this option to enable real-time change monitoring. For details, see <a href="#">Configure real-time monitoring</a> .
Set user permissions	Select this option to set user permissions for this device.

4. If CyberArk credential management is enabled, enter the following details:

☒ Retrieve credentials from CyberArk Vault (?)

Platform (PolicyID)

Safe

Folder

Object

For more details, see [Integrate AFA and CyberArk](#).

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

appears.

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

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.

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.

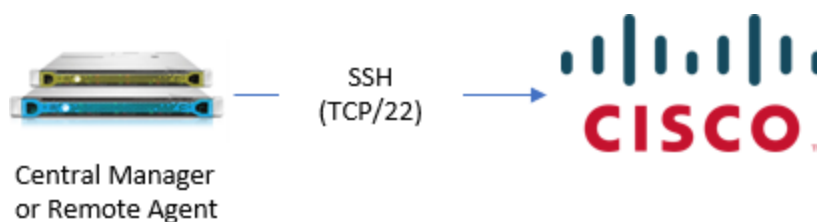
## Cisco Nexus routers in AFA

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

<b>Host</b>	Enter the host name or IP address of the device.
-------------	--

<b>User Name</b>	Enter the user name to use for SSH access to the device.
<b>Password</b>	Enter the password to use for SSH access to the device.

### CyberArk fields

The following options only appear when CyberArk is configured in AFA. For details, see [Integrate AFA and CyberArk](#).

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

### 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

<b>Include risk analysis and policy optimization</b>	<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><b>Note:</b> Selecting this option will increase the analysis time for this router significantly and might result in performance degradation.</p>
<b>Automatically add/remove VRF instances upon detection (Applies for all Cisco Routers)</b>	<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:

<b>Custom Port</b>	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
<b>Number of allowed encryption keys</b>	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 <b>1</b> , the connection to the node will fail, resulting in a failed analysis.

### Options

<b>Real-time change monitoring</b>	Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a> .
<b>Set user permissions</b>	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.

## Add a Cisco ASA firewall

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

Do the following:

1. Create an ASA user for AFA data collection, with read-only permissions, or read-write permissions if you're using ActiveChange. This user must also be allowed to run the commands required for data collection.

### Define a limited-privilege Cisco user for data collection

AlgoSec recommends creating a new user specifically for the purpose of AFA data collection. The following procedure describes how to create a Cisco ASA user with only the privileges required by AFA. You can then provide this user (and its credentials) when defining the device in AFA.

#### Note:

- This procedure changes the global permission levels for these permissions, and may affect other users defined with limited privilege levels.
- A limited-privilege user does not provide enough permissions to use ActiveChange. Devices using ActiveChange must be defined with a user with write permissions.

Do the following:

1. Log in to the Cisco device as a privileged user.
2. Enter **enable** mode.
3. Run the following commands:

All scenarios	<b>configure terminal</b> <b>username &lt;username&gt; password &lt;password&gt; privilege 5</b> <b>privilege show level 5 command version</b> <b>privilege show level 5 command mode</b> <b>privilege show level 5 command access-list</b> <b>privilege show level 5 command running-config</b> <b>privilege show level 5 command route</b> <b>privilege configure level 5 command pager</b>
ASA devices with an IPV6 ACL	<b>privilege show level 5 command ipv6</b>
ASA devices with security group tags	<b>privilege configure level 5 command cts sgt-map</b>
ASA devices with security context	<b>privilege show level 5 command context</b>

The new user is created. This user only has privileges to run the required show commands (all of which are read-only). with the specified permissions.

For more details, see [Required device permissions](#).

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

## Cisco ASA Properties Fields

In this field...	Do this...
<b>Access Information</b>	
Host	Type the host name or IP address of the device.
User Name	<p>Type the user name to use for SSH access to the device.</p> <p>For details regarding defining a Cisco user with the minimum permissions required for AFA data collections, see <a href="#">Defining a Limited-Privilege Cisco User for Data Collection</a> (see <a href="#">Define a limited-privilege Cisco user for data collection</a>).</p> <p><b>Note:</b> In order to be able to automatically implement changes on the device with ActiveChange, read-write permissions are required.</p> <p><b>Note:</b> AFA partially supports user awareness for Cisco ASA devices. The network user appears as a field for each rule in the <b>Policy</b> tab but is not used in traffic simulation queries.</p>
Password	<p>Type the password to use for SSH access to the device.</p> <p>For Cisco ASA devices enabled for CyberArk, the <b>Password</b> and <b>Enable User Password</b> must be the same.</p>
Enable User Password	<p>Enter the enable user password to use:</p> <ul style="list-style-type: none"> <li>• <b>noenable</b>. Skip running the <b>enable</b> command.</li> <li>• <b>Algosec_no_passwd</b>. The enable password is empty.</li> <li>• Leave the field empty. AFA will issue a <b>login</b> command instead of the <b>enable</b> command, using the same password provided for the SSH connection.</li> </ul> <p>For Cisco ASA devices enabled for CyberArk, the <b>Password</b> and <b>Enable User Password</b> must be the same.</p>

In this field...	Do this...
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><b>Note:</b> This option only appears when CyberArk is configured in AFA. See Configuring CyberArk Integration (see <a href="#">Integrate AFA and CyberArk</a>).</p>
Platform (Policy ID)	<p>Type the Platform for this device which will be authenticated via CyberArk.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
Safe	<p>Type the safe for this device which will be authenticated via CyberArk.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
Folder	<p>Type the folder for this device which will be authenticated via CyberArk.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
Object	<p>Type this device's CyberArk Object.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
<b>Geographic Distribution</b>	
Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p>This field is relevant when a Geographic Distribution architecture is configured. See <b>Using a Distributed System</b>.</p>

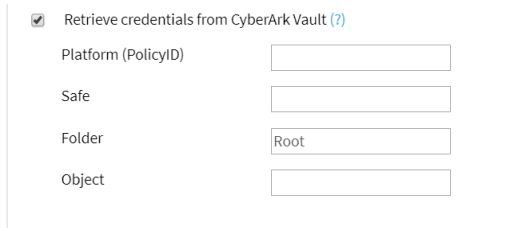
In this field...	Do this...
<b>Baseline Configuration Compliance</b>	
Baseline Configuration Compliance Profile	<p>To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.</p> <p>The drop-down list includes all baseline compliance profiles in the system. For more information on baseline compliance profiles and instructions for adding new baseline compliance profiles, see Customizing Baseline Configuration Compliance Profiles (see <a href="#">Customize baseline configuration profiles</a>).</p> <p>To disable Baseline Compliance Report generation for this device, select <b>None</b>.</p>
<b>Remote Management Capabilities</b>	<p>Choose the method of data transmission.</p> <p><b>Note:</b> Telnet is the least secure method.</p>
Custom Port	<p>To specify a custom port, select this option and type the port.</p> <p>This option is only relevant when SSH is selected.</p>
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>

In this field...	Do this...
<b>Route Collection</b>	<p>Specify how AFA should acquire the device's routing information:</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA will automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA will take the device's routing information from a static file you provide. For more information, see Manually Specifying Routing Information (see <a href="#">Specify routing data manually</a>).</li> </ul>
<b>Rules view</b>	<p>Specify how rules should be displayed in device reports:</p> <ul style="list-style-type: none"> <li>• <b>ASDM:</b> Display rules in the Cisco Adaptive Security Device Manager (ASDM) graphical interface.</li> <li>• <b>CLI:</b> Display rules in command line format.</li> </ul> <p>The default value is <b>CLI</b>.</p> <p><b>Note:</b> Intelligent Policy Tuner and the "Unused objects within rules" list are available only with ASDM.</p>
<b>Log Collection and Monitoring</b>	

In this field...	Do this...
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"> <li>• <b>Hit-counters:</b> Only use hit-counter data. The <b>Change History</b> report page will be based on "last modified" timestamps, and Intelligent Policy Tuner is disabled.</li> <li>• <b>Standard:</b> Use hit-counter data for rule usage, and Syslog data for the <b>Change History</b> report page. Intelligent Policy Tuner is disabled.</li> <li>• <b>Extensive:</b> Combine data from both hit-counters and Syslog. Intelligent Policy Tuner is enabled.</li> </ul> <p>The default value is <b>Extensive</b>.</p> <p><b>Note:</b> The <b>Extensive</b> method is only available when <b>ADSM</b> is selected in the <b>Rules view</b> area.</p> <p><b>Note:</b> Intelligent Policy Tuner analysis is supported for Cisco ASA version 7.1. To use this feature, you must configure log collection when defining the device in AFA. For the device to send the correct log messages (type 106100), the device's ACLs must contain the keyword "log".</p>
Syslog-ng server	<p>If you selected <b>Standard</b> or <b>Extensive</b> in the <b>Log collection method</b> field, you must specify the syslog-ng server. See Specifying a Syslog-ng server (see <a href="#">Specify a Syslog-ng server</a>).</p>

In this field...	Do this...
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><b>Note:</b> 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 Adding Additional Device Identifiers for Sub-Systems (see <a href="#">Add additional device identifiers for sub-systems</a>).</p>
Log collection frequency (minutes)	Type the interval of time in minutes, at which AFA should collect logs for the device.
<b>ActiveChange</b>	
Enable ActiveChange for all supported Cisco firewalls	<p>Select this option to enable FireFlow to generate CLI recommendations and push them to the device.</p> <p>Checking this box will enable ActiveChange for all the supported Cisco firewalls, Cisco IOS routers, and Juniper SRX firewalls (not only for this device).</p>
<b>Options</b>	
Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a> .
Set user permissions	Select this option to set user permissions for this device.

5. If CyberArk credential management is enabled, enter the following details:



☒ Retrieve credentials from CyberArk Vault (?)

Platform (PolicyID)

Safe

Folder

Object

For more details, see [Integrate AFA and CyberArk](#).

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

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

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.

## Add a Cisco Application Centric Infrastructure (ACI)

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:

<b>Access Information</b>	<p>Enter the host name or IP address, user name, and password used to access the device.</p> <p><b>Tip:</b> Typically, your APIC cluster has three nodes. In the <b>Host</b> field, specify the host name or IP address of only one of the APIC nodes.</p> <p>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.</p>
<b>Geographic Distribution</b>	<p>Select a remote agent to perform data collection for the device, if relevant.</p> <p>To configure the device to be managed locally, select <b>Central Manager</b>.</p>
<b>Route Collection</b>	<p>Determine how AFA acquires the device's routing information. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA automatically generates the device's routing upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA takes the device's routing information from a static file you provide. For details, see <a href="#">Specify routing data manually</a>.</li> </ul>
<b>Options</b>	<p>Select either of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Real-time change monitoring.</b> Enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a>.</li> <li>• <b>Set user permissions.</b> Set user permissions for this device.</li> </ul>

4. 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](#).
- **vzAny objects** are shown with the following syntax: **<VRF\_name>/vzAny**. AFA updates the contents of these objects upon change monitoring and analysis.

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.

### EPG identification

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.

### 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: **fip\_additional\_devices\_set\_support = yes**.
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.

## 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 fields as needed.

## Cisco FirePower fields

In this field...	Do this...
<b>Access Information</b>	
Host	Type the host name or IP address of the device.
User Name	<p>Type the user name to use for SSH access to the device.</p> <p><b>Note:</b> You must create a user specifically for AFA because the device requires a different user for each connection. For more information, see <a href="#">Device User Permission Requirements</a> (see <a href="#">Required device permissions</a>).</p> <p><b>Note:</b> AFA does not support user or network application awareness for Cisco FirePower. The network application appears as a field for each rule in the <b>Policy</b> tab, but is not used in traffic simulation queries.</p>
Password	Type the password to use for SSH access to the device.
<b>Geographic Distribution</b>	
Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p>This field is relevant when a Geographic Distribution architecture is configured.</p>
<b>ActiveChange</b>	
Enable ActiveChange	Select this option to allow FireFlow to automatically implement changes on the device.
<b>Options</b>	

- Click **Next** to continue on to the **FirePower - Step2/2** page. This page lists the FTDs that are managed by the FirePower.

For example:

The screenshot shows the 'Administration' section of the Firewall Analyzer interface. A progress bar at the top indicates the current step is 'DEVICES SETUP'. Below the progress bar, the text reads 'Configure the settings needed to collect the device policies'. The main heading is 'Firepower - Step 2/2'. A table with the header 'Host Name' contains three rows, each with a checked checkbox and an IP address: 10.20.1.78, 10.20.1.79, and 10.20.1.16. Below the table, the section 'Direct access to managed devices' is shown, with the instruction 'Configure direct access to the managed devices in order to:' and a 'Configure' button.

	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

**Direct access to managed devices**

Configure direct access to the managed devices in order to:

[Configure](#)

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** for each FTD.

**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. To test connectivity to the FTD, click **Test Connectivity**.
8. 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.

## Add F5 devices

This topic describes how to add F5 devices to AFA.

For full AFA support, and FireFlow support for devices that do not use AFM, add an **F5 BIG-IP LTM Only** device. If your device uses AFM and you do not need FireFlow support, add an **F5 BIG-IP LTM and AFM** device. For more details, see [Which F5 Device Type Should I Choose ASMS 2018.2 and Above](#) on [AlgoPedia](#).

### Add an F5 BIG-IP LTM Only

This procedure describes how to add an F5 BIG-IP LTM only device to AFA, and should be used when you want to use FireFlow with devices that don't use AFM.

Do the following:

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

#### F5 BIG-IP LTM Only fields

In this field...	Do this...
<b>Access Information</b>	

In this field...	Do this...
Type	F5 BIG-IP LTM Only This field is read-only.
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. For information on the requirements for this use, see Device User Permission Requirements (see <a href="#">Required device permissions</a> ).
Password	Type the password to use for SSH access to the device.
<b>Geographic Distribution</b>	
Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p><b>Note:</b> This field is relevant when a Geographic Distribution architecture is configured. See Using a Distributed System.</p>
<b>Baseline Configuration Compliance</b>	

In this field...	Do this...
Baseline Configuration Profile	<p>To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.</p> <ul style="list-style-type: none"> <li>• <b>F5 BigIP.</b> Select the baseline compliance profile 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 <a href="#">Customize baseline configuration profiles</a>).</li> <li>• <b>None.</b> To disable Baseline Compliance Report generation for this device.</li> </ul>
Route Collection	
Routing Information Collection Method	<p>Specify how AFA should acquire the device's routing information:</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA will automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA will take the device's routing information from a static file you provide. For more information, see Manually Specifying Routing Information (see <a href="#">Specify routing data manually</a>).</li> </ul>
Remote Management Capabilities	
SSH	<p>The connection type.</p> <p><b>Note:</b> SSH is required for baseline configuration compliance purposes. All the other functionality is delivered by collecting data from the F5 BIG-IP LTM Only device using REST.</p>

In this field...	Do this...
Custom Port	<p>The port to use for the SSH connection.</p> <p>The default value is <b>22</b>.</p> <p>To use a port other than the default port, select the <b>Custom Port</b> check box and type the port number.</p>
Number of allowed encryption keys	<p>The permitted number of different RSA keys AFA can receive from the device's IP address.</p> <p><b>Note:</b> Different RSA keys might be sent from the same IP address in cases of cluster fail-over, device operating system upgrades. and so on.</p> <p>1 2</p> <ul style="list-style-type: none"> <li>• <b>unlimited</b> (Default)</li> </ul>
Log Collection and Monitoring	
Log collection method	<p>Specify the log collection method that AFA should use when collecting audit logs for the F5 BIG-IP LTM Only device, by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Extensive:</b> Not applicable. Intelligent Policy Tuner (IPT) is not available for F5 devices.</li> <li>• <b>Standard:</b> Use Syslog data for the Change History report page. IPT is disabled.</li> </ul> <p><b>None</b></p> <p>The default value is <b>Extensive</b>.</p> <p><b>Note:</b> Selecting <b>None</b> disables the following fields: <b>Syslog-ng server</b>, <b>Additional firewall identifiers</b>, and <b>Log collection frequency (minutes)</b>.</p>
Syslog-ng server	<p>(If enabled) Specify the syslog-ng server. See Specifying a Syslog-ng server (see <a href="#">Specify a Syslog-ng server</a>).</p>

In this field...	Do this...
Additional firewall identifiers	<p>(If enabled) 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>
Log collection frequency (minutes)	<p>(If enabled) Type the interval of time in minutes, at which AFA should collect logs for the device.</p> <p>The default value is <b>60</b>.</p>
<b>Options</b>	
Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes. For more details, see <a href="#">Configure real-time monitoring</a>,</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.

## Add an F5 BIG-IP LTM and AFM

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.

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**.

#### F5 BIG-IP LTM and AFM Properties Fields

In this field...	Do this...
<b>Access Information</b>	
Type	F5 BIG-IP LTM and AFM This field is read-only.
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. For information on the requirements for this use, see Device User Permission Requirements (see <a href="#">Required device permissions</a> ).
Password	Type the password to use for SSH access to the device.
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. <b>Note:</b> This option only appears when CyberArk is configured in AFA. See Configuring CyberArk Integration (see <a href="#">Integrate AFA and CyberArk</a> ).
Platform (Policy ID)	Type the platform for this device that will be authenticated via CyberArk.  <b>Note:</b> This field is only relevant when retrieving credentials for the device from a CyberArk vault.

In this field...	Do this...
Safe	<p>Type the safe for this device that will be authenticated via CyberArk.</p> <p><b>Note:</b> This field is only relevant when retrieving credentials for the device from a CyberArk vault.</p>
Folder	<p>Type the folder for this device that will be authenticated via CyberArk.</p> <p><b>Note:</b> This field is only relevant when retrieving credentials for the device from a CyberArk vault.</p>
Object	<p>Type the device's CyberArk Object.</p> <p><b>Note:</b> This field is only relevant when retrieving credentials for the device from a CyberArk vault.</p>
Geographic Distribution	
Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p><b>Note:</b> This field is relevant when a Geographic Distribution architecture is configured. See Using a Distributed System.</p>
Baseline Configuration Compliance	

In this field...	Do this...
Baseline Configuration Profile	<p>To enable generation of Baseline Compliance Reports for this device, select the baseline compliance profile to use.</p> <ul style="list-style-type: none"> <li>• <b>F5 BigIP.</b> Select the baseline compliance profile 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 <a href="#">Customize baseline configuration profiles</a>).</li> <li>• <b>None.</b> To disable Baseline Compliance Report generation for this device.</li> </ul>
Route Collection	
Routing Information Collection Method	<p>Specify how AFA should acquire the device's routing information:</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA will automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA will take the device's routing information from a static file you provide. For more information, see Manually Specifying Routing Information (see <a href="#">Specify routing data manually</a>).</li> </ul>
Remote Management Capabilities	
SSH	<p>The connection type.</p> <p><b>Note:</b> SSH is required for baseline configuration compliance purposes. All the other functionality is delivered by collecting data from the F5 BIG-IP LTM and AFM device using REST.</p>

In this field...	Do this...
Custom Port	<p>The port to use for the SSH connection.</p> <p>The default value is <b>22</b>.</p> <p>To use a port other than the default port, select the <b>Custom Port</b> check box and type the port number.</p>
Number of allowed encryption keys	<p>The permitted number of different RSA keys AFA can receive from the device's IP address.</p> <p><b>Note:</b> Different RSA keys might be sent from the same IP address in cases of cluster fail-over, device operating system upgrades. and so on.</p> <p>1 2</p> <ul style="list-style-type: none"> <li>• <b>unlimited</b> (Default)</li> </ul>
Log Collection and Monitoring	

In this field...	Do this...
Log collection method	<p>Specify the log collection method that AFA should use when collecting audit logs, by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Extensive:</b> Not applicable. Intelligent Policy Tuner (IPT) is not available for F5 devices.</li> <li>• <b>Standard:</b> Use Syslog data for the Change History report page. IPT is disabled.</li> </ul> <p><b>None</b></p> <p>The default value is <b>Extensive</b>.</p> <p><b>Note:</b> Selecting <b>None</b> disables the following fields: <b>Syslog-ng server</b>, <b>Additional firewall identifiers</b>, and <b>Log collection frequency (minutes)</b>.</p> <p><b>Note:</b> This device type supports audit logs, but not traffic logs. Therefore, the Intelligent Policy Tuner (IPT) is not supported for this device.</p>
Syslog-ng server	(If enabled) Specify the syslog-ng server. See Specifying a Syslog-ng server (see <a href="#">Specify a Syslog-ng server</a> ).
Additional firewall identifiers	<p>(If enabled) 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>
Log collection frequency (minutes)	<p>(If enabled) Type the interval of time in minutes, at which AFA should collect logs for the device.</p> <p>The default value is <b>60</b>.</p>
Options	

In this field...	Do this...
Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For more details, see <a href="#">Configure real-time monitoring</a> .
Set user permissions	Select this option to set user permissions for the device.

4. If CyberArk credential management is enabled, enter the following details:

☒ Retrieve credentials from CyberArk Vault (?)

Platform (PolicyID)

Safe

Folder

Object

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.

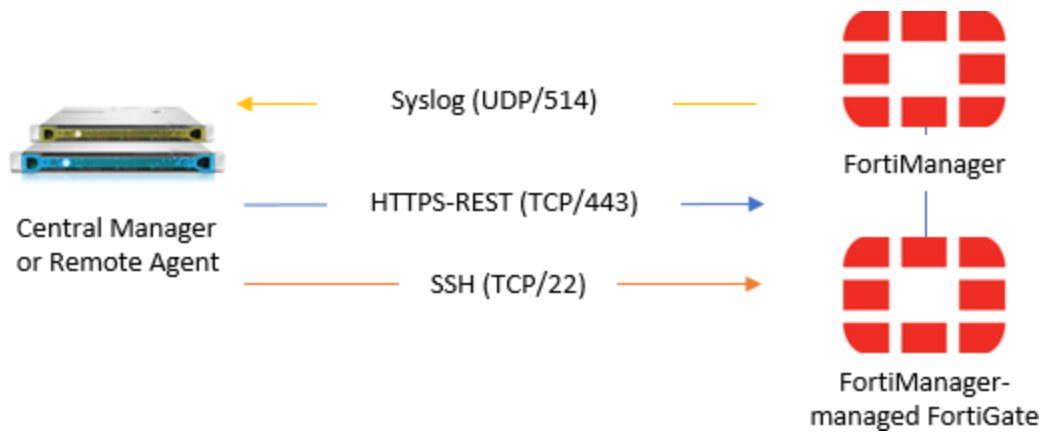
A success message appears to confirm that the device is added.

## 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):

	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:

**Edit Profile**

Profile Name:

Description:

Type: ☒ System Admin ☐ 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

<b>Host</b>	Enter the host name or IP address of the device.
<b>User Name</b>	<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"> <li>• <b>To analyze only devices under a specific ADOM</b>, specify a specific ADOM's administrator credentials.</li> <li>• <b>To analyze all devices under all ADOMs</b>, provide the credentials of a global administrator.</li> <li>• <b>When analyzing devices as a global administrator</b>, no other action is required. Otherwise, some manual configuration may be required. Contact AlgoSec support for more information.</li> </ul>
<b>Password</b>	Enter the password to use for accessing the device.

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

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

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

<b>Log collection method</b>	<p>Specify whether AFA should collect logs for the device, by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> Do not collect logs.</li> <li>• <b>Standard:</b> Enable log collection.</li> <li>• <b>Extensive:</b> Enable log collection and the Intelligent Policy Tuner.</li> </ul> <p>The default value is <b>Extensive</b>.</p>
<b>Syslog-ng server</b>	<p>If you selected <b>Standard</b> or <b>Extensive</b> in the <b>Log collection method</b> field, you must specify the syslog-ng server. For more details, see <a href="#">Specify a Syslog-ng server</a>.</p> <p><b>Tip:</b> Alternately, see <a href="#">Configure your FortiManager to forward syslog messages to AFA</a>.</p>
<b>Log collection frequency</b>	<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 .
- b. In the **Direct Access Configuration**, enter the following details, and then click **OK**.

<b>Host IP</b>	Type the IP address of the device.
<b>User Name</b>	Type the user name to access the device.

<b>Password</b>	Type the password to access the device.
<b>Baseline Profile</b>	<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 <a href="#">Customize baseline configuration profiles</a>.</p> <p>To disable Baseline Compliance Report generation for this device, select <b>None</b>.</p>
<b>Test Connectivity</b>	<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:

<b>Real-time change monitoring</b>	Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a> .
<b>Set user permissions</b>	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:

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

### 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

<b>Host</b>	Type the host name or IP address of the device.
<b>User Name</b>	Type the user name to use for SSH access to the device.
<b>Password</b>	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:

<b>Custom Port</b>	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
<b>Number of allowed encryption keys</b>	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

<b>Log collection method</b>	<p>Specify whether AFA should collect logs for the device, by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> Do not collect logs.</li> <li>• <b>Standard:</b> Enable log collection.</li> <li>• <b>Extensive:</b> Enable log collection and the Intelligent Policy Tuner.</li> </ul> <p>The default value is <b>Extensive</b>.</p>
<b>Syslog-ng server</b>	<p>If you selected <b>Standard</b> or <b>Extensive</b> in the <b>Log collection method</b> field, you must specify the syslog-ng server. For details, see <a href="#">Specify a Syslog-ng server</a>.</p>
<b>Additional firewall identifiers</b>	<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: <b>1.1.1.1:2.2.2.2:ServerName</b>.</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><b>Note:</b> This field is only relevant for the parent device. For more details, see <a href="#">Add additional device identifiers for sub-systems</a>.</p>
<b>Log collection frequency</b>	<p>Enter the interval of time in minutes, at which AFA should collect logs for the device.</p>

## Options

<b>Real-time change monitoring</b>	<p>Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a>.</p>
<b>Set user permissions</b>	<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.

## Add Juniper devices

This topic describes how to add Juniper devices to AFA.

If you have multiple Juniper Netscreen or SRX devices, you may want to add the Juniper NSM that manages these devices. AFA analyzes any of the devices managed by the added NSM. If you have a Juniper NSM 2007, you must add each Netscreen device separately, and specify that the Netscreen device logs are collected from the NSM. 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.

## Add a Juniper NSM

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 to listen to port 8443 on the IP address of its interface. For more details, see the [Juniper Knowledge Base](#).
2. If you are using a Juniper NSM 2007 or 2008, enable translation of rule numbers to rule IDs. For more details, see [Enable rule number translation](#).

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 fields as needed.

**Juniper NSM Properties Step 1 fields**

In this field...	Do this...
<b>Access Information</b>	
NSM GUI server	Type 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 accessing the primary NSM GUI server fails, AFA will access the secondary NSM GUI server.</p> <p>You must complete the <b>Secondary NSM GUI server</b> field.</p> <p><b>Note:</b> NSM HA cluster support is only available if the NSM GUI server and Dev server are running on the same server.</p>
Secondary NSM GUI server	Type the host name or IP address of the secondary NSM GUI server.

In this field...	Do this...
User Name	<p>Type the user name to use for SSH access to the NSM GUI server.</p> <p><b>Note:</b> AlgoSec recommends using a "read-only" user account on the NSM GUI server. See <a href="#">Configuring a Read-Only NSM User for Data Collection</a> (see <a href="#">Configure a read-only NSM user for data collection</a>).</p> <p><b>Tip:</b> You can configure AFA to connect to the device using SSH with Public-Key authentication. To do so, select the <b>Use public key authentication in data collection</b> check box in the <b>General</b> sub-tab of the <b>Options</b> tab in the Administration area. For details, see <a href="#">Define AFA preferences</a>.</p>
Password	Type the password to use for SSH access to the NSM GUI server.
Port	<p>Type the port number to use on the NSM GUI server.</p> <p>The default value is 8443.</p> <p>The default port on NSMXpress appliances is 443.</p>
Geographic Distribution	
Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p>This field is relevant when a Geographic Distribution architecture is configured.</p>

In this field...	Do this...
<b>Log Collection and Monitoring</b>	<b>Note:</b> 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 details, see <a href="#">Add additional device identifiers for sub-systems</a> .
Collect Logs (via SSH)	Select this option to specify that AFA should collect traffic logs for the device using SSH.
From	Specify from where AFA should collect logs, by selecting one of the following: <ul style="list-style-type: none"> <li>• <b>NSM:</b> AFA should collect logs from the NSM.</li> <li>• <b>Syslog-ng:</b> AFA should collect logs from a syslog-ng server.</li> </ul> The default value is <b>NSM</b> .

In this field...	Do this...
NSM Dev server	<p>Specify the NSM's location by choosing one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Same as NSM GUI server:</b> The NSM Devices server is located on the same machine as the NSM GUI server.</li> <li>• <b>Separate server:</b> The NSM is located separately from the NSM GUI server. If you chose this option, you must type the NSM's host name or IP address in the field provided.</li> </ul> <p>The default value is <b>Same as NSM GUI server</b>.</p> <p><b>Note:</b> 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 information on how to configure STRM to forward the logs, see <a href="#">Configuring Juniper STRM to Forward Logs to a Syslog-ng Server</a> (see <a href="#">Configuring Juniper STRM to forward logs to a Syslog-ng server</a>).</p> <p><b>Note:</b> In the NSMXpress appliance's setup, the NSM GUI server and the NSM Devices server are installed on the same machine.</p> <p>This area is only relevant if you selected <b>NSM</b> in the <b>From</b> field.</p>
SSH User Name	<p>Type the user name for connecting to the NSM.</p> <p>This field is only relevant if you selected <b>NSM</b> in the <b>From</b> field.</p>
SSH Password	<p>Type the password for connecting to the NSM.</p> <p>This field is only relevant if you selected <b>NSM</b> in the <b>From</b> field.</p>
Test Connectivity	<p>Click this button to test connectivity to the defined NSM server.</p> <p>A message informs you whether AFA connected to the NSM server successfully.</p> <p>This button is only relevant if you selected <b>NSM</b> in the <b>From</b> field.</p>
NSM forwarding	<p>Select this option to indicate that logs are collected on the NSM and then forwarded to the syslog-ng server.</p> <p>This field is only relevant if you selected <b>Syslog-ng</b> in the <b>From</b> field.</p>

In this field...	Do this...
Syslog-ng server	Specify the syslog-ng server. See Specifying a Syslog-ng server (see <a href="#">Specify a Syslog-ng server</a> ).  This field is only relevant if you selected <b>Syslog-ng</b> in the <b>From</b> field.
Collect audit logs from the same server	Select this option to specify that AFA should collect audit logs in addition to traffic logs.
Log collection frequency	Type the interval of time in minutes, at which AFA should collect logs.

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.

**Note:** If one of the Netscreen devices is already defined in AFA, the **Migrate from currently defined Netscreen** column appears.

If a Juniper SRX is already defined in AFA, there will not be an option to migrate it to the NSM. In order to define the device in AFA as managed by the NSM, you must first delete the SRX from AFA, and then define it in AFA under the NSM.

7. 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.

- c. If this device is a Netscreen device that is already defined directly in AFA and you want to migrate it into the NSM, select the device to migrate in the **Migrate from currently defined Netscreen** column.

The selected device will be deleted from AFA as a separate device, and added to the NSM along with any existing reports.

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

- a. Click .
- b. In the **Direct Access Configuration**, enter the following details:

<b>Host IP</b>	Type the IP address of the device.
<b>User Name</b>	Type the user name to access the device.
<b>Password</b>	Type the password to access the device.
<b>Baseline Profile</b>	<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 <a href="#">Customize baseline configuration profiles</a>.</p> <p>To disable Baseline Compliance Report generation for this device, select <b>None</b>.</p>

<b>Test Connectivity</b>	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.

- c. To access the managed device through the NSM machine, select **Access the managed devices through the NSM machine**, and enter the **SSH User Name** and **SSH Password**.

**Note:** AFA will connect to the NSM via SSH, and will open another SSH connection from the NSM towards the managed devices.

Do this if you do not want to specify credentials for each device and have AFA access each device directly.

- d. Click **OK**.

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

#### Juniper NSM Properties Step 2 Fields

In this field...	Do this...
<b>Advanced</b>	Click the arrow next to the <b>Advanced</b> heading, to display the fields in this area.

In this field...	Do this...
Display virtual routers (Netscreen devices)	<p>Select this option 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.</p> <p><b>Note:</b> This is not supported for Juniper SRX devices under the NSM, although this functionality is supported for SRX devices defined directly in AFA.</p>
<b>Options</b>	
Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a> .
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.

### Enable rule number translation

During log collection, AFA relies on rule IDs, available in NSM 2009 traffic logs.

Therefore, if you have a Juniper NSM 2007 or 2008, you must enable AFA to translate rule numbers to the rule IDs.

**Do the following:**

1. In the AFA **Administration** area, navigate to the **Advanced Configuration** tab.
2. Click **Add** to add a new parameter and enter the following details:
  - **Name.** Enter **Use\_Rulenum**.
  - **Value.** Enter **yes**.
3. Click **OK** and **OK** again, and continue with [Add a Juniper NSM](#).

### Configure a read-only NSM user for data collection

You must configure a read-only user in the NSM for the purpose of AFA data collection.

Do the following:

1. Log in to the NSM and select **Tools > Manage Administrators and Domains**.
2. In the **Manage Administrators and Domains** dialog, 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.

### Configuring 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 a Junos Space Security Director

Add a Junos Space Security Director enables AFA to analyze all the Juniper SRX devices it manages. This procedure must be performed with a device user with super administrator permissions.

Additionally, consider the following when working with Junos Space Security Directory devices:

<b>Data collection</b>	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.
<b>Changes in A30.00</b>	Juniper Space devices defined in AFA before version A30.00 have different behavior and support options. You may want to continue using your legacy device, or remove it and add it back.  For more details, see <a href="#">Juniper Space Security Director - Older ASMS versions and A30.00 Support</a> on AlgoPedia.
<b>Converting SRX devices</b>	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 <a href="#">Delete a device</a> and <a href="#">Juniper SRX devices in AFA</a> .

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.

### Juniper Space Properties Step 1 Fields

In this field...	Do this...
<b>Access Information</b>	
Host	Type the host name or IP address of the device.
User Name	Type the user name to use to access the device. <b>Important:</b> For user requirements, see <a href="#">Required device permissions</a> .
Password	Type the associated password.
<b>Geographic Distribution</b>	
Device managed by	Select the remote agent that should perform data collection for the device.  To specify that the device is managed locally, select <b>Central Manager</b> .  This field is relevant when a Geographic Distribution architecture is configured.
<b>Log Collection</b>	<b>Note:</b> 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. See <a href="#">Add additional device identifiers for sub-systems</a> .

In this field...	Do this...
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"> <li>• <b>None:</b> Do not collect logs.</li> <li>• <b>Standard:</b> Enable log collection.</li> <li>• <b>Extensive:</b> Enable log collection and the Intelligent Policy Tuner.</li> </ul> <p>The default value is <b>Extensive</b>.</p>
Syslog-ng server	<p>If you selected <b>Standard</b> or <b>Extensive</b> in the <b>Log collection method</b> field, you must specify the syslog-ng server. See <a href="#">Specify a Syslog-ng server</a>.</p> <p><b>Note:</b> 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 information on how to configure STRM to forward the logs, see <a href="#">Configuring Juniper STRM to forward logs to a Syslog-ng server</a>.</p>
Log collection frequency	Select the interval of time in minutes, at which AFA should collect logs for the device.

- 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 virtual systems.

- To specify that AFA should use the logs created by a managed device / virtual system, do the following:
  - In the **Add Device** column, select the check box next to the device's name.
  - 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.

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

1. Click .
2. In the **Direct Access Configuration**, enter the following details, and then click **OK**.

<b>Host IP</b>	Type the IP address of the device.
<b>User Name</b>	Type the user name to access the device.
<b>Password</b>	Type the password to access the device.
<b>Baseline Profile</b>	<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 <a href="#">Customize baseline configuration profiles</a>.</p> <p>To disable Baseline Compliance Report generation for this device, select <b>None</b>.</p>
<b>Test Connectivity</b>	<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.

7. Select the remaining options as needed:

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

8. Click **Finish**.

The new device is added to the device tree.

Juniper Space devices appear in the AFA device tree with a three tier hierarchy:

**Juniper Space Management Device > SRX device > LSYS.**

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.

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.

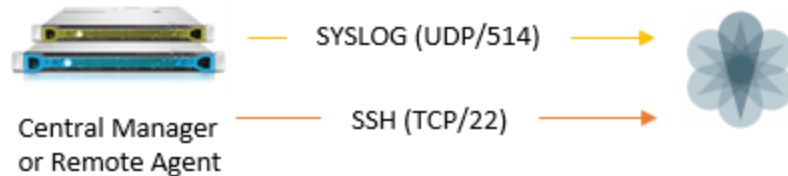
## Juniper SRX devices in AFA

The following sections describe how ASMS connects to Juniper SRX devices:

- [Network connection](#)
- [Device permissions](#)
- [Configure Juniper SRX devices to send syslog messages](#)
- [Add a Juniper SRX device to AFA](#)

## 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. It has two tabs: 'Users' and 'Authentication Method And Order'. The 'Users' tab is active. Below the tabs is a table with columns 'User Name', 'Full Name', and 'Login Class'. Overlaid on this is the 'Add User' dialog box. The 'Add User' dialog has the following fields: 'User name:' with the value 'AlgosecUser', 'User Id:' (empty), 'Full name:' with the value 'Algosec Admin', 'Password:' (masked with dots), 'Confirm password:' (masked with dots), and 'Login class:' with a dropdown menu showing 'super-user'. There are 'OK' and 'Cancel' buttons at the bottom of the 'Add User' dialog. To the right of the 'Add User' dialog, there are buttons for 'Add...', 'Edit...', and 'Delete'. At the bottom of the 'Edit User Management' window, there are also 'OK' and 'Cancel' buttons.

**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.

## Configure Juniper SRX devices to send syslog messages

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

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

**Do the following:**

1. Log in to the Juniper SRX web interface.
2. Select **Configure > CLI Tools > Point and Click CLI**.
3. Expand the **System > Syslog** nodes.
4. Add a new **Host** entry, and configure the ASMS appliance IP address.
5. Select **Contents**, and configure the **Facility / Level** as follows:
  - **Facility** = any
  - **Level** = any
6. Commit the policy.

## 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

<b>Host</b>	Enter the host name or IP address of the device.
<b>User Name</b>	Enter the user name.
<b>Password</b>	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:

<b>Custom Port</b>	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
<b>Number of allowed encryption keys</b>	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

<b>Log collection method</b>	<p>Specify whether AFA should collect logs for the device, by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> Do not collect logs.</li> <li>• <b>Standard:</b> Enable log collection.</li> <li>• <b>Extensive:</b> Enable log collection and the Intelligent Policy Tuner.</li> </ul> <p>The default value is <b>Extensive</b>.</p>
<b>Syslog-ng server</b>	<p>If you selected <b>Standard</b> or <b>Extensive</b> in the <b>Log collection method</b> field, you must specify the syslog-ng server. For details, see <a href="#">Specify a Syslog-ng server</a>.</p> <p><b>Note:</b> 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 <a href="#">Configuring Juniper STRM to forward logs to a Syslog-ng server</a>.</p>
<b>Additional firewall identifiers</b>	<p>Enter any additional IP addresses or host names that identify the device. Separate multiple entries by colons (:).</p> <p>For example: <b>1.1.1.1:2.2.2.2:ServerName</b></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><b>Note:</b> This field is only relevant for the parent device, and you may want to specify additional identifiers for sub-systems. For details, see <a href="#">Add additional device identifiers for sub-systems</a>.</p>
<b>Log collection frequency</b>	<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

<b>Real-time change monitoring</b>	Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a> .
<b>Set user permissions</b>	Select this option to 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**.

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.

The new device is added to the device tree, and a success message appears to confirm that the device is added.

## Add a Juniper Netscreen

This procedure describes how to add a Juniper Netscreen to AFA.

If individual Netscreen devices are already defined in AFA, AFA enables you to migrate these devices when you add the NSM that manages them. When a device is migrated, it is added as a member of the NSM and deleted as a separate device from AFA. The

reports for the device that were created before the migration are preserved and associated with the NSM.

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:

#### Juniper Netscreen Properties Fields

In this field...	Do this...
<b>Access Information</b>	
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. <b>Note:</b> AlgoSec requires using a "super-user" user account on the device.
Password	Type the password to use for SSH access to the device.
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. <b>Note:</b> This option only appears when CyberArk is configured in AFA. See Configuring CyberArk Integration (see <a href="#">Integrate AFA and CyberArk</a> ).
Platform (Policy ID)	Type the Platform for this device which will be authenticated via CyberArk.  This field is only relevant when retrieving credentials for this device from a CyberArk vault.

In this field...	Do this...
Safe	<p>Type the safe for this device which will be authenticated via CyberArk.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
Folder	<p>Type the folder for this device which will be authenticated via CyberArk.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
Object	<p>Type this device's CyberArk Object.</p> <p>This field is only relevant when retrieving credentials for this device from a CyberArk vault.</p>
<b>Geographic Distribution</b>	
Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p>This field is relevant when a Geographic Distribution architecture is configured.</p>
<b>Baseline Configuration Compliance</b>	

In this field...	Do this...
Baseline Configuration Compliance 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. For more information on baseline compliance profiles and instructions for adding new baseline compliance profiles, see Customizing Baseline Configuration Compliance Profiles (see <a href="#">Customize baseline configuration profiles</a>).</p> <p>To disable Baseline Compliance Report generation for this device, select <b>None</b>.</p>
<b>Advanced</b>	Click the arrow next to the <b>Advanced</b> heading, to display the fields in this area.
Display virtual routers	<p>Select this option to analyze each virtual router separately. Each virtual router will appear in the device tree immediately below the netscreen device and parallel to virtual systems.</p> <p><b>Note:</b> 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.</p>
<b>Remote Management Capabilities</b>	<p>Choose the method of data collection.</p> <p><b>Note:</b> Telnet is the least secure method.</p> <p><b>Tip:</b> You can configure AFA to connect to the device using SSH with Public-Key authentication. To do so, select the <b>Use public key authentication in data collection</b> check box in the <b>General</b> sub-tab of the <b>Options</b> tab in the Administration area. For details, see <a href="#">Define AFA preferences</a>.</p>
Custom Port	<p>To specify a custom port, select this option and type the port.</p> <p>This option is only relevant when SSH is selected.</p>

In this field...	Do this...
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>
<b>Firewall Log</b>	
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"> <li>• <b>None.</b> Do not collect logs.</li> <li>• <b>Standard.</b> Enable log collection.</li> <li>• <b>Extensive.</b> Enable log collection and the Intelligent Policy Tuner.</li> </ul> <p>The default value is <b>Extensive</b>.</p>
From	<p>Specify from where AFA should collect logs, by selecting one of the following:</p> <ul style="list-style-type: none"> <li>• <b>NSM.</b> AFA should collect logs from the NSM.</li> <li>• <b>Syslog-ng.</b> AFA should collect logs from a syslog-ng server.</li> </ul> <p>The default value is <b>NSM</b>.</p>
NSM Dev server	<p>Type the NSM host name or IP address.</p> <p>This field only appears if you selected <b>NSM</b> in the <b>From</b> field.</p>
User Name	<p>Type the user name for connecting to the NSM.</p> <p>This field only appears if you selected <b>NSM</b> in the <b>From</b> field.</p>
Password	<p>Type the password for connecting to the NSM.</p> <p>This field only appears if you selected <b>NSM</b> in the <b>From</b> field.</p>

In this field...	Do this...
Test Connectivity	<p>Click this button to test connectivity to the defined NSM server. A message informs you whether AFA connected to the NSM server successfully.</p> <p>This field only appears if you selected <b>NSM</b> in the <b>From</b> field.</p>
Syslog-ng server	<p>If you selected <b>Syslog-ng</b> in the <b>From</b> field, you must specify the syslog-ng server. See Specifying a Syslog-ng server (see <a href="#">Specify a Syslog-ng server</a>).</p> <p><b>Note:</b> 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 information on how to configure STRM to forward the logs, see Configuring Juniper STRM to Forward Logs to a Syslog-ng Server (see <a href="#">Configuring Juniper STRM to forward logs to a Syslog-ng server</a>).</p>
Collect audit logs from the same server	<p>Select this option to specify that AFA should collect audit logs in addition to traffic logs.</p> <p>If you clear this check box, you must specify the audit log server in the <b>Collect audit logs from</b> and the <b>Syslog-ng server</b> fields. Complete these fields in the same manner as for the traffic log server.</p>

In this field...	Do this...
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><b>Note:</b> 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 <a href="#">Adding Additional Device Identifiers for Sub-Systems</a> (see <a href="#">Add additional device identifiers for sub-systems</a>).</p> <p>This field only appears if you selected <b>Syslog-ng</b> in the <b>From</b> field.</p>
Log collection frequency	Type the interval of time in minutes, at which AFA should collect logs for the device.
ActiveChange	
Enable ActiveChange	Select this option to enable FireFlow to generate CLI recommendations and push them to the device.
Options	
Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a> .
Set user permissions	Select this option to set user permissions for this device.

4. If CyberArk credential management is enabled, enter the following details:

☒ Retrieve credentials from CyberArk Vault [\(?\)](#)

Platform (PolicyID)

Safe

Folder

Root

Object

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.

## Add a Juniper M/E router

This procedure describes how to add a Juniper M/E router to AFA.

**Note:** AFA only supports routing analysis for Juniper M/E routers. Even if the router has a policy filtering traffic, no policy analysis is supported.

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.

### Juniper M/E router fields

In this field...	Do this...
Access Information	

In this field...	Do this...
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. <b>Note:</b> AlgoSec requires using a "super-user" user account on the device.
Password	Type the password to use for SSH access to the device.
<b>Geographic Distribution</b>	
Device managed by	Select the remote agent that should perform data collection for the device.  To specify that the device is managed locally, select <b>Central Manager</b> .  This field is relevant when a Geographic Distribution architecture is configured.
<b>Baseline Configuration Compliance</b>	
Baseline Configuration Compliance Profile	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 <a href="#">Customize baseline configuration profiles</a> ).  To disable Baseline Compliance Report generation for this device, select <b>None</b> .

In this field...	Do this...
<b>Route Collection</b>	<p>Specify how AFA should acquire the device's routing information:</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA will automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA will take the device's routing information from a static file you provide. For more information, see Manually Specifying Routing Information (see <a href="#">Specify routing data manually</a>).</li> </ul>
<b>Remote Management Capabilities</b>	<p>Choose the method of data transmission.</p> <p><b>Note:</b> Telnet is a less secure method.</p>
Custom Port	<p>To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.</p>
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>
<b>Options</b>	
Real-time change monitoring	<p>Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a>.</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.

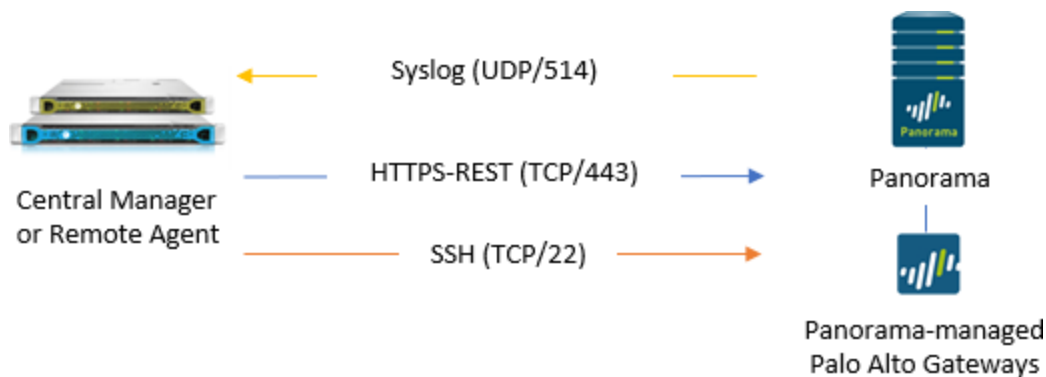
A success message appears to confirm that the device is added.

## Add Palo Alto Networks devices

This topic describes how AFA connects to Palo Alto Panorama and firewall devices.

### Palo Alto network connection

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.

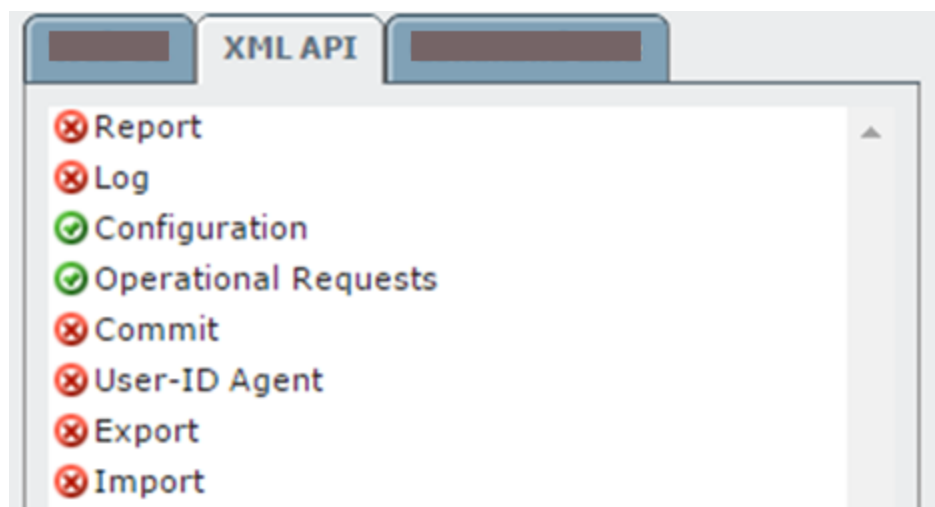
### Panorama device permissions

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.

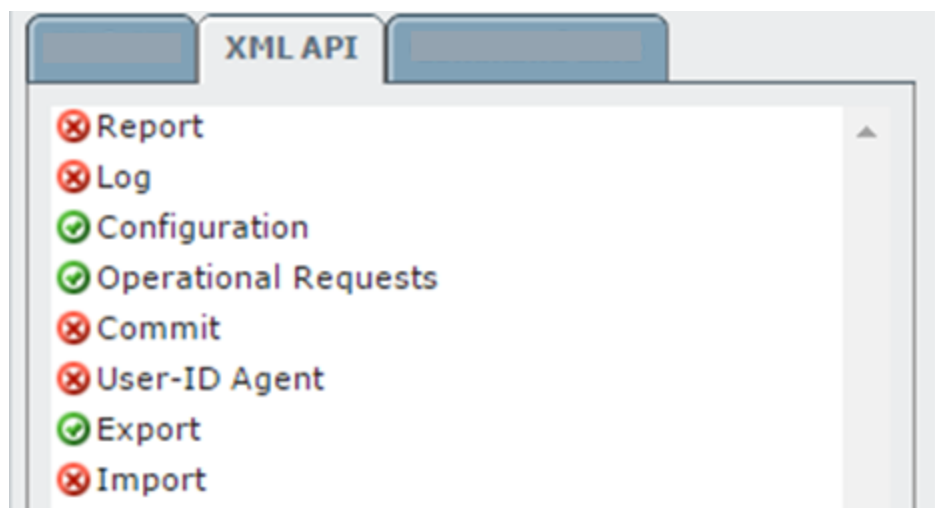
For example:



### 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.

### 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.

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

<b>Host</b>	Enter the host name or IP address of the device.
<b>User name</b>	Enter the administrative user name to use for SSH access to the device.  For more details, see <a href="#">Panorama device permissions</a> .
<b>Password</b>	Enter the associated password.
<b>High Availability</b>	Select this option to configure a High Availability cluster.  If selected, you must also enter a value for the <b>Secondary</b> field.
<b>Secondary Panorama</b>	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

<b>Syslog-ng server</b>	Specify the syslog-ng server. For more details, see <a href="#">Specify a Syslog-ng server</a> .
<b>Log collection frequency</b>	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 .
- b. In the **Direct Access Configuration**, enter the following details, and then click **OK**.

<b>Host IP</b>	Type the IP address of the device.
<b>User Name</b>	Type the user name to access the device.
<b>Password</b>	Type the password to access the device.
<b>Baseline Profile</b>	<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 <a href="#">Customize baseline configuration profiles</a>.</p> <p>To disable Baseline Compliance Report generation for this device, select <b>None</b>.</p>
<b>Test Connectivity</b>	<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:

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

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.

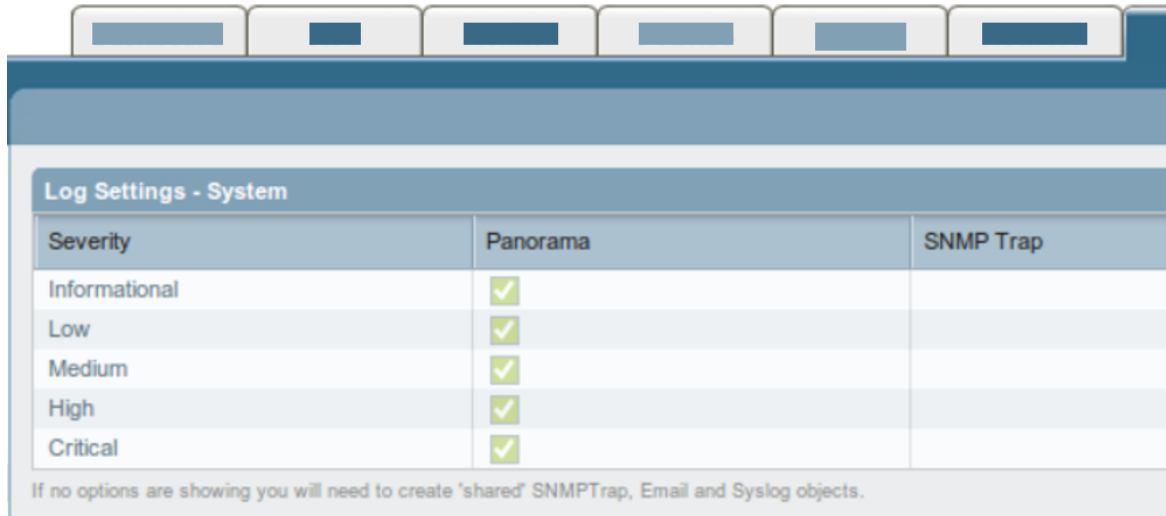
### Configure log collection on a Panorama device

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:



Log Settings - System		
Severity	Panorama	SNMP Trap
Informational	<input checked="" type="checkbox"/>	
Low	<input checked="" type="checkbox"/>	
Medium	<input checked="" type="checkbox"/>	
High	<input checked="" type="checkbox"/>	
Critical	<input checked="" type="checkbox"/>	

If no options are showing you will need to create 'shared' SNMPTrap, Email and Syslog objects.

## 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	<p>Type the administrative user name to use for SSH access to the device.</p> <p>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.</p> <p>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).</p>
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:

<b>Custom Port</b>	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.
<b>Number of allowed encryption keys</b>	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

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:

<b>Syslog-ng server</b>	If you selected <b>Standard</b> or <b>Extensive</b> in the <b>Log collection method</b> field, you must specify the syslog-ng server. For more details, see <a href="#">Specify a Syslog-ng server</a> .
<b>Additional firewall identifiers</b>	<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: <b>1.1.1.1:2.2.2.2:ServerName</b></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><b>Note:</b> 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 <a href="#">Add additional device identifiers for sub-systems</a>).</p>
<b>Log collection frequency</b>	Type the interval of time in minutes, at which AFA should collect logs for the device.

## Options

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

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.

# 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. If CyberArk credential management is enabled, enter the following details:

☒ Retrieve credentials from CyberArk Vault (?)

Platform (PolicyID)

Safe

Folder

Root

Object

4. Complete the remaining fields as needed.

## Symantec Blue Coat Properties Fields

In this field...	Do this...
Access Information	

In this field...	Do this...
Supported Capabilities	Displays a list of supported device capabilities. This field is read-only.
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.
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. <b>Note:</b> This option only appears when CyberArk is configured in AFA. For more details, see <a href="#">Integrate AFA and CyberArk</a> .
Platform (Policy ID)	Type the Platform for this device which will be authenticated via CyberArk. This field is only relevant when retrieving credentials for this device from a CyberArk vault.
Safe	Type the safe for this device which will be authenticated via CyberArk. This field is only relevant when retrieving credentials for this device from a CyberArk vault.
Folder	Type the folder for this device which will be authenticated via CyberArk. This field is only relevant when retrieving credentials for this device from a CyberArk vault.
Object	Type this device's CyberArk Object. This field is only relevant when retrieving credentials for this device from a CyberArk vault.
Geographic Distribution	

In this field...	Do this...
Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p>This field is relevant when a Geographic Distribution architecture is configured.</p>
<b>Baseline Configuration Compliance</b>	
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. For more information on baseline compliance profiles and instructions for adding new baseline compliance profiles, see Customizing Baseline Configuration Compliance Profiles (see <a href="#">Customize baseline configuration profiles</a>).</p> <p>To disable Baseline Compliance Report generation for this device, select <b>None</b>.</p>
<b>SNMP Polling</b>	
SNMP version	Select the SNMP version in the drop-down menu.
SNMP community	<p>Type the SNMP community string.</p> <p>This field is only relevant for <b>SNMP v2c</b>.</p>
Security Name (username)	<p>Type the security name.</p> <p>This field is only relevant for <b>SNMP v3</b>.</p>
Authentication Protocol	<p>If desired, select the authentication protocol in the drop-down menu.</p> <p>This field is only relevant for <b>SNMP v3</b>.</p>

In this field...	Do this...
Authentication Password	If you selected an authentication protocol, type the password. This field is only relevant for <b>SNMP v3</b> .
Privacy Protocol	If desired, select a privacy protocol in the drop-down menu. This field is only relevant for <b>SNMP v3</b> .
Privacy Password	If you selected a privacy protocol, type the password. This field is only relevant for <b>SNMP v3</b> .
<b>Additional Information</b>	
Enable password	Type the password for switching to enabled mode.
<b>Route Collection</b>	Specify how AFA should acquire the device's routing information: <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA will automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA will take the device's routing information from a static file you provide. For more information, see Manually Specifying Routing Information (see <a href="#">Specify routing data manually</a>).</li> </ul>
<b>Remote Management Capabilities</b>	Choose the method of data transmission. <b>Note:</b> Telnet is a less secure method.
Custom Port	To specify a custom port, select this option and type the port. This option is only relevant when SSH is selected.

In this field...	Do this...
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>
<b>Policy Configuration Method</b>	<p>Choose the method of policy configuration. The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>Visual Policy Manager - VPM.</b> The device policy is configured via the Visual Policy Manager (VPM) only.</li> <li>• <b>Content Policy Language - CPL (Command-Line).</b> The device policy is configured via <i>both</i> the command line (CPL) <i>and</i> the Visual Policy Manager (VPM).</li> </ul>
<b>Options</b>	
Real-time change monitoring	Select this option to enable real-time alerting upon configuration changes. For details, see <a href="#">Configure real-time monitoring</a> .
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.

## Add a VMware NSX

This procedure describes how to add a VMware NSX 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.

#### VMware NSX Properties Fields

In this field...	Do this...
<b>Access Information</b>	
Host	Type the host name or route name of the device. This is the name that will be displayed in the devices tree.
User Name	Type the user name to use for REST access to the device. See Device User Permission Requirements (see <a href="#">Required device permissions</a> ).
Password	Type the password to use for REST access to the device.
<b>Geographic Distribution</b>	
Device managed by	Select the remote agent that should perform data collection for the device.  To specify that the device is managed locally, select <b>Central Manager</b> .  This field is relevant when a Geographic Distribution architecture is configured.
<b>Additional Information</b>	

In this field...	Do this...
Learning mode	<p>Select this option to specify that AFA traffic simulation should treat traffic that is not specified in a rule as blocked.</p> <p>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.</p>
Route Collection	<p>Specify how AFA should acquire the device's routing information:</p> <ul style="list-style-type: none"> <li>• <b>Automatic.</b> AFA will automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> AFA will take the device's routing information from a static file you provide. For more information, see <a href="#">Manually Specifying Routing Information</a> (see <a href="#">Specify routing data manually</a>).</li> </ul>
ActiveChange	
Enable ActiveChange	<p>Select this option to enable ActiveChange for the device.</p> <p><b>Note:</b> Enabling ActiveChange rollback for this device requires special configuration on the device.</p>
Options	
Real-time change monitoring	<p>Select this option to enable real-time change monitoring. For details, see <a href="#">Configure real-time monitoring</a>.</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.

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

## Check Point device requirements

See [Check Point device permissions](#).

## Cisco device requirements

<b>Cisco ASA</b>	<p>User requires permission to go into privileged mode, using "enable" (security level 15).</p> <p>To use ActiveChange, read-write permissions are required.</p> <p>There is a mitigation to this requirement, allowing the user to be in security level 5. See here (<a href="https://knowledge.algosec.com/skn/tu/e5272">https://knowledge.algosec.com/skn/tu/e5272</a>).</p> <p>If ActiveChange is being used, this mitigation is not applicable.</p>
<b>Cisco Firewalls via CSM</b>	<p>Requires enabling the CSM API service.</p> <p>To enable this, in the CSM management application, click <b>Tools &gt; Security Manager Administration &gt; API</b>, and check the <b>Enable API Service</b> setting.</p>

<b>Cisco IOS</b>	User requires the ability to go into privileged mode (using "enable"). There is a mitigation to this requirement, allowing the user to have read only permissions and use the special 'show running-config view full' command. See here ( <a href="https://knowledge.algosec.com/skn/tu/e4951">https://knowledge.algosec.com/skn/tu/e4951</a> ).
<b>Cisco Nexus</b>	For details, see <a href="#">Device permissions</a> .
<b>Cisco ACI</b>	At least <b>readPriv</b> permissions are required on <b>Security Domains All</b> . To use ActiveChange, read-write permissions are required.
<b>Cisco ISE</b>	The following user permissions are required: <ul style="list-style-type: none"> <li>• An ISE administrator with the "ERS-Operator" group assignment</li> <li>• REST connection over port 9060</li> <li>• Cisco ISE TrustSec SXP feature enabled for the device</li> </ul> AFA does not currently support the use of a Geographical Distribution Remote Agent to manage this device.
<b>Cisco FirePower</b>	The REST API must be enabled: <b>System &gt; Configuration &gt; REST API Preferences &gt; "Enable REST API"</b> . The user must be exclusively for AFA, must be in the global domain, and must have the "Administrator" role.  When using SSH, the user must be exclusively for AFA and must have the "read only" role.  AFA requires a unique Firepower user because Firepower allows only one open connection per user.

## Arista device requirements

The following user permissions are required:

- User with read permissions
- Rest connection over port 443

AFA does not currently support the use of a Geographical Distribution Remote Agent to manage this device.

## Juniper device requirements

<b>Juniper Netscreen</b>	<p>Read only permissions are sufficient.</p> <p>For ActiveChange, the following permission is additionally required:</p> <ul style="list-style-type: none"> <li>• Read-Write</li> </ul>
<b>Juniper SRX</b>	<p>For details, see <a href="#">Device permissions</a>.</p>
<b>Juniper NSM</b>	<p>For data collection (via SOAP, from the NSM GUI server), the user must have the read only System Administrator admin role.</p> <p>For collecting logs from the NSM (from its DEV server), one of the following is required:</p> <ul style="list-style-type: none"> <li>• The user is the "root" user</li> <li>• You deploy the <code>install_nsm_sudo</code> script on the NSM DEV server to change a minimal set of folder permissions.</li> </ul> <p>For retrieving dynamic routing data from the devices the NSM manages, SNMP access is required. See here (<a href="https://knowledge.algosec.com/skn/tu/e5116">https://knowledge.algosec.com/skn/tu/e5116</a>).</p> <p>For more details on the <code>install_nsm_sudo</code> script, see here (<a href="https://knowledge.algosec.com/skn/tu/e5605">https://knowledge.algosec.com/skn/tu/e5605</a>).</p> <p>For collecting global-zone rules for SRX devices managed by an NSM, the NSM user defined in AFA must be associated with a role which has permissions to view the Junos Global Rulebase. To enable this permission, in the NSM application, go to <b>Administer&gt;Common&gt;Tasks&gt;Manage Administrator and domains&gt;Roles</b>, and check "View Junos Global Rulebase".</p>
<b>Junos Space Security Director</b>	<p>The configured user must have one of the following user roles:</p> <ul style="list-style-type: none"> <li>• Super Administrator</li> <li>• A custom created read-only role. For details about how to create this custom role, see <a href="#">Create a Juniper Space user-defined role for AFA</a>.</li> </ul>

<b>Juniper M/E Routers</b>	<p>User must have the super-user login class.</p> <p>Juniper allows 4 types of user login-class: super-user, operator, read-only and unauthorized.</p> <p>Only "super-user" works properly in AFA. All of the other login classes will result in "ACCESS-DENIED" results for the data collection commands AFA runs.</p> <p>There is a mitigation to this requirement, allowing the user to be in login-class which is not super-user. Contact AlgoSec support for assistance.</p>
----------------------------	---

### Create a Juniper Space user-defined role for AFA

The following steps describe how to create a read-only, non-super-admin user for the Juniper Space user.

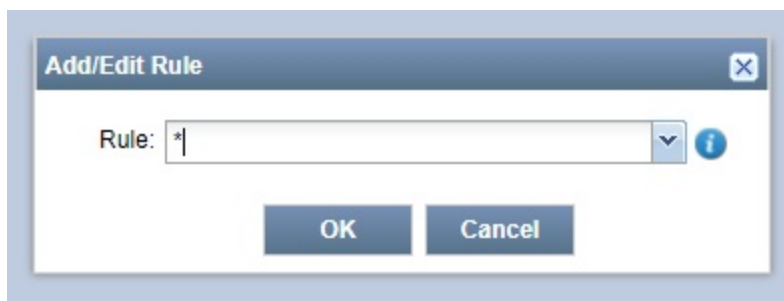
For more details about how to perform these steps, see [Junos Space - Network Management Platform documentation](#).

Do the following:

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:

<b>Log Collector Management</b>	<b>Read Log Collector info</b>
<b>Event Viewer</b>	<b>View Device Logs</b>
<b>Reports</b>	<b>Reports &gt; View Report</b>
<b>Firewall Policies</b>	<p>The following, without sub-permissions:</p> <ul style="list-style-type: none"> <li>• View Policy</li> <li>• Export Policy</li> <li>• Policy Profiles</li> <li>• Schedulers</li> <li>• AccessProfile</li> <li>• AppFirewall Policy</li> <li>• SSL Proxy Profile</li> <li>• End User Profile</li> <li>• Active Directory</li> <li>• Condition</li> <li>• Environment Variable</li> <li>• Identity Management</li> <li>• Application Signatures</li> </ul>
<b>NAT Policies</b>	<ul style="list-style-type: none"> <li>• Export NAT Policy</li> <li>• View NAT Policy</li> <li>• View NAT Dirty Policy</li> <li>• NAT Pools (without sub-permissions)</li> <li>• Ports Sets (without sub-permissions)</li> </ul>
<b>VPNs</b>	<b>View VPN</b>
<b>Shared Objects</b>	<p>The following, without sub-permissions:</p> <ul style="list-style-type: none"> <li>• Services</li> <li>• Addresses</li> <li>• Zones Sets</li> <li>• Variables</li> </ul>

<b>Security Director Devices</b>	<b>View Security Director Devices</b>
<b>Devices</b>	<ul style="list-style-type: none"> <li>• <b>Unmanaged Devices</b></li> <li>• <b>Model Devices &gt;</b> <ul style="list-style-type: none"> <li>• View Modeled Instance</li> <li>• View Modeled Device Status</li> <li>• View Configlet</li> <li>• Connection Profiles &gt; View Connection Profile</li> </ul> </li> <li>• <b>Device Management &gt;</b> <ul style="list-style-type: none"> <li>• Device Inventory &gt; <ul style="list-style-type: none"> <li>• View Physical Inventory</li> <li>• View Physical Interfaces</li> <li>• View Logical Interfaces</li> <li>• View License Inventory</li> <li>• View Software Inventory</li> </ul> </li> <li>• <b>Device Access &gt; SSH to Device</b></li> <li>• <b>Device Configuration &gt;</b> <ul style="list-style-type: none"> <li>• View Active Configuration (without the sub-permissions)</li> <li>• View Template Association</li> <li>• View Configuration Change Log</li> </ul> </li> </ul> </li> </ul>
<b>Device Templates</b>	<b>Templates &gt;</b> <ul style="list-style-type: none"> <li>• View Template Details</li> <li>• View Template Association</li> </ul>
<b>CLI Configlets</b>	<ul style="list-style-type: none"> <li>• <b>Configlets &gt; View CLI Configlet Details</b></li> <li>• <b>Configuration View &gt;</b> <ul style="list-style-type: none"> <li>• View Configuration View Details</li> <li>• Export Configuration View</li> </ul> </li> </ul>

<b>Configuration Files</b>	<b>Config Files Management &gt; Export Configuration File</b>
<b>Jobs</b>	<b>Job Management &gt; View Recurrence</b>
<b>Audit Logs</b>	<b>Audit Log &gt; Export Audit Logs</b>
<b>Administration</b>	<b>Fabric</b> (without sub-permissions) <b>Applications</b> (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.

## 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

<b>F5 BIG-IP LTM Only</b>	<p>User can have any role. User Partition must be "ALL". Terminal access must be "tmsh" or "Advanced shell".</p> <p>For further details, see here (<a href="http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos_management_guide_10_1/tmos_users.html#1023762">http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos_management_guide_10_1/tmos_users.html#1023762</a>).</p>
---------------------------	--

<b>F5 BIG-IP LTM and +AFM</b>	<p>User must have "Administrator" role on all partitions. Terminal access must be "tmsh" (for baseline compliance).</p> <p>For further details, see here (<a href="https://knowledge.algosec.com/skn/c6/AlgoPedia/e14466/F5_BIG_IP_LTM_AFM_data_collection_authentication_method">https://knowledge.algosec.com/skn/c6/AlgoPedia/e14466/F5_BIG_IP_LTM_AFM_data_collection_authentication_method</a>).</p>
-------------------------------	---

## 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

The IP should be the NSX Manager IP.

<p>User permissions required for most actions</p> <p>Such as: analysis, monitoring, log collection, and so on</p>	<p>The user must have one of the following roles:</p> <ul style="list-style-type: none"> <li>• Auditor</li> <li>• Security Admin</li> <li>• NSX Admin</li> <li>• Enterprise Admin</li> </ul> <p><b>Note:</b> Read Only permissions are sufficient.</p>
<p>User permissions required for ActiveChange</p>	<p>The user must have the following roles:</p> <ul style="list-style-type: none"> <li>• Security Admin</li> <li>• Enterprise Admin</li> </ul> <p><b>Note:</b> Read/Write permissions are sufficient.</p>

**Note:** When adding an NSX 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

## 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

<b>Supported Capabilities</b>	Displays a list of device capabilities. This field is read-only and only appears for some devices.
<b>Host</b>	Type the host name or IP address of the device.
<b>User Name</b>	Type the user name to use for SSH access to the device.
<b>Password</b>	Type the password to use for SSH access to the device.

### Geographic Distribution **fields**

<b>Device managed by</b>	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p>This field is relevant when a Geographic Distribution architecture is configured.</p>
--------------------------	--

### Baseline Configuration Compliance

<b>Baseline Configuration Profile</b>	<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 <b>None</b>.</p> <p>For more details, see <a href="#">Customize baseline configuration profiles</a>.</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.

<b>SNMP version</b>	Select the SNMP version in the drop-down menu.
<b>SNMP community</b>	Type the SNMP community string. This field is only relevant for <b>SNMP v2c</b> .
<b>Security Name (username)</b>	Type the security name. This field is only relevant for <b>SNMP v3</b> .
<b>Authentication Protocol</b>	If desired, select the authentication protocol in the drop-down menu. This field is only relevant for <b>SNMP v3</b> .
<b>Authentication Password</b>	If you selected an authentication protocol, type the password. This field is only relevant for <b>SNMP v3</b> .
<b>Privacy Protocol</b>	If desired, select a privacy protocol in the drop-down menu. This field is only relevant for <b>SNMP v3</b> .
<b>Privacy Password</b>	If you selected a privacy protocol, type the password. This field is only relevant for <b>SNMP v3</b> .

## 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:

<b>Custom Port</b>	<p>To specify a custom port, select this option and type the port.</p> <p>This option is only relevant when SSH is selected.</p>
<b>Number of allowed encryption keys</b>	<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 <b>1</b>, the connection to the node will fail, resulting in a failed analysis.</p>

### Options

<b>Real-time change monitoring</b>	<p>Select this option to enable real-time change monitoring.</p> <p>For more details, see <a href="#">Configure real-time monitoring</a>.</p>
<b>Set user permissions</b>	<p>Select this option to set user permissions for this 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.

## 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

<b>Supported Capabilities</b>	Displays a list of device capabilities. This field is read-only.
<b>Host</b>	Type the host name or IP address of the device.

### Geographic Distribution fields

Device managed by	<p>Select the remote agent that should perform data collection for the device.</p> <p>To specify that the device is managed locally, select <b>Central Manager</b>.</p> <p>This field is relevant when a Geographic Distribution architecture is configured.</p>
-------------------	--

### 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	<p>Type the SNMP community string.</p> <p>This field is only relevant for <b>SNMP v2c</b>.</p>
Security Name (username)	<p>Type the security name.</p> <p>This field is only relevant for <b>SNMP v3</b>.</p>
Authentication Protocol	<p>If desired, select the authentication protocol in the drop-down menu.</p> <p>This field is only relevant for <b>SNMP v3</b>.</p>
Authentication Password	<p>If you selected an authentication protocol, type the password.</p> <p>This field is only relevant for <b>SNMP v3</b>.</p>
Privacy Protocol	<p>If desired, select a privacy protocol in the drop-down menu.</p> <p>This field is only relevant for <b>SNMP v3</b>.</p>
Privacy Password	<p>If you selected a privacy protocol, type the password.</p> <p>This field is only relevant for <b>SNMP v3</b>.</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 details, see [Specify routing data manually](#).

### Options

<b>Update Network Map upon routing change</b>	Select this option to enable automatically updating the graphic network map upon routing changes.
<b>Set user permissions</b>	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 Mange 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:

<b>Adding or updating</b>	Your CSV file can include either devices to add or update, but not both.
<b>Devices that must be handled on their own</b>	<p>The following device types cannot be listed in a CSV file together with other device types:</p> <ul style="list-style-type: none"> <li>• <b>Cisco IOS</b></li> <li>• <b>Cisco ASA</b> and all types of Cisco firewalls</li> <li>• <b>Juniper Netscreen</b></li> </ul> <p>These devices must be added or updated using a CSV file of their own.</p>
<b>Missing headers</b>	<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>
<b>Syslog values for sub-systems</b>	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)

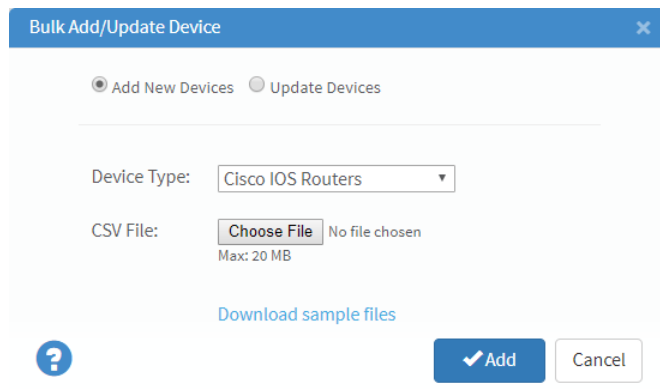
This procedure describes how to import a CSV file of device data into AFA via the Administration UI.

**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:

The screenshot shows a modal dialog box titled "Bulk Add/Update Device" with a close button (X) in the top right corner. Inside the dialog, there are two radio buttons: "Add New Devices" (which is selected) and "Update Devices". Below these, there is a "Device Type:" label followed by a dropdown menu currently showing "Cisco IOS Routers". Underneath, the "CSV File:" label is followed by a "Choose File" button, the text "No file chosen", and "Max: 20 MB". A blue link "Download sample files" is positioned below the file selection area. At the bottom left is a blue circular help icon with a white question mark. At the bottom right are two buttons: a blue "Add" button with a white checkmark and a white "Cancel" button.

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:

<b>-f &lt;CSVFile&gt;</b>	Defines the name of the CSV file. This file must be located in the current directory.
<b>-t &lt;deviceType&gt;</b>	<p>Defines the type of devices to import or update. Supported values include:</p> <ul style="list-style-type: none"> <li>• <b>ASA.</b> A Cisco ASA device.</li> <li>• <b>IOS.</b> A Cisco IOS Router.</li> <li>• <b>NSC.</b> A Juniper NetScreen device.</li> <li>• <b>GEN.</b> Any of the other supported device brands. In this case, specify the brand in the CSV <b>brand</b> column. For more details, see <a href="#">CSV import file format</a>.</li> </ul> <p>For additional device types and configurations, see <a href="#">Bulk import support scope</a>.</p>
<b>-u</b>	<p>Determines that the script updates existing devices.</p> <p>When absent, the script imports the data as new devices.</p>

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 AFA **Administration** area:

<b>Device types</b>	<p>Add the following types of devices individually in the AFA <b>Administration</b> area:</p> <ul style="list-style-type: none"><li>• <b>Management devices</b>, including any device that manages other devices. For example, Juniper NSM, Check Point devices, cloud "device" accounts, and so on.</li><li>• <b>Routing elements</b></li><li>• <b>Cisco Firewall via a CSM</b></li><li>• <b>Cisco Application Centric Infrastructure (ACI)</b></li><li>• <b>H3c</b></li><li>• <b>SECUI MF2</b></li></ul>
---------------------	--

<b>Device options</b>	<p>The following options must be configured manually in the AFA <b>Administration</b> area after importing:</p> <ul style="list-style-type: none"> <li>• Enabling <b>ActiveChange</b></li> <li>• Enabling <b>Learning mode</b> for a VMware NSX device. <b>Learning mode</b> 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.</li> <li>• Specifying the <b>policy configuration method</b> for a Symantec Blue Coat device to VPM. The default is CPL.</li> <li>• Specifying a <b>static URT file</b>.</li> </ul>
-----------------------	---

## 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 Mange Devices in Bulk from a .CSV File](#) AlgoPedia article.

**Tip:** Additionally, 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
<b>brand</b>	<p>The device brand. For more details, see <a href="#">Supported device brand values</a>.</p> <p>Required for all devices except for the following:</p> <ul style="list-style-type: none"> <li>• Cisco IOS</li> <li>• Cisco ASA/PIX/FWSM</li> <li>• Juniper Netscreen</li> </ul> <p>Specify these brand types in the <b>Bulk Add/Update Device</b> dialog instead.</p>
<b>name</b>	<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>
<b>display_name</b>	<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><b>Default:</b> 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:

<b>Analysis and monitoring devices</b>	<ul style="list-style-type: none"> <li>• <b>asa.</b> Cisco ASA</li> <li>• <b>bluecoat.</b> Symantec Blue Coat</li> <li>• <b>f5bigip</b></li> <li>• <b>f5bigip_afm.</b> F5 BIG-IP LTM and AFM</li> <li>• <b>f5bigip_full.</b> F5 BIG-IP LTM Only</li> <li>• <b>fortigate.</b> Fortinet Fortigate</li> <li>• <b>fwsn</b> (Cisco FWSM)</li> <li>• <b>ios.</b> Cisco IOS</li> <li>• <b>junos.</b> Juniper SRX</li> <li>• <b>junosmxrouter.</b> Juniper M/E Routers</li> <li>• <b>nexus.</b> Cisco Nexus</li> <li>• <b>nsc.</b> Juniper Netscreen</li> <li>• <b>nsx.</b> VMware NSX</li> <li>• <b>paloalto.</b> Palo Alto Networks firewall</li> </ul>
<b>Monitoring-only devices</b>	<ul style="list-style-type: none"> <li>• <b>ace.</b> Cisco ACE</li> <li>• <b>avaya.</b> Avaya Routing Switch</li> <li>• <b>brocade.</b> Brocade VDX</li> <li>• <b>junipersa.</b> Juniper Secure Access (SSL VPN)</li> <li>• <b>junosrouter.</b> Juniper Routers (non-M/E)</li> <li>• <b>netfilter.</b> Linux netfilter iptables</li> <li>• <b>sonicwall.</b> SonicWall</li> <li>• <b>topsec.</b> Topsec Firewall</li> <li>• <b>watchguard.</b> WatchGuard</li> </ul>

## Access information headers

Header name	Description
<b>host_name</b>	The device host name or IP address. Required for all device types.
<b>user_name</b>	The username used to access the device. Required for all device types.

Header name	Description
<b>passwd</b>	<p>The password used to access the device.</p> <p>Required for all device types unless CyberArk authentication is used.</p> <p><b>Note:</b> For Cisco IOS or ASA devices enabled for CyberArk, the <b>Password</b> and <b>Enable User Password</b> must be the same.</p>
<b>enable_user_name</b>	<p>The enable user name.</p> <p>Relevant and required only for Cisco ISO devices.</p>
<b>epasswd</b>	<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"> <li>• Cisco IOS</li> <li>• Cisco ASA</li> <li>• Symantec Blue Coat</li> </ul> <p>For more details, see <a href="#">CyberArk-related headers</a>.</p> <p><b>Note:</b> For Cisco IOS or ASA devices enabled for CyberArk, the <b>Password</b> and <b>Enable User Password</b> must be the same.</p>

## Cisco-related headers

Header name	Description
<b>rules_view</b>	<p>Determines how rules are displayed in device reports, as one of the following:</p> <ul style="list-style-type: none"> <li>• <b>ASDM</b>. (Default) Display rules in the Cisco Adaptive Security Device Manager (ASDM) graphical interface.</li> <li>• <b>CLI</b>. Display rules in command line format.</li> </ul> <p>Relevant for Cisco ASA devices only.</p>

## CyberArk-related headers

Header name	Description
<b>use_cyberark</b>	<p>Determines whether to use CyberArk authentication:</p> <ul style="list-style-type: none"> <li>• <b>yes</b></li> <li>• <b>no</b></li> </ul> <p>Required for CyberArk devices.</p>
<b>cyberark_platform</b>	<p>Defines the CyberArk platform name.</p> <p>Required for CyberArk devices.</p>
<b>cyberark_safe</b>	<p>Defines the CyberArk safe.</p> <p>Required for CyberArk devices.</p>
<b>cyberark_folder</b>	<p>Defines the CyberArk folder.</p> <p>Required for CyberArk devices.</p>
<b>cyberark_object</b>	<p>Defines the CyberArk object.</p> <p>Required for CyberArk devices.</p>
<b>cyberark_enable_platform</b>	<p>Defines the CyberArk platform for the enable password.</p> <p>Optional, and relevant only for CyberArk devices.</p>
<b>cyberark_enable_safe</b>	<p>Defines the CyberArk safe for the enable password.</p> <p>Optional, and relevant only for CyberArk devices.</p>
<b>cyberark_enable_folder</b>	<p>Defines the CyberArk folder for the enable password.</p> <p>Optional, and relevant only for CyberArk devices.</p>
<b>cyberark_enable_object</b>	<p>Defines the CyberArk object for the enable password.</p> <p>Optional, and relevant only for CyberArk devices.</p>

## Advanced headers

Header name	Description
<b>separate_vrfs</b>	<p>Determines whether to split the device into VRFs:</p> <ul style="list-style-type: none"> <li>• <b>yes</b> (Default)</li> <li>• <b>no</b></li> </ul> <p>Relevant only for the following devices:</p> <ul style="list-style-type: none"> <li>• Juniper Netscreen</li> <li>• Juniper SRX</li> <li>• Cisco IOS</li> <li>• Cisco Nexus</li> </ul>
<b>full_analysis</b>	<p>Determines whether to include risk analysis and policy optimization details in the device reports:</p> <ul style="list-style-type: none"> <li>• <b>yes</b> (Default)</li> <li>• <b>no</b></li> </ul> <p>Relevant for Cisco IOS and Cisco Nexus devices only.</p>

## Remote management headers

Header name	Description
<b>con</b>	<p>Determines the connection type as one of the following:</p> <ul style="list-style-type: none"> <li>• <b>SSH</b></li> <li>• <b>SSH (3des)</b>. Cisco ASA only</li> <li>• <b>SSH (des)</b>. Cisco ASA only</li> <li>• <b>TELNET</b>. For the following device types: <ul style="list-style-type: none"> <li>• Juniper</li> <li>• Cisco</li> <li>• Blue Coat</li> <li>• Fortigate</li> <li>• Palo Alto</li> <li>• Linux Netfilter</li> </ul> </li> </ul> <p>Required for all devices except the following:</p> <ul style="list-style-type: none"> <li>• VMware NSX</li> <li>• Cisco ACI</li> </ul> <p>These devices connect to AFA via REST.</p>
<b>number_of_allowed_encryption_keys</b>	<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"> <li>• 1</li> <li>• 2</li> <li>• unlimited (Default)</li> </ul> <p><b>Note:</b> Relevant only when using SSH. This might be required in cases of cluster fail-over, device operating system upgrades, and so on.</p>
<b>ssh_port</b>	<p>Defines the port to use for an SSH connection.</p> <p>Relevant only when using SSH.</p> <p><b>Defaults:</b></p> <ul style="list-style-type: none"> <li>• <b>4118</b> for WatchGuard devices</li> <li>• <b>22</b> for all other devices</li> </ul>

## 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
<b>collect_log</b>	<p>Determines whether AFA collects logs for the device:</p> <ul style="list-style-type: none"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul> <p>Relevant for the following device types:</p> <ul style="list-style-type: none"> <li>• Cisco ASA/FWSM</li> <li>• F5 BIG-IP</li> <li>• FortiGate,</li> <li>• Juniper Netscreen</li> <li>• Juniper SRX</li> <li>• Palo Alto</li> </ul> <p><b>Note:</b> For Cisco ASA and FWSM devices, set to <b>no</b> to enable logging with only hit-counter data.</p>
<b>log_collection_mode</b>	<p>Determines the method for collecting logs for the device:</p> <ul style="list-style-type: none"> <li>• <b>standard</b>. Enable log collection.</li> <li>• <b>extensive</b>. (Default) Enable log collection and the Intelligent Policy Tuner.</li> </ul> <p>Relevant when log collection is enabled.</p>

Header name	Description
<b>collect_log_from</b>	<p>Determines whether AFA collects logs from the NSM or a syslog-ng server:</p> <ul style="list-style-type: none"> <li>• <b>nsm</b> (Default)</li> <li>• <b>syslog</b></li> </ul> <p>Relevant for Juniper Netscreen when log collection is enabled.</p> <p><b>Note:</b> 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>
<b>log_host_name</b>	<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>
<b>log_user_name</b>	<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><b>Note:</b> To collect logs from a remote syslog-ng server using a user other than root, you must configure the server separately.</p>
<b>log_passwd</b>	<p>Defines a password for connecting to the server/device sending logs to AFA.</p> <p>Relevant when log collection is enabled.</p>
<b>collect_log_from_adt</b>	<p>Determines whether AFA collects audit logs from the NSM or a syslog-ng server:</p> <ul style="list-style-type: none"> <li>• <b>nsm</b></li> <li>• <b>syslog</b></li> </ul> <p>Relevant for Juniper Netscreen when log collection is enabled.</p> <p><b>Note:</b> By default, the audit log server is the same as the traffic log server.</p>

Header name	Description
<b>log_host_name_adt</b>	<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"> <li>• Log collection is enabled</li> <li>• The audit log server is different from the traffic log server</li> </ul>
<b>log_user_name_adt</b>	<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"> <li>• Log collection is enabled</li> <li>• The audit log server is different from the traffic log server</li> </ul>
<b>log_passwd_adt</b>	<p>Defines the password for connecting to the server/device sending audit logs to AFA.</p>
<b>log_collection_frequency</b>	<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"> <li>• Log collection is enabled</li> <li>• The audit log server is different from the traffic log server</li> </ul>
<b>additional_fw_ips</b>	<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
<b>collector</b>	<p>Defines a server to manage the device's data:</p> <ul style="list-style-type: none"> <li>• <b>Central Manager</b> (default)</li> <li>• The name of any remote agent</li> </ul> <p>Relevant only when AFA is configured for geographic distribution.</p>

Header name	Description
<b>baseline_profile</b>	<p>Defines the baseline compliance profile to use when generating reports for the device.</p> <p>Optional for all devices.</p>
<b>root_psw</b>	<p>Defines a password to increase permissions on the device to <b>root</b> user permissions.</p> <p>Relevant only for Linux Netfilter IPTables</p> <p><b>Tip:</b> Devices usually block the ability to access the device as user <b>root</b>. Enable root access to the device to improve AFA support.</p>
<b>monitoring</b>	<p>Determines whether to enable real-time alerts for configuration changes:</p> <ul style="list-style-type: none"> <li>• <b>yes</b>. Default for real/live devices.</li> <li>• <b>no</b>. Default for file devices.</li> </ul> <p>Optional for all devices.</p> <p>For more details, see <a href="#">Configure real-time monitoring</a>.</p>
<b>set_user_permissions</b>	<p>Determines whether you can set user permissions for the device:</p> <ul style="list-style-type: none"> <li>• <b>yes</b> (Default)</li> <li>• <b>no</b></li> </ul> <p>Optional for all devices.</p>
<b>firewall_users</b>	<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
<b>snmp_version</b>	<p>Determines the SNMP version:</p> <ul style="list-style-type: none"> <li>• <b>snmpv2c</b></li> <li>• <b>snmpv3</b></li> </ul> <p>Relevant only for the following devices:</p> <ul style="list-style-type: none"> <li>• Symantec Blue Coat</li> <li>• Juniper Secure Access (SSL VPN)</li> <li>• Linux netfilter iptables</li> <li>• SonicWall</li> <li>• Topsec</li> <li>• WatchGuard</li> <li>• SECUI MF2</li> <li>• Avaya Routing Switch</li> <li>• Brocade VDX</li> </ul>
<b>snmp_community</b>	<p>Defines the SNMP community string.</p> <p>Required and relevant only when using SNMPv2c.</p>
<b>snmp_username</b>	<p>Defines the SNMP Security Name (username).</p> <p>Required and relevant only when using SNMPv2c.</p>
<b>snmp_auth_password</b>	<p>Defines the authentication password.</p> <p>Required and relevant only when:</p> <ul style="list-style-type: none"> <li>• Using SNMPv2c</li> <li>• The authentication protocol is specified</li> </ul>
<b>snmp_auth_protocol</b>	<p>Determines the authentication protocol:</p> <ul style="list-style-type: none"> <li>• <b>md5</b></li> <li>• <b>sha</b></li> <li>• empty</li> </ul> <p>Required and relevant only when using SNMPv2c.</p>

Header name	Description
<b>snmp_priv_password</b>	<p>Defines the authentication password.</p> <p>Required and relevant only when:</p> <ul style="list-style-type: none"> <li>• Using SNMPv2c</li> <li>• The privacy protocol is specified</li> </ul>
<b>snmp_priv_protocol</b>	<p>Determines the privacy protocol:</p> <ul style="list-style-type: none"> <li>• <b>des</b></li> <li>• <b>aes</b></li> <li>• empty</li> </ul> <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. 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 delete, and then click **Delete**.
3. 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:

<b>Find a device quickly</b>	Enter a name in the box at the top to select it automatically.
<b>Navigate across pages</b>	Click <b>Previous</b> or <b>Next</b> below the grid to navigate back and forth
<b>Sort the grid</b>	Click a column header to sort the devices shown
<b>Filter the grid</b>	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](#).

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 from the map

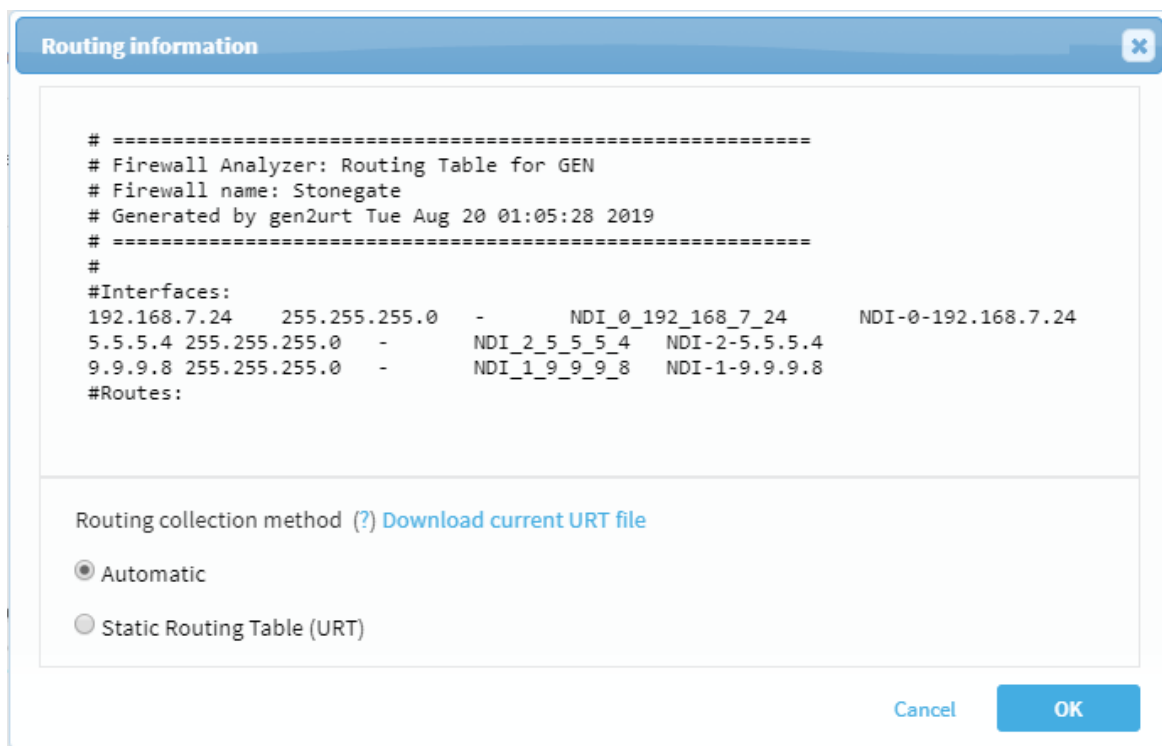
This procedure describes how to specify routing data manually directly from the map instead of the Devices Setup page.

For more details, see [Manage the map](#).

Do the following:

1. In AFA, view the graphic network map. Click **DEVICES**, select a device, and then click **MAP**.
2. 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:



3. 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

AFA supports CyberArk integration, enabling AFA to access devices without having to save credentials locally to ASMS servers, and retrieving credentials from CyberArk instead.

**Note:** When integrating with AFA, credentials for syslog collection still need to be provided separately to AFA.

## 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

## 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. In the AFA **Administration** area, navigate to the **Options > Authentication** tab.
2. Scroll down to the **CyberArk** area, and select the **Allow to setup devices with CyberArk credentials management** checkbox.
3. (Optional) Define default values for all devices authenticated via CyberArk, as follows:

<b>Platform (Policy ID)</b>	Enter a default CyberArk Platform.
<b>Safe</b>	Enter a default CyberArk safe.
<b>Folder</b>	Enter a default CyberArk folder. Default : <b>root</b>

4. Click **OK** to save your changes.

From now on, CyberArk options will appear in the DEVICES SETUP page for all relevant device brands.

5. (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.
6. 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](#)
7. 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, as follows:

<b>Check Point</b>	<p>For details, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">Check Point FireWall-1 devices (semi-automatic)</a>. 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.</li> <li>• <a href="#">Check Point devices (manual)</a>. Semi-automatic and manual data collection is supported only for Check Point device versions R77.X and below.</li> </ul>
<b>Cisco</b>	For details, see <a href="#">Cisco routers and devices</a> .
<b>Juniper</b>	For details, see <a href="#">Juniper devices</a> .
<b>Fortinet Fortigate</b>	For details, see <a href="#">Fortinet Fortigate (manual)</a> .
<b>Palo Alto Networks</b>	For details, see <a href="#">Palo Alto Networks (manual)</a> .
<b>McAfee Firewall Enterprise (Forcepoint Sidewinder)</b>	<p>For details, see <a href="#">McAfee Firewall Enterprise (Sidewinder) (manual)</a>.</p> <p><b>Note:</b></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. For more details, see the relevant <a href="#">AlgoPedia</a> KB article.</p>
<b>Symantec BlueCoat</b>	For details, see <a href="#">Symantec Blue Coat (manual)</a> .

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:

<b>Use a recent AFA report</b>	<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 <a href="#">Access log and configuration files</a>.</p> <p><b>Tip:</b> 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 <a href="#">Extend device support</a>.</p>
<b>Create a JSON file manually</b>	<p>If you do not have another device to collect the data from, create the file manually.</p> <p>For details, see <a href="#">Static support for generic devices</a>.</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 AFA **Administration** 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:

<b>Upload new</b>	<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 <code>/home/afa/algosec/fwfiles</code> directory, and use the <b>Existing on server</b> option.</p> <p>For more details, see <a href="#">Recommended device data collection per device type</a>.</p>
<b>Existing on server</b>	<p>Select a file already saved on the AFA server, in the <code>/home/afa/algosec/fwfiles</code> 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:

<b>Automatic</b>	<ul style="list-style-type: none"> <li>• <b>Automatic.</b> Automatically generate the device's routing information upon analysis or monitoring.</li> <li>• <b>Static Routing Table (URT).</b> Take the device's routing information from a static file you provide. For more details, see <a href="#">Specify routing data manually</a>.</li> </ul>
<b>Static Routing Table (URT).</b>	<p>Take the device's routing information from a static file you provide. For more details, see <a href="#">Specify routing data manually</a>.</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:

<b>name</b>	The device's display name, used in the device tree and all other locations around ASMS.
<b>path_name</b>	The location of the device file on the AFA machine, in the <b>/home/afa/algosec/fwfiles</b> directory.
<b>full_analysis</b>	Determines whether to perform full analysis. To optimize performance during device analysis, enter <b>no</b> .

For example:

<b>name</b>	<b>path_name</b>	<b>full_analysis</b>
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, navigate to: [Downloads > Evaluation and Requirements > Semi-Automatic Data Collection Procedures](#).
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:

<b>Sun platforms</b>	<b>uncompress ckp_collect.Z</b>
<b>SecurePlatform or Linux platforms</b>	<b>gunzip ckp_collect.Z</b>

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.

## Check Point devices (manual)

This topic describes how to collect data manually from Check Point devices.

### Check Point SmartCenter on Solaris/Nokia/Secure Platform/Linux

On a Unix-based platform (Solaris/Nokia/Secure Platform/Linux), we assume that the environment variable `$FWDIR` points to the root of the Check Point directory tree.

**Warning:** Do not perform this procedure on Check Point R80 versions or higher. Doing so may lead to unexpected results in your database.

1. At the Unix prompt, create a temporary work directory, by entering the following commands:

```
mkdir /tmp/algoseccd /tmp/algosec
```

2. Copy files from the Check Point directory to the work directory, as follows:

```
cp $FWDIR/conf/objects_5_0.C .
```

```
cp $FWDIR/conf/rulebases_5_0.fws .
```

```
cp $FWDIR/conf/gui-clients .
```

```
cp $FWDIR/conf/mv_tag.C .
```

```
cp $FWDIR/conf/asm.C .
```

```
cp $FWDIR/state/links.C .
```

**Tip:** Some of these files may be missing in your SmartCenter system, and AFA will be able to produce a report without them. The truly essential files are only `objects_5_0.C`, `rulebases_5_0.fws`, `links.C`, and the routing table file `net-`

```
rt.cpstat (see below).
```

3. Run the following three commands

```
fwm dbexport -f users.C
```

```
fwm dbexport -g -f groups.C
```

```
fwm ver | sed 's/fwm ver/' | sed 's/This is/' | sed 's/^ */' | sed 's/\n/' | sed 's/\r/'  
> ckp_version
```

4. Get the routing table using the “cpstat” command, as follows:

```
cpstat os -f routing -h a.b.c.d > net-rt.cpstat
```

where “a.b.c.d” is the IP address of the filter module

5. Create an archive that contains all the files in the `/tmp/algosec` directory, as follows:

```
cd /tmp/algosec tar cvf filename.tar *
```

You can now generate reports for the device. See [Setting Up Analysis from a File](#) (see [Add other devices and routing elements](#)).

## Check Point Provider-1

**Warning:** Do not perform this procedure on Check Point R80 versions or higher. Doing so may lead to unexpected results in your database.

1. Log in to the Provider-1 computer as `admin` or `root` (or a user that has access to the Check Point files).
2. At the Unix prompt, create a temporary work directory, by entering the following commands:

```
mkdir /tmp/algosec
```

```
cd /tmp/algosecs:
```

3. Copy one file from the Check Point's global Provider-1 directory to the work

directory, and store it with a different name, as follows:

- a. If you know the IP address of the CMA that contains the device for analysis, skip this step.

If you do not know the IP address, run the following command to generate a list of all the CMAs available:

```
mdsstat
```

- b. Run:

```
cp $FWDIR/conf/objects_5_0.C pv1_objects_5_0.C
```

- c. Run:

```
mdsenv <IP_address>
```

with the IP address of the CMA you need to access.

4. Verify that the environment variable \$FWDIR now points to the root of your CMA's Check Point directory tree by running:

```
echo $FWDIR
```

A correct output should show a directory name.

5. Copy files from the Check Point directory to the work directory, as follows:

```
cp $FWDIR/conf/objects_5_0.C .
```

```
cp $FWDIR/conf/rulebases_5_0.fws .
```

```
cp $FWDIR/conf/gui-clients .
```

```
cp $FWDIR/conf/mv_tag.C .
```

```
cp $FWDIR/conf/asm.C .
```

```
cp $FWDIR/state/links.C .
```

**Tip:** Some of these files may be missing in your Provider-1 system, and AFA

will be able to produce a report without them. The truly essential files are only `objects_5_0.C`, `rulebases_5_0.fws`, `links.C`, and the routing table file `net-rt.cpstat` (see below).

6. Run the following two commands:

```
fwm dbexport -f users.C
```

```
fwm dbexport -g -f groups.C
```

7. Get the routing table using the “cpstat” command, as follows:

```
cpstat os -f routing -h a.b.c.d > net-rt.cpstat
```

where “a.b.c.d” is the IP address of the filter module

8. Create an archive that contains all the files in the `/tmp/algosec` directory, as follows:

```
cd /tmp/algosec tar cvf filename.tar *
```

You can now generate reports for the device. See [Setting Up Analysis from a File](#) (see [Add other devices and routing elements](#)).

## Check Point SmartCenter on Microsoft Windows

**Warning:** Do not perform this procedure on Check Point R80 versions or higher. Doing so may lead to unexpected results in your database.

1. Open a Command Prompt window. Verify that the environment variable `%FWDIR%` points to the root of the Check Point directory tree by typing:

```
echo %FWDIR%
```

A correct output should show a directory name

2. Create a temporary work directory, by entering the following commands:

```
>mkdir C:\algosec>cd C:\algosec
```

3. Copy files from the Check Point directory to the work directory, as follows:

```
>copy %FWDIR%\conf\objects_5_0.C C:\algosec>copy
%FWDIR%\conf\rulebases_5_0.fws C:\algosec>copy %FWDIR%\conf\gui-
clients C:\algosec>copy %FWDIR%\conf\mv_tag.C C:\algosec>copy
%FWDIR%\conf\asm.C C:\algosec>copy %FWDIR%\state\links.C C:\algosec
```

**Tip:** Some of these files may be missing in your SmartCenter system, and AFA will be able to produce a report without them. The truly essential files are only `objects_5_0.C`, `rulebases_5_0.fws`, `links.C`, and the routing table file `net-rt.cpstat` (see below).

4. Run the following two commands:

```
fwm dbexport -f users.C
```

```
fwm dbexport -g -f groups.C
```

5. Get the routing table using the “cpstat” command, as follows:

```
>cpstat os -f routing -h a.b.c.d > C:\algosec\net-rt.cpstat
```

where “a.b.c.d” is the IP address of the filter module

6. Create a WinZip archive that contains all the files in the `C:\algosec` directory. It is recommended that you give the archive file a mnemonic name, such as

```
mydevice.zip.
```

You can now generate reports for the device. See [Add other devices and routing elements](#).

## Alternative Methods for Obtaining the Routing Table

In all the procedures described above, we used the “cpstat” command to collect the filter module's routing table. There may be circumstances in which the cpstat command is unavailable, or unable to connect to the module for some reason. For such situations, AlgoSec also lets you collect the module's routing table directly from the module's

command prompt. The exact command differs according to the module's operating system.

### SecurePlatform:

1. Log in to the filter module (use the default “admin” login).
2. Switch to Expert mode by typing:

**expert**

3. Get the filter module's routing table by issuing the command:

**netstat -rn > /tmp/netstat-rn.lnx**

**Note:** Make sure you give the file exactly the name shown.

4. Copy the file `/tmp/netstat-rn.lnx` from the SecurePlatform and place it in the management machine in the directory:

`C:\algosec\` (or `/tmp/algosec` on Unix SmartCenter servers )

**Note:** Make sure you keep the exact file name.

5. Create a Zip archive that contains all the files in the `C:\algosec` directory. It is recommended that you give the archive file a mnemonic name, such as `mydevice.zip`.

### Nokia:

1. Log in to the filter module (you do not need to be `root` on the filter module).
2. Get the filter module's routing table, as follows:

**(echo show route | iclid ) > nokia-iclid**

**Note:** Make sure you type the command, including the file name, exactly as

shown.

3. Copy the `nokia-iclid` file to the SmartCenter server and place it in the directory:

`C:\algosec\` (or `/tmp/algosec` on Unix SmartCenter servers)

**Note:** Make sure you keep the exact file name.

4. Create a Zip archive that contains all the files in the `C:\algosec` directory. It is recommended that you give the archive file a mnemonic name, such as

`mydevice.zip`.

## Sun Solaris:

1. Log in to the filter module (you do not need to be `root` on the filter module).
2. Get the filter module's routing table, as follows:

**netstat -v -rn > netstat-rn**

**Note:** Make sure you type the command, including the file name, exactly as shown.

3. Copy the `netstat-rn` file to the SmartCenter server and place it in the directory:

`C:\algosec\` (or `/tmp/algosec` on Unix SmartCenter servers)

**Note:** Make sure you keep the exact file name.

4. Create a Zip archive that contains all the files in the `C:\algosec` directory. It is recommended that you give the archive file a mnemonic name, such as

`mydevice.zip`

### Alteon:

1. Log in to the filter module (use the default “admin” login).
2. Get the filter module's routing table, by issuing the command:

```
netstat -rn > /tmp/netstat-rn.Inx
```

**Note:** Make sure you give the file exactly the name shown.

3. Copy the file /tmp/netstat-rn.Inx from the Alteon and place it in the management machine in the directory:

```
C:\algosec\ (or /tmp/algosec on Unix SmartCenter servers)
```

**Note:** Make sure you keep the exact file name.

4. Create a Zip archive that contains all the files in the C:\algosec directory. It is recommended that you give the archive file a mnemonic name, such as mydevice.zip.

### Microsoft Windows:

1. Open a Command Prompt window.
2. Get the filter module's routing table, as follows:

```
>route print > route-print
```

3. Copy the route-print file to the SmartCenter server and place it in the directory:

```
C:\algosec\ or /tmp/algosec on Unix SmartCenter servers)
```

**Note:** Make sure you keep the exact file name.

4. Create a Zip archive that contains all the files in the C:\algosec directory. It is recommended that you give the archive file a mnemonic name, such as mydevice.zip

## Check Point FireWall-1 devices (semi-automatic)

You can collect FireWall-1 device data using the AlgoSec data collection script `ckp_collect`, and then use the collected data to generate device reports. Such reports contain all of the data in a normal report, except for optimization information that is based on log analysis (such as Unused/Most used/Least used rules, Rule reordering optimization, Unused objects, and Unused objects within rules).

On Sun/Nokia/SecurePlatform/Alteon/Linux platforms, you can generate reports that contain log-based optimization information as well, by using the `ckp_log_collect` script to collect device logs.

### Sun/Nokia/SecurePlatform/Alteon/Linux Platforms

#### Check Point FireWall-1 with a Separate SmartCenter Server and Filter Module

The following procedure applies when you have a FireWall-1 SmartCenter server that is *separate* from the filter modules.

To collect Check Point FireWall-1 data:

1. Log in to the SmartCenter server as root (or as a user who has read access to the Check Point configuration files).
2. To collect device logs, do the following:
  - a. Copy the `ckp_log_collect` script to the log server where the device logs are located. For more details, see [Semi-automatic data collection scripts](#).

This can be the SmartCenter server or a CMA.

- b. Enter one of the following commands:

**`ckp_log_collect`** Runs the script and prompts you for all fields.

**`ckp_log_collect <profile>`** Runs the script and collects logs using the information in the specified profile. See [Using Saved Profiles](#).

**ckp\_log\_collect -l.** Runs the script, prompts you to select a profile from a list of available profiles, and then collects logs using the information in the selected profile. See [Using Saved Profiles](#).

**ckp\_log\_collect -a.** Runs the script and calls for automatic data collection from `ckp_data_push`.

**Note:** You can view help information for the script, by entering the command **ckp\_log\_collect -h**.

The script creates a log archive file containing log extracts.

**Note:** Log collection can take a while. Please make sure that your timeout variable is large enough.

To set the it from cpshell, enter the command: **idle 999**

To set it from expert mode, enter the command: `export TMOUT=59940`

- c. If the log server is a CMA, copy the file to the SmartCenter server, to the same location where you placed the `ckp_collect` script.
3. Change directory to the location in which you placed the `ckp_collect` script (which you uncompressed in [Semi-automatic data collection scripts](#)), and make it executable by typing:

```
chmod a+x ckp_collect
```

4. Enter the following command:

```
./ckp_collect
```

The following prompt appears on the screen:

```
Work directory is /tmp/ckp_collect
```

```
Enter 'y' if the firewall module you wish to analyze is remote.
```

```
Enter 'n' if the local machine is also the firewall module.
```

```
Do you wish to analyze a remote firewall?[y]
```

5. Enter **y**.

A list of the devices managed from the machine is displayed.

6. At the prompt, select the device number you wish to analyze.

**Note:** The default is always listed in brackets before the cursor.

A summary of your choices appears.

`ckp_collect` displays the chosen device to be analyzed.

7. Enter **y** to continue.

`ckp_collect` obtains a routing table of the remote filter module using Check Point's 'cpstat' command, which uses the OPSEC AMON protocol.

8. At the prompt, enter the IP address or DNS name of the remote filter module.

`ckp_collect` collects the routing table.

You are asked whether you want to save the created profile of your answers for later use. Saving the profile will let you to store the answers you provided to the script just described. See Using Saved Profiles (see [Using Saved Profiles](#)).

To save the profile for later use:

- a. Enter **y**.
- b. Enter the name of the new profile. (The name of the device is displayed by default.)

The data archive `~/fa-files/ckp-<hostname>-<date>.tar` is created. If you collected logs, the log archive file is added to the data archive file.

9. Copy `~/fa-files/ckp-<hostname>-<date>.tar` to the AFA machine.

You can now generate reports for the device. See Setting Up Analysis from a File (see [Add other devices and routing elements](#)).

The process describe above should usually run smoothly, however, difficulties may occur due to various factors such as your device configuration. Below are some possible solutions and workarounds.

- In case the cpstat connection attempt to the remote computer fails, you will be prompted whether you wish to correct the IP address. If you choose not to correct the IP address, `ckp_collect` will attempt to collect the routing table via ssh.
- If the ssh is unable to connect to the remote machine, you will be alerted of the fact and given instructions on how to manually collect the routing table:
  - a. A list of commands, based on the OS installed on the remote machine, will be displayed in order to create a routing table. Select the appropriate command, and follow the instructions.
  - b. Finish by copying the resulting file to the directory `/tmp/ckp_collect` on the SmartCenter server and run `ckp_collect` again.
- In case you entered the *wrong* operating system of the remote computer, you will be instructed to login to the remote device and check the OS with the `'uname'` command. You will then be asked to repeat the data collection process.

**Note:** The first time connect via ssh to the remote device you may see messages regarding the authenticity of the remote device host.

**Note:** You may safely ignore messages about inappropriate `"ioctl"`.

## Check Point Provider-1

To collect the device data:

1. Log in to the Provider-1 server.
2. To collect device logs, do the following:
  - a. Copy the `ckp_log_collect` script (which you uncompressed in [Semi-automatic data collection scripts](#)) to the log server where the device logs are located.

This can be the Provider-1 or a CMA.

- b. Enter one of the following commands:
  - **`ckp_log_collect -p`**. Runs the script and prompts you for all fields.
  - **`ckp_log_collect <profile>`**. Runs the script and collects logs using the information in the specified profile. See Using Saved Profiles (see [Using Saved Profiles](#)).
  - **`ckp_log_collect -l`**. Runs the script, prompts you to select a profile from a list of available profiles, and then collects logs using the information in the selected profile. See Using Saved Profiles (see [Using Saved Profiles](#)).
  - **`ckp_log_collect -a`**. Runs the script and calls for automatic data collection from `ckp_data_push`.
  - **`ckp_log_collect -t`**. Runs the script and prints a line to the screen every 100,000 logs, specifying the amount of time it took to extract these logs and the average rate of extraction.

Note that this rate only reflects the log extraction speed on the log server, and does not take into account the time it takes to copy the extracted records to the AFA machine.

For example, the script output may appear as follows:

```

All files from chosen: (1) = 2011-05-01_142143.log(fwm
logexport -i 2011-05-01_142143.log -n -p -z | awk -f fa_
cmd.awk >/dev/tty) >& /dev/nullProcessed record: 100000 In 4
seconds Rate: 25000 records/secProcessed record: 200000 In
6 seconds Rate: 33333 records/secProcessed record: 300000
In 8 seconds Rate: 37500 records/sec...

```

**Note:** You can view help information for the script, by entering the command **ckp\_log\_collect -h**.

The script creates a log archive file containing log extracts.

**Note:** Log collection can take a while. Please make sure that your timeout variable is large enough.

To set the it from cpshell, enter the command: **idle 999**

To set it from expert mode, enter the command: **export TMOUT=59940**

- c. If the log server is a CMA, copy the file to the Provider-1, to the same location where you placed the **ckp\_collect** script.

3. Enter the following command:

```
./ckp_collect -p
```

A list of CMAs (Customer Management Add-ons) appears with their associated IP addresses.

4. Choose the desired CMA by entering its number.

The following prompt appears on the screen:

```
Work directory is /tmp/ckp_collect
```

```
Enter 'y' if the firewall module you wish to analyze is remote.
```

```
Enter 'n' if the local machine is also the firewall module.
```

```
Do you wish to analyze a remote firewall?[y]
```

5. Enter **y**.

A list of the devices managed from the machine is displayed.

6. At the prompt, select the device number you wish to analyze.

**Note:** The default is always listed in brackets before the cursor.

A summary of your choices appears.

7. `ckp_collect` will display the chosen device to be analyzed. Enter **y** to continue.

8. `ckp_collect` will now obtain a routing table of the remote filter module using Check Point's 'cpstat' command, which uses the OPSEC AMON protocol. At the prompt, enter the IP address or DNS name of the remote filter module.

9. `ckp_collect` will collect the routing table.

10. Next, you will be asked to save the created profile of your answers for later use. Saving the profile will let you to store the answers you provided to the script just described. See section **Using Saved Profiles** below.

a. To Save the profile for later enter **y**.

**Note:** The stored profile includes the Provider-1 information.

b. Enter the name of the new profile e.g. (the name of the device is displayed by default)

The data archive file `~/fa-files/ckp-<hostname>-<date>.tar` is created. If you collected logs, the log archive file is added to the data archive file.

11. Copy `~/fa-files/ckp-<hostname>-<date>.tar` to the AFA machine.

You can now generate reports for the device. See [Add other devices and routing elements](#).

The process describe above should usually run smoothly, however, difficulties may occur due to various factors such as your device configuration. Below are some possible solutions and workarounds.

- In case the cpstat connection attempt to the remote computer fails, you will be prompted whether you wish to correct the IP address. If you choose not to correct the IP address, `ckp_collect` attempts to collect the routing table via ssh.
- If the ssh is unable to connect to the remote machine, you will be alerted of the fact and given instructions on how to manually collect the routing table:
  - a. A list of commands, based on the OS installed on the remote machine, will be displayed in order to create a routing table. Select the appropriate command, and follow the instructions.
  - b. Finish by copying the resulting file to the directory `/tmp/ckp_collect` on the Provider-1 server and run `ckp_collect` again.
- In case you entered the *wrong* operating system of the remote computer, you will be instructed to login to the remote device and check the OS with the `'uname'` command. You will then be asked to repeat the data collection process.

**Note:** The first time connect via ssh to the remote device, you may see messages regarding the authenticity of the remote device host.

**Note:** You may safely ignore messages about inappropriate `"ioctl"`.

## Check Point FireWall-1 with an Integrated Management and Filter Module

To collect the device data:

1. Log in to the device.
2. To collect device logs, do the following:
  - a. Copy the `ckp_log_collect` script (which you uncompressed in [Semi-automatic data collection scripts](#)) to the log server where the device logs are located.

This can be the management server or a CMA.

- b. Enter one of the following commands:
  - `ckp_log_collect -p`. Runs the script and prompts you for all fields.
  - `ckp_log_collect <profile>`. Runs the script and collects logs using the information in the specified profile. See [Using Saved Profiles](#).
  - `ckp_log_collect -l`. Runs the script, prompts you to select a profile from a list of available profiles, and then collects logs using the information in the selected profile. See [Using Saved Profiles](#).
  - `ckp_log_collect -a`. Runs the script and calls for automatic data collection from `ckp_data_push`.

**Note:** You can view help information for the script, by entering the command `ckp_log_collect -h`.

The script creates a log archive file containing log extracts.

**Note:** Log collection can take a while. Please make sure that your timeout variable is large enough.

To set it from `cpshell`, enter the command: `idle 999`

To set it from expert mode, enter the command: `export TMOUT=59940`

- c. If the log server is a CMA, copy the file to the management server, to the same location where you placed the `ckp_collect` script.

3. Enter the following command:

**ckp\_collect**

The following prompt appears on the screen:

```
Work directory is /tmp/ckp_collect
```

```
Enter 'y' if the firewall module you wish to analyze is remote.
```

```
Enter 'n' if the local machine is also the firewall module.
```

```
Do you wish to analyze a remote firewall?[y]
```

4. Enter **n**.

A list of policy names appears.

5. Choose the desired policy by entering its number.

**Note:** The default is always listed in brackets before the cursor.

A summary of your choices appears.

6. Confirm your choices if they are correct by selecting **y**.
7. Next, you will be asked to save the created profile of your answers for later use. Saving the profile will let you to store the answers you provided to the script just described. See **Using Saved Profiles below**.
  - a. To save the profile for later enter **y**.
  - b. Enter the name of the new profile e.g. (the name of the device is displayed by default).

The data archive file `~/fa-files/ckp-hostname-time.tar` is created. If you collected logs, the log archive file is added to the data archive file.

8. Copy `~/fa-files/ckp-hostname-time.tar` to the AFA machine.

You can now generate reports for the device. See [Setting Up Analysis from a File](#) (see [Add other devices and routing elements](#)).

## Using Saved Profiles

Collecting data entails answering many questions. Saving a profile of the answers to these questions allows you to reuse these answers without going through the whole process again.

### Using a saved profile:

- To recollect the data using a saved profile, type:

```
./ckp_collect <profile name>
```

(where profile name is the name of the saved profile). You will be prompted for your ssh password. The script will use all the stored answers to collect the data (see details in the section [Check Point FireWall-1](#) above) and an archive will be created.

#### Note:

- The saved profiles do not store your ssh password for security reasons.
- The stored profiles are located in `$home/.fa/datacollection`.
- Using this procedure will collect the default policy installed on the device.

### Listing saved profiles and choosing a saved profile:

1. Type:

```
./ckp_collect -l
```

A list of your saved profiles appears and you will be prompted to select a listed profile.

2. Choose a profile by entering its corresponding number.
3. Enter your ssh password.

The process is complete.

**Note:** To view online help, type:

```
./ckp_collect -h
```

## Windows Platform

**Note:** These procedures apply only if you have a Check Point FireWall-1 whose SmartCenter server runs on Windows. If your Windows computer is used only to run the graphical management client (SmartConsole), the Windows computer is probably *not* your SmartCenter server. In particular, if you use Check Point SecurePlatform, follow the procedures for the Sun/Nokia/SecurePlatform/Alteon/Linux platforms described in [Sun/Nokia/SecurePlatform/Alteon/Linux Platforms](#).

### Check Point FireWall-1 with Separate SmartCenter Server and Filter Module

To collect the device data:

1. Copy the batch file `ckp_collect.bat` to the Windows SmartCenter server.
2. Log in to the Windows SmartCenter server.
3. Open a Command Prompt window.
4. Enter the following command:

```
ckp_collect /remote <filter-module-IP-address>
```

**ckp\_collect** will now obtain a routing table of the remote filter module using Check Point's 'cpstat' command, which uses the OPSEC AMON protocol.

An archive file called `c:\Algosec\ckp_collect\ckp_collect.tar.gz` is created.

5. Copy `ckp_collect.tar.gz` to the AFA machine.

You can now generate reports for the device. See Setting Up Analysis from a File (see [Add other devices and routing elements](#)).

## To collect the device's routing table:

There may be situations in which the 'cpstat' command is not present or fails to retrieve the filter module's routing table. In these cases, you can extract the routing table manually, and add it to the collected archive, as follows.

1. Copy the batch file `ckp_collect.bat` to the Windows SmartCenter server.
2. Log in to the Windows SmartCenter server.
3. Open a Command Prompt window.
4. Enter the following command:  
  
**`ckp_collect /manual`**
5. You will see instructions on how to extract the routing table from each possible module platform.
6. Log in to the filter module.
7. Execute the command that is appropriate for the device's operating system, exactly as shown in step 5.
8. Copy the routing table file that is created (e.g., `netstat-rn`, `netstat-rn.lnx`, or `nokia-iclid`) to the directory `c:\Algosec\ckp_collect` on the SmartCenter server.

### Note:

1. Keep the file name exactly as it was created.
2. Use the command that is appropriate for the filter module's operating system

9. On the SmartCenter server, run the following command again:

**`ckp_collect /manual`**

An archive file called `c:\Algosec\ckp_collect\ckp_collect.tar.gz` is created.

10. Copy `ckp_collect.tar.gz` to the AFA machine.

You can now generate reports for the device. See [Setting Up Analysis from a File](#) (see [Add other devices and routing elements](#)).

### Check Point FireWall-1 with Integrated SmartCenter Server and Filter Module

To collect the device data:

1. Log in to the Windows SmartCenter server.
2. Open a Command Prompt window.
3. Enter the following command:

```
ckp_collect /local
```

Stand by while the script runs. All data files are placed in the directory

```
c:\Algosec\ckp_collect
```

 on the SmartCenter server.

4. Copy `ckp_collect.tar.gz` to the AFA machine.

You can now generate reports for the device. See [Setting Up Analysis from a File](#) (see [Add other devices and routing elements](#)).

## Cisco routers and devices

This topic describes how to collect device data semi-automatically or manually from Cisco routers and devices, ensuring that any third-party toolset collects and prepares data appropriately.

For more details, see [Alternate data collection methods](#).

### Collect data semi-automatically from Cisco IOS or Nexus routers

This procedure describes how to run the **routerdump.pl** script to obtain device data from your Cisco IOS or Nexus router.

Run this script on a single device or in bulk mode on multiple devices.

**Tip:** If you need to collect data manually, see [Collect data manually from Cisco IOS](#)

[routers.](#)

Do the following:

1. Ensure that Perl is running on the computer to which the router information will be extracted.

Perl is available on most Unix systems. If you are running Windows, install Perl. For details, see <https://www.perl.com/>.

2. Ensure that you have direct access to the device. Authenticating via CyberArk is not supported.
3. From the command line, run one of the following commands:

### Single device

To collect data from a single device, run the following:

```
routerdump.pl [-v] -u <user> -p <password> [-U <enable-user>] [-P <enable-password>] [-s <connection-type>] [-o <ssh-port>] -t <device-brand> -O <output_path router-IP>
```

Where:

- Brackets [ ] indicate optional elements.
- **-v** specifies verbose mode.
- **-u** specifies the user name.
- **-p** specifies the password.
- **-U** specifies the enable username.
- **-P** specifies the enable password.
- **-s** specifies the connection type. Default = **SSH**
- **-o** specifies the port number. Default = **22**
- **-t** specifies the device brand, and is one of the following: **nexus** or **ios**

- **-O** specifies the output file path
- *router-IP* is the router's IP address

**Example:**

```
routerdump.pl -u admin -p cisco -t nexus -O ~/test_me_now  
10.20.1.148
```

This example runs the **routerdump.pl** script on a single Nexus device with access credentials of **admin** and **cisco**.

The file is saved at **~/test\_me\_now**, and the device's IP address is **10.20.1.148**.

**Bulk mode for multiple devices**

To collect data from multiple devices in bulk, do the following:

- a. Create a CSV file to list the devices you want to collect from.

In the CSV file, reserve the first row for headlines, and then list devices using the following syntax:

```
router,brand,username,password,enable_username,enable_  
password,connection_type,ssh_port,verbose_mode
```

For example:

```
10.20.1.148,nexus,admin,cisco,,,SSH,22,V  
10.20.15.1,ios,admin,algosec,admin,algosec1,telnet,,
```

- b. Run the following:

```
routerdump.pl -b [-v] input_file
```

Where:

- **-b** specifies bulk mode
- **-v** specifies verbose mode

- *input\_file* is a CSV file that describes the devices

For example:

```
routerdump.pl -b routrdumpTest.txt
```

4. If you are prompted for a username, enter your router username.
5. At the password prompt, enter the router's Telnet password.
6. At the enable password prompt, enter the enable password.

The **routerdump.pl** script extracts the relevant router information and creates a flat ASCII file named **routername-<date>.rd**.

For example, for the router named **gw2600**, a router information file created on November 1, 2019, would be named: **gw2600-20191101.rd**.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add a static file device to AFA \(CLI\)](#).

## Collect data manually from Cisco IOS routers

If you must collect data from the router manually, construct the **.rd** file using a text editor such as vi, emacs, or gedit.

**Tip:** Alternately, use a script to collect data semi-automatically. For details, see [Collect data semi-automatically from Cisco IOS or Nexus routers](#).

Do the following:

1. Log in to the router in **enable** mode.
2. Run the commands listed below.

As you run the commands, paste the output for each command into a file editor.

Separate each output by command with the following separator syntax:

```
===== <command name> =====
```

For example, replace **iosrouter# show interface** with **===== show interface =====**.

For more details, see [Tips for copying command line output](#).

**Run the following commands:**

```
show version
show interface
show ip interface
show ipv6 interface
show ipaccess-list
show ipv6 access-list
show bgp summary | include router identifier
show running-config
show ip route
```

For IOS devices with VRFs in use, also run the following commands:

```
show ip bgp vpnv4 all labels
show ip vrf interfaces
show iproute vrf <VRF NAME>
```

For example:

```
show ip bgp vpnv4 all labels
show ip vrf interfaces
show ip route vrf vrf1
```

**Note:** The **ip rout vrf <VRF NAME>** command must be run against each unique VRF.

3. Save your file with an **.rd** file extension.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add a static file device to AFA \(CLI\)](#).

## Collect data manually from Cisco IOS-XR routers

If you must collect data from the router manually, construct the `.rd` file using a text editor such as `vi`, `emacs`, or `gedit`.

**Tip:** Alternately, use a script to collect data semi-automatically. For details, see [Collect data semi-automatically from Cisco IOS or Nexus routers](#).

Do the following:

1. Log into the Cisco IOS-XR router.
2. Run the commands listed below.

As you run the commands, paste the output for each command into a file editor.

Separate each output by command with the following separator syntax:

```
===== <command name> =====
```

For example, replace `iosxrrouter# show ip access-list` with `===== show show ip access-list=====`.

For more details, see [Tips for copying command line output](#).

Run the following commands:

```
show version
show interface
show ipv4 vrf all interface
show ipv6 interface
show ip access-list
show ipv6 access-list
show bgp summary | include router identifier
```

```
show running-config
show ip route
```

For IOS devices with VRFs in use, also run the following commands:

```
show bgp vpnv4 unicast labels
show ipv4 vrf all interface brief
show ip route vrf <VRF NAME>
```

For example:

```
show bgp vpnv4 unicast labels
show ipv4 vrf all interface brief
show ip route vrf vrf1
```

**Note:** The `ip route vrf <VRF NAME>` command must be run against each unique VRF.

3. Replace the output for `show ipv4 vrf all interface` with `show ip interface`.

For example, replace `[ios_prompt]# show ipv4 vrf all interface` with `==== show ip interface =====`.

4. Save your file with an `.rd` file extension.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add a static file device to AFA \(CLI\)](#).

## Collect data manually from Cisco Nexus routers

If you must collect data from the router manually, construct a `.nexus` file using a text editor such as `vi`, `emacs`, or `gedit`.

**Tip:** Alternately, use a script to collect data semi-automatically. For details, see [Collect data semi-automatically from Cisco IOS or Nexus routers](#).

1. Log in to the Cisco Nexus router using SSH (or Telnet), and log the session to a file.
2. Run the commands listed below.

```
show version
show interface
show ip interface
show ip access-list
show running-config
```

For NX-OS versions 5 and higher, run:

```
show vrf interface | xml
```

For NX-OS versions lower than 5, run:

```
show vrf interface
```

In all cases, continue by running:

```
show ip route
show ip route vrf all
show vrf all
show bgp vpv4 unicast labels
```

3. Edit the file created by the session recording using a text editor.

**Note:** Do not use Microsoft Word to edit this file.

Replace each command line with a separator.

For example, replace **nexusfirewall# show version** with **=== show version ===**.

When replacing the **nexusfirewall# show ip access-list** and **nexusfirewall# show running-config** lines, replace the hyphen (-) with a space.

4. Save your file with an **.nexus** file extension.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add a static file device to AFA \(CLI\)](#).

## Collect data manually from Cisco ASA devices

This procedure describes how to collect data manually from Cisco ASA devices. AlgoSec does not provide semi-automatic scripts for ASA devices.

Do the following:

1. Log into the ASA firewall using SSH (or Telnet), and log the session to a file.
2. Switch to **enable** mode by entering **enable** and the enable password.
3. Run the following commands:

```
show version
show running-config
```

If you use dynamic routing, run:

```
show route
```

In all cases, run:

```
show access-list
exit
```

4. Edit the file created by the session recording using a text editor.

**Note:** Do not use Microsoft Word to edit this file.

Replace each command line with separators, as follows:

Replace...	With...
<b>asafirewall# show access-list</b>	<b>=== show access list ===</b> Make sure to replace the hyphen (-) with a space.
<b>asafirewall# show route</b>	<b>=== show route ===</b>

5. Save your file with an **.pix** file extension.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add a static file device to AFA \(CLI\)](#).

## Tips for copying command line output

When creating \*.rd files for manual data collection, we recommend doing the following to ensure that you copy the correct data:

- Set the terminal emulator display to be wide enough so lines don't get truncated or wrapped.
- Make sure you grab the whole output of each command. You'll need a large history buffer in your terminal emulator so you can scroll up.
- Make sure not to copy any pager prompts such as **More...**

## Juniper devices

This topic describes how to collect data semi-automatically or manually from Juniper devices, ensuring that any third-party toolset collects and prepares data appropriately.

For more details, see [Alternate data collection methods](#).

## Collect device data semi-automatically from Juniper Netscreen devices

This procedure describes how to collect device configuration files from Juniper Netscreen devices and use them to collect data for AFA.

**Note:** By default, reports generated from these configuration files do not contain optimization data based on log analysis, such as unused, most used, and least used rules, rule reordering optimization, unused objects, and unused objects within rules. To generate reports that generate log-based optimization information, use the **nsm\_log\_collect** script to collect those device logs.

Do the following:

1. In your browser, connect to the Netscreen device and navigate to **Configuration > Update > Config file**.
2. Click **Save To File**.
3. When prompted, save the file with an **.nsc** extension. For example, **myNetscreen.nsc**.
4. To collect device logs, do the following:
  - a. Copy the **nsm\_log\_collect** script to the relevant NSM server.
  - b. Enter one of the following commands:

<b>nsm_log_collect</b>	Runs the script and prompts you for all fields.
<b>nsm_log_collect &lt;profile&gt;</b>	Runs the script and collects logs using the information in the specified profile. For details, see <a href="#">Using Saved Profiles</a> .
<b>nsm_log_collect -l</b>	Runs the script, prompts you to select a profile from a list of available profiles, and then collects logs using the information in the selected profile. For details, see <a href="#">Using Saved Profiles</a> .

**Note:** View help information for the script by entering **nsm\_log\_collect -h**.

The script creates a log archive file containing log extracts.

- c. Add both the log file and the Netscreen device's configuration to a new **.zip** or **.tar** file.

5. Do one of the following:

<b>If you only collected the Netscreen configuration file</b>	Copy the <b>*.nsc</b> file to the AFA machine.
<b>If you collected both the Netscreen configuration file and device logs</b>	Copy the archive file to the AFA machine.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add other devices and routing elements](#).

## Collect data manually from Juniper Netscreen devices

This procedure describes how to collect data manually from Juniper Netscreen devices.

**Note:** Alternately, collect data semi-automatically using files accessed from your device interface.

For details, see [Collect device data semi-automatically from Juniper Netscreen devices](#).

Do the following:

1. Log in to the Netscreen device using SSH and log the session to a file.
2. Run the following commands:

```
get system | include Software
get system | include System
get config get service pre-defined
```

If you are analyzing a VSYS, run the following:

```
vsys vsys_name
```

In all cases, run:

```
get route
exit
```

3. Edit the file created by the session recording using a text editor.

**Note:** Do not use Microsoft Word to edit this file.

Replace the following strings:

Replace...	With...
Firewall_name-> get system   include Software	===== NETSCREEN VERSION =====
Firewall_name-> get system   include System	===== SYSTEM MODE =====
Firewall_name-> get config	===== get config =====
Firewall_name-> get service pre-defined	===== get service pre-defined =====
Firewall_name-> get route	===== get route =====
Firewall_name-> enter vsys vsys_name	===== enter vsys vsys_name =====

4. Save the file with an **.nsc** extension.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add other devices and routing elements](#).

## Collect data manually from Juniper M/MX routers

This procedure describes how to collect data manually from Juniper SRX routers.

Do the following:

1. Log into the SRX firewall using SSH (or Telnet), and log the session to a file.
2. Run the following commands:

```
cli
```

```
set cli logical-system <logical-system name>
show configuration | display inheritance | no-more
show route active-path all | no-more
clear cli logical-system
show version | no-more
exit
exits
```

3. Edit the file created by the session recording using a text editor.

**Note:** Do not use Microsoft Word to edit this file.

Replace each command line with a separator.

For example, replace `[junosmxdevice]> show configuration | display inheritance | no-more` with `=== show configuration | display inheritance | no-more ===`.

Replace...	With...
<code>root@srx_firewall&gt; show configuration</code>	<code>=== show configuration ===</code>
If dynamic routing is used: <code>root@srx_firewall&gt; show route extensive all</code>	<code>=== show route extensive all ===</code>
<code>root@srx_firewall&gt; show configuration groups junos-defaults applications</code>	<code>=== show configuration groups junos-defaults applications ===</code>

4. Save the file with an `.junosmxrouterfile` extension.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add other devices and routing elements](#).

## Collect data manually from Juniper SRX devices

This procedure describes how to collect data manually from Juniper SRX devices.

Do the following:

- 1. Log into the SRX firewall using SSH (or Telnet), and log the session to a file.
- 2. Run the following commands:

```
cli
show configuration
```

When dynamic routing is used, run:

```
show route extensive all
```

In all cases, run:

```
show configuration groups junos-defaults applications
exit
```

- 3. Edit the file created by the session recording using a text editor.

**Note:** Do not use Microsoft Word to edit this file.

Replace each command line with separators, as follows:

Replace...	With...
root@srx_firewall> show configuration	=== show configuration ===
If dynamic routing is used: root@srx_firewall> show route extensive all	=== show route extensive all ===
root@srx_firewall> show configuration groups junos-defaults applications	=== show configuration groups junos-defaults applications ===

- 4. Save the file with an .srx extension.

Use the file created to add the device to AFA and generate AFA reports. For details, see [Add other devices and routing elements](#).

## Fortinet Fortigate (manual)

**Note:** If the device has several VDOMs, the following procedure should be implemented for each VDOM in separate, hence a separate file for each VDOM.

1. Log into the FortiGate firewall using SSH (or Telnet), and log the session to a file.
2. Run the following commands:

```
config global
get system status
show full-configuration | grep ''
end
```

3. If there are one or more VDOMs configured on the device, run the following additional command:

```
config vdom
```

4. Run the following additional commands for each VDOM:

```
edit
get system status
show full-configuration | grep ''
```

5. If dynamic routing is used, run one of the following commands (depending if the user is read-only or not):

```
diagnose ip route list | grep ''
get router info kernel | grep '
end
```

6. Run the following command:

```
exit
```

7. Edit the file with the session recording. Use a text editor such as 'notepad' or 'WordPad', but **not** Microsoft Word.
8. Replace the line:

```
FortiGateFirewall (global) # show full-configuration
```

with:

```
=== show full-configuration ===
```

**Note:** Start in the 1st column; use the exact syntax, with one space between each two words. This is necessary for all of the following replacements as well.

9. Replace the line (if applicable):

```
FortiGateFirewall (vdom_name) # get system status
```

with:

```
=== get system status ===
```

10. Replace the line (if applicable):

```
FortiGateFirewall (vdom_name) # show full-configuration
```

with:

```
=== show full-configuration ===
```

11. Replace the line (if applicable):

```
FortiGateFirewall (vdom_name) # diagnose ip route list
```

with:

```
=== diagnose ip route list ===
```

12. Save the file with **.fortigate** file type.

Upload the file to AFA using **Analyze from File**. For details, see [Add other devices and routing elements](#).

## Palo Alto Networks (manual)

1. Log into the Palo Alto firewall using SSH (or Telnet), and log the session to a file.
2. Run the following commands:

**set cli pager offshow config runningconfigshow predefinedexit**

**show config pushed** (please see the note below regarding this command)

**show system info**show routing fibexit

**Note:** The **show config pushed** command is required only when using Panorama to manage the device. Issuing this command requires super-user privileges on the Palo Alto Networks device. If Panorama is not used, this command should be omitted.

If the Palo Alto device is version 5 or above, replace this command with:

**show config pushed-shared-policy**

If the analysis you want to perform is on a Palo Alto vsys configuration enter one of the following commands:

- **show config pushed vsys**, if the version is under 5.0.
- **show config pushed-shared-policy vsys** if the version is 5.0 or above.

where *vsys* is the internal name (e.g. "vsys1" rather than "Georgia\_vsys").

3. Edit the file with the session recording. Use a text editor such as 'notepad' or 'WordPad', but **not** Microsoft Word.

4. Replace the line:

```
admin@PA-2020# show config running
```

with:

```
=== show config running ===
```

**Note:** Start in the 1st column; use the exact syntax, with one space between each two words. This is necessary for all of the following replacements as well.

5. Replace the line:

```
admin@PA-2020# show predefined
```

with:

```
=== show predefined ===
```

6. Replace the line:

```
admin@PA-2020# show config pushed (or the alternatives as specified above)
```

with:

```
=== show config pushed ===
```

7. Replace the line:

```
admin@PA-2020> show system info
```

with:

```
=== show system info ===
```

8. Replace the line:

```
admin@PA-2020> show routing fib
```

with:

```
=== show routing fib ===
```

9. Save the file with .paloalto file type.

Upload the file to AFA using **Analyze from File**. See [Add other devices and routing elements](#).

## McAfee Firewall Enterprise (Sidewinder) (manual)

This section describes how to collect device data manually from a McAfee Firewall Enterprise (Forcepoint Sidewinder) devices.

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

Do the following:

1. Log into the Sidewinder firewall using SSH (or Telnet), and log the session to a file using the following command:

```
ssh @ | tee -ia
```

2. Run the following commands:

```
sroleecho "VERSION_NUMBER:" `uname -r` cf policy export type=rulecf policy  
export type=net_object
```

```
cf service query (for version 7)
```

```
cf application query (for version 8)
```

```
cf appdb list verbose=on (for version 8)
```

```
cf interface query
```

```
cf burb query (for version 7)
```

```
cf burbgroup query (for version 7)
```

```
netstat -rncf usergroup querycf hostname querycf timeperiod query
```

```
cf zone query (for version 8)
```

**cf zonegroup query** (for version 8)

**cf ipsec query**  
**cf policy query**  
**exit**

3. Edit the file with the session recording. Use a text editor such as 'notepad' or 'WordPad', but **not** Microsoft Word.

4. At the head of the page add the line:

```
# Connecting to:
```

5. In the file, perform the following find and replaces. Start in the 1st column; use the exact syntax, with one space between each two words.

Find	Replace
:Admn {1} % echo "VERSION_NUMBER:" `uname -r`	=== echo "VERSION_NUMBER:" `uname -r` ===
:Admn {2} % cf policy export type=rule	=== cf policy export type=rule ===
:Admn {3} % cf policy export type=net_object	=== cf policy export type=net_ object ===
<b>Sidewinder 7 only</b> :Admn {4} % cf service query	=== cf service query ===
<b>Sidewinder 8 only</b> :Admn {5} % cf application query	=== cf application query ===
<b>Sidewinder 8 only</b> :Admn {6} % cf appdb list verbose=on	=== cf appdb list verbose=on ===
<b>Sidewinder 7 only</b> :Admn {5} % cf interface query	=== cf interface query ===
<b>Sidewinder 7 only</b> :Admn {6} % cf burb query	=== cf burb query ===
<b>Sidewinder 7 only</b> :Admn {7} % cf burbgroup query	=== cf burbgroup query ===

Find	Replace
:Admn {8} % netstat -rn	=== netstat -rn ===
:Admn {9} % cf usergroup query	=== cf usergroup query ===
:Admn {10} % cf hostname query	=== cf hostname query ===
:Admn {11} % cf timeperiod query	=== cf timeperiod query ===
<b>Sidewinder 8 only</b> :Admn {11} % cf zone query	=== cf zone query ===
<b>Sidewinder 8 only</b> :Admn {12} % cf zonegroup query	=== cf zonegroup query ===
:Admn {12} % cf ipsec query	=== cf ipsec query ===
:Admn {13} % cf policy query	=== cf policy query ===

6. Save the file with the **.sidewinder** extension.
7. Upload the file to AFA using the Analyze from File option. For details, see [Add other devices and routing elements](#).

## Symantec Blue Coat (manual)

1. Log into the Symantec BlueCoat SGOS device using SSH, enter enable mode and log the session to a file.
2. Run the following commands:

```
show appliance-name
show version
show interface all
show configuration noprompts
configure
content-filter
categories
exit
```

```
exit
```

3. Edit the file with the session recording. Use a text editor such as 'notepad' or 'WordPad', but **not** Microsoft Word.
4. Replace the line:

```
admin@SGOS> show appliance-name
```

with:

```
=== show appliance-name ===
```

**Note:** Start in the 1st column; use the exact syntax, with one space between each two words. This is necessary for all of the following replacements as well.

5. Replace the line:

```
admin@SGOS> show version
```

with:

```
=== show version ===
```

6. Replace the line:

```
admin@SGOS> show interface all
```

with:

```
=== show interface all ===
```

7. Replace the line:

```
admin@SGOS> show configuration noprompts
```

with:

```
=== show configuration noprompts ===
```

8. Save the file with **.bluecoat** file type.

Upload the file to AFA using **Analyze from File**. For details, see [Add other devices and routing elements](#).

# 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](#).

To enable support for Huawei devices, install the Huawei provided plug-in using the information in this [AlgoPedia article](#).

## Static configuration file support

You provide a JSON file which represents the device's configuration. This option provides full support in AFA, FireFlow, and BusinessFlow. 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 file>'
```

### Tag list

Tag	Description
config_type	The policy model.

Tag	Description
device	The definition of the device.
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](#)
- [Generic Device JSON File Examples](#)
- [Static support troubleshooting](#)

## Tag Reference

**Note: 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 [Generic Device JSON File Examples](#)).

## 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	<b>1</b> or <b>0</b> . 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><b>Note:</b> The name of the rule group should be the same as the rule group id value in rule_group tag.</p> <p><b>Note:</b> This parameter is only relevant for INTERFACE_BASED configuration.</p>

## services

Parameter	Description
name	Service name.
service_definitions	<p>List of service definitions in the following format:</p> <pre>protocol: The protocol name: tcp/udp/icmp/any/protocol number.</pre> <ul style="list-style-type: none"> <li>• <b>src_port:</b> The <b>source port number/source port range (if there is no source port, or range is any, it will be *)/ICMP type.</b> (optional)</li> </ul> <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: <b>static/dynamic</b> .
dst_nat	List of destination NAT hosts/addresses.
dst_nat_type	Destination NAT type - one of the values: <b>static/dynamic</b> .
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: `ddMMMyyyy, HHmm`.
end_date	End date in format of: `ddMMMyyyy, HHmm`.

## Generic Device JSON File Examples

The following are three examples of JSON files for a generic device.

### JSON File Example for a Policy-Based Device

```
{
  "config_type" : "POLICY_BASED",
  "device" : {
    "name" : "Francesca",
    "hostname" : "",
    "policy" : "new_policy, Firewall Template 1"
  },
  "services" : {
    "Address Mask Reply (Any Code)" : {
      "name" : "Address Mask Reply (Any Code)",
      "service_definitions" : [
        {
          "protocol" : "icmp",
          "src_port" : "18",
          "dst_port" : "0"
        }
      ],
      "type" : "ICMP",
      "comment" : "\"Address mask reply\" messages with any code."
    },
    "Comodo-OCSP" : {
      "name" : "Comodo-OCSP",
```

```

"service_definitions" : [
{
"protocol" : "tcp",
"src_port" : "80",
"dst_port" : "0"
}
],
"type" : "APPLICATION",
"comment" : "Comodo Online Certificate Status service usage detected"
},
},
"services_groups" : {
"Ping" : {
"name" : "Ping",
"members" : [
"Echo Request (Any Code)"
]
},
"H.323" : {
"name" : "H.323",
"members" : [
"H.323 (Call Signaling)",
"T.120"
]
},
},
"hosts" : {
"ALL-SYSTEMS.MCAST.NET" : {
"name" : "ALL-SYSTEMS.MCAST.NET",
"type" : "IP_ADDRESS",
"ips" : [
"224.0.0.1/32"

```

```

]
},
"DHCP Broadcast Destination" : {
  "name" : "DHCP Broadcast Destination",
  "type" : "IP_ADDRESS",
  "ips" : [
    "255.255.255.255/32"
  ]
},
"Microsoft Lync Online Servers 19" : {
  "name" : "Microsoft Lync Online Servers 19",
  "type" : "IP_RANGE",
  "ips" : [
    "66.119.158.0-66.119.158.127"
  ]
},
},
"hosts_groups" : {
  "Microsoft Ex-Fed servers" : {
    "name" : "Microsoft Ex-Fed servers",
    "members" : [ ],
    "type" : "GROUP"
  },
  "Microsoft Exchange Online Protection servers" : {
    "name" : "Microsoft Exchange Online Protection servers",
    "members" : [
      "Microsoft Exchange Online Protection Servers 1",
      "Microsoft Exchange Online Protection Servers 10",
      "Microsoft Exchange Online Protection Servers 11",
      "Microsoft Exchange Online Protection Servers 12",
      "Microsoft Exchange Online Protection Servers 13",
      "Microsoft Exchange Online Protection Servers 14",

```

```
"Microsoft Exchange Online Protection Servers 15",  
"Microsoft Exchange Online Protection Servers 16",  
"Microsoft Exchange Online Protection Servers 17",  
"Microsoft Exchange Online Protection Servers 18",  
"Microsoft Exchange Online Protection Servers 19",  
"Microsoft Exchange Online Protection Servers 2",  
"Microsoft Exchange Online Protection Servers 20",  
"Microsoft Exchange Online Protection Servers 21",  
"Microsoft Exchange Online Protection Servers 22",  
"Microsoft Exchange Online Protection Servers 23",  
"Microsoft Exchange Online Protection Servers 24",  
"Microsoft Exchange Online Protection Servers 25",  
"Microsoft Exchange Online Protection Servers 26",  
"Microsoft Exchange Online Protection Servers 27",  
"Microsoft Exchange Online Protection Servers 28",  
"Microsoft Exchange Online Protection Servers 29",  
"Microsoft Exchange Online Protection Servers 3",  
"Microsoft Exchange Online Protection Servers 30",  
"Microsoft Exchange Online Protection Servers 31",  
"Microsoft Exchange Online Protection Servers 32",  
"Microsoft Exchange Online Protection Servers 33",  
"Microsoft Exchange Online Protection Servers 34",  
"Microsoft Exchange Online Protection Servers 35",  
"Microsoft Exchange Online Protection Servers 36",  
"Microsoft Exchange Online Protection Servers 37",  
"Microsoft Exchange Online Protection Servers 38",  
"Microsoft Exchange Online Protection Servers 4",  
"Microsoft Exchange Online Protection Servers 5",  
"Microsoft Exchange Online Protection Servers 6",  
"Microsoft Exchange Online Protection Servers 7",  
"Microsoft Exchange Online Protection Servers 8",  
"Microsoft Exchange Online Protection Servers 9"
```

```

],
"type" : "GROUP"
},
},
"hosts_v6" : {
  "All Routers (Interface-Local)" : {
    "name" : "All Routers (Interface-Local)",
    "type" : "IP_ADDRESS",
    "ips" : [
      "FF01::1"
    ]
  },
  "All Routers (Link-Local)" : {
    "name" : "All Routers (Link-Local)",
    "type" : "IP_ADDRESS",
    "ips" : [
      "FF02::2"
    ]
  },
},
},
"policies" : {
  "160" : {
    "rule_id" : "160",
    "rule_name" : "160.0",
    "rule_display_name" : "160.0",
    "rule_num" : "1",
    "line_number" : "0",
    "policy" : "Firewall Template 1",
    "type" : "Template",
    "enable" : "enabled",
    "src" : [
      "ANY"
    ]
  }
}

```

```

],
"dst" : [
  "ANY"
  "DNS (UDP)"
],
"action" : "continue",
"additional_properties" : {
  "scope" : "before"
}
},
"161" : {
  "rule_id" : "161",
  "rule_name" : "161.0",
  "rule_display_name" : "161.0",
  "rule_num" : "2",
  "line_number" : "0",
  "policy" : "Firewall Template 1",
  "type" : "Template",
  "enable" : "enabled",
  "src" : [
    "NOT Loopback network"
  ],
  "dst" : [
    "Loopback network"
  ],
  "service" : [
    "ANY"
  ],
  "action" : "discard",
  "log" : "1",
  "additional_properties" : {
    "logging" : "Stored",

```

```

"scope" : "before"
}
},
},
"nat_rules" : {
  "167" : {
    "rule_id" : "167",
    "rule_name" : "167.0",
    "rule_display_name" : "167.0",
    "rule_num" : "1",
    "line_number" : "0",
    "policy" : "Firewall Template 1",
    "type" : "Template",
    "action" : "allow",
    "enable" : "enabled",
    "src" : [
      "ANY"
    ],
    "dst" : [
      "DHCP Broadcast Destination",
      "Localhost"
    ],
    "service" : [
      "ANY"
    ],
    "src_nat_type" : "STATIC",
    "dst_nat_type" : "STATIC"
  }
},
"policies_v6" : {
  "169" : {
    "rule_id" : "169",

```

```

"rule_name" : "169.0",
"rule_display_name" : "169.0",
"rule_num" : "1",
"line_number" : "0",
"policy" : "Firewall Template 1",
"type" : "Template",
"enable" : "enabled",
"src" : [
  "ANY"
],
"dst" : [
  "ANY"
],
"service" : [
  "DNS (UDP)"
],
"action" : "continue",
"additional_properties" : {
  "scope" : "after"
}
},
"170" : {
  "rule_id" : "170",
  "rule_name" : "170.0",
  "rule_display_name" : "170.0",
  "rule_num" : "2",
  "line_number" : "0",
  "policy" : "Firewall Template 1",
  "type" : "Template",
  "enable" : "enabled",
  "src" : [
    "ANY"

```

```

],
"dst" : [
"ANY"
],
"service" : [
"IPv6 Neighbor Advertisement",
"IPv6 Neighbor Solicitation",
"IPv6 Redirect",
"IPv6 Router Advertisement",
"IPv6 Router Solicitation"
],
"action" : "allow",
"additional_properties" : {
"scope" : "after"
}
},
},
"interfaces" : {
"NDI-0-192.168.7.24" : {
"name" : "NDI-0-192.168.7.24",
"zone" : "DMZ",
"hwdevice" : "0",
"ips" : [
"192.168.7.24/24"
]
},
"NDI-1-9.9.9.8" : {
"name" : "NDI-1-9.9.9.8",
"zone" : "Internal",
"hwdevice" : "1",
"ips" : [
"9.9.9.8/24"
]
}
}
}

```

```

]
},
"NDI-2-5.5.5.4" : {
  "name" : "NDI-2-5.5.5.4",
  "zone" : "Internal",
  "hwdevice" : "2",
  "ips" : [
    "5.5.5.4/24"
  ]
},
"device_interfaces" : {
  "NDI-0-192.168.7.24" : {
    "name" : "NDI-0-192.168.7.24",
    "ips" : [
      "192.168.7.24"
    ]
  },
  "NDI-1-9.9.9.8" : {
    "name" : "NDI-1-9.9.9.8",
    "ips" : [
      "9.9.9.8"
    ]
  },
  "NDI-2-5.5.5.4" : {
    "name" : "NDI-2-5.5.5.4",
    "ips" : [
      "5.5.5.4"
    ]
  }
},
"zones" : {

```

```

"DMZ" : {
  "name" : "DMZ",
  "interfaces" : [
    "NDI-0-192.168.7.24"
  ],
  "description" : "Interfaces connected to DMZ networks"
},
"External" : {
  "name" : "External",
  "interfaces" : [ ],
  "description" : "Interfaces connected to the Internet or other external
networks"
},
"Guest" : {
  "name" : "Guest",
  "interfaces" : [ ],
  "description" : "Interfaces connected to guest networks"
},
"Internal" : {
  "name" : "Internal",
  "interfaces" : [
    "NDI-1-9.9.9.8",
    "NDI-2-5.5.5.4"
  ],
  "description" : "Interfaces connected to internal networks"
},
"Node-internal" : {
  "name" : "Node-internal",
  "interfaces" : [ ],
  "description" : "Firewall nodes themselves"
}
},

```

```

"routes" : {
  "1" : {
    "id" : "1",
    "route" : "0.0.0.0",
    "route_mask" : "0.0.0.0",
    "gateway" : "192.168.7.254",
    "interface" : "0"
  }
}

```

## JSON File Example for an Interface-Based Device

```

{
  "config_type" : "INTERFACES_BASED",
  "device" : {
    "name" : "i-91d8adbe",
    "version" : "",
    "policy" : "GROUP_1, TestGroup, acl-a22588c7",
    "major_version" : "",
    "protected_cloud_host_ips" : [ "172.31.50.24" ],
    "public_ip" : "",
    "private_ip" : "172.31.50.24"
  },
  "policies" : {
    "745e667b82c09f32e08b7ede79cd0827" : {
      "service" : [ "tcp/8080" ],
      "direction" : "inbound",
      "action" : "deny",
      "enable" : "enabled",
      "log" : 0,
      "rule_id" : "745e667b82c09f32e08b7ede79cd0827",
      "rule_name" : "745e667b82c09f32e08b7ede79cd0827",

```

```

"rule_display_name" : "200",
"line_number" : 0,
"rule_num" : 2,
"rule_grp" : "acl-a22588c7",
"src" : [ "8.8.0.0/16" ],
"dst" : [ "Host" ],
"src_negate" : 0,
"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",
"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"additional_properties" : { }
},
"ce2ead998e1591cb9cc8bd70a21f7f6e" : {
"service" : [ "icmp/*" ],
"direction" : "outbound",
"action" : "allow",
"enable" : "enabled",
"log" : 0,
"rule_id" : "ce2ead998e1591cb9cc8bd70a21f7f6e",
"rule_name" : "ce2ead998e1591cb9cc8bd70a21f7f6e",
"line_number" : 0,
"rule_num" : 13,
"rule_grp" : "GROUP_1",
"src" : [ "Host" ],
"dst" : [ "80.1.1.88/32" ],
"src_negate" : 0,

```

```

"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",
"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"additional_properties" : { }
},
"6dec3120ea84e60b382675f690705f96" : {
"service" : [ "tcp/8080" ],
"direction" : "outbound",
"action" : "allow",
"enable" : "enabled",
"log" : 0,
"rule_id" : "6dec3120ea84e60b382675f690705f96",
"rule_name" : "6dec3120ea84e60b382675f690705f96",
"rule_display_name" : "200",
"line_number" : 0,
"rule_num" : 5,
"rule_grp" : "acl-a22588c7",
"src" : [ "Host" ],
"dst" : [ "10.20.0.0/16" ],
"src_negate" : 0,
"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",

```

```

"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"additional_properties" : { }
},
"7a066e3eb1bc600dac42a35bd8b5d736" : {
"service" : [ "tcp/143" ],
"direction" : "inbound",
"action" : "allow",
"enable" : "enabled",
"log" : 0,
"rule_id" : "7a066e3eb1bc600dac42a35bd8b5d736",
"rule_name" : "7a066e3eb1bc600dac42a35bd8b5d736",
"line_number" : 0,
"rule_num" : 18,
"rule_grp" : "TestGroup",
"src" : [ "0.0.0.0/0" ],
"dst" : [ "Host" ],
"src_negate" : 0,
"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",
"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"additional_properties" : { }
}
},
"hosts" : {

```

```

"959234629017/sg-4cb53a2a" : {
  "name" : "959234629017/sg-4cb53a2a",
  "comment" : "Allow SSH/HTTP(S)",
  "ips" : [ "172.31.52.241" ],
  "negate" : false,
  "type" : "INTERNAL",
  "is_negate" : false
},
"959234629017/sg-d9b4edbc" : {
  "name" : "959234629017/sg-d9b4edbc",
  "comment" : "Yarin",
  "ips" : [ "172.31.50.24", "172.31.7.212", "172.31.33.73", "172.31.33.70" ],
  "negate" : false,
  "type" : "INTERNAL",
  "is_negate" : false
},
"959234629017/sg-d5c47cad" : {
  "name" : "959234629017/sg-d5c47cad",
  "comment" : "1234",
  "ips" : [ "172.31.52.241" ],
  "negate" : false,
  "type" : "INTERNAL",
  "is_negate" : false
},
"959234629017/sg-fec47c86" : {
  "name" : "959234629017/sg-fec47c86",
  "comment" : "1234",
  "ips" : [ "10.2.0.166" ],
  "negate" : false,
  "type" : "INTERNAL",
  "is_negate" : false
}

```

```

},
"Host" : {
  "name" : "Host",
  "comment" : "i-91d8adbe",
  "ips" : [ "172.31.50.24", "172.31.50.24" ],
  "negate" : false,
  "type" : "INTERNAL",
  "is_negate" : false
},
"959234629017/sg-a60f57c0" : {
  "name" : "959234629017/sg-a60f57c0",
  "comment" : "launch-wizard-2",
  "ips" : [ "10.2.0.166" ],
  "negate" : false,
  "type" : "INTERNAL",
  "is_negate" : false
},
"959234629017/sg-0c683b69" : {
  "name" : "959234629017/sg-0c683b69",
  "comment" : "launch-wizard-1",
  "ips" : [ "172.31.33.73", "172.31.33.70" ],
  "negate" : false,
  "type" : "INTERNAL",
  "is_negate" : false
},
"959234629017/sg-3ee52c5a" : {
  "name" : "959234629017/sg-3ee52c5a",
  "comment" : "Test1",
  "ips" : [ "172.31.50.24", "172.31.7.212", "172.31.33.73", "172.31.33.70" ],
  "negate" : false,
  "type" : "INTERNAL",

```

```

"is_negate" : false
},
"959234629017/sg-21683b44" : {
"name" : "959234629017/sg-21683b44",
"comment" : "default",
"ips" : [ "172.31.52.241" ],
"negate" : false,
"type" : "INTERNAL",
"is_negate" : false
}
},
"interfaces" : {
"internal" : {
"name" : "internal",
"enable" : "enabled",
"ips" : [ "layer2" ],
"rules_groups" : [ "TestGroup", "GROUP_1" ]
},
"external" : {
"name" : "external",
"enable" : "enabled",
"ips" : [ "layer2" ],
"rules_groups" : [ "acl-a22588c7" ]
}
},
"routes" : {
"0" : {
"id" : 0,
"route" : "0.0.0.0",
"gateway" : "0.0.0.0",
"interface_name" : "external",
"route_mask" : "0.0.0.0"
}
}
}

```

```

},
"1" : {
  "id" : 1,
  "route" : "172.31.50.24",
  "gateway" : "-",
  "interface_name" : "internal",
  "route_mask" : "255.255.255.255"
}
},
"rules_groups" : {
  "TestGroup" : {
    "id" : "sg-3ee52c5a",
    "name" : "TestGroup",
    "enable" : "enabled",
    "comments" : "TestGroup",
    "type" : "SECURITY_GROUP",
    "rule_display_name" : "TestGroup",
    "owner_id" : "959234629017",
    "vpc_id" : "vpc-4dbb1128"
  },
  "GROUP_1" : {
    "id" : "sg-d9b4edbc",
    "name" : "Yarin",
    "enable" : "enabled",
    "comments" : "GROUP_1 test",
    "type" : "SECURITY_GROUP",
    "rule_display_name" : "GROUP_1",
    "owner_id" : "959234629017",
    "vpc_id" : "vpc-4dbb1128"
  },
  "acl-a22588c7" : {
    "id" : "acl-a22588c7",

```

```

    "name" : "TEST_NACL",
    "enable" : "enabled",
    "type" : "NACL",
    "rule_display_name" : "TEST_NACL",
    "vpc_id" : "vpc-4dbb1128"
  }
},
}

```

## JSON File Example for a Zone-Based Device

```

{
}

```

```

{
  "device" : {
    "name" : "Lieberman",
    "hostname" : "Lieberman",
    "mode" : "layer3",
    "version" : "5.2.5,build701",
    "serial" : "FG100D3G13808144",
    "domain" : "PT_domain",
    "major_version" : "5.0",
    "protected_cloud_host_ips" : [ ],
    "is_layer2" : 0
  },
  "policies" : {
    "1073741825" : {
      "service" : [ "gALL" ],
      "action" : "deny",
      "enable" : "enabled",
      "log" : 0,
      "comments" : "TreeSource",

```

```

"rule_id" : "1073741825",
"rule_name" : "1073741825",
"rule_display_name" : "1073741825",
"line_number" : 1,
"rule_num" : 1,
"rule_grp" : "before",
"src" : [ "gnone" ],
"dst" : [ "gappstore" ],
"src_negate" : 0,
"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_zone" : [ "any" ],
"dst_zone" : [ "any" ],
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",
"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"security-profiles" : { },
"target" : [ ],
"additional_properties" : { }
},
"1074741826" : {
"service" : [ "gALL" ],
"action" : "accept",
"enable" : "disabled",
"log" : 0,
"comments" : "",
"rule_id" : "1074741826",
"rule_name" : "1074741826",

```

```

"rule_display_name" : "1074741826",
"line_number" : 5,
"rule_num" : 5,
"rule_grp" : "after",
"src" : [ "gnone" ],
"dst" : [ "gadobe" ],
"src_negate" : 0,
"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_zone" : [ "any" ],
"dst_zone" : [ "any" ],
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",
"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"security-profiles" : { },
"target" : [ ],
"additional_properties" : { }
},
"1073741827" : {
"service" : [ "service_5" ],
"action" : "deny",
"enable" : "enabled",
"log" : 0,
"comments" : "",
"rule_id" : "1073741827",
"rule_name" : "1073741827",
"rule_display_name" : "1073741827",
"line_number" : 2,

```

```

"rule_num" : 2,
"rule_grp" : "before",
"src" : [ "AddressGlobal1" ],
"dst" : [ "address_5" ],
"src_negate" : 0,
"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_zone" : [ "any" ],
"dst_zone" : [ "any" ],
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",
"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"security-profiles" : { },
"target" : [ ],
"additional_properties" : { }
},
"1073741828" : {
"service" : ["service_5" ],
"action" : "deny",
"enable" : "disabled",
"log" : 0,
"comments" : "",
"rule_id" : "1073741828",
"rule_name" : "1073741828",
"rule_display_name" : "1073741828",
"line_number" : 3,
"rule_num" : 3,
"rule_grp" : "before",

```

```

"src" : [ "address_5" ],
"dst" : [ "address_5" ],
"src_negate" : 0,
"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_zone" : [ "any" ],
"dst_zone" : [ "any" ],
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",
"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"security-profiles" : { },
"target" : [ ],
"additional_properties" : { }
},
"1074741825" : {
"service" : [ "gGOPHER" ],
"action" : "deny",
"enable" : "enabled",
"log" : 0,
"comments" : "",
"rule_id" : "1074741825",
"rule_name" : "1074741825",
"rule_display_name" : "1074741825",
"line_number" : 4,
"rule_num" : 4,
"rule_grp" : "after",
"src" : [ "33_Global" ],
"dst" : [ "address_5" ],

```

```

"src_negate" : 0,
"dst_negate" : 0,
"object_nat_source" : false,
"object_nat_destination" : false,
"src_zone" : [ "any" ],
"dst_zone" : [ "any" ],
"src_nat" : [ ],
"dst_nat" : [ ],
"nat" : "enabled",
"global_nat" : "enabled",
"map_source_to_interface" : false,
"bi-directional" : 0,
"security-profiles" : { },
"target" : [ ],
"additional_properties" : { }
}
},
"hosts" : {
"ip-10.150.191.25" : {
"name" : "ip-10.150.191.25",
"comment" : "",
"ips" : [ "10.150.191.25/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"google-play" : {
"name" : "google-play",
"comment" : "",
"ips" : [ "82.102.155.49" ],
"negate" : false,

```

```

"type" : "DOMAIN",
"is_negate" : false,
"object_container" : "device_group"
},
"10.30.193.1" : {
"name" : "10.30.193.1",
"comment" : "",
"ips" : [ "10.30.193.1/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.192.28" : {
"name" : "ip-10.30.192.28",
"comment" : "",
"ips" : [ "10.30.192.28/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.120.191.44" : {
"name" : "ip-10.120.191.44",
"comment" : "",
"ips" : [ "10.120.191.44/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"none" : {

```

```

"name" : "none",
"comment" : "",
"ips" : [ "0.0.0.0/0" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"Addr" : {
"name" : "Addr",
"comment" : "",
"ips" : [ "1.2.3.4/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"Address_2" : {
"name" : "Address_2",
"comment" : "",
"ips" : [ "1.1.1.1-20.20.255.1" ],
"negate" : false,
"type" : "IP_RANGE",
"is_negate" : false,
"object_container" : "device_group"
},
"Address_1" : {
"name" : "Address_1",
"comment" : "",
"ips" : [ "192.168.0.0/16" ],
"negate" : false,
"type" : "SUBNET",

```

```

"is_negate" : false,
"object_container" : "device_group"
},
"Address_3" : {
"name" : "Address_3",
"comment" : "",
"ips" : [ "100.0.0.1-200.0.0.2" ],
"negate" : false,
"type" : "IP_RANGE",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.10.125.75" : {
"name" : "ip-10.10.125.75",
"comment" : "",
"ips" : [ "10.10.125.75/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.191.57" : {
"name" : "ip-10.30.191.57",
"comment" : "",
"ips" : [ "10.30.191.57/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.192.25" : {
"name" : "ip-10.30.192.25",

```

```

"comment" : "",
"ips" : [ "10.30.192.25/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"10.110.193.1" : {
"name" : "10.110.193.1",
"comment" : "",
"ips" : [ "10.110.193.1/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.10.193.25" : {
"name" : "ip-10.10.193.25",
"comment" : "",
"ips" : [ "10.10.193.25/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.20.191.25" : {
"name" : "ip-10.20.191.25",
"comment" : "",
"ips" : [ "10.20.191.25/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,

```

```
"object_container" : "device_group"
},
"ip-10.10.192.55" : {
  "name" : "ip-10.10.192.55",
  "comment" : "",
  "ips" : [ "10.10.192.55/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.10.191.85" : {
  "name" : "ip-10.10.191.85",
  "comment" : "",
  "ips" : [ "10.10.191.85/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.20.192.75" : {
  "name" : "ip-10.20.192.75",
  "comment" : "",
  "ips" : [ "10.20.192.75/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.30.191.46" : {
  "name" : "ip-10.30.191.46",
  "comment" : "",
```

```

"ips" : [ "10.30.191.46/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.10.192.87" : {
"name" : "ip-10.10.192.87",
"comment" : "",
"ips" : [ "10.10.192.87/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.120.191.175" : {
"name" : "ip-10.120.191.175",
"comment" : "",
"ips" : [ "10.120.191.175/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"update.microsoft.com" : {
"name" : "update.microsoft.com",
"comment" : "",
"ips" : [ "134.170.58.221" ],
"negate" : false,
"type" : "DOMAIN",
"is_negate" : false,
"object_container" : "device_group"
}

```

```

},
"ip-10.110.191.85" : {
  "name" : "ip-10.110.191.85",
  "comment" : "",
  "ips" : [ "10.110.191.85/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.40.192.28" : {
  "name" : "ip-10.40.192.28",
  "comment" : "",
  "ips" : [ "10.40.192.28/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.110.193.27" : {
  "name" : "ip-10.110.193.27",
  "comment" : "",
  "ips" : [ "10.110.193.27/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.110.191.158" : {
  "name" : "ip-10.110.191.158",
  "comment" : "",
  "ips" : [ "10.110.191.158/32" ],

```

```

"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.192.47" : {
"name" : "ip-10.30.192.47",
"comment" : "",
"ips" : [ "10.30.192.47/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.141.191.25" : {
"name" : "ip-10.141.191.25",
"comment" : "",
"ips" : [ "10.141.191.25/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"gauth.gfx.ms" : {
"name" : "gauth.gfx.ms",
"comment" : "",
"ips" : [ "23.37.40.70" ],
"negate" : false,
"type" : "DOMAIN",
"is_negate" : false,
"object_container" : "shared"
},

```

```

"33" : {
  "name" : "33",
  "comment" : "",
  "ips" : [ "33.33.33.0/24" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "shared"
},
"ip-10.110.191.71" : {
  "name" : "ip-10.110.191.71",
  "comment" : "",
  "ips" : [ "10.110.191.71/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.110.191.75" : {
  "name" : "ip-10.110.191.75",
  "comment" : "",
  "ips" : [ "10.110.191.75/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.20.192.57" : {
  "name" : "ip-10.20.192.57",
  "comment" : "",
  "ips" : [ "10.20.192.57/32" ],
  "negate" : false,

```

```

"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"a_10.132.22.10" : {
"name" : "a_10.132.22.10",
"comment" : "",
"ips" : [ "10.132.22.10/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"44" : {
"name" : "44",
"comment" : "",
"ips" : [ "44.44.44.0/24" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "shared"
},
"ip-10.10.191.55" : {
"name" : "ip-10.10.191.55",
"comment" : "",
"ips" : [ "10.10.191.55/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.191.14" : {

```

```
"name" : "ip-10.30.191.14",
"comment" : "",
"ips" : [ "10.30.191.14/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.191.15" : {
"name" : "ip-10.30.191.15",
"comment" : "",
"ips" : [ "10.30.191.15/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.10.192.25" : {
"name" : "ip-10.10.192.25",
"comment" : "",
"ips" : [ "10.10.192.25/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.10.192.55-1" : {
"name" : "ip-10.10.192.55-1",
"comment" : "",
"ips" : [ "10.10.192.55/32" ],
"negate" : false,
"type" : "SUBNET",
```

```

"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.120.191.88" : {
"name" : "ip-10.120.191.88",
"comment" : "",
"ips" : [ "10.120.191.88/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.140.191.48" : {
"name" : "ip-10.140.191.48",
"comment" : "",
"ips" : [ "10.140.191.48/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.110.191.175" : {
"name" : "ip-10.110.191.175",
"comment" : "",
"ips" : [ "10.110.191.175/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"all" : {
"name" : "all",

```

```
"comment" : "",
"ips" : [ "0.0.0.0/0" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.193.28" : {
"name" : "ip-10.30.193.28",
"comment" : "",
"ips" : [ "10.30.193.28/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.10.191.47" : {
"name" : "ip-10.10.191.47",
"comment" : "",
"ips" : [ "10.10.191.47/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.10.191.45" : {
"name" : "ip-10.10.191.45",
"comment" : "",
"ips" : [ "10.10.191.45/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
```

```

"object_container" : "device_group"
},
"@345" : {
"name" : "@345",
"comment" : "",
"ips" : [ "1.1.1.1/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"h_10.10.192.44" : {
"name" : "h_10.10.192.44",
"comment" : "",
"ips" : [ "10.10.192.44/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.110.191.56" : {
"name" : "ip-10.110.191.56",
"comment" : "",
"ips" : [ "10.110.191.56/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.120.191.72" : {
"name" : "ip-10.120.191.72",
"comment" : "",

```

```

"ips" : [ "10.120.191.72/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.110.191.58" : {
"name" : "ip-10.110.191.58",
"comment" : "",
"ips" : [ "10.110.191.58/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.191.178" : {
"name" : "ip-10.30.191.178",
"comment" : "",
"ips" : [ "10.30.191.178/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"33_Global" : {
"name" : "33_Global",
"comment" : "",
"ips" : [ "33.33.33.0/24" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "shared"
}

```

```

},
"ip-10.30.191.88" : {
  "name" : "ip-10.30.191.88",
  "comment" : "",
  "ips" : [ "10.30.191.88/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.30.193.25" : {
  "name" : "ip-10.30.193.25",
  "comment" : "",
  "ips" : [ "10.30.193.25/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.30.191.85" : {
  "name" : "ip-10.30.191.85",
  "comment" : "",
  "ips" : [ "10.30.191.85/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"gnone" : {
  "name" : "gnone",
  "comment" : "",
  "ips" : [ "0.0.0.0/0" ],

```

```

"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "shared"
},
"ip-10.110.191.5" : {
"name" : "ip-10.110.191.5",
"comment" : "",
"ips" : [ "10.110.191.5/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"AddressGlobal1" : {
"name" : "AddressGlobal1",
"comment" : "",
"ips" : [ "10.10.192.75/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "shared"
},
"h_10.30.192.50" : {
"name" : "h_10.30.192.50",
"comment" : "",
"ips" : [ "10.30.192.50/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},

```

```

"address_4" : {
  "name" : "address_4",
  "comment" : "",
  "ips" : [ "192.168.3.96/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "shared"
},
"net-10.120.191.56-30" : {
  "name" : "net-10.120.191.56-30",
  "comment" : "",
  "ips" : [ "10.120.191.56/30" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.110.191.44" : {
  "name" : "ip-10.110.191.44",
  "comment" : "",
  "ips" : [ "10.110.191.44/32" ],
  "negate" : false,
  "type" : "SUBNET",
  "is_negate" : false,
  "object_container" : "device_group"
},
"ip-10.10.191.72" : {
  "name" : "ip-10.10.191.72",
  "comment" : "",
  "ips" : [ "10.10.191.72/32" ],
  "negate" : false,

```

```

"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.110.191.46" : {
"name" : "ip-10.110.191.46",
"comment" : "",
"ips" : [ "10.110.191.46/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.120.192.75" : {
"name" : "ip-10.120.192.75",
"comment" : "",
"ips" : [ "10.120.192.75/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.110.191.48" : {
"name" : "ip-10.110.191.48",
"comment" : "",
"ips" : [ "10.110.191.48/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"a_172.20.120.100" : {

```

```

"name" : "a_172.20.120.100",
"comment" : "",
"ips" : [ "172.20.120.100/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.120.191.28" : {
"name" : "ip-10.120.191.28",
"comment" : "",
"ips" : [ "10.120.191.28/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.120.191.27" : {
"name" : "ip-10.120.191.27",
"comment" : "",
"ips" : [ "10.120.191.27/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.191.25" : {
"name" : "ip-10.30.191.25",
"comment" : "",
"ips" : [ "10.30.191.25/32" ],
"negate" : false,
"type" : "SUBNET",

```

```

"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.191.26" : {
"name" : "ip-10.30.191.26",
"comment" : "",
"ips" : [ "10.30.191.26/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.191.28" : {
"name" : "ip-10.30.191.28",
"comment" : "",
"ips" : [ "10.30.191.28/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"h_10.10.191.56" : {
"name" : "h_10.10.191.56",
"comment" : "",
"ips" : [ "10.10.191.56/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"address_5" : {
"name" : "address_5",

```

```

"comment" : "address_5",
"ips" : [ "0.0.0.0/0" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "shared"
},
"ip-10.120.191.13" : {
"name" : "ip-10.120.191.13",
"comment" : "",
"ips" : [ "10.120.191.13/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"ip-10.30.191.158" : {
"name" : "ip-10.30.191.158",
"comment" : "",
"ips" : [ "10.30.191.158/32" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,
"object_container" : "device_group"
},
"Address-SUBNET" : {
"name" : "Address-SUBNET",
"comment" : "Simple comment",
"ips" : [ "192.168.0.0/16" ],
"negate" : false,
"type" : "SUBNET",
"is_negate" : false,

```

```

"object_container" : "device_group"
}
},
"services" : {
  "gFTP_GET" : {
    "name" : "gFTP_GET",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "21"
    } ],
    "object_container" : "shared"
  },
  "POP3" : {
    "name" : "POP3",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "110"
    } ],
    "object_container" : "device_group"
  },
  "SMTPS" : {
    "name" : "SMTPS",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "465"
    } ],
    "object_container" : "device_group"
  },
  "gOSPF" : {

```

```

"name" : "gOSPF",
"service_definitions" : [ {
"protocol" : "89",
"src_port" : "*",
"dst_port" : "*"
} ],
"object_container" : "shared"
},
"gSSH" : {
"name" : "gSSH",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "22"
} ],
"object_container" : "shared"
},
"VDOLIVE" : {
"name" : "VDOLIVE",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "7000-7010"
} ],
"object_container" : "device_group"
},
"NNTP" : {
"name" : "NNTP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "119"
} ]
}

```

```

    } ],
    "object_container" : "device_group"
  },
  "gDCE-RPC" : {
    "name" : "gDCE-RPC",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "135"
    }, {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "135"
    } ],
    "object_container" : "shared"
  },
  "gPOP3S" : {
    "name" : "gPOP3S",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "995"
    } ],
    "object_container" : "shared"
  },
  "RSH" : {
    "name" : "RSH",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "512-1023",
      "dst_port" : "514"
    } ],

```

```

"object_container" : "device_group"
},
"AH" : {
"name" : "AH",
"service_definitions" : [ {
"protocol" : "51",
"src_port" : "*",
"dst_port" : "*"
} ],
"object_container" : "device_group"
},
"GUUCP" : {
"name" : "GUUCP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "540"
} ],
"object_container" : "shared"
},
"QUAKE" : {
"name" : "QUAKE",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "26000"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "27000"
}, {
"protocol" : "udp",

```

```

"src_port" : "*",
"dst_port" : "27910"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "27960"
} ],
"object_container" : "device_group"
},
"GOPHER" : {
"name" : "GOPHER",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "70"
} ],
"object_container" : "device_group"
},
"service_1" : {
"name" : "service_1",
"service_definitions" : [ {
"protocol" : "120",
"src_port" : "*",
"dst_port" : "*"
} ],
"object_container" : "device_group"
},
"service_2" : {
"name" : "service_2",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "2-400",

```

```

    "dst_port" : "1-500"
  } ],
  "object_container" : "device_group"
},
"ginfo_request" : {
  "name" : "ginfo_request",
  "service_definitions" : [ {
    "protocol" : "icmp",
    "src_port" : "15",
    "dst_port" : "*"
  } ],
  "object_container" : "shared"
},
"gaol" : {
  "name" : "gaol",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "5190-5194"
  } ],
  "object_container" : "shared"
},
"rtsp" : {
  "name" : "rtsp",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "554"
  }, {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "7070"
  } ]
}

```

```

    }, {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "8554"
    }, {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "554"
    } ],
    "object_container" : "device_group"
  },
  "IRC" : {
    "name" : "IRC",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "6660-6669"
    } ],
    "object_container" : "device_group"
  },
  "PC-Anywhere" : {
    "name" : "PC-Anywhere",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "5631"
    }, {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "5632"
    } ],
    "object_container" : "device_group"
  }
}

```

```

},
"INFO_ADDRESS" : {
  "name" : "INFO_ADDRESS",
  "service_definitions" : [ {
    "protocol" : "icmp",
    "src_port" : "17",
    "dst_port" : "*"
  } ],
  "object_container" : "device_group"
},
"WINS" : {
  "name" : "WINS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1512"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "1512"
  } ],
  "object_container" : "device_group"
},
"DCE-RPC" : {
  "name" : "DCE-RPC",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "135"
  }, {
    "protocol" : "udp",
    "src_port" : "*",

```

```

    "dst_port" : "135"
  } ],
  "object_container" : "device_group"
},
"L2TP" : {
  "name" : "L2TP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1701"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "1701"
  } ],
  "object_container" : "device_group"
},
"gTALK" : {
  "name" : "gTALK",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "517-518"
  } ],
  "object_container" : "shared"
},
"gSAMBA" : {
  "name" : "gSAMBA",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "139"
  } ]
}

```

```

    } ],
    "object_container" : "shared"
  },
  "tcp-441" : {
    "name" : "tcp-441",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "441-441"
    } ],
    "object_container" : "device_group"
  },
  "IMAPS" : {
    "name" : "IMAPS",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "993"
    } ],
    "object_container" : "device_group"
  },
  "TFTP" : {
    "name" : "TFTP",
    "service_definitions" : [ {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "69"
    } ],
    "object_container" : "device_group"
  },
  "H323" : {
    "name" : "H323",

```

```

"service_definitions" : [ {
  "protocol" : "tcp",
  "src_port" : "*",
  "dst_port" : "1720"
}, {
  "protocol" : "tcp",
  "src_port" : "*",
  "dst_port" : "1503"
}, {
  "protocol" : "udp",
  "src_port" : "*",
  "dst_port" : "1719"
} ],
"object_container" : "device_group"
},
"udp-16992" : {
  "name" : "udp-16992",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "16992"
  } ],
  "object_container" : "device_group"
},
"gRSH" : {
  "name" : "gRSH",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "512-1023",
    "dst_port" : "514"
  } ],
  "object_container" : "shared"
}

```

```

},
"gMYSQL" : {
  "name" : "gMYSQL",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "3306"
  } ],
  "object_container" : "shared"
},
"gFTP_PUT" : {
  "name" : "gFTP_PUT",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "21"
  } ],
  "object_container" : "shared"
},
"PPTP" : {
  "name" : "PPTP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1723"
  } ],
  "object_container" : "device_group"
},
"RADIUS-OLD" : {
  "name" : "RADIUS-OLD",
  "service_definitions" : [ {
    "protocol" : "udp",

```

```

"src_port" : "*",
"dst_port" : "1645"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1646"
} ],
"object_container" : "device_group"
},
"gIRC" : {
"name" : "gIRC",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "6660-6669"
} ],
"object_container" : "shared"
},
"RDP" : {
"name" : "RDP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "3389"
} ],
"object_container" : "device_group"
},
"FTP_GET" : {
"name" : "FTP_GET",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",

```

```

    "dst_port" : "21"
  } ],
  "object_container" : "device_group"
},
"udp-16992-16995" : {
  "name" : "udp-16992-16995",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "16992-16995"
  } ],
  "object_container" : "device_group"
},
"SMTP" : {
  "name" : "SMTP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "25"
  } ],
  "object_container" : "device_group"
},
"IMAP" : {
  "name" : "IMAP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "143"
  } ],
  "object_container" : "device_group"
},
"LDAP_UDP" : {

```

```

"name" : "LDAP_UDP",
"service_definitions" : [ {
  "protocol" : "udp",
  "src_port" : "*",
  "dst_port" : "389"
} ],
"object_container" : "device_group"
},
"RLOGIN" : {
  "name" : "RLOGIN",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "512-1023",
    "dst_port" : "513"
  } ],
  "object_container" : "device_group"
},
"gSCCP" : {
  "name" : "gSCCP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "2000"
  } ],
  "object_container" : "shared"
},
"gMS-SQL" : {
  "name" : "gMS-SQL",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1433"
  } ]
}

```

```

    }, {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "1434"
    } ],
    "object_container" : "shared"
  },
  "tcp-16995" : {
    "name" : "tcp-16995",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "16995"
    } ],
    "object_container" : "device_group"
  },
  "gTIMESTAMP" : {
    "name" : "gTIMESTAMP",
    "service_definitions" : [ {
      "protocol" : "icmp",
      "src_port" : "13",
      "dst_port" : "*"
    } ],
    "object_container" : "shared"
  },
  "ALL_TCP" : {
    "name" : "ALL_TCP",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "1-65535"
    } ],

```

```

"object_container" : "device_group"
},
"tcp-16996" : {
"name" : "tcp-16996",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "16996"
} ],
"object_container" : "device_group"
},
"tcp-16993" : {
"name" : "tcp-16993",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "16993"
} ],
"object_container" : "device_group"
},
"tcp-16994" : {
"name" : "tcp-16994",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "16994"
} ],
"object_container" : "device_group"
},
"tcp-16992" : {
"name" : "tcp-16992",
"service_definitions" : [ {

```

```

"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "16992"
} ],
"object_container" : "device_group"
},
"gL2TP" : {
"name" : "gL2TP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "1701"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1701"
} ],
"object_container" : "shared"
},
"gTFTP" : {
"name" : "gTFTP",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "69"
} ],
"object_container" : "shared"
},
"VNC" : {
"name" : "VNC",
"service_definitions" : [ {
"protocol" : "tcp",

```

```

"src_port" : "*",
"dst_port" : "5900"
} ],
"object_container" : "device_group"
},
"TALK" : {
"name" : "TALK",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "517-518"
} ],
"object_container" : "device_group"
},
"SAMBA" : {
"name" : "SAMBA",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "139"
} ],
"object_container" : "device_group"
},
"SCCP" : {
"name" : "SCCP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "2000"
} ],
"object_container" : "device_group"
},

```

```

"gh323" : {
  "name" : "gh323",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1720"
  }, {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1503"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "1719"
  } ],
  "object_container" : "shared"
},
"ghHTTP" : {
  "name" : "ghHTTP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "80"
  } ],
  "object_container" : "shared"
},
"gsip-MSNmessenger" : {
  "name" : "gsip-MSNmessenger",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1863"
  } ]
}

```

```

    } ],
    "object_container" : "shared"
  },
  "gwebproxy" : {
    "name" : "gwebproxy",
    "service_definitions" : [ ],
    "object_container" : "shared"
  },
  "gRDP" : {
    "name" : "gRDP",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "3389"
    } ],
    "object_container" : "shared"
  },
  "BGP" : {
    "name" : "BGP",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "179"
    } ],
    "object_container" : "device_group"
  },
  "HTTP" : {
    "name" : "HTTP",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "80"
    } ]
  }
}

```

```

}, {
  "protocol" : "tcp",
  "src_port" : "*",
  "dst_port" : "81"
} ],
"object_container" : "device_group"
},
"FTP_PUT" : {
  "name" : "FTP_PUT",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "21"
  } ],
  "object_container" : "device_group"
},
"tcp-759" : {
  "name" : "tcp-759",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "759"
  } ],
  "object_container" : "device_group"
},
"gFINGER" : {
  "name" : "gFINGER",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "79"
  } ],

```

```

"object_container" : "shared"
},
"tcp-757" : {
  "name" : "tcp-757",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "757"
  } ],
  "object_container" : "device_group"
},
"gPING6" : {
  "name" : "gPING6",
  "service_definitions" : [ ],
  "object_container" : "shared"
},
"MMS" : {
  "name" : "MMS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1755"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "1024-5000"
  } ],
  "object_container" : "device_group"
},
"gpPTP" : {
  "name" : "gpPTP",
  "service_definitions" : [ {

```

```

"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "1723"
} ],
"object_container" : "shared"
},
"gALL_ICMP6" : {
"name" : "gALL_ICMP6",
"service_definitions" : [ ],
"object_container" : "shared"
},
"X-WINDOWS" : {
"name" : "X-WINDOWS",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "6000-6063"
} ],
"object_container" : "device_group"
},
"gALL_ICMP" : {
"name" : "gALL_ICMP",
"service_definitions" : [ {
"protocol" : "icmp",
"src_port" : "0",
"dst_port" : "*"
} ],
"object_container" : "shared"
},
"GRE" : {
"name" : "GRE",
"service_definitions" : [ {

```

```

"protocol" : "47",
"src_port" : "*",
"dst_port" : "*"
} ],
"object_container" : "device_group"
},
"SIP" : {
"name" : "SIP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "5060"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "5060"
} ],
"object_container" : "device_group"
},
"gMMS" : {
"name" : "gMMS",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "1755"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1024-5000"
} ],
"object_container" : "shared"
},

```

```

"gsip" : {
  "name" : "gsip",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "5060"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "5060"
  } ],
  "object_container" : "shared"
},
"gbgp" : {
  "name" : "gbgp",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "179"
  } ],
  "object_container" : "shared"
},
"tcp-527" : {
  "name" : "tcp-527",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "527"
  } ],
  "object_container" : "device_group"
},
"gah" : {

```

```

"name" : "gAH",
"service_definitions" : [ {
"protocol" : "51",
"src_port" : "*",
"dst_port" : "*"
} ],
"object_container" : "shared"
},
"gSMTPS" : {
"name" : "gSMTPS",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "465"
} ],
"object_container" : "shared"
},
"gQUAKE" : {
"name" : "gQUAKE",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "26000"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "27000"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "27910"
}, {

```

```

"protocol" : "udp",
"src_port" : "*",
"dst_port" : "27960"
} ],
"object_container" : "shared"
},
"gRTSP" : {
"name" : "gRTSP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "554"
}, {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "7070"
}, {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "8554"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "554"
} ],
"object_container" : "shared"
},
"HTTPS" : {
"name" : "HTTPS",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",

```

```

    "dst_port" : "443"
  } ],
  "object_container" : "device_group"
},
"gInternet-Locator-Service" : {
  "name" : "gInternet-Locator-Service",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "389"
  } ],
  "object_container" : "shared"
},
"gPOP3" : {
  "name" : "gPOP3",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "110"
  } ],
  "object_container" : "shared"
},
"gGRE" : {
  "name" : "gGRE",
  "service_definitions" : [ {
    "protocol" : "47",
    "src_port" : "*",
    "dst_port" : "*"
  } ],
  "object_container" : "shared"
},
"MYSQL" : {

```

```

"name" : "MYSQL",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "3306"
} ],
"object_container" : "device_group"
},
"TELNET" : {
"name" : "TELNET",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "23"
} ],
"object_container" : "device_group"
},
"tcp-775" : {
"name" : "tcp-775",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "775"
} ],
"object_container" : "device_group"
},
"CVSPSERVER" : {
"name" : "CVSPSERVER",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "2401"
} ]
}

```

```

}, {
  "protocol" : "udp",
  "src_port" : "*",
  "dst_port" : "2401"
} ],
"object_container" : "device_group"
},
"INFO_REQUEST" : {
  "name" : "INFO_REQUEST",
  "service_definitions" : [ {
    "protocol" : "icmp",
    "src_port" : "15",
    "dst_port" : "*"
  } ],
  "object_container" : "device_group"
},
"tcp-1433" : {
  "name" : "tcp-1433",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1433"
  } ],
  "object_container" : "device_group"
},
"gSMTP" : {
  "name" : "gSMTP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "25"
  } ],

```

```

"object_container" : "shared"
},
"gVDOLIVE" : {
"name" : "gVDOLIVE",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "7000-7010"
} ],
"object_container" : "shared"
},
"gNNTP" : {
"name" : "gNNTP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "119"
} ],
"object_container" : "shared"
},
"gVNC" : {
"name" : "gVNC",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "5900"
} ],
"object_container" : "shared"
},
"FINGER" : {
"name" : "FINGER",
"service_definitions" : [ {

```

```

"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "79"
} ],
"object_container" : "device_group"
},
"gIMAP" : {
"name" : "gIMAP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "143"
} ],
"object_container" : "shared"
},
"RIP" : {
"name" : "RIP",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "520"
} ],
"object_container" : "device_group"
},
"gGOPHER" : {
"name" : "gGOPHER",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "70"
} ],
"object_container" : "shared"
}

```

```

    },
    "gKERBEROS" : {
      "name" : "gKERBEROS",
      "service_definitions" : [ {
        "protocol" : "tcp",
        "src_port" : "*",
        "dst_port" : "88"
      }, {
        "protocol" : "udp",
        "src_port" : "*",
        "dst_port" : "88"
      } ],
      "object_container" : "shared"
    },
    "POP3S" : {
      "name" : "POP3S",
      "service_definitions" : [ {
        "protocol" : "tcp",
        "src_port" : "*",
        "dst_port" : "995"
      } ],
      "object_container" : "device_group"
    },
    "TRACEROUTE" : {
      "name" : "TRACEROUTE",
      "service_definitions" : [ {
        "protocol" : "udp",
        "src_port" : "*",
        "dst_port" : "33434-33535"
      } ],
      "object_container" : "device_group"
    },
  },

```

```

"OSPF" : {
  "name" : "OSPF",
  "service_definitions" : [ {
    "protocol" : "89",
    "src_port" : "*",
    "dst_port" : "*"
  } ],
  "object_container" : "device_group"
},
"GTP" : {
  "name" : "GTP",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "2123"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "2152"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "3386"
  } ],
  "object_container" : "device_group"
},
"gRIP" : {
  "name" : "gRIP",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "520"
  } ]
}

```

```

    } ],
    "object_container" : "shared"
  },
  "DNS" : {
    "name" : "DNS",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "53"
    }, {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "53"
    } ],
    "object_container" : "device_group"
  },
  "MS-SQL" : {
    "name" : "MS-SQL",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "1433"
    }, {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "1434"
    } ],
    "object_container" : "device_group"
  },
  "RAUDIO" : {
    "name" : "RAUDIO",
    "service_definitions" : [ {

```

```

    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "7070"
  } ],
  "object_container" : "device_group"
},
"gDHCP" : {
  "name" : "gDHCP",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "67-68"
  } ],
  "object_container" : "shared"
},
"gGTP" : {
  "name" : "gGTP",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "2123"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "2152"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "3386"
  } ],
  "object_container" : "shared"
},

```

```

"gTRACEROUTE" : {
  "name" : "gTRACEROUTE",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "33434-33535"
  } ],
  "object_container" : "shared"
},
"SNMP" : {
  "name" : "SNMP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "161-162"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "161-162"
  } ],
  "object_container" : "device_group"
},
"NONE" : {
  "name" : "NONE",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "0"
  } ],
  "object_container" : "device_group"
},
"testService" : {

```

```
"name" : "testService",
"service_definitions" : [ {
  "protocol" : "tcp",
  "src_port" : "*",
  "dst_port" : "5500-5555"
} ],
"object_container" : "shared"
},
"gINFO_ADDRESS" : {
  "name" : "gINFO_ADDRESS",
  "service_definitions" : [ {
    "protocol" : "icmp",
    "src_port" : "17",
    "dst_port" : "*"
  } ],
  "object_container" : "shared"
},
"gTELNET" : {
  "name" : "gTELNET",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "23"
  } ],
  "object_container" : "shared"
},
"gHTTPS" : {
  "name" : "gHTTPS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "443"
```

```

    } ],
    "object_container" : "shared"
  },
  "SMB" : {
    "name" : "SMB",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "445"
    } ],
    "object_container" : "device_group"
  },
  "UUCP" : {
    "name" : "UUCP",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "540"
    } ],
    "object_container" : "device_group"
  },
  "gWINS" : {
    "name" : "gWINS",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "1512"
    }, {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "1512"
    } ],

```

```

"object_container" : "shared"
},
"gSYSLOG" : {
"name" : "gSYSLOG",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "514"
} ],
"object_container" : "shared"
},
"RADIUS" : {
"name" : "RADIUS",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1812"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1813"
} ],
"object_container" : "device_group"
},
"NetMeeting" : {
"name" : "NetMeeting",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "1720"
} ],
"object_container" : "device_group"

```

```

    },
    "gCVSPSERVER" : {
      "name" : "gCVSPSERVER",
      "service_definitions" : [ {
        "protocol" : "tcp",
        "src_port" : "*",
        "dst_port" : "2401"
      }, {
        "protocol" : "udp",
        "src_port" : "*",
        "dst_port" : "2401"
      } ],
      "object_container" : "shared"
    },
    "tcp-24601" : {
      "name" : "tcp-24601",
      "service_definitions" : [ {
        "protocol" : "tcp",
        "src_port" : "*",
        "dst_port" : "24601"
      } ],
      "object_container" : "device_group"
    },
    "AFS3" : {
      "name" : "AFS3",
      "service_definitions" : [ {
        "protocol" : "tcp",
        "src_port" : "*",
        "dst_port" : "7000-7009"
      }, {
        "protocol" : "udp",
        "src_port" : "*",

```

```

    "dst_port" : "7000-7009"
  } ],
  "object_container" : "device_group"
},
"gLdap" : {
  "name" : "gLdap",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "389"
  } ],
  "object_container" : "shared"
},
"FTP" : {
  "name" : "FTP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "21"
  } ],
  "object_container" : "device_group"
},
"RExec" : {
  "name" : "RExec",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "512"
  } ],
  "object_container" : "device_group"
},
"NTP" : {

```

```

"name" : "NTP",
"service_definitions" : [ {
  "protocol" : "tcp",
  "src_port" : "*",
  "dst_port" : "123"
}, {
  "protocol" : "udp",
  "src_port" : "*",
  "dst_port" : "123"
} ],
"object_container" : "device_group"
},
"ONC-RPC" : {
  "name" : "ONC-RPC",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "111"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "111"
  } ],
  "object_container" : "device_group"
},
"SIP-MSNmessenger" : {
  "name" : "SIP-MSNmessenger",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1863"
  } ],

```

```

"object_container" : "device_group"
},
"gSMB" : {
  "name" : "gSMB",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "445"
  } ],
  "object_container" : "shared"
},
"my_service" : {
  "name" : "my_service",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "0"
  } ],
  "object_container" : "device_group"
},
"gFTP" : {
  "name" : "gFTP",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "21"
  } ],
  "object_container" : "shared"
},
"WINFRAME" : {
  "name" : "WINFRAME",
  "service_definitions" : [ {

```

```

    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1494"
  }, {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "2598"
  } ],
  "object_container" : "device_group"
},
"PING" : {
  "name" : "PING",
  "service_definitions" : [ {
    "protocol" : "icmp",
    "src_port" : "8",
    "dst_port" : "*"
  } ],
  "object_container" : "device_group"
},
"WAIS" : {
  "name" : "WAIS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "210"
  } ],
  "object_container" : "device_group"
},
"tcp-175" : {
  "name" : "tcp-175",
  "service_definitions" : [ {
    "protocol" : "tcp",

```

```

"src_port" : "*",
"dst_port" : "175"
} ],
"object_container" : "device_group"
},
"IKE" : {
"name" : "IKE",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "500"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "4500"
} ],
"object_container" : "device_group"
},
"ALL_UDP" : {
"name" : "ALL_UDP",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1-65535"
} ],
"object_container" : "device_group"
},
"ESP" : {
"name" : "ESP",
"service_definitions" : [ {
"protocol" : "50",
"src_port" : "*",

```

```

    "dst_port" : "*"
  } ],
  "object_container" : "device_group"
},
"gDNS" : {
  "name" : "gDNS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "53"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "53"
  } ],
  "object_container" : "shared"
},
"gNetMeeting" : {
  "name" : "gNetMeeting",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1720"
  } ],
  "object_container" : "shared"
},
"gSOCKS" : {
  "name" : "gSOCKS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1080"
  } ]
}

```

```

}, {
  "protocol" : "udp",
  "src_port" : "*",
  "dst_port" : "1080"
} ],
"object_container" : "shared"
},
"gSQUID" : {
  "name" : "gSQUID",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "3128"
  } ],
  "object_container" : "shared"
},
"gLDAP_UDP" : {
  "name" : "gLDAP_UDP",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "389"
  } ],
  "object_container" : "shared"
},
"ALL" : {
  "name" : "ALL",
  "service_definitions" : [ {
    "protocol" : "6",
    "src_port" : "*",
    "dst_port" : "*"
  } ],

```

```

"object_container" : "device_group"
},
"webproxy" : {
"name" : "webproxy",
"service_definitions" : [ ],
"object_container" : "device_group"
},
"gRAUDIO" : {
"name" : "gRAUDIO",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "7070"
} ],
"object_container" : "shared"
},
"LDAP" : {
"name" : "LDAP",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "389"
} ],
"object_container" : "device_group"
},
"gALL_UDP" : {
"name" : "gALL_UDP",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1-65535"
} ],

```

```

"object_container" : "shared"
},
"gX-WINDOWS" : {
"name" : "gX-WINDOWS",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "6000-6063"
} ],
"object_container" : "shared"
},
"ALL_ICMP6" : {
"name" : "ALL_ICMP6",
"service_definitions" : [ ],
"object_container" : "device_group"
},
"gwAIS" : {
"name" : "gwAIS",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "210"
} ],
"object_container" : "shared"
},
"gPING" : {
"name" : "gPING",
"service_definitions" : [ {
"protocol" : "icmp",
"src_port" : "8",
"dst_port" : "*"
} ],

```

```

"object_container" : "shared"
},
"TCP-Serv" : {
"name" : "TCP-Serv",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "2-400",
"dst_port" : "1-500"
} ],
"object_container" : "device_group"
},
"tcp-225" : {
"name" : "tcp-225",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "225"
} ],
"object_container" : "device_group"
},
"PING6" : {
"name" : "PING6",
"service_definitions" : [ ],
"object_container" : "device_group"
},
"tcp-55" : {
"name" : "tcp-55",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "55-55"
} ],

```

```

"object_container" : "device_group"
},
"gALL" : {
  "name" : "gALL",
  "service_definitions" : [ {
    "protocol" : "0",
    "src_port" : "*",
    "dst_port" : "*"
  } ],
  "object_container" : "shared"
},
"TIMESTAMP" : {
  "name" : "TIMESTAMP",
  "service_definitions" : [ {
    "protocol" : "icmp",
    "src_port" : "13",
    "dst_port" : "*"
  } ],
  "object_container" : "device_group"
},
"NFS" : {
  "name" : "NFS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "111"
  }, {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "2049"
  }, {
    "protocol" : "udp",

```

```

"src_port" : "*",
"dst_port" : "111"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "2049"
} ],
"object_container" : "device_group"
},
"Internet-Locator-Service" : {
"name" : "Internet-Locator-Service",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "389"
} ],
"object_container" : "device_group"
},
"gmGCP" : {
"name" : "gmGCP",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "2427"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "2727"
} ],
"object_container" : "shared"
},
"MGCP" : {

```

```

"name" : "MGCP",
"service_definitions" : [ {
  "protocol" : "udp",
  "src_port" : "*",
  "dst_port" : "2427"
}, {
  "protocol" : "udp",
  "src_port" : "*",
  "dst_port" : "2727"
} ],
"object_container" : "device_group"
},
"gService" : {
  "name" : "gService",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "999",
    "dst_port" : "0"
  } ],
  "object_container" : "shared"
},
"SQUID" : {
  "name" : "SQUID",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "3128"
  } ],
  "object_container" : "device_group"
},
"gALL_TCP" : {
  "name" : "gALL_TCP",

```

```

"service_definitions" : [ {
  "protocol" : "tcp",
  "src_port" : "*",
  "dst_port" : "1-65535"
} ],
"object_container" : "shared"
},
"tcp-232" : {
  "name" : "tcp-232",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "232-232"
  } ],
  "object_container" : "device_group"
},
"ALL_ICMP" : {
  "name" : "ALL_ICMP",
  "service_definitions" : [ {
    "protocol" : "icmp",
    "src_port" : "0",
    "dst_port" : "*"
  } ],
  "object_container" : "device_group"
},
"gwINFRAME" : {
  "name" : "gwINFRAME",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1494"
  } ], {

```

```

"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "2598"
} ],
"object_container" : "shared"
},
"tcp-*" : {
"name" : "tcp-*",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "0-65535"
} ],
"object_container" : "device_group"
},
"service_5" : {
"name" : "service_5",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "75"
} ],
"object_container" : "shared"
},
"gIMAPS" : {
"name" : "gIMAPS",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "993"
} ],
"object_container" : "shared"
}

```

```

    },
    "gIKE" : {
      "name" : "gIKE",
      "service_definitions" : [ {
        "protocol" : "udp",
        "src_port" : "*",
        "dst_port" : "500"
      }, {
        "protocol" : "udp",
        "src_port" : "*",
        "dst_port" : "4500"
      } ],
      "object_container" : "shared"
    },
    "gNTP" : {
      "name" : "gNTP",
      "service_definitions" : [ {
        "protocol" : "tcp",
        "src_port" : "*",
        "dst_port" : "123"
      }, {
        "protocol" : "udp",
        "src_port" : "*",
        "dst_port" : "123"
      } ],
      "object_container" : "shared"
    },
    "gESP" : {
      "name" : "gESP",
      "service_definitions" : [ {
        "protocol" : "50",
        "src_port" : "*",

```

```

    "dst_port" : "*"
  } ],
  "object_container" : "shared"
},
"SOCKS" : {
  "name" : "SOCKS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1080"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "1080"
  } ],
  "object_container" : "device_group"
},
"DHCP6" : {
  "name" : "DHCP6",
  "service_definitions" : [ {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "546"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "547"
  } ],
  "object_container" : "device_group"
},
"GREXEC" : {
  "name" : "GREXEC",

```

```

"service_definitions" : [ {
  "protocol" : "tcp",
  "src_port" : "*",
  "dst_port" : "512"
} ],
"object_container" : "shared"
},
"grLOGIN" : {
  "name" : "grLOGIN",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "512-1023",
    "dst_port" : "513"
  } ],
  "object_container" : "shared"
},
"grNONE" : {
  "name" : "grNONE",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "0"
  } ],
  "object_container" : "shared"
},
"tcp-1701" : {
  "name" : "tcp-1701",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "1701"
  } ],

```

```

"object_container" : "device_group"
},
"AOL" : {
"name" : "AOL",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "5190-5194"
} ],
"object_container" : "device_group"
},
"tcp-72" : {
"name" : "tcp-72",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "72-72"
} ],
"object_container" : "device_group"
},
"gRADIUS-OLD" : {
"name" : "gRADIUS-OLD",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1645"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1646"
} ],
"object_container" : "shared"

```

```

},
"SSH" : {
  "name" : "SSH",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "22"
  } ],
  "object_container" : "device_group"
},
"KERBEROS" : {
  "name" : "KERBEROS",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "88"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "88"
  } ],
  "object_container" : "device_group"
},
"gPC-Anywhere" : {
  "name" : "gPC-Anywhere",
  "service_definitions" : [ {
    "protocol" : "tcp",
    "src_port" : "*",
    "dst_port" : "5631"
  }, {
    "protocol" : "udp",
    "src_port" : "*",

```

```

"dst_port" : "5632"
} ],
"object_container" : "shared"
},
"DHCP" : {
"name" : "DHCP",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "67-68"
} ],
"object_container" : "device_group"
},
"gONC-RPC" : {
"name" : "gONC-RPC",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "111"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "111"
} ],
"object_container" : "shared"
},
"udp/16994" : {
"name" : "udp/16994",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "16994"

```

```

    } ],
    "object_container" : "device_group"
  },
  "gSNMP" : {
    "name" : "gSNMP",
    "service_definitions" : [ {
      "protocol" : "tcp",
      "src_port" : "*",
      "dst_port" : "161-162"
    }, {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "161-162"
    } ],
    "object_container" : "shared"
  },
  "SYSLOG" : {
    "name" : "SYSLOG",
    "service_definitions" : [ {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "514"
    } ],
    "object_container" : "device_group"
  },
  "gRADIUS" : {
    "name" : "gRADIUS",
    "service_definitions" : [ {
      "protocol" : "udp",
      "src_port" : "*",
      "dst_port" : "1812"
    }, {

```

```

"protocol" : "udp",
"src_port" : "*",
"dst_port" : "1813"
} ],
"object_container" : "shared"
},
"gNFS" : {
"name" : "gNFS",
"service_definitions" : [ {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "111"
}, {
"protocol" : "tcp",
"src_port" : "*",
"dst_port" : "2049"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "111"
}, {
"protocol" : "udp",
"src_port" : "*",
"dst_port" : "2049"
} ],
"object_container" : "shared"
},
"gDHCP6" : {
"name" : "gDHCP6",
"service_definitions" : [ {
"protocol" : "udp",
"src_port" : "*",

```

```

    "dst_port" : "546"
  }, {
    "protocol" : "udp",
    "src_port" : "*",
    "dst_port" : "547"
  } ],
  "object_container" : "shared"
}
},
"zones" : {
  "Internal" : {
    "name" : "Internal",
    "interfaces" : [ "port3" ],
    "description" : ""
  },
  "root-Internal" : {
    "name" : "root-Internal",
    "interfaces" : [ "port4" ],
    "description" : ""
  }
},
"interfaces" : {
  "VLAN-103" : {
    "name" : "VLAN-103",
    "enable" : "enabled",
    "ips" : [ "10.30.22.2/24" ],
    "rules_groups" : [ ]
  },
  "VLAN-104" : {
    "name" : "VLAN-104",
    "enable" : "enabled",
    "ips" : [ "10.40.22.2/24" ],

```

```
"rules_groups" : [ ]
},
"VLAN-102" : {
  "name" : "VLAN-102",
  "enable" : "enabled",
  "ips" : [ "10.20.22.2/24" ],
  "rules_groups" : [ ]
},
"port7" : {
  "name" : "port7",
  "enable" : "enabled",
  "ips" : [ "10.120.192.1/24" ],
  "rules_groups" : [ ]
},
"port5" : {
  "name" : "port5",
  "enable" : "enabled",
  "ips" : [ "10.30.192.1/24" ],
  "rules_groups" : [ ]
},
"port6" : {
  "name" : "port6",
  "enable" : "enabled",
  "ips" : [ "10.110.192.1/24" ],
  "rules_groups" : [ ]
},
"port3" : {
  "name" : "port3",
  "zone" : "Internal",
  "enable" : "enabled",
  "ips" : [ "10.10.192.1/24" ],
  "rules_groups" : [ ]
}
```

```

    },
    "port4" : {
      "name" : "port4",
      "zone" : "root-Internal",
      "enable" : "enabled",
      "ips" : [ "10.20.192.1/24" ],
      "rules_groups" : [ ]
    },
    "port41" : {
      "name" : "port41",
      "enable" : "enabled",
      "ips" : [ "10.40.192.1/24" ],
      "rules_groups" : [ ]
    },
    "port42" : {
      "name" : "port42",
      "enable" : "enabled",
      "ips" : [ "10.50.192.1/24" ],
      "rules_groups" : [ ]
    }
  },
  "routes" : { },
  "schedules" : { },
  "global_nat_rules" : {
    "1" : {
      "id" : "1",
      "nattype" : "DYNAMIC",
      "origin_ips" : [ "ip-10.10.192.87" ],
      "mapped_ips" : [ "NAT_Pool" ],
      "nat_type" : "DYNAMIC",
      "rule_number" : 1,
      "enable" : "enabled"
    }
  }
}

```

```

}
},
"nat_objects" : {
  "10.30.191.0_vip" : {
    "id" : "10.30.191.0_vip",
    "comment" : "",
    "nattype" : "STATIC",
    "origin_ips" : [ "10.30.191.0" ],
    "mapped_ips" : [ "10.110.191.1-10.110.191.1" ],
    "nat_type" : "STATIC"
  },
  "VipObj1" : {
    "id" : "VipObj1",
    "comment" : "",
    "nattype" : "STATIC",
    "origin_ips" : [ "10.30.191.158" ],
    "mapped_ips" : [ "10.110.191.1-10.110.191.1" ],
    "nat_type" : "STATIC"
  },
  "Vip_under_all_lan" : {
    "id" : "Vip_under_all_lan",
    "comment" : "",
    "nattype" : "STATIC",
    "origin_ips" : [ "192.168.100.100" ],
    "mapped_ips" : [ "192.168.101.18" ],
    "nat_type" : "STATIC"
  },
  "new_vip" : {
    "id" : "new_vip",
    "comment" : "",
    "nattype" : "STATIC",
    "origin_ips" : [ "10.110.191.5-10.110.191.6" ],

```

```
"mapped_ips" : [ "10.10.191.5" ],
"nat_type" : "STATIC"
}
},
"nat_pools" : {
  "NAT_Pool" : {
    "name" : "NAT_Pool",
    "ips" : [ "10.10.192.44" ],
    "negate" : false,
    "type" : "NAT_POOL",
    "is_negate" : false
  },
  "overload" : {
    "name" : "overload",
    "ips" : [ "10.10.191.1-10.10.191.20" ],
    "negate" : false,
    "type" : "NAT_POOL",
    "is_negate" : false
  },
  "ippool-new" : {
    "name" : "ippool-new",
    "ips" : [ "0.0.0.0" ],
    "negate" : false,
    "type" : "NAT_POOL",
    "is_negate" : false
  }
},
"hosts_groups" : {
  "Address_Group_1" : {
    "name" : "Address_Group_1",
    "members" : [ "Address_1", "Address_2" ],
    "negate" : false,
```

```

"object_container" : "device_group",
"is_negate" : false
},
"Address_Group_Test" : {
"name" : "Address_Group_Test",
"members" : [ "33", "44", "55" ],
"negate" : false,
"object_container" : "device_group",
"is_negate" : false
}
},
"services_groups" : {
"gWindows AD" : {
"name" : "gWindows AD",
"members" : [ "gDCE-RPC", "gDNS", "gKERBEROS", "gLDAP", "gLDAP_UDP",
"gSAMBA", "gSMB" ],
"object_container" : "shared"
},
"Windows AD" : {
"name" : "Windows AD",
"members" : [ "DCE-RPC", "DNS", "KERBEROS", "LDAP", "LDAP_UDP", "SAMBA",
"SMB" ],
"object_container" : "device_group"
},
"SaHTTP" : {
"name" : "SaHTTP",
"members" : [ "tcp-16992", "tcp-16994" ],
"object_container" : "device_group"
},
"Foo" : {
"name" : "Foo",
"members" : [ "SaHTTP", "tcp-16996" ],
"object_container" : "device_group"
}
}

```

```

    },
    "Service_Group_Test" : {
      "name" : "Service_Group_Test",
      "members" : [ "AH", "ESP", "DNS" ],
      "object_container" : "device_group"
    },
    "Web Access" : {
      "name" : "Web Access",
      "members" : [ "DNS", "HTTP", "HTTPS" ],
      "object_container" : "device_group"
    },
    "Email Access" : {
      "name" : "Email Access",
      "members" : [ "DNS", "IMAP", "IMAPS", "POP3", "POP3S", "SMTP", "SMTPS" ],
      "object_container" : "device_group"
    },
    "Exchange Server" : {
      "name" : "Exchange Server",
      "members" : [ "DCE-RPC", "DNS", "HTTPS" ],
      "object_container" : "device_group"
    },
    "gWeb Access" : {
      "name" : "gWeb Access",
      "members" : [ "gDNS", "gHTTP", "gHTTPS" ],
      "object_container" : "shared"
    },
    "gExchange Server" : {
      "name" : "gExchange Server",
      "members" : [ "gDCE-RPC", "gDNS", "gHTTPS" ],
      "object_container" : "shared"
    },
    "gEmail Access" : {

```

```

"name" : "gEmail Access",
"members" : [ "gDNS", "gIMAP", "gIMAPS", "gPOP3", "gPOP3S", "gSMTP",
"gSMTPS" ],
"object_container" : "shared"
}
},
"nat_objects_groups" : {
  "VipGroupObj1" : {
    "name" : "VipGroupObj1",
    "members" : [ "VipObj1" ],
    "object_container" : "device_group",
    "nat_type" : "STATIC"
  }
},
"device_interfaces" : {
  "VLAN-103" : {
    "name" : "VLAN-103",
    "enable" : "enabled",
    "ips" : [ "10.30.22.2/24" ],
    "rules_groups" : [ ]
  },
  "VLAN-104" : {
    "name" : "VLAN-104",
    "enable" : "enabled",
    "ips" : [ "10.40.22.2/24" ],
    "rules_groups" : [ ]
  },
  "VLAN-102" : {
    "name" : "VLAN-102",
    "enable" : "enabled",
    "ips" : [ "10.20.22.2/24" ],
    "rules_groups" : [ ]
  }
}

```

```
},
"port7" : {
  "name" : "port7",
  "enable" : "enabled",
  "ips" : [ "10.120.192.1/24" ],
  "rules_groups" : [ ]
},
"port5" : {
  "name" : "port5",
  "enable" : "enabled",
  "ips" : [ "10.30.192.1/24" ],
  "rules_groups" : [ ]
},
"port6" : {
  "name" : "port6",
  "enable" : "enabled",
  "ips" : [ "10.110.192.1/24" ],
  "rules_groups" : [ ]
},
"port3" : {
  "name" : "port3",
  "zone" : "Internal",
  "enable" : "enabled",
  "ips" : [ "10.10.192.1/24" ],
  "rules_groups" : [ ]
},
"port4" : {
  "name" : "port4",
  "zone" : "root-Internal",
  "enable" : "enabled",
  "ips" : [ "10.20.192.1/24" ],
  "rules_groups" : [ ]
}
```

```

},
"port41" : {
  "name" : "port41",
  "enable" : "enabled",
  "ips" : [ "10.40.192.1/24" ],
  "rules_groups" : [ ]
},
"port42" : {
  "name" : "port42",
  "enable" : "enabled",
  "ips" : [ "10.50.192.1/24" ],
  "rules_groups" : [ ]
}
},
"from_to_zone" : {
  "any" : {
    "any" : [ "1073741825", "1074741826", "1073741827", "1073741828",
      "1074741825" ]
  }
},
"rules_groups" : {
  "middle" : {
    "id" : "middle",
    "name" : "Main",
    "enable" : "enabled",
    "rule_display_name" : "Main"
  },
  "before" : {
    "id" : "before",
    "name" : "Header",
    "enable" : "enabled",
    "rule_display_name" : "Header"
  }
}

```

```

},
"after" : {
  "id" : "after",
  "name" : "Footer",
  "enable" : "enabled",
  "rule_display_name" : "Footer"
}
},
"config_type" : "ZONE_BASED"
}

```

## Static support troubleshooting

This section provides troubleshooting information.

### Troubleshooting Files and Folders

The following table specifies relevant paths and file names that contain relevant data, based on the context.

	Device Definition	Analysis
<b>Working folder</b>	/home/afa/algosec/work/ collect_gen-<PID> e.g.: /home/afa/algosec/work/ collect_gen-62123	/home/afa/algosec/firewalls/afa-<###> e.g.: /home/afa/algosec/firewalls/afa-88
<b>Configuration file</b>	gen_data.txt	<device name>.<device brand suffix> e.g. 10_20_74_1.secui Note- At the end of analysis this file is compressed and contained in raw_files.zip. To clarify, when the partner parser is launched the configuration file is not compressed yet.
<b>Log file</b>	/home/afa/.fa-history	/home/afa/algosec/firewalls/afa-<###>/fwa.history

## Problem: Analysis Failed

### Probable Cause

The JSON configuration is invalid. The required data is missing and/or the file structure is wrong.

### Confirming the Problem

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, by doing the following:
  1. Open an SSH connection to AFA.
  2. Run the following command:  
**su - afa**
  3. Run the following command:  
**curl -si '127.0.0.1:8080/afa/configParser/validate?path=<full path to JSON file>'**
  4. 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.
  5. Fix the error identified in the error message.

## Example

1. After the analysis failed, you search the failed analysis's error logs. You find 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.

2. 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
```

3. 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>&lt;brand_id&gt;.16.png</code>	16x16 pixel png
<code>&lt;brand_id&gt;.35.png</code>	35x35 pixel png
<code>&lt;brand_id&gt;.45.png</code>	45x45 pixel png
<code>&lt;brand_id&gt;.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 effect only after logging out and logging back in.

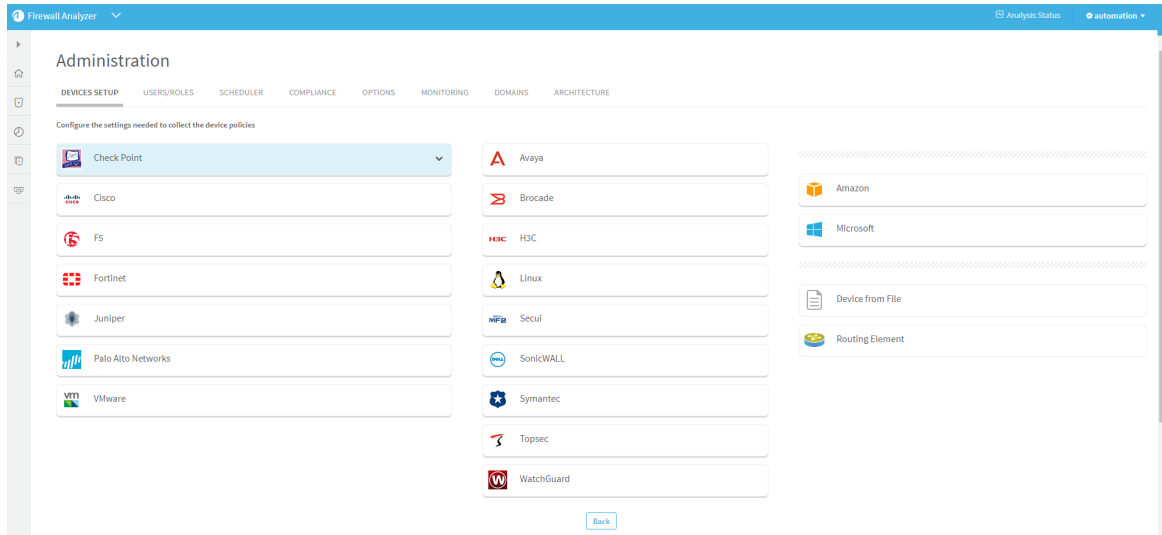
The new device will now appear as an option in the web interface when adding a new device to AFA.

## 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 <b>Overview</b> and <b>Changes</b> tabs).
Title	String. The full name of the device brand. The title represents the device in the list of device types in the <b>Devices</b> tab of the <b>Administration</b> 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

<b>id</b>	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> .
<b>title</b>	String. The label representing the field in the Web interface.
<b>type</b>	String. The field's type. This can have the following values: <ul style="list-style-type: none"> <li><code>text</code>. The user must input free text in this field.</li> <li><code>password</code>. The user must input a password in this field.</li> </ul> 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

<b>id</b>	<p>String. The ID of the connection option.</p> <p>It can include only the following characters: a-z, A-Z, 0-9, @, _, !, +, ., :, -, ), (</p> <p>The ID is used as a tag in the file <code>firewall_data.xml</code>.</p>
<b>command</b>	<p>String. The connection command.</p> <p>This may include the following parameters from the file <code>firewall_data.xml</code>:</p> <ul style="list-style-type: none"> <li>• <code>%attribute%</code>. An attribute, where <i>attribute</i> represents the name of any attribute defined in the <code>FORM_FIELD</code> tag.</li> </ul> <p><code>%password%</code></p> <p><code>%user_name%</code></p> <p><code>%host_name%</code></p>
<b>title</b>	<p>String. The label representing the connection option in the Web interface.</p>

## 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

<b>prompt</b>	String. The basic device prompt that appears when the AFA automatic data collection client connects to the device. This is a regular expression.
<b>more_prompt</b>	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

<b>prompt</b>	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.
<b>response</b>	String. The command or string that the AFA automatic data collection client should send after receiving the prompt.
<b>try_again</b>	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"> <li><code>yes</code>. Attempt to log in again.</li> <li><code>no</code>. Do not attempt to log in again. Instead, wait for the device prompt specified by the <code>prompt</code> parameter.</li> </ul>

## 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

<b>prompt</b>	String. The device prompt that appears after the AFA automatic data collection client has logged in to the device. This is a regular expression.
<b>response</b>	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"><li>• <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></li></ul>
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"><li>• <code>yes</code>. Add the result of the command to the output device configuration file.</li><li>• <code>no</code>. Do not add the result of the command to the output device configuration file.</li></ul>

<b>id</b>	Integer. The command's ID and order number. Commands are implemented in numerical order.
<b>condition</b>	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"> <li>The name of any attribute added in the <code>FORM_FIELD</code> tag</li> <li><b>FW_VIRT</b>. Run the command only if the device has a virtual system.</li> </ul>
<b>prompt</b>	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"> <li><code>%attribute%</code>. An attribute, where <i>attribute</i> represents the attribute's name.   <pre>%password%</pre> <pre>%user_name%</pre> <pre>%host_name%</pre> </li> </ul> <p><b>Note:</b> 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"><li>• <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></li></ul>
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"><li>• <code>yes</code>. Add the result of the command to the output device configuration file.</li><li>• <code>no</code>. Do not add the result of the command to the output device configuration file.</li></ul>

<b>id</b>	Integer. The command's ID and order number. Commands are implemented in numerical order.
<b>condition</b>	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"> <li>The name of any attribute added in the <code>FORM_FIELD</code> tag.</li> <li><b>FW_VIRT</b>. Run the command only if the device has a virtual system.</li> </ul>
<b>prompt</b>	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"> <li><code>%attribute%</code>. An attribute, where <i>attribute</i> represents the attribute's name.   <pre>%password%</pre> <pre>%user_name%</pre> <pre>%host_name%</pre> </li> </ul> <p><b>Note:</b> 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

<b>command</b>	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

<b>contextLines</b>	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

<b>regex</b>	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.
<b>line_before</b>	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.
<b>lines_after</b>	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.
<b>inline</b>	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"> <li><code>yes</code>. Exclude only the part of the line that matches the regular expression.</li> <li><code>no</code>. Exclude the whole line (or any lines before or after).</li> </ul>

## 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

<b>script</b>	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

<b>name</b>	String. The name of the feature.
<b>script</b>	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

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.

This topic describes how to enable ASMS's Early Availability features.

- [Enable / Disable support for Cisco ISE](#)
- [Enable /Disable support for Arista](#)
- [Enable / Disable map support for Azure](#)

- [Enable /Disable ActiveChange for Azure](#)
- [Enable support for Check Point R80 layers](#)

## Enable / Disable support for Cisco ISE

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 BusinessFlow features that rely on FireFlow
- Support does *not* include using a Geographic Distribution Remote Agent to manage Cisco ISE devices.

## Enable / disable early availability support for Cisco ISE

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** page appears.

4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

5. In the **Name** field, type `AlgoSec_EA_CISCOISE`.

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**.

## Add a Cisco ISE device to AFA

When support for Cisco ISE is enabled, do the following:

1. Enable the Cisco ISE TrustSec SXP feature for the device. This is required for AFA to be able to collect your device routing information.
2. Add your Cisco ISE to AFA using the standard procedure for defining devices. For details, see [Add devices to AFA](#).

## Enable /Disable support for Arista

Support for Arista 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 support for Arista is enabled, you can add an Arista device to AFA using the standard procedure for defining devices.

**Note:** Arista is not supported in FireFlow.

**Note: Note:** AFA does not currently support the use of a Geographical Distribution Remote Agent to manage this device.

## To enable/disable early availability support for Arista:

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_ARISTA`.
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 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: 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: 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.

CaramelVSX (16 Rules)													
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 BusinessFlow 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.

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:

<b>Name</b>	<b>AlgoSec_EA_CKP_R80_Layers</b>
<b>Value</b>	This parameter is set to <b>no</b> by default. Define the value as <b>yes</b> 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.

**Create a New Group**

Name:

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	


Showing 1 to 8 of 40 devices

Previous 1 2 3 4 5 Next

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.

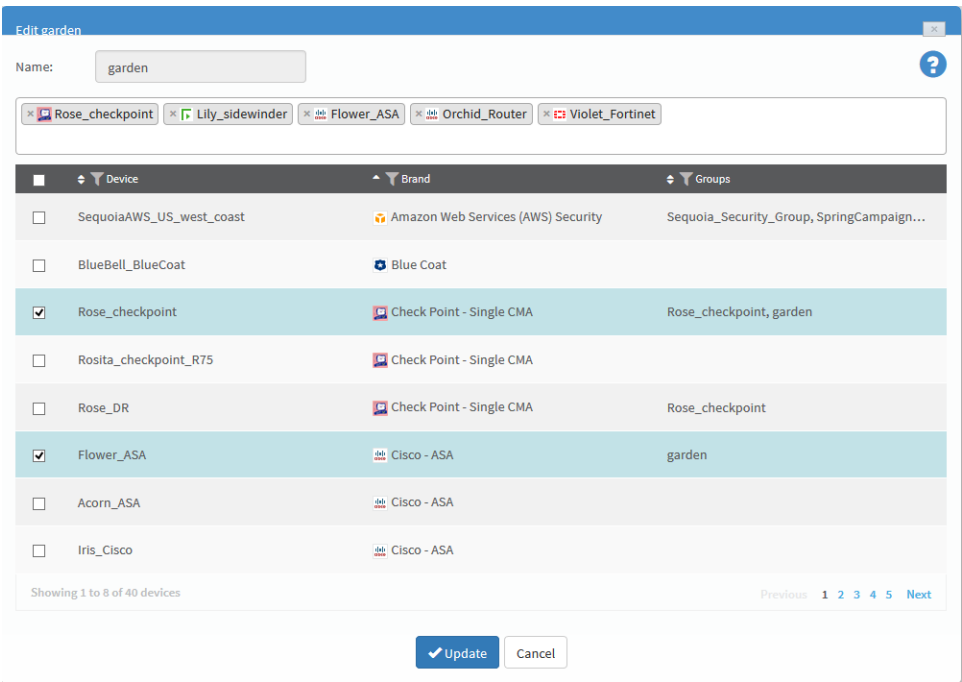
7. Click **OK**.

## 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.

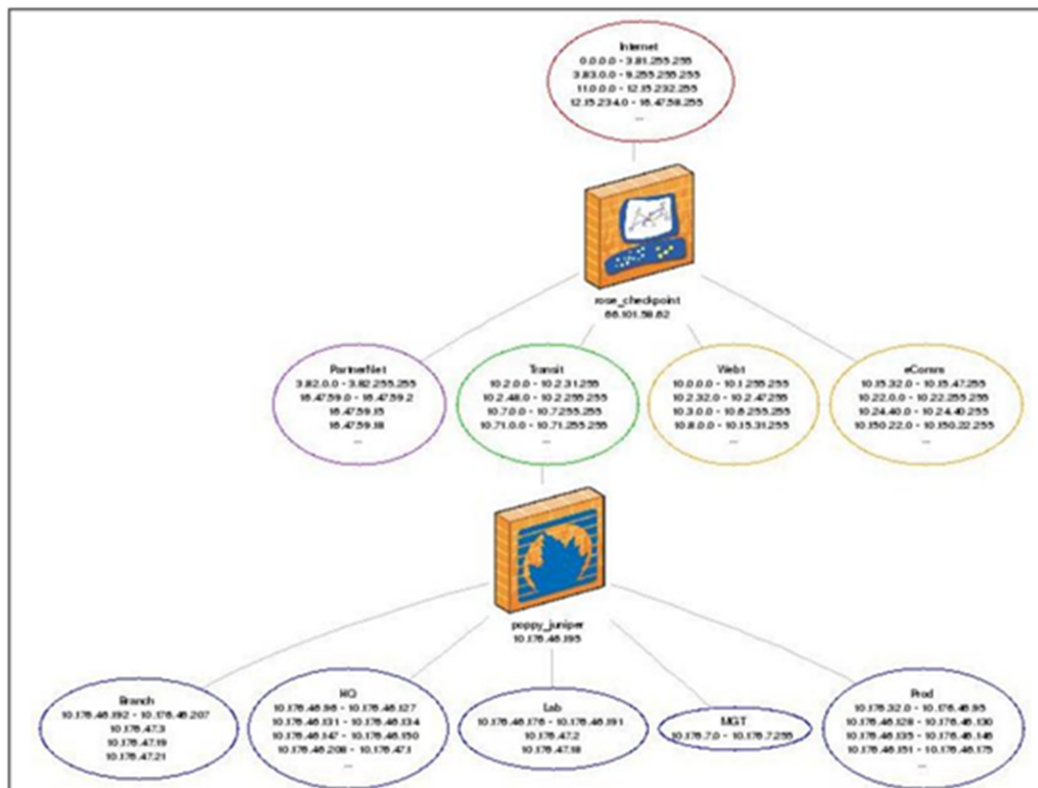
# Manage matrices

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	


Showing 1 to 8 of 27 devices

Previous 1 2 3 4 Next

Create Cancel

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.

5. 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.

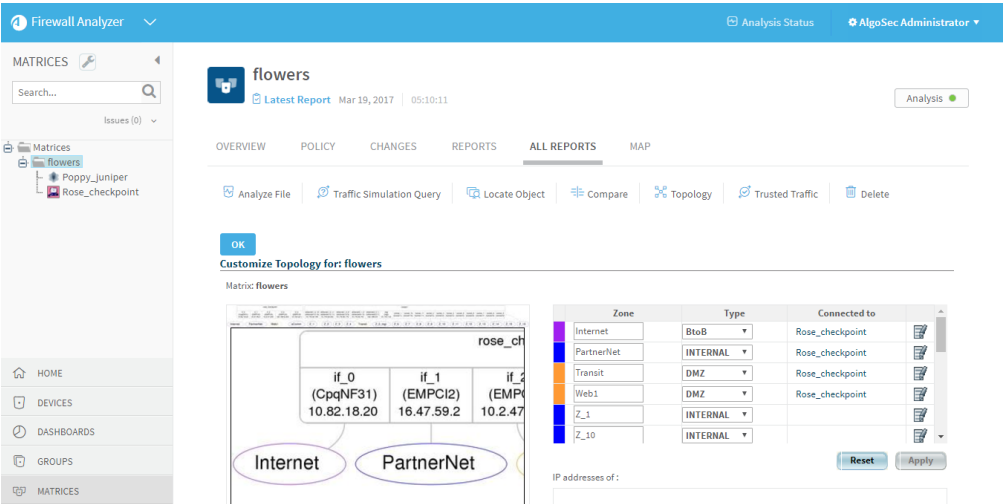
6. Click **Create**.

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.



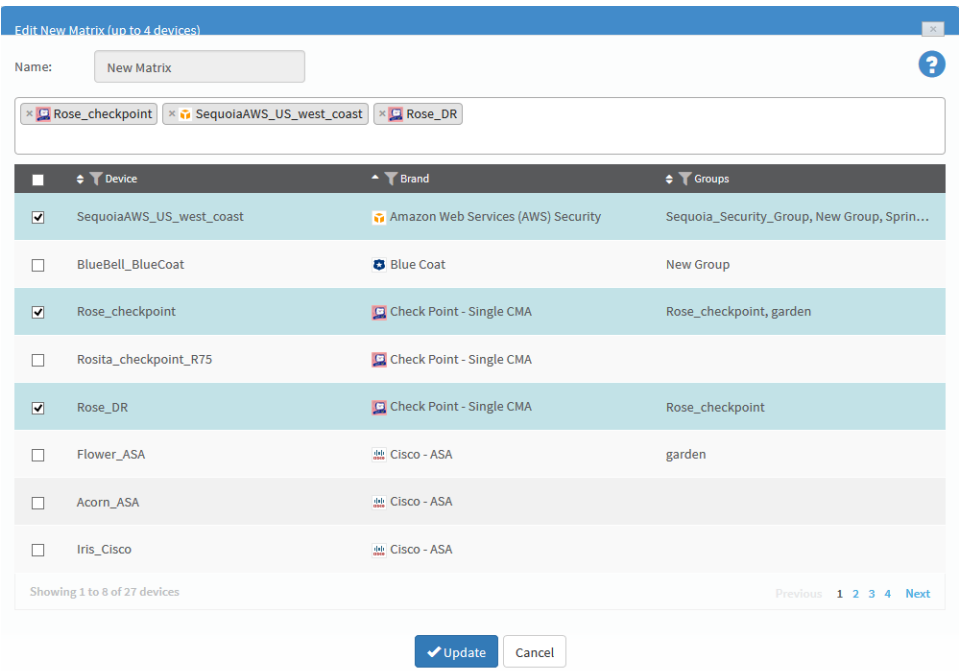
- b. Customize the matrix topology.
- c. Click **OK**.

## 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.

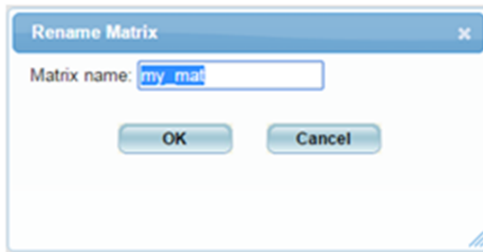
- c. Click **OK**.

## 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.

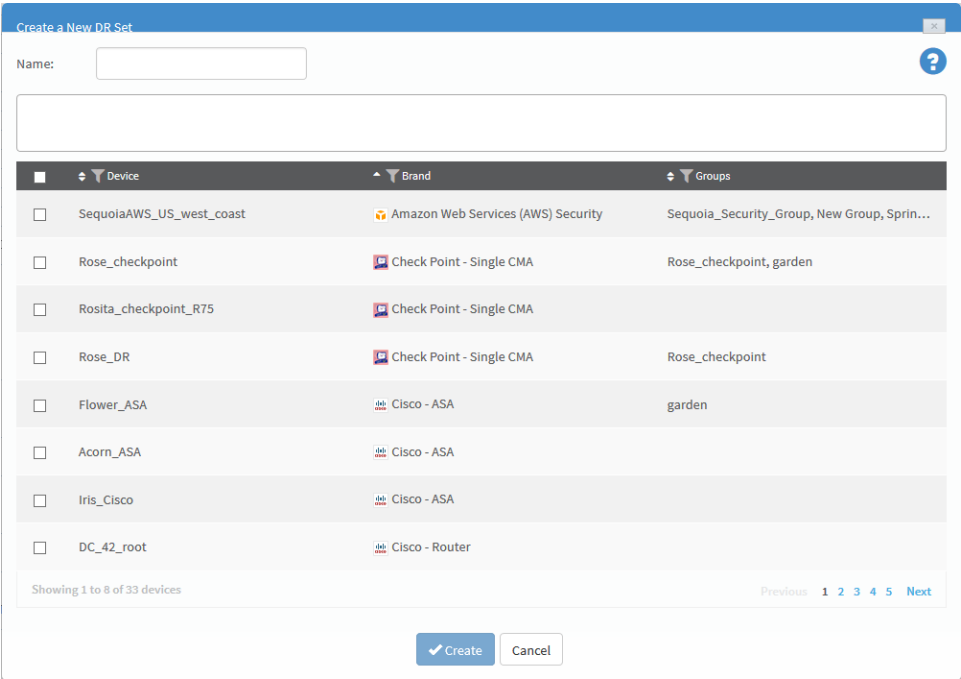
This section describes how to configure disaster recovery (DR) sets in AFA.

## 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.



- 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.

Dialog Title: Edit Check Point Recovery

Name: Check Point Recovery

Members: Rose\_checkpoint, Rose\_DR

Device	Brand	Groups
<input type="checkbox"/> SequoiaAWS_US_west_coast	Amazon Web Services (AWS) Security	Sequoia_Security_Group, New Group, Sprin...
<input checked="" type="checkbox"/> Rose_checkpoint	Check Point - Single CMA	Rose_checkpoint, garden
<input type="checkbox"/> Rosita_checkpoint_R75	Check Point - Single CMA	
<input checked="" 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	


Showing 1 to 8 of 33 devices

Previous 1 2 3 4 5 Next

Buttons: Update, Cancel

- 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](#)

See also [Specify routing data from the map](#).

## 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.

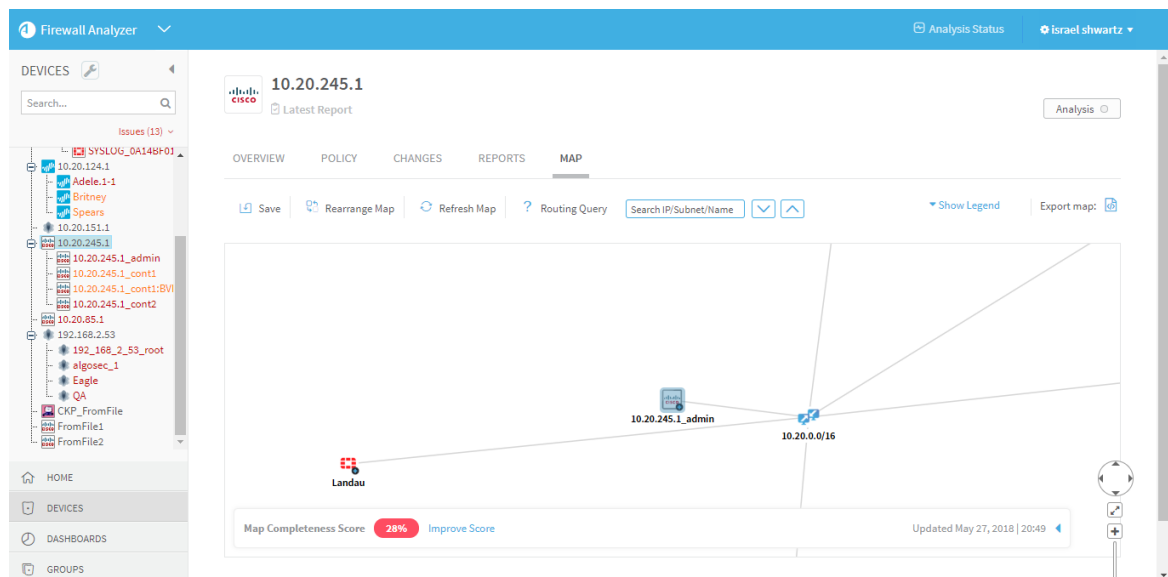
If desired, you can complete the map using a CLI tool (instead of the AFA web interface). See [Completing the Map via the CLI](#) (see [Complete the map \(CLI\)](#)).

## Identify routers to define in AFA

Do the following:

1. View the graphic network map.

The **Map** appears in the workspace.



The 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. See Adding Devices (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.

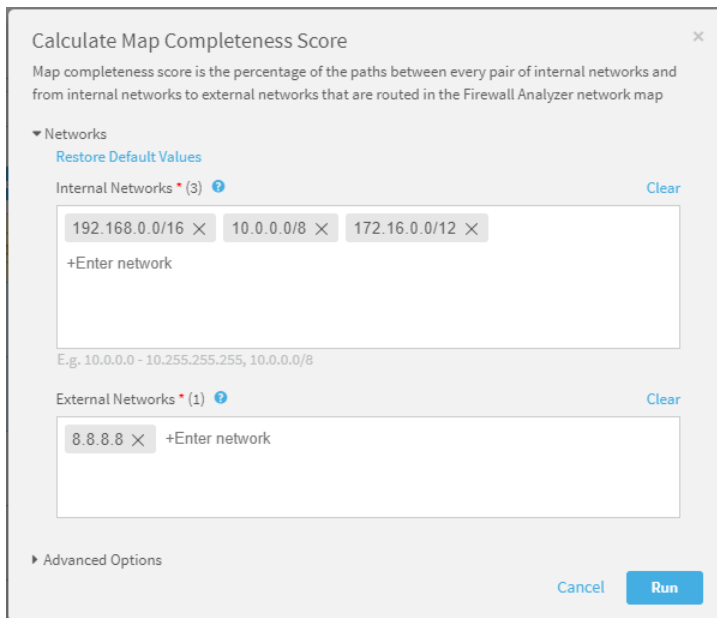
The **Merge Selected** button at the top of the list becomes enabled when two or more routers are selected.

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** [X]

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 X 10.0.0.0/8 X 172.16.0.0/12 X

+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 X +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 [Configure subnet prioritization](#).

**Note:** Make sure to revert these parameters to the 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:

```
10.0.0.0/8192.168.0.0/16
```

- 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:

```
8.8.8.882.102.187.174
```

- **(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:

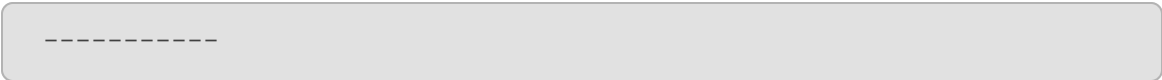
```
map_completeness -i <internal_nets.txt> -e <external_IPs.txt>
```

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.
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
<b>-i</b> <internal_nets.txt>	Yes	Passes the internal networks input file. The value is the relative path to the file.
<b>-e</b> <external_IPs.txt>	Yes	Passes the external IPs input file. The value is the relative path to the file.
<b>-s</b> <snmp_credentials.txt>	No	Passes the SNMP credentials input file. The value is the relative path to the file.
<b>-r</b> <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> .
<b>-m</b> <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> .
<b>-n</b> <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.  <b>Note:</b> This CLI tool does not simulate every possible route, but a sampling. This parameter specifies the size of the sample.
<b>-v</b>	No	Enables verbose mode. The output files will contain additional information which may be useful for debugging. By default, verbose mode is disabled.
<b>-p</b>	No	Specifies the output files should be printed in human-readable format. The default is CSV format.

Parameters	Mandatory?	Description
-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.

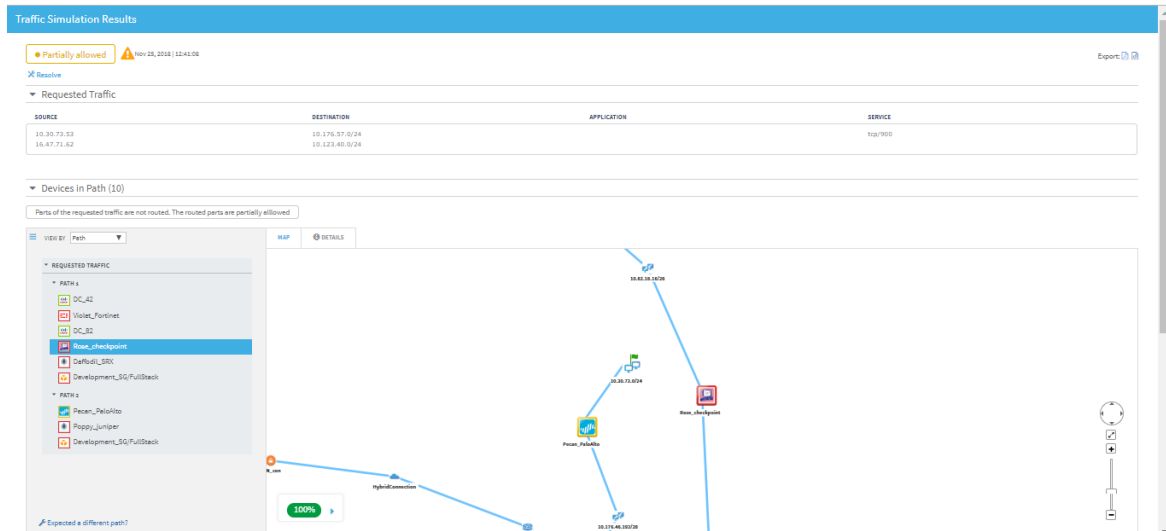
**Note:** The traffic simulation query troubleshooting feature is for AFA administrators only.

**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.



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.

The screenshot shows the 'Troubleshoot Query Results' wizard, Step 1 of 3. It prompts the user to 'Select the traffic line you wish to troubleshoot'. Below this is a table with the following data:

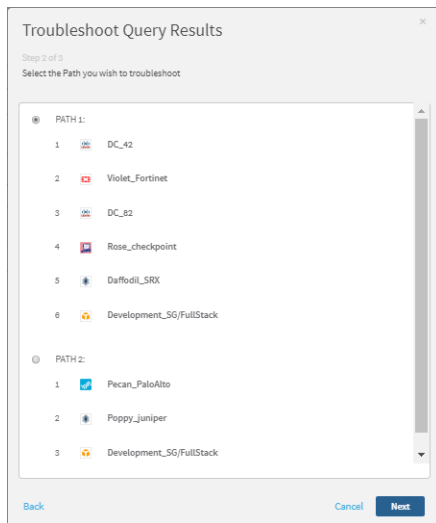
#	Source	User	Destination	Application	Service
1	10.30.73.53		10.178.87.0/24		tcp/900

At the bottom right are 'Cancel' and 'Next' buttons.

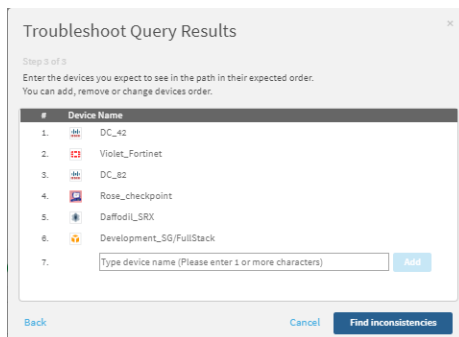
**Note:** If the query has more than one traffic line with unexpected results, you can only troubleshoot one path at a time from one of those traffic lines.

## 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**.



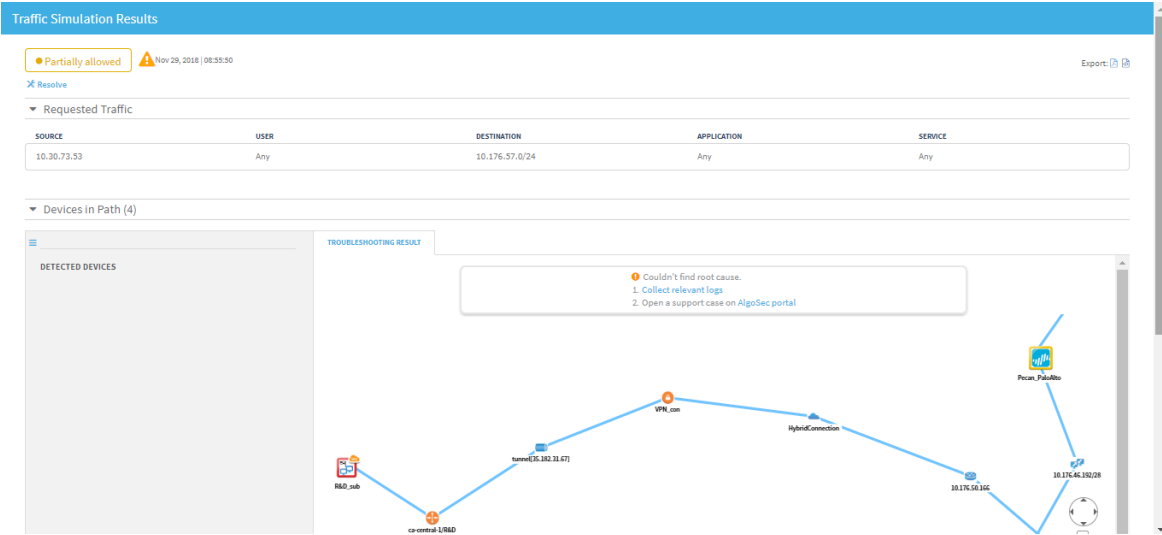
5. Specify the expected path for the query. You can optionally add new devices, change the order of the devices, and/or delete devices.

**Note:** You can only add devices to the path that are currently defined in AFA.

6. 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.



7. Do one of the following:

<p><b>For any of the following cases:</b></p> <ul style="list-style-type: none"><li>Identified problem is an issue with a device</li><li>Root cause could not be detected</li><li>Too many paths were found</li></ul>	<p><b>Do the following:</b></p> <ol style="list-style-type: none"><li>Collect the relevant logs.</li><li>Open a support case on the AlgoSec portal.</li></ol>
<p><b>If there is a missing device</b></p>	<ol style="list-style-type: none"><li>Define the device in AFA.</li><li>Run analysis on the device</li><li>Run the query again.</li></ol>

**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:

<p><b>Remove a range from all clouds except for specific clouds</b></p>	<p>Enter the following command:</p> <pre>fa_map -remove_from_all CIDR -except_stub stub_router_IP [-comment comment]</pre> <p>where, <i>CIDR</i> is the CIDR you want to exclude, <i>stub_router_IP</i> is the IP address of the adjacent router for which you want to keep the CIDR, and <i>comment</i> is a comment for the cloud edit entry (in quotations).</p> <p>You can use the <b>except_stub</b> parameter multiple times to include the CIDR in multiple clouds, as in the following example:</p> <pre>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"</pre>
<p><b>Remove a range from a specific cloud</b></p>	<p>Enter the following command:</p> <pre>fa_map -remove CIDR -stub stub_router_IP [-comment comment]</pre> <p>where, <i>CIDR</i> is the CIDR you want to exclude, <i>stub_router_IP</i> is the IP address of the adjacent router, and <i>comment</i> is a comment for the cloud edit entry (in quotations).</p>

**Note:** The **comment** parameter is optional.

**Note:** The input range must be in CIDR format.

The range is removed from the cloud.

- 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.

The screenshot shows the 'Administration' page in the 'SCHEDULER' tab. The page has a sidebar with navigation icons and a top header with 'Firewall Analyzer', 'Analysis Status', and 'AlgoSec Administrator'.

**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' section of the Firewall Analyzer interface, specifically the 'SCHEDULER' tab. The page title is 'Administration' and the sub-header is 'Schedule Recurring Analysis'. The form is divided into several sections:

- Job Details:**
  - Job name: A text input field containing 'Job 3'.
  - ☐ Base group reports on existing device reports.
  - ☐ Select risk profile: A dropdown menu showing 'Standard'.
  - Run device analysis: A dropdown menu showing 'Default (Always (slow))' with a help icon (?) next to it.
- Select a device/group:**
  - Schedule job for the device / group: Please select a device or a group.
  - A button labeled 'Select device / group'.
- Recurrence:**
  - ☒ Daily
  - ☐ Weekly
  - ☐ Monthly
  - ☐ Quarterly
  - ☐ Yearly
  - ☐ Upon policy install
- Recurrence Pattern:**
  - Set time: Two dropdown menus showing '19' and '30'.

At the bottom right of the form are 'Cancel' and 'OK' buttons.

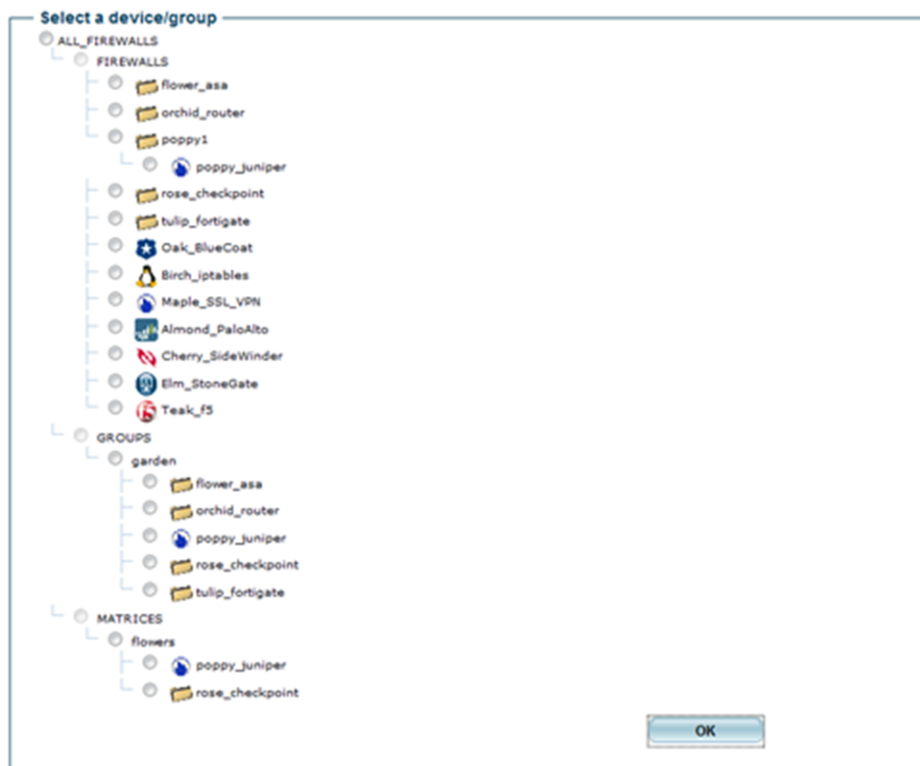
5. In the **Job name** field, type a name for the job.
6. (Optional) To aggregate a group/matrix members' existing reports into a group/matrix report, (instead of generating new reports for each member and using those reports to generate a group/matrix report), select the **Base group reports on existing 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.

- 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:
- Click **Select device/group**.

A tree of all the devices, groups, and matrices appears.



- 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. See [Configuring Event-Triggered Notifications](#) (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.

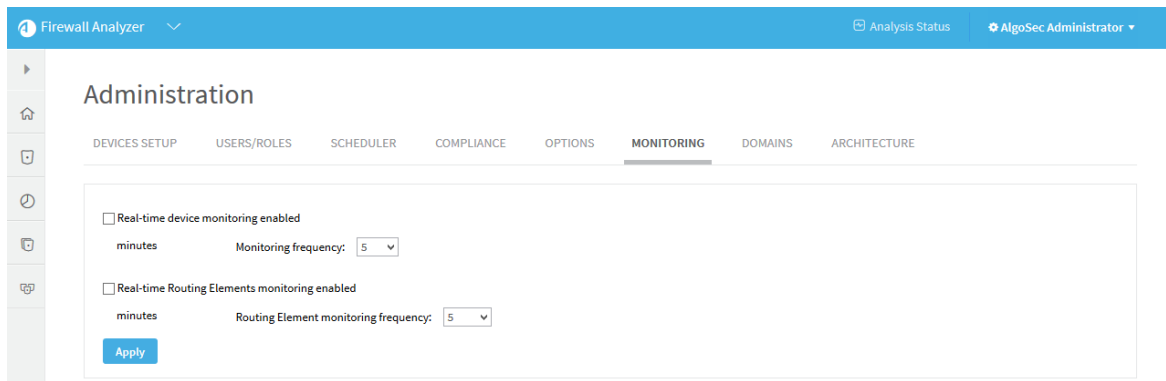
A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Monitoring** tab.

The **Monitoring** page appears.



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**.

# Manage users and roles

This section describes how AFA administrators can manage ASMS users and roles.

## AFA authentication

Users can be authenticated via an authentication server (LDAP or RADIUS) or Single Sign On, in addition to the local AFA database. When an authentication server or SSO is configured, you can additionally fetch user data, enabling other functionality.

For details, see [Configure user authentication](#).

## AFA permissions

There are two types of AlgoSec Firewall Analyzer users:

<b>Non-administrator privileged users</b>	Can run analyses, generate reports, view policies and reports, view network map and monitoring changes, and run traffic simulation queries.
<b>Administrators</b>	<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"> <li>• Manage other users</li> <li>• Define and edit monitored devices</li> <li>• Configure AFA general settings and preferences</li> <li>• Schedule AFA analyses.</li> </ul>

Each user is assigned one of the following access levels as part of their *default permission profile*:

<b>Standard Access</b>	Enables users to view existing reports, run traffic simulation queries, initiate new device analyses, and use the customization features such as customizing the topology.
<b>ReadOnly Access</b>	Enables users to view existing reports and run traffic simulation queries on these reports.

<b>None</b>	<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](#).

When importing user data from an LDAP server is enabled, each AFA role can be associated with an LDAP group. In this case, users will automatically be assigned AFA roles upon login, according to their user group membership on the LDAP. For more details, see [Import user data from an LDAP server](#).

**Important:** When authenticating with an authentication server or Single Sign on, user credentials must be managed on the external server. When importing user data from an LDAP, and assigning roles based on user group membership, roles must all be managed on the LDAP server. In these cases, any changes made in AFA will be overridden the next time the user logs in.

## Configure user authentication

This topic describes how to configure ASMS user authentication, including single sign-on, authentication servers, and LDAP forests.

 **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:

<b>A service provider (SP)</b>	In our case, AlgoSec is a service provider that provides ASMS.
<b>An identity provider (IdP)</b>	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:

<b>Assertion Consumer Service, or the Single Sign On URL</b>	<p>Informs the IdP where ASMS redirects the user for Single Sign On (login) requests.</p> <p>Configured as:</p> <p><code>https://&lt;ASMS URL&gt;/simplesaml/module.php/saml/sp/saml2-accs.php/&lt;SP Identifier&gt;</code></p>
--	---

<b>Single Logout Service</b>	<p>May not be required in all situations. Informs the IdP where ASMS redirects the user for Single Sign Out (logout) requests.</p> <p>Configured as:</p> <p><b>https://&lt;ASMS URL&gt;/simplesaml/module.php/saml/sp/saml2-logout.php/&lt;SP Identifier&gt;</b></p>
------------------------------	--

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
<b>UID</b>	Username	laura
<b>email</b>	Email address	lauras@email.com
<b>displayName</b>	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:

<b>Service Provider identifier</b>	<p>The identifier of the AlgoSec SP.</p> <p>This identifier must be unique, and it must be added to the list of known SPs in your identity provider's configuration.</p>
------------------------------------	--

<b>Identity Provider identifier</b>	The identifier of your installed IdP.
<b>IdP's Single Sign On service URL</b>	The URL of the IdP's Login page.
<b>IdP's Single Sign Out service URL</b>	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

<b>Server</b>	Type the IP address of the LDAP server's host computer.
<b>LDAP Version</b>	Select the version of LDAP used on the LDAP server.

<b>Port</b>	Type the port number on the LDAP server's host computer.
<b>Timeout</b>	Use the arrow buttons to select the maximum amount of time in seconds to wait for the LDAP server's reply.
<b>Secure Connection</b>	<p>Select this option to secure connections with the LDAP server, then choose the method to use for securing the connection: <b>LDAPS</b> or <b>StartTLS</b>.</p> <p>The default method is <b>LDAPS</b>.</p> <p>The value of the <b>Port</b> field changes according to the method selected.</p>
<b>Verify Server Certificate</b>	<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 <b>CA Certificate</b> field appears.</p>
<b>CA Certificate</b>	<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>

<b>Bind Type</b>	<p>Select the bind type to use:</p> <ul style="list-style-type: none"> <li>• <b>Simple.</b> 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.</li> <li>• <b>Regular.</b> 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.</li> <li>• <b>Anonymous.</b> 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.</li> </ul> <p>If you chose <b>Regular</b> or <b>Anonymous</b>, additional fields appear. The default value is <b>Regular</b>.</p>
<b>User DN</b>	<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>
<b>Password</b>	<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

<b>Name</b>	<p>Type the attribute that contains a user's name, in user objects in the database. The default value is <code>sAMAccountName</code>.</p>
<b>Group Membership</b>	<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

<b>Associated Roles</b>	<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 BusinessFlow roles.</p> <p>To manage roles from within the AlgoSec Suite (not the LDAP), do not select this option.</p>
<b>Full Name</b>	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow <b>Full Name</b> field.
<b>Email</b>	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow <b>Email</b> field.
<b>Notes</b>	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow <b>Notes</b> field.

#### FireFlow specific fields

<b>Organization</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Organization</b> field.
<b>Address</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Address</b> field.
<b>City</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>City</b> field.
<b>State</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>State</b> field.
<b>Zip Code</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Zip Code</b> field.
<b>Country</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Country</b> field.
<b>Home Phone</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Home Phone</b> field.

<b>Work Phone</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Work Phone</b> field.
<b>Mobile Phone</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Mobile Phone</b> field.
<b>Pager</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Pager</b> 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

<b>Full Name</b>	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow <b>Full Name</b> field.
<b>Email</b>	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow <b>Email</b> field.
<b>Notes</b>	Type the name of the LDAP server user field from which you want to import data to the AlgoSec Firewall Analyzer and FireFlow <b>Notes</b> field.

### FireFlow specific fields

<b>Organization</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Organization</b> field.
<b>Address</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Address</b> field.
<b>City</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>City</b> field.

<b>State</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>State</b> field.
<b>Zip Code</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Zip Code</b> field.
<b>Country</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Country</b> field.
<b>Home Phone</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Home Phone</b> field.
<b>Work Phone</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Work Phone</b> field.
<b>Mobile Phone</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Mobile Phone</b> field.
<b>Pager</b>	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Pager</b> 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 it's value as the name of the IdP certificate file.

For example:

```
SSOSAML_IdP_Certificate=MyIdPCert.cr
```

## Configure IdP-initated, or unsolicited, SSO

By default, ASMS uses **SP-initiated**, or **solicited SSO**, in which the SP signs the Assertion Certificated passed between the two systems. This is the recommended usage.

ASMS also supports **IdP-initated**, 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:

<b>SSOSAML_IdP_Unsolicited_SSO</b>	<b>Yes/No.</b> Specifies whether to use the IdP method first.
<b>SSOSAML_IdP_Unsolicited_SSO_URL</b>	The IdP's URL.
<b>SSOSAML_IdP_Unsolicited_SSO_SP_ID_KEY</b>	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:
- 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><b>Time assertion failures, such as:</b></p> <ul style="list-style-type: none"><li>• <b>[message:protected] =&gt; Received an assertion that is valid in the future. Check clock synchronization on IdP and SP.</b></li><li>• <b>[message:protected] =&gt; Received an assertion that is valid in the future. Check clock synchronization on IdP and SP.</b></li></ul>	<p>Check the clock configurations on the ASMS machine and the SSO Provider. Both of these clocks must be synchronized, including timezone.</p>
<p><b>Lost sessions and STATE-related errors</b></p>	<p>Verify that the SSO Provider directs the user to ASMS using the same hostname as accessed by the user.</p>

<b>cause:SimpleSAML_Error_Exception:private] =&gt; SimpleSAML_Error_UnserializableException Object</b>	<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 its name in the AFA configuration file: <b>/usr/share/fa/simplesaml/cert/</b></p>
<b>[ message:protected] =&gt; saml20-idp-remote/'Test': Could not find PEM encoded certificate in "/usr/share/fa/simplesaml/cert/server.crt".</b>	<p>The certificate may have an incorrect format.</p> <p>Ensure that the certificate format is PEM.</p>
<b>Users are able to connect from expired sessions</b>	<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:

<b>Local user database</b>	<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>
<b>LDAP server</b>	<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><b>Note:</b> It is possible to use multiple LDAP servers to authenticate users. For more details, see <a href="#">Import user data from an LDAP server</a>.</p>

<b>RADIUS server</b>	<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 <a href="#">Import user data from an LDAP server</a>.</p> <p><b>Note:</b> 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 left sidebar contains various icons for navigation. The main content area is titled 'Administration' and features a tabbed interface with 'OPTIONS' selected. Under the 'OPTIONS' tab, the 'Authentication' sub-tab is active. The 'Authentication' page is divided into several sections: 'User Authentication' (with radio buttons for 'Authentication Server' and 'Single Sign On'), 'Radius Authentication' (with input fields for 'Server', 'Secret key', 'Port', and 'Timeout', and checkboxes for 'Fetch user data from LDAP' and 'Use Secondary Servers'), 'Default for new users' (with radio buttons for 'Local', 'Radius', and 'LDAP'), 'Default Mail Domain' (with a text input field), and 'CyberArk' (with a checkbox for 'Allow to setup devices with CyberArk credentials management' and a 'CYBERARK' logo). At the bottom, there are 'Cancel' and 'OK' buttons.

Firewall Analyzer

Analysis Status

AlgoSec Administrator

### Administration

DEVICES SETUP | USERS/ROLES | SCHEDULER | COMPLIANCE | **OPTIONS** | MONITORING | DOMAINS | ARCHITECTURE

General | Language | Display | Log analysis | Proxy | Mail | Storage | Workflow | **Authentication** | Backup/Restore | Advanced Configuration

#### 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

[Test connectivity](#)

#### 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:

[Cancel](#) [OK](#)

## 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 of Firewall Analyzer. The 'Options' tab is selected, and the 'Authentication' sub-tab is active. Under 'User Authentication', the 'Authentication Server' section has 'Local' and 'RADIUS' checked. The 'Radius Authentication' section contains the following fields:

- Server: [Text field]
- Secret key: [Text field]
- Port: [1812]
- Timeout: [3]
- Fetch user data from LDAP (?): [ ]
- Use Secondary Servers: [ ]

Below these fields, the 'Default for new users' section has 'Local' selected. The 'Default Mail Domain' is empty. At the bottom, there are 'Cancel' and 'OK' buttons.

b. Complete the fields using the information in RADIUS Authentication Fields (see [RADIUS authentication fields](#)).

If you selected the **Use Secondary Servers** check box, additional fields appear.

Continue completing the fields using the information in RADIUS Authentication Fields (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><b>Important:</b> When this option is selected, you must additionally define the LDAP server and configure the import with the <b>Fetch user data from LDAP</b> check box.</p> <p>For more information, see Importing User Data from an LDAP Server (see <a href="#">Import user data from an LDAP server</a>).</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 <b>Secondary Radius Servers</b> area.</p>

### LDAP authentication fields

In this field...	Do this...
<b>LDAP Server Credentials</b>	
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: <b>LDAPS</b> or <b>StartTLS</b>.</p> <p>The default method is <b>LDAPS</b>.</p> <p>The value of the <b>Port</b> 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 <b>CA Certificate</b> 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"> <li>• <b>Simple.</b> 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.</li> <li>• <b>Regular.</b> 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.</li> <li>• <b>Anonymous.</b> 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.</li> </ul> <p>If you chose <b>Regular</b> or <b>Anonymous</b>, additional fields appear.</p> <p>The default value is <b>Regular</b>.</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	Type the attribute that contains a user's name, in user objects in the database. The default value is <code>sAMAccountName</code> .
Group Membership	Type the attribute that contains a user's groups, in user objects in the database. The default value is <code>member</code> .
<b>Permitted Users</b>	
Users Under Base DN	Type the base DN. The baseDN is the highest level in the LDAP tree, where AFA should search. Any entries above this level will not be searched.
Members of Group DN	Type the DN of the LDAP group that includes all users who may log in to AFA and FireFlow.  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.  <b>Note:</b> 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.
Extra Filtering	Type any additional criteria that users must meet in order to be authenticated. The default value is <code>(objectClass=*)</code> .

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 <b>Fields Mapping</b> area.</p> <div> <p><b>Note:</b> 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> </div>
<b>Fields Mapping</b>	
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 BusinessFlow roles.</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 <b>Full Name</b> 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 <b>Email</b> 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 <b>Notes</b> field.
<b>FireFlow specific fields</b>	
Organization	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Organization</b> 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 <b>Address</b> field.
City	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>City</b> field.
State	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>State</b> field.
Zip Code	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Zip Code</b> field.
Country	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Country</b> field.
Home Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Home Phone</b> field.
Work Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Work Phone</b> field.
Mobile Phone	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Mobile Phone</b> field.
Pager	Type the name of the LDAP server user field from which you want to import data to the FireFlow <b>Pager</b> field.
Use Secondary Servers	Select this option to configure one or more secondary LDAP servers. You must complete the fields in the <b>Secondary LDAP Servers</b> area. (See <b>LDAP Server Credentials</b> 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.

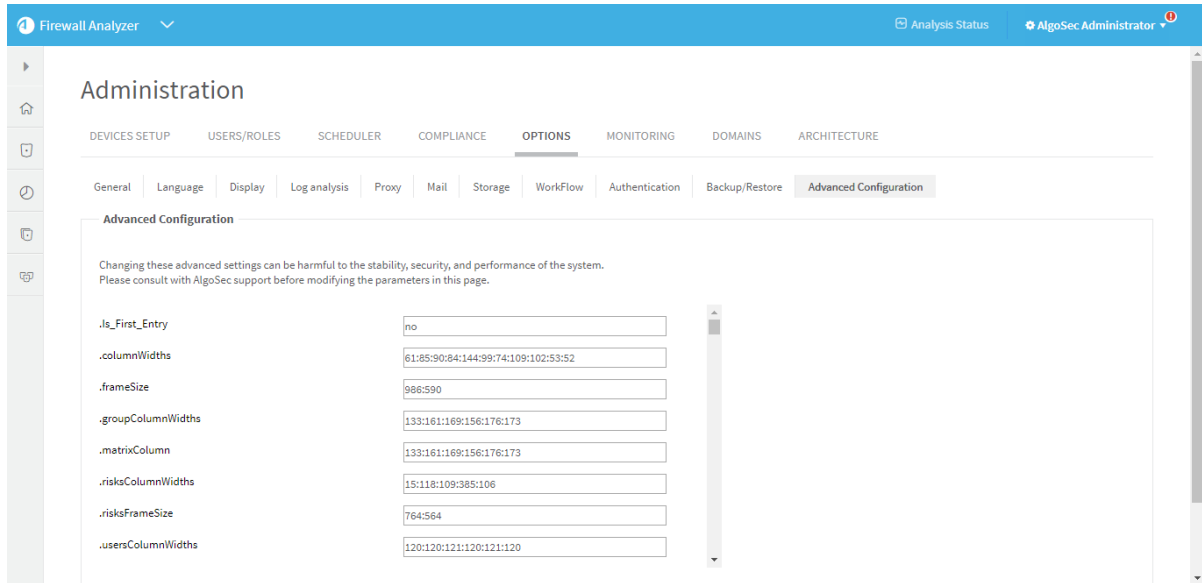
A drop-down menu appears.

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"> <li>• <b>ldaps</b></li> <li>• <b>starttls</b></li> </ul> 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"> <li>• <b>yes</b></li> <li>• <b>no</b></li> </ul> 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"> <li>• <b>yes</b></li> <li>• <b>no</b></li> </ul> <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"> <li>• <b>Simple.</b> 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.</li> <li>• <b>Regular.</b> 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.</li> <li>• <b>Anonymous.</b> 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.</li> </ul> <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	The DN of the user group to which users must belong in order to be authenticated. This parameter is optional.
LDAP_AttrEmail	The name of the LDAP server user field from which you want to import data to AFA and FireFlow <b>Email</b> field. This parameter is optional.
LDAP_AttrFullName	The name of the LDAP server user field from which you want to import data to AFA and FireFlow <b>Full Name</b> field. This parameter is optional.
LDAP_AttrNotes	The name of the LDAP server user field from which you want to import data to AFA and FireFlow <b>Notes</b> field. This parameter is optional.
LDAP_AttrOrganization	The name of the LDAP server user field from which you want to import data to the FireFlow <b>Organization</b> field. This parameter is optional.
LDAP_AttrAddress1	The name of the LDAP server user field from which you want to import data to the FireFlow <b>Address</b> field. This parameter is optional.
LDAP_AttrCity	The name of the LDAP server user field from which you want to import data to the FireFlow <b>City</b> field. This parameter is optional.
LDAP_AttrState	The name of the LDAP server user field from which you want to import data to the FireFlow <b>State</b> field. This parameter is optional.
LDAP_AttrZip	The name of the LDAP server user field from which you want to import data to the FireFlow <b>Zip Code</b> field. This parameter is optional.

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 <b>Country</b> 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 <b>Home Phone</b> 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 <b>Work Phone</b> 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 <b>Mobile Phone</b> 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 <b>Pager</b> 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=*)
LDAP_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,departmen
t

```

## 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

**Important:** When authenticating with an authentication server or Single Sign on, user credentials must be managed on the external server. When importing user data from an LDAP, and assigning roles based on user group membership, roles must all be managed on the LDAP server. In these cases, any changes made in AFA will be overridden the next time the user logs in.

**Note:** AFA administrators who are not FireFlow administrators can manage FireFlow roles and unprivileged users (requestors) via the AFA web interface. The procedure begins in AFA and you are transferred to FireFlow.

## Add and edit users

**Note:** It is possible to import users from a CSV file. For details, see [Import users via CSV](#).

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 'Administration' page of the Firewall Analyzer. The top navigation bar includes 'Firewall Analyzer', 'Analysis Status', and 'AlgoSec Administrator'. The left sidebar contains icons for home, dashboard, and settings. The main content area is titled 'Administration' and features a horizontal menu with tabs: 'DEVICES SETUP', 'USERS/ROLES', 'SCHEDULER', 'COMPLIANCE', 'OPTIONS' (selected), 'MONITORING', 'DOMAINS', and 'ARCHITECTURE'. Below this, there is a sub-menu for the 'OPTIONS' tab with items: 'General', 'Language', 'Display', 'Log analysis', 'Proxy', 'Mail', 'Storage', 'WorkFlow', 'Authentication', 'Backup/Restore', and 'Advanced Configuration'. The 'General' sub-tab is active, showing 'Analysis Options' with several checkboxes and input fields. The checkboxes are: 'Comprehensive mode - analyze every service defined on the device (slow)' (checked), 'With IP address name lookups (slow)' (unchecked), 'Include traffic changes analysis in Change History (slow)' (checked), 'Timed rules: only apply rules active at analysis time' (checked), and 'Use public key authentication in data collection' (unchecked). The input fields are: 'Simulation timeout (seconds):' (120), 'Data collection timeout (seconds):' (120), 'Days before expiration alerts:' (31), and 'Report rules whose comment field' (does not match). There is a 'Details' button next to the 'Report rules' field. Below the 'Analysis Options' section is the 'Default Scheduled Analysis Options' section, which includes a dropdown for 'Run device analysis:' set to 'Only if the policy/topology changed'. At the bottom are 'Cancel' and 'OK' buttons.

3. In the **Options** tab, click the **Users/Roles** sub-tab.

The **User and Role Management** page appears.

Firewall Analyzer Analysis Status AlgoSec Administrator

## Administration

DEVICES SETUP **USERS/ROLES** SCHEDULER COMPLIANCE OPTIONS MONITORING DOMAINS ARCHITECTURE

Manage the users, roles, their permissions and configurations

	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	

[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	

[Delete](#) [New](#)

[Manage FireFlow roles](#)

[Manage FireFlow requestors](#)

#### 4. Do one of the following:

- To add a new user, under the list of users, click **New**.
- To edit an existing user, click in the desired user's row.

New fields appear.

Firewall Analyzer

Analysis Status

AlgoSec Administrator

Administration

DEVICES SETUPUSERS/ROLES

SCHEDULERCOMPLIANCEOPTIONS

MONITORINGDOMAINSARCHITECTURE

Manage the users, roles, their permissions and configurations

User details

Username:

Full name:

E-Mail:

Notes:

Authentication:

Local

Landing Page:

Automatic

Password

New password:

Confirm password:

The authorized devices and permissions granted to a user include all permissions granted specifically for the user (below) as well as permissions derived from the user's roles.

General Permissions

☐ Administrator

☐ FireFlow Administrator - Allow FireFlow Advanced Configuration

☒ Enable Analysis from file

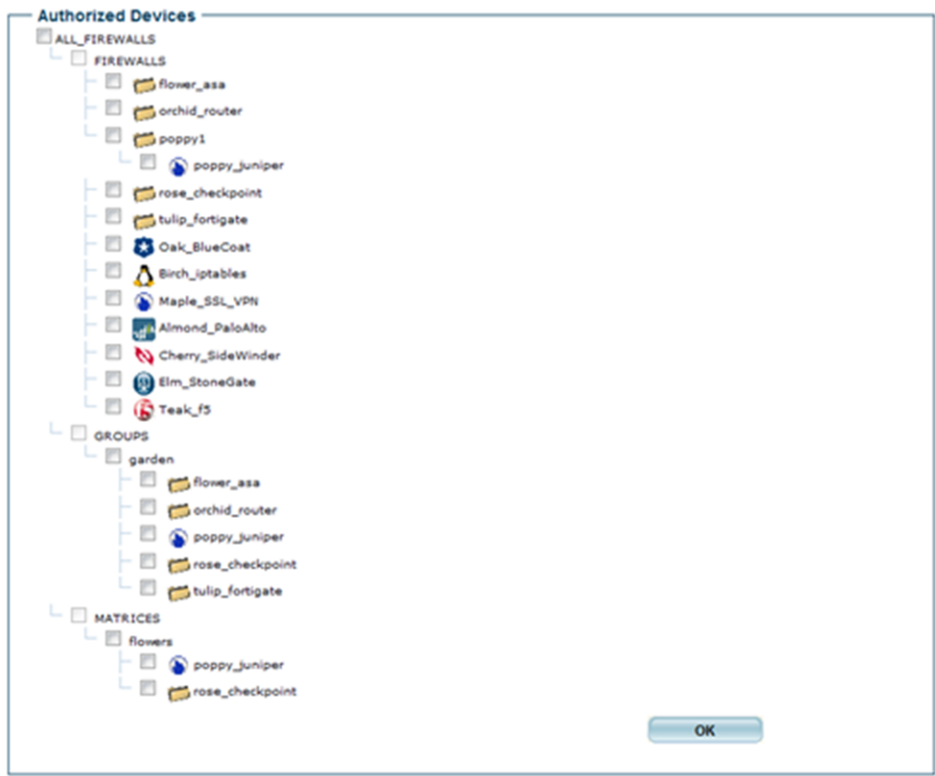
☒ Enable Trusted Traffic -> global

Roles

	Role Name	Role Description
<input type="checkbox"/>	Admins	AFA + FF Admins - full access
<input type="checkbox"/>	helpdesk	For helpdesk staff - query only

5. Complete the fields using the information in User Fields (see [User fields](#)).
6. Specify the devices and groups that the user should be able to view , by doing the following in the **Authorized Devices** area:
- a. Click **Select devices**.

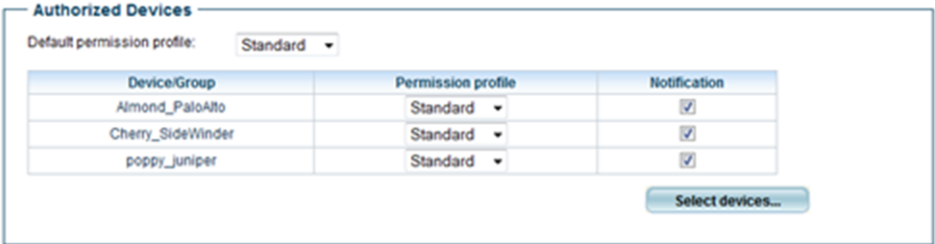
A tree of all the devices and groups appear.



b. Choose the desired devices and groups.

c. Click OK.

The selected devices and groups are listed in the **Authorized Devices** area. Each device or group is assigned the access level specified in the default permission profile.



d. To change the access level for a device or group, in the device or group's **Permission profile** drop-down list, select the desired access level.

e. To specify that AFA should send e-mail notifications regarding a device or

group, select the device or group's **Notification** check box.

7. Click **OK**.

### User fields

In this field...	Do this...
<b>User details</b>	
Username	Type a username for the user. Usernames can contain any alpha-numeric character and the following special characters: "@", "_", ".", or "-". See <a href="#">ASMS username and password requirements</a> .
Full name	Type the user's full name.
E-Mail	Type the user's e-mail address.
Notes	Type any notes about the user.
Authentication	Select how to authenticate this user: <ul style="list-style-type: none"> <li>• <b>Local</b>. Authenticate the user against the local ASMS user database.</li> <li>• <b>RADIUS</b>. Authenticate the user against a RADIUS server.</li> <li>• <b>LDAP</b>. Select this option to enable user authentication against an LDAP server.</li> </ul> For more details, see <a href="#">Configure user authentication</a> .
Landing Page	Select one of the three products, or <b>Automatic</b> . For more details, see <a href="#">Default landing pages per role</a> .
<b>Password</b>	
New password	Type a password for the user. Passwords can contain any alpha-numeric character or any special character, excluding back ticks (`). See <a href="#">ASMS username and password requirements</a> .
Confirm password	Re-type the password you entered in the <b>New password</b> field.

In this field...	Do this...
<b>General Permissions</b>	
Administrator	Select this option to make the user an administrator.
FireFlow Administrator - Allow FireFlow Advanced Configuration	Select this option to make the user a FireFlow configuration administrator. This enables the user to perform advanced configuration tasks in FireFlow.
Enable Analysis from file	Select this option to allow the user to perform analyses from configuration files.
Enable Trusted Traffic -> global	Select this option to allow the user to view trusted traffic.
<b>Roles</b>	
	<p>Select the user roles to assign the user. The user will automatically be granted the permissions specified in the assigned roles.</p> <p><b>Note:</b> You can assign additional permissions to this user, as desired. The user will then have both the permissions inherited from their roles, as well as the permissions assigned specifically to this user.</p>
<b>E-mail Notifications</b>	
Changes in risks	Select this option to specify that the AFA system should send notifications to the user when there are changes in risks.
Changes in policy	Select this option to specify that the AFA system should send notifications to the user when changes are made to policies.
Every group report	Select this option to specify that the AFA system should send notifications to the user when a group report is generated.
Every report	Select this option to specify that the AFA system should send notifications to the user when a report is generated.

In this field...	Do this...
Every configuration change	Select this option to specify that the AFA system should send notifications to the user when configuration changes are made.
Rules and VPN Users about to expire	<p>Select this option to specify that the AFA system should send notifications to the user when device rules and/or VPN users are about to expire.</p> <p>To configure the number of days before rule or VPN user expiration that AFA should send a notification, complete the <b>Days before expiration alerts</b> field in the <b>General</b> sub-tab of the <b>Options</b> tab in the Administration area. For details, see <a href="#">Define AFA preferences</a>.</p>
Error messages	<p>Select this option to specify that the AFA system should send error messages to the user. These include low disk space and license expiration warnings.</p> <p>This field is only relevant for administrators.</p>
Changes in customization	<p>Select this option to specify that 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 field is only relevant for administrators.</p>
Hide change details	<p>Select this option to omit change details from emails about new reports and from change alerts, and include only the device name and a link to the AFA Web interface.</p> <p><b>Note:</b> It is possible to hide change details globally, for all users. The global setting overrides individual users' <b>Hide change details</b> setting. For details, see <a href="#">Configure change detail display</a>.</p>
Authorized Views and Actions	

In this field...	Do this...
Report	<p>Select the report pages/information that the user can view. Select <b>Full Report</b> to indicate that the user can view all report information. Pages that are not selected will be inaccessible to the user.</p> <p><b>Note:</b> A user can only be given access to <b>Configuration and Logs</b> information if they have access to the <b>Explore Policy</b> page.</p>
Home Views	<p>Select the <b>Home</b> page elements that the user can view. Select <b>All Home Views</b> To indicate that the user can view all <b>Home</b> 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><b>Note:</b> 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 <b>All Actions</b> to indicate that the user can perform all actions.</p> <p>Controls used to perform actions that are not selected will be disabled.</p>
<b>Authorized Devices</b>	
Default permission profile	Select the user's default access level to devices.

## 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 as follows:

1. BusinessFlow
2. FireFlow
3. AlgoSec Firewall Analyzer

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
<b>Administrators</b>	AlgoSec Firewall Analyzer
<b>AFA Users</b>	The following, in order of priority: <ol style="list-style-type: none"> <li>1. FireFlow, if licensed and activated</li> <li>2. BusinessFlow, if licensed, and activated with a minimum of 5 applications</li> <li>3. AlgoSec Firewall Analyzer</li> </ol>
<b>Requestors (unprivileged users)</b>	<ol style="list-style-type: none"> <li>1. BusinessFlow, if licensed, and activated with a minimum of 5 applications</li> <li>2. AlgoSec Firewall Analyzer</li> </ol>

## Delete users

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 **Users/Roles** sub-tab.

The **User and Role Management** page appears.

4. Select the check box next to the desired user.
5. Under the list of users, click **Delete**.

A confirmation message appears.

6. Click **OK**.

The user is deleted from AFA.

## Add and edit user roles

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 **Users/Roles** tab.

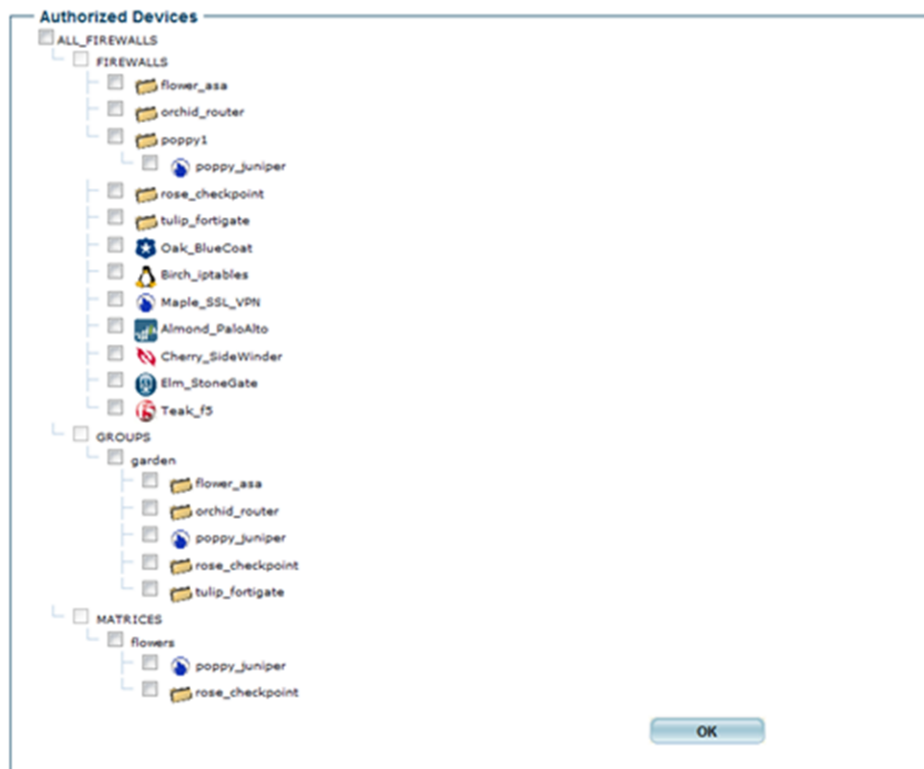
The **User and Role Management** tab appears.

4. Do one of the following:
  - To add a new role, under the list of roles, click **New**.
  - To edit an existing role, click  in the desired role's row.

New fields appear.

5. Complete the fields using the information in Role Fields (see [Role fields](#)).
6. Specify the devices and groups that a user with this role should be able to view, by doing the following in the **Authorized Devices** area:
  - a. Click **Select devices**.

A tree of all the devices and groups appears.



- b. Choose the desired devices and groups.
- c. Click **OK**.

The selected devices and groups appear in the **Authorized Devices** area. Each device or group is assigned the access level specified in the default permission profile.

**Authorized Devices**

Default permission profile: Standard ▾

Device/Group	Permission profile	Notification
Almond_PaloAlto	Standard ▾	<input checked="" type="checkbox"/>
Cherry_SideWinder	Standard ▾	<input checked="" type="checkbox"/>
poppy_juniper	Standard ▾	<input checked="" type="checkbox"/>

Select devices...

- d. To change the access level for a device or group, in the device or group's **Permission profile** drop-down list, select the desired access level.
- e. To specify that AFA should send e-mail notifications regarding a device or group, select the device or group's **Notification** check box.

7. Click **OK**.

## Role fields

In this field...	Do this...
<b>Role details</b>	
Role name	Type a name for the role.
Role description	Type a description of the role.
Role LDAP DN	<p>Type the DN of the LDAP group that corresponds to this role. 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><b>Note:</b> 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 <b>Fetch user data from LDAP</b> option on the <b>OPTIONS &gt; Authentication</b> tab in the AFA <b>Administration</b> area. For details, see <a href="#">Import user data from an LDAP server</a>.</p>
Landing Page	Select one of the three products, or <b>Automatic</b> . For more information, see <a href="#">Default landing pages per role</a> .

In this field...	Do this...
<b>General Permissions</b>	
Administrator	Select this option to make the user an administrator.
FireFlow Administrator - Allow FireFlow Advanced Configuration	Select this option to make the user a FireFlow configuration administrator. This enables the user to perform advanced configuration tasks in FireFlow.
Enable Analysis from file	Select this option to allow the user to perform analyses from configuration files.
Enable Trusted Traffic -> global	Select this option to allow the user to view and edit trusted traffic settings.
<b>Authorized Views and actions</b>	
Report	Select the report pages that the user can view. Select <b>Full Report</b> to indicate that the user can view all report pages. Pages that are not selected will be inaccessible to the user.
Home Views	Select the <b>Home</b> page elements that the user can view. Select <b>All Home Views</b> to indicate that the user can view all <b>Home</b> page elements. Pages that are not selected will be inaccessible to the user.
Actions	Select the actions that the user can perform in AFA. Select <b>All Actions</b> to indicate that the user can perform all actions. Controls used to perform actions that are not selected will be disabled.
<b>Authorized Devices</b>	
Default permission profile	Select the user's default access level to devices.

## Delete user roles

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 **Users/Roles** tab.

The **User and Role Management** page appears.

4. Select the check box next to the desired role.

5. Under the list of roles, click **Delete**.

A confirmation message appears.

6. Click **OK**.

The role is deleted.

## 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,customer support,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"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>
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"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>

Header Name	Description	Possible Values
all_changes	Indicates whether the AFA system should send notifications to the user when a report is generated.	<ul style="list-style-type: none"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>
configuration_changes	Indicates whether the AFA system should send notifications to the user when configuration changes are made.	<ul style="list-style-type: none"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>
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"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>
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"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>

Header Name	Description	Possible Values
customizations	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.  This header is only relevant for administrators.	<ul style="list-style-type: none"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>
authentication_type	The type of authentication to use for this user.  For information on configuring AFA to work with a RADIUS Server or an LDAP server, see <a href="#">Configure user authentication</a> .	<ul style="list-style-type: none"> <li>• <b>local</b>. Authenticate the user against the local AFA user database.</li> <li>• <b>radius</b>. Authenticate the user against a RADIUS server.</li> <li>• <b>ldap</b>. Authenticate the user against an LDAP server.</li> </ul>
administrator	Indicates whether to make the user an administrator.	<ul style="list-style-type: none"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>
run_file_analysis	Indicates whether to allow the user to perform analyses from configuration files.	<ul style="list-style-type: none"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>

Header Name	Description	Possible Values
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"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>
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"> <li>• <b>yes</b></li> <li>• <b>no</b> (Default)</li> </ul>
default_fw_profile	The user's default access level to devices.	<ul style="list-style-type: none"> <li>• <b>readonly</b></li> <li>• <b>none</b></li> <li>• <b>standard</b> (Default)</li> </ul>
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>  where:</p> <ul style="list-style-type: none"> <li>• <code>deviceName</code> is the device's name</li> <li>• <code>notify</code> indicates whether the user should receive notifications about the device (<code>yes/no</code>)</li> <li>• <code>permissionProfile</code> is the user's access level to the device (<code>readonly/none/standard</code>)</li> </ul> <p>Multiple devices should not be separated by anything  For example:</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <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
<code>-f CSVFile</code>	The name of the CSV file.  <b>Note:</b> The file must be located in the current directory.

# 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.

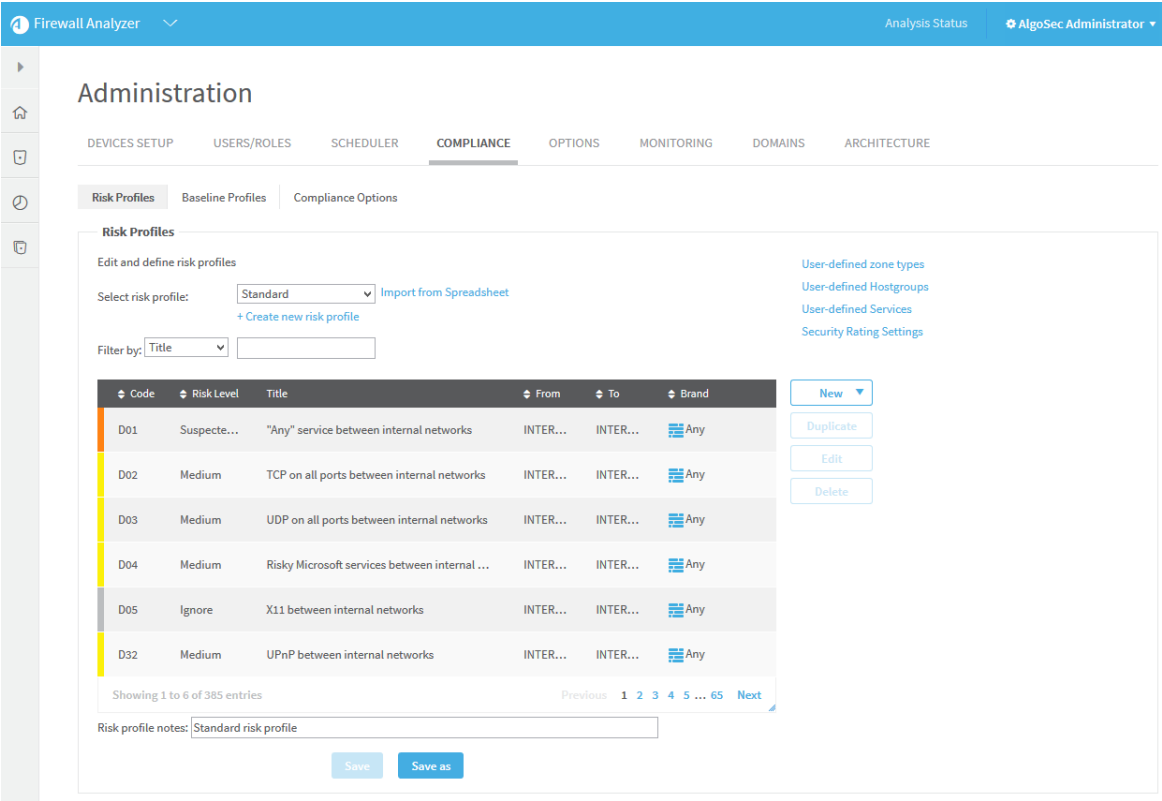
 **Edit a Risk Profile:** Watch to learn how to edit a risk profile to suit your network needs.

## 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"><li>• <b>Brown</b> = Low</li><li>• <b>Yellow</b> = Medium</li><li>• <b>Orange</b> = Suspected High</li><li>• <b>Red</b> = High</li><li>• <b>Grey</b> = Ignored</li></ul> <p><b>Note:</b> Ignored risk items are listed in AFA reports towards the bottom of the <b>Risk Assessment</b> page, and not in the main page with other detected risks.</p>
Title	The risk item's title, or name.

<b>From / To</b>	The source and destination zone of connections specified by the risk item.
<b>Brand</b>	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](#).

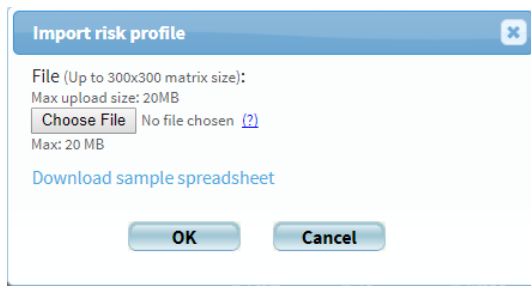
## Create a new risk profile from a spreadsheet

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:

<b>Source / destinations</b>	<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 <b>Networks</b> tab, or the predefined <b>Other</b> object.</p> <p>The <b>Other</b> object includes all IP addresses that are not included in network objects listed on the <b>Networks</b> tab, and generally includes the public internet.</p>
------------------------------	---

<b>Service objects</b>	<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"> <li>To define safe traffic, enter the name of a safe service object.</li> <li>To define risky traffic, enter the name of a risky service object using the following syntax: <b>not(service_object)</b> or <b>!service_object</b></li> <li>To define multiple service objects in a single cell, enter each object name on a new line in the cell (<b>ALT+ENTER</b>).</li> </ul> <p>Service object values must either be listed on the <b>Services</b> tab, or be one of the following predefined services:</p> <ul style="list-style-type: none"> <li><b>Any</b>. All services</li> <li><b>None</b>. No services.</li> </ul>
------------------------	--

**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:

<b>Object names</b>	List object names in the left column.
<b>Object content</b>	<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>
<b>Object names</b>	Object names support lowercase and uppercase letters, digits, and underscores (_).
<b>Network objects</b>	Network objects support single IP addresses, subnets, or ranges.
<b>Service objects</b>	<p>Service objects support:</p> <ul style="list-style-type: none"> <li>Protocol/port format for TCP, UDP, and ICMP protocols</li> <li>Other standard names such as SSH, FTP, and so on, including AlgoSec standard services</li> </ul>

## 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:

<b>Specify severity for all traffic from a specific source</b>	Indicate the severity level with the network object in the left column.
<b>Specify severity for all traffic from a specific destination</b>	Indicate the severity level with the network object in the header row.
<b>Specify severity for all traffic from a specific source and to a specific destination</b>	<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"> <li>• By default, the generated risk will be relevant to all traffic between the services, via services other than those included in the service object.</li> <li>• 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.</li> </ul>

<b>Specify multiple severity levels for traffic from a specific source to a specific destination</b>	<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"> <li>Place each object on a new line in the cell (ALT+ENTER)</li> <li>The first object in the cell can be safe or negated. All other objects must be negated.</li> </ul>
--	---

**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	PClzone;S	Other
<b>Net1</b>	-	!(forbiddenSvc)	SecureSrvs ; C2	Any	SecureSrvs	Any
<b>Net2</b>	Any	-	Any	Any	SecureSrvs	Any
<b>Net3</b>	OnlySrv/X	!(OnlySrv/X)	-	Any	SecureSrvs	Any
<b>PartnerNet</b>	PartnerSrv	!PartnerSrv ; C1	!PartnerSrv ; C1	Any	SecureSrvs	Any
<b>PClzone;S</b>	SecureSrvs ; M !forbiddenSvc ; H	SecureSrvs	SecureSrvs ; C2	SecureSrvs ; C3	-	None;H
<b>Other</b>	-	-	http_Services	-	None;H	Any

In this example, AFA will use the data in the highlighted cell to generate risks with the following severities:


<b>High</b>	Traffic from <b>PCIZone</b> to <b>Net1</b> , via <b>forbiddenSvc</b>
<b>Medium</b>	Traffic from <b>PCIZone</b> to <b>Net1</b> , via any services other than those defined in <b>forbiddenSvc</b> or <b>SecureSrvs</b>
<b>Not risky</b>	Traffic from <b>PCIZone</b> to <b>Net1</b> , via <b>SecureSrvs</b>

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.

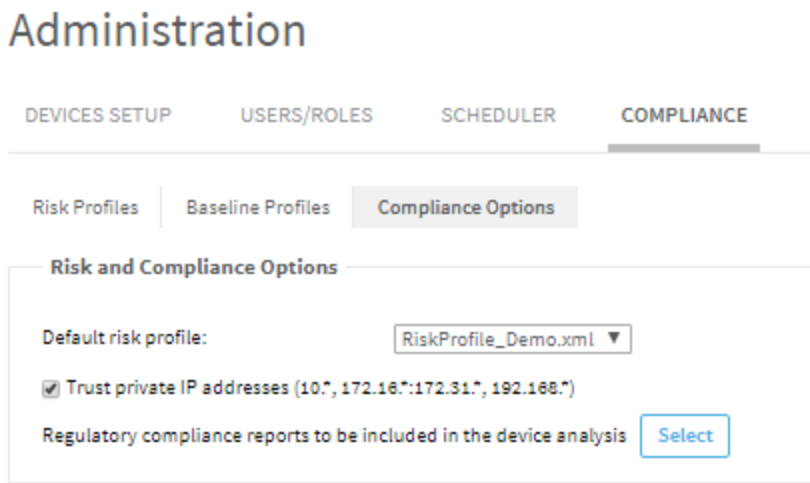
## Set a default risk profile

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:



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:

<b>Edit an existing risk item</b>	Select the risk in the grid, and click <b>Edit</b> .  The risk item is opened for editing. Make your changes as needed, and then click <b>OK</b> .
-----------------------------------	--

<b>Duplicate an existing risk item</b>	<p>Select the risk in the grid, and click <b>Duplicate</b>.</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 <b>OK</b>.</p>
<b>Create a new risk item</b>	<p>Click <b>New</b>, and then select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Basic risk.</b> Create a basic risk</li> <li>• <b>Risk with destination threshold.</b> Create a risk item with a specific destination threshold</li> <li>• <b>Risk with source threshold.</b> Create a risk with a specific source threshold</li> <li>• <b>Risk with specific IP addresses.</b> Create a risk with specific IP addresses, an IP address range, or a subnet</li> <li>• <b>PCI risk.</b> Create a risk that refers to PCI zones</li> </ul>

3. Populate the fields as needed for your risk item type. For details, see:

- [Risk Info fields](#)
- [Risk Query fields](#)
- [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
<b>From zone / To Zone</b>	<p><b>Relevant for</b> 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>
<b>With service</b>	<p><b>Relevant for</b> 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><b>Note:</b> 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 <b>algosec_</b>.</p> <p><b>Tip:</b> Alternately, create a new service group that consists of one or more services. To do this, click <b>Create New</b>. For more details, see <a href="#">Customize services</a>.</p>
<b>Source / Destination / PCI zone</b>	<p><b>Relevant for:</b> 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 <b>Add</b> to use a wizard. There, select a method to use to define your source or destination, including:</p> <ul style="list-style-type: none"> <li>• An individual <b>IP address</b></li> <li>• An <b>IP address range</b></li> <li>• <b>Host group</b> defined on the device</li> <li>• <b>AlgoSec Hostgroup</b>, a host group defined by AlgoSec</li> </ul> <p>Enter subsequent values to continue through the wizard, following on-screen instructions as needed.</p>
<b>Trust VPN IP addresses</b>	<p><b>Relevant for</b> 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><b>Default</b> = Enabled</p>

Name	Description
<b>Threshold on Destination / Source IP address</b>	<p><b>Relevant for</b> 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>
<b>Advanced</b>	<p><b>Relevant for</b> all risk types</p> <p>Define an XQL query for the risk item.</p> <p>Click <b>Advanced</b> and enter your query in the <b>Advanced Query Editor</b>.</p> <p><b>Warning:</b> 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 <a href="#">Advanced risk editing</a>.</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:

<b>Assessment / Remedy</b>	<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"> <li>Both <b>Assessment</b> and <b>Remedy</b> values can be written in any language.</li> <li>Optionally, include keywords that link the risk item's assessment or remedy to other parts of the AFA report.</li> </ul> <p>Insert keywords by typing them directly or click <b>Insert Field</b> to select them from a list.</p> <p>For more details, see <a href="#">Assessment and remedy keywords</a>.</p>
----------------------------	--

<b>Description</b>	<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>
<b>Suppressed by</b>	<p>Enter the codes of other risk items that should prevent the current risk item from appearing in AFA reports or click <b>Select</b> to select them from a list.</p> <p><b>Note:</b> 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 <a href="#">Suppression in AFA</a>.</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:

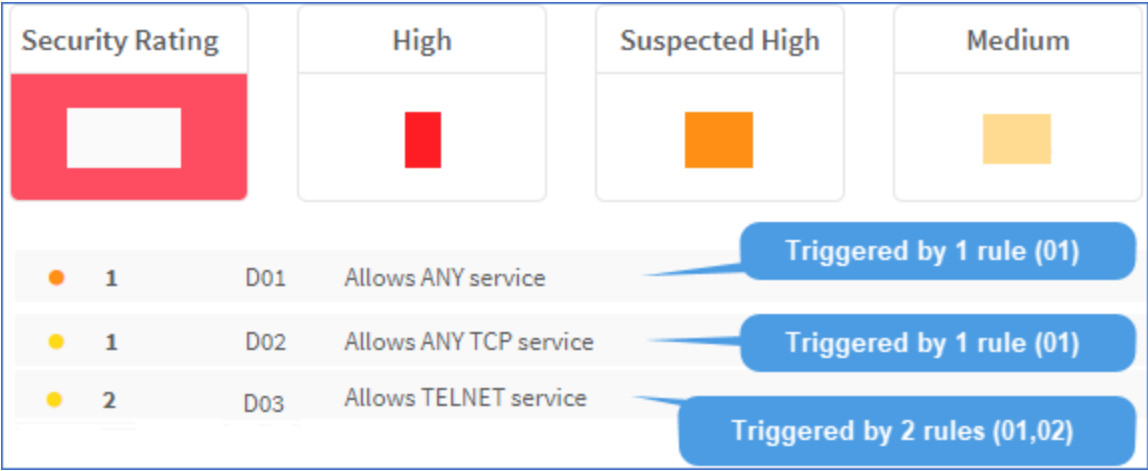
If you have a device with the following rules ...

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:



If suppression is configured:

If you've configured the device's risk profile to include suppression as follows:

- D02 is suppressed by D01:

Risk Info

Title:

Allows ANY TCP service

Risk details

Suppressed by:

D01 (Allows ANY service)

Select

- D03 is suppressed by D02:

Risk Info

Title:

Allows TELNET service

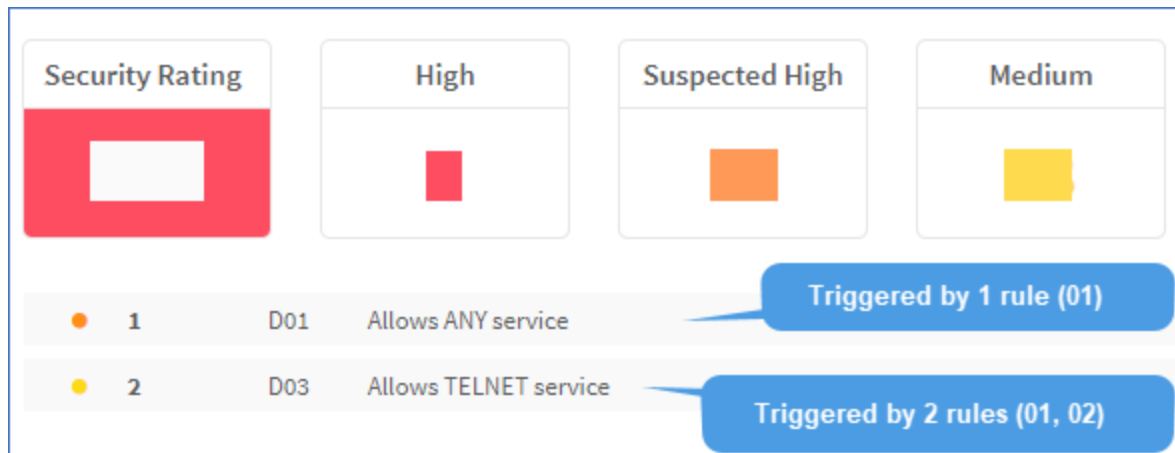
Risk details

Suppressed by:

D02 (Allows ANY TCP service)

Select

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
<b>External</b>	Red	Represents network zones that are directly connected to the Internet.	The "Outside" zone is assigned to this zone type.
<b>Internal</b>	Blue	Represents network zones that are not connected to the Internet.	The "Inside" zone is assigned to this zone type.
<b>DMZ</b>	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**.

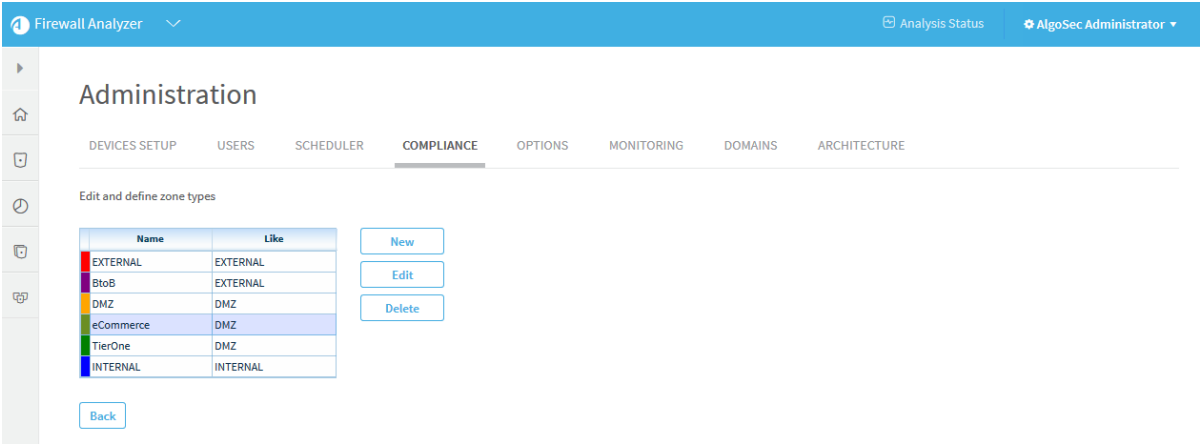
The **Administration** page appears, displaying the **Options** tab.

3. Click the **Compliance** tab.

The **Compliance** tab appears, displaying the **Risk Profiles** sub-tab.

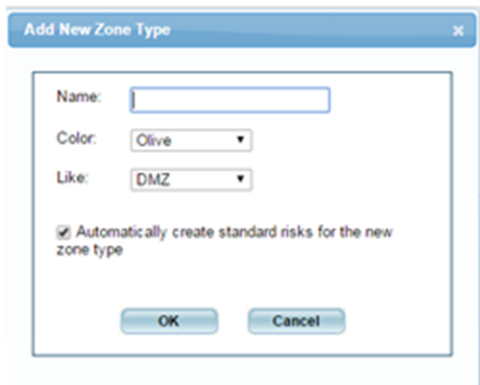
4. Click [User-defined zone types](#).

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**.

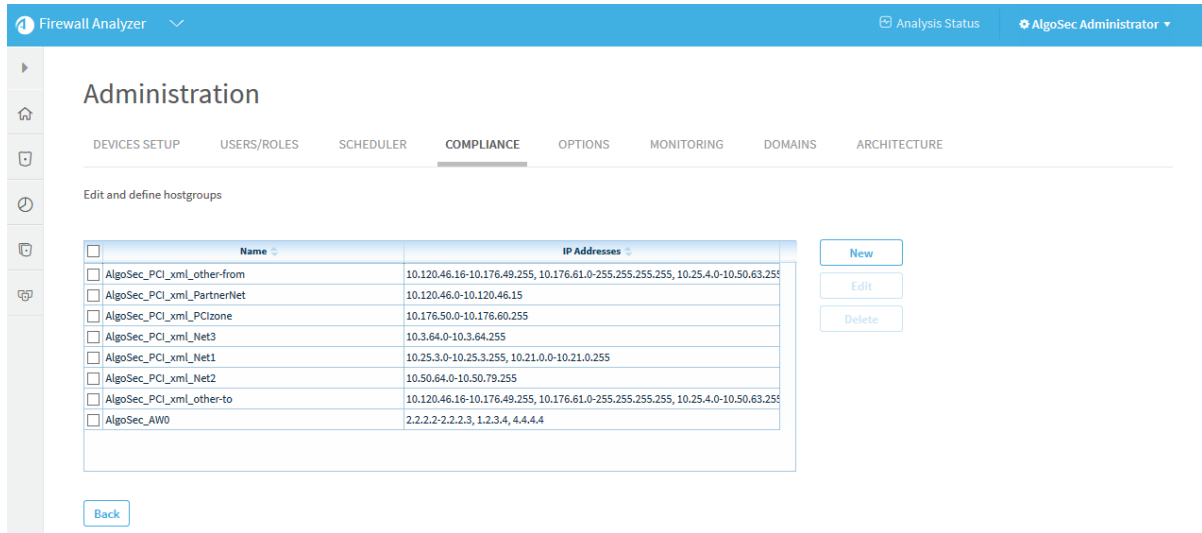
The **Administration** page appears, displaying the **Options** tab.

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.



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**.

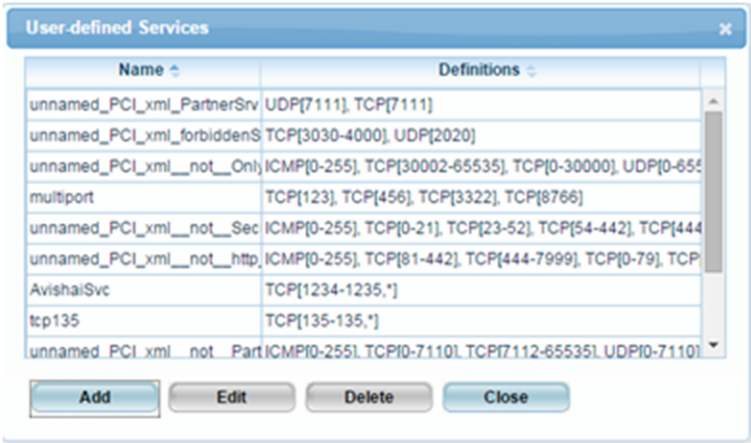
The **Administration** page appears, displaying the **Options** tab.

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.



- 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.



- In the **Service group name** field, type the service group's name.
- 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 <b>High</b> risks. <b>Default = 10.</b>
$W_2$	The weight of <b>Suspected High</b> risks. <b>Default = 4.</b>
$W_3$	The weight of <b>Medium</b> risks. <b>Default = 2.</b>

This variable...	Represents...
$W_4$	The weight of <b>Low</b> risks. <b>Default</b> = 1.
$X_1$	The number of <b>High</b> risks detected in the current device policy.
$X_2$	The number of <b>Suspected High</b> risks detected in the current device policy.
$X_3$	The number of <b>Medium</b> risks detected in the current device policy.
$X_4$	The number of <b>Low</b> risks detected in the current device policy.
$T_1$	The maximum number of <b>High</b> risks possible for the device. This is determined by the device's brand and topology.
$T_2$	The maximum number of <b>Suspected High</b> risks possible for the device. This is determined by the device's brand and topology.
$T_3$	The maximum number of <b>Medium</b> risks possible for the device. This is determined by the device's brand and topology.
$T_4$	The maximum number of <b>Low</b> 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:

<b>If the same risk item is flagged on all 100 devices</b>	The group security rating will also be <b>99</b> , since 99 of the 100 possible risk items are still not flagged.
<b>If each device is flagged for a different risk item</b>	The group security rating will be <b>0</b> , 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**.

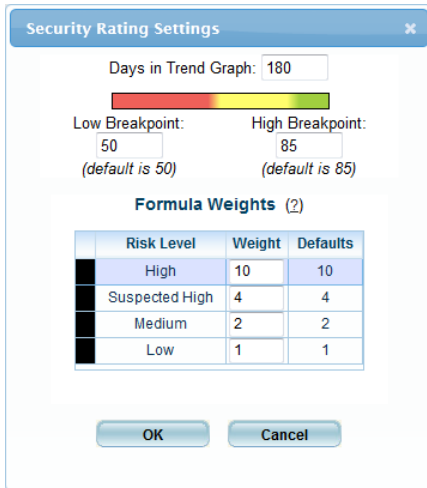
The **Administration** page appears, displaying the **Options** tab.

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.



The **Security Rating Settings** dialog box contains the following elements:

- Days in Trend Graph:** A text box with the value 180.
- Low Breakpoint:** A text box with the value 50, with "(default is 50)" below it.
- High Breakpoint:** A text box with the value 85, with "(default is 85)" below it.
- Formula Weights (2):** A table with 4 columns: Risk Level, Weight, and Defaults.
- Buttons:** OK and Cancel buttons at the bottom.

Risk Level	Weight	Defaults
High	10	10
Suspected High	4	4
Medium	2	2
Low	1	1

5. Complete the fields using the information in the following table.

<b>Days in Trend Graph</b>	Type the number of days to include in the <b>Security Rating Trend</b> graph in the <b>Risks</b> page of reports. The default value is 180 days.
<b>Low Breakpoint</b>	Type a number representing the point on the security ratings bar where the bar should changes from red to yellow, if the leftmost end of the bar is 0 and the rightmost end is 100. The default value is 50.
<b>High Breakpoint</b>	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.
<b>Formula Weights</b>	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.

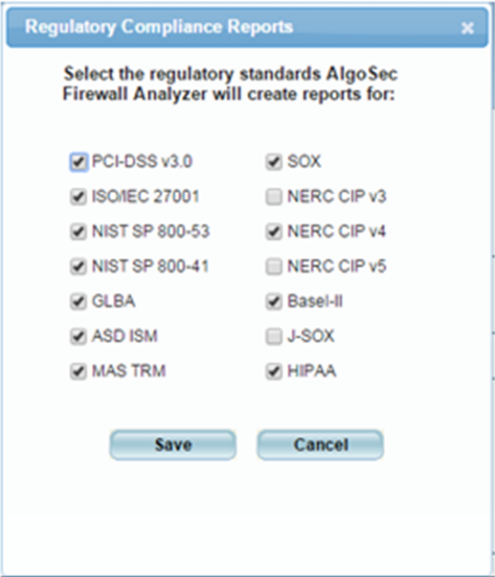
3. Click the **Compliance** tab.

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.
<b>Europe Centric</b>	
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).
<b>Global</b>	
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 BusinessFlow to provide you with more specific security information for PCI applications. See <a href="#">Configure the PCI zone</a>.</p>
<b>Australia Centric</b>	
ASD-ISM	Firewall configuration guidelines from Australian Government.
<b>Japan Centric</b>	
J-SOX	Japanese version of SOX.




Standard	Description
<b>Singapore Centric</b>	
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.

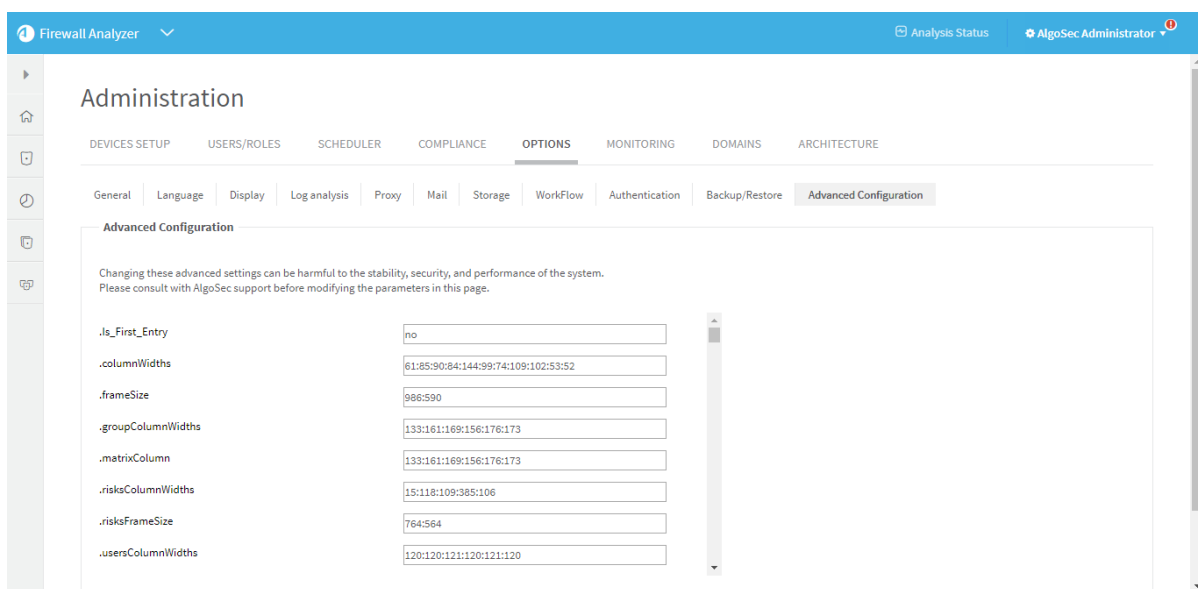
A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

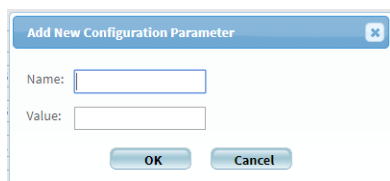
3. Click the **Advanced Configuration** tab.

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.

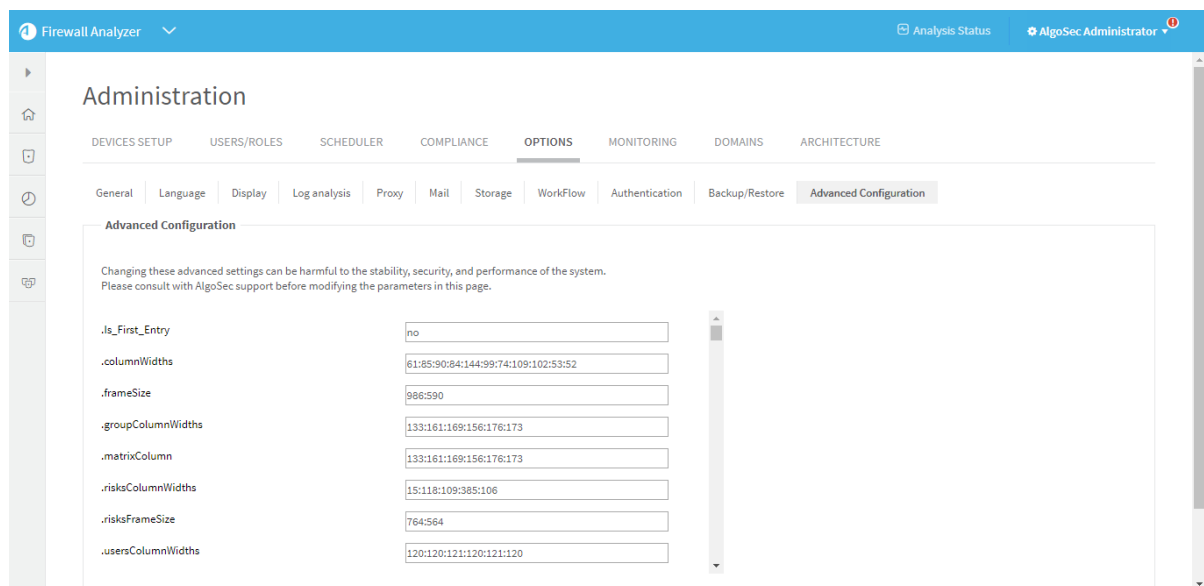
A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

3. Click the **Advanced Configuration** tab.

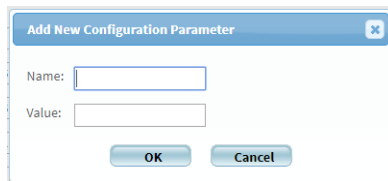
The **Advanced Configuration** tab appears.



4. To adjust the threshold for a bad score, do the following:

- a. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

A screenshot of the 'Add New Configuration Parameter' dialog box. It has a title bar with the text 'Add New Configuration Parameter' and a close button. Inside, there are two text input fields: 'Name:' and 'Value:'. Below the fields are two buttons: 'OK' and 'Cancel'.

- 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 BusinessFlow to tag which network objects intersect the PCI Zone and the applications that use these servers.

**Note:** This feature is only relevant when using BusinessFlow.

AFA can only show the vulnerability of PCI applications in the PCI report when BusinessFlow is integrated with a vulnerability scanner. When using BusinessFlow without a vulnerability scanner, BusinessFlow 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 BusinessFlow 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**.

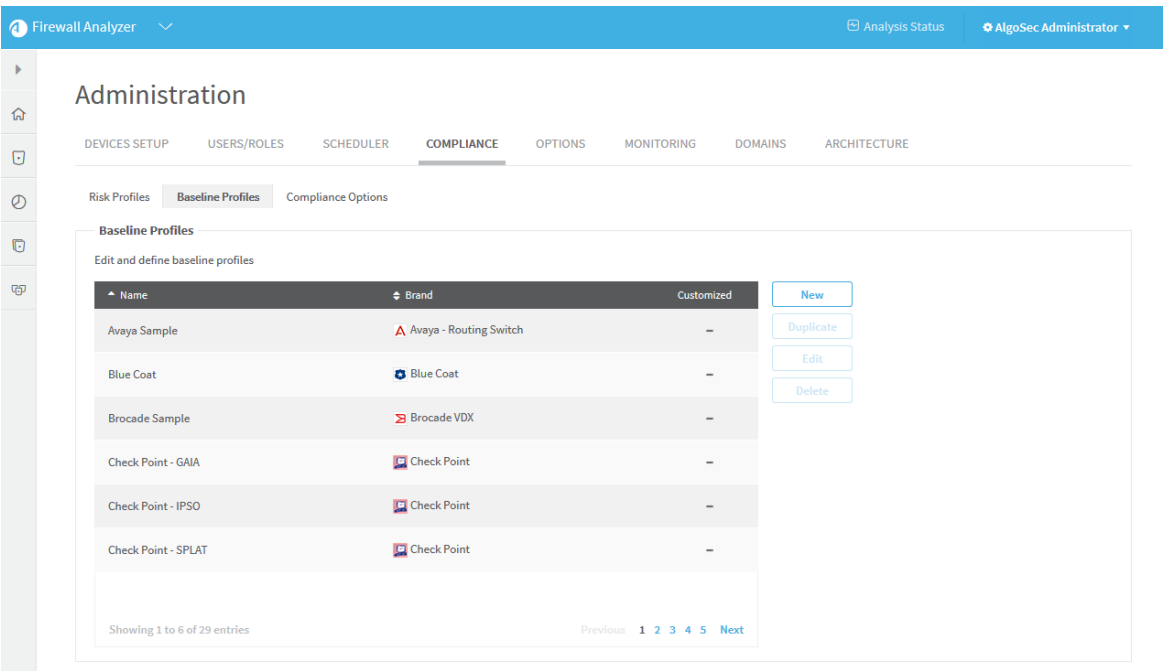
The **Administration** page appears, displaying the **Options** tab.

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.



## 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.

- ## Firewall Analyzer (A30.00)

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 'Administration' interface of the Firewall Analyzer. The 'COMPLIANCE' tab is active, showing 'Baseline Profiles'. The 'Baseline Profiles' section includes a table of existing profiles and an 'Editor' for creating or modifying a profile. The 'Editor' shows a profile named 'Blue Coat' with the brand 'bluecoat'. Below this, there is a 'Commands' section with five entries, each with a Command ID, Command Name, and Command Syntax.

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

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 'Administration' section of the Firewall Analyzer interface. The 'COMPLIANCE' tab is selected, and the 'Baseline Profiles' sub-tab is active. The 'Baseline Profiles' section shows a list of profiles, with 'Check Point - GAIA' selected. The 'Edit' button is clicked, opening the 'Baseline Profile' form. The form includes fields for 'Brand' (set to 'cma') and 'Profile Name' (set to 'Check Point - GAIA'). Below these are three 'Command' sections, each with 'Command Syntax', 'Command Name', and 'Command ID' fields. The first command is 'service dhcpd status' with ID '1' and name 'DHCP Server'. The second is 'route -n | grep D' with ID '2' and name 'Dynamic routing'. The third is 'ifconfig' with ID '3' and name 'Unused Interface'. A 'Save' button is visible at the bottom right of the form.

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:

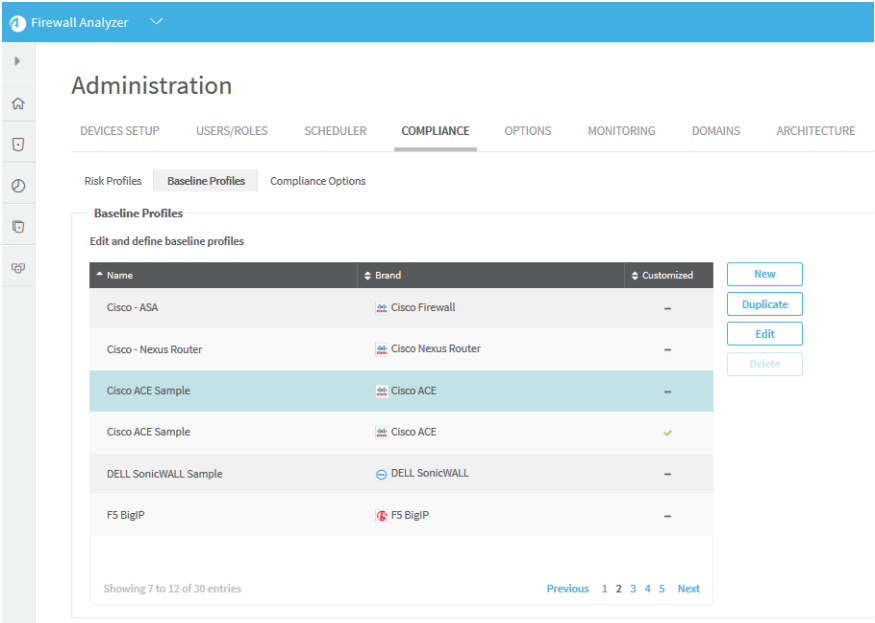
1. Access the Baseline Profile configuration area. For details, see [Access baseline profiles configuration](#).
2. Select one of the custom baseline profiles.
3. Click **Delete**.
4. Click **OK**.

## 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.



3. Click **Edit**.

The baseline profile form appears.

The screenshot shows the 'Administration' section of the Firewall Analyzer, specifically the 'COMPLIANCE' tab. Under 'Baseline Profiles', the 'Edit and define baseline profiles' section is active. The 'Editor' tab is selected, showing a form for a baseline profile named 'Cisco ACE Sample'. The 'Commands (CommandDef)' section is highlighted in blue and contains two commands: 'Show Route' and 'Show Config'. The 'Baseline Requirement' section is also visible, showing requirements for 'Routing details' and 'Device details'.

**Firewall Analyzer** | Analysis Status | AlgoSec Administrator

**Administration**

DEVICES SETUP | USERS/ROLES | SCHEDULER | **COMPLIANCE** | OPTIONS | MONITORING | DOMAINS | ARCHITECTURE

Risk Profiles | Baseline Profiles | Compliance Options

**Baseline Profiles**

Edit and define baseline profiles

Edit Select Insert View Options **Editor** XML **Save** **Cancel**

**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 (CommandDef)**

**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

**Baseline Requirement**

✖ 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**

✖ Requirement Name (name) Device details ✖ Requirement Description (description) General hardware settings.

✖ Requirement ID (id) 2

**Command**

**Document is unchanged**

Add Subelement  
Add Attribute  
Add Nodes  
Add Nodes  
Add CDATA  
Add Attribute  
Add Nodes  
Add CDATA  
Add comment  
Add Subelement  
Add Attribute  
Add Nodes  
Add CDATA  
Add comment  
Add Subelement  
Add Attribute  
Add Nodes  
Add CDATA  
Add comment  
Add text  
Add Top Element  
CommandsDef  
BaselineRequirement

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

Document is unchanged

**Add Subelement** ▼

- Command
- Add Attribute ▼
- Add Nodes ▼
- 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 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.

Commands (CommandsDef)		
Command ID (id)	Command Name (name)	Command Syntax (cmd)
1	Show Route	show ip route
2	Show Config	show running-config
3	Show Password Strength	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.

**Baseline Requirement**

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.

Baseline Requirement

Requirement Name (name) Device details

Requirement Description (description) General hardware settings

Requirement ID (id) 2

Command

Command ID (id) 2

Criterion

Criterion Type (type) Forbidden Line

Line (item)

This line should not appear in the configuration

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"><li>• <code>Required Line</code>. The line specified in the <code>Item</code> sub-tag must be present in the command output.</li><li>• <code>Required Regexp</code>. The regular expression specified in the <code>Item</code> sub-tag must be present in the command output.</li><li>• <code>Forbidden Line</code>. The line specified in the <code>Item</code> sub-tag must <i>not</i> be present in the command output.</li><li>• <code>Forbidden Regexp</code>. The regular expression specified in the <code>Item</code> sub-tag must <i>not</i> be present in the command output.</li><li>• <code>Custom Function</code>. The custom function specified in the <code>Item</code> sub-tag must return <code>true</code> when run on the command output.</li><li>• <code>Manual Review</code>. The regular expression or line specified in the <code>Item</code> sub-tag will be searched for in the command output.</li></ul>
------	---

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 Customizing Risk Profiles (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 <i>Outside</i>, <i>Inside</i>, <i>DMZs</i>, and any user-defined zone type</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• In the preceding example, the file name is <code>q_srv_Outside_Inside</code>.</li> <li>• For traffic going from <i>Inside</i> to <i>DMZs</i>, the relevant file name would be <code>q_srv_Inside_DMZs</code>.</li> <li>• For traffic between different Internal zones, the relevant file name would be <code>q_srv_Inside_Inside</code>.</li> </ul> <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"> <li>• <b>PASS</b>. Traffic was passed by the device.</li> <li>• <b>DROP</b>. Traffic was blocked by the device.</li> </ul>
@is_external_src	<p>Indicates whether the source zone of the traffic is external or not:</p> <ul style="list-style-type: none"> <li>• <b>yes</b>. The source zone is external.</li> <li>• <b>no</b>. The source zone is not external.</li> </ul>
@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"> <li>yes. Encrypted traffic should trigger the risk.</li> <li>no. Encrypted traffic should not trigger the risk.</li> </ul>
@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	<p>The host group's name.</p> <p>Only alphanumeric characters, '_', '.', and '-' can be used. Other characters are automatically replaced by '_'.</p>
@n_Total	The number of IP addresses contained in the host group.
@internal	<p>Indicates whether this host group contains internal IP addresses:</p> <ul style="list-style-type: none"> <li>• yes. This host group contains internal IP addresses.</li> <li>• no. This host group does not contain internal IP addresses.</li> </ul>
@external	<p>Indicates whether this host group contains external IP addresses:</p> <ul style="list-style-type: none"> <li>• yes. This host group contains external IP addresses.</li> <li>• no. This host group does not contain external IP addresses.</li> </ul>
@zone_spanning	<p>Indicates whether this host group spans multiple zones:</p> <ul style="list-style-type: none"> <li>• yes. This host group spans multiple zones.</li> <li>• no. This host group does not span multiple zones.</li> </ul>

## 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"><li>PASS. Pass the specified traffic.</li><li>DROP. Drop the specified traffic.</li></ul>
@orig_rule	The original rule number (in vendor format).

@src	The source object of the rule.
@vpn	<p>Indicates whether the rule is a VPN rule, as well as whether traffic is encrypted:</p> <ul style="list-style-type: none"> <li>• A number. The rule is a VPN rule, and the number indicates the relevant VPN rule's number. Traffic is not encrypted.</li> <li>• <code>VPN</code> or <code>VPN_PERMIT</code>. The rule is a VPN rule. Traffic is encrypted.</li> <li>• Empty ("" ). The rule is not a VPN rule.</li> </ul>

**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> }	<p>A link to the specified host group, <i>hostgroup</i>.</p> <p>Can contain a zone name: <i>Inside</i>, <i>Outside</i>, <i>DMZs</i>, or a user-defined zone name.</p>
%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> }	<p>A "Details" button linking to the query results for the specified traffic, where:</p> <p><i>QueryInputFile</i> is the query input file, and</p> <p><i>service</i> is the service, as defined in the AFA's device topology.</p> <p>For example: %QREF{q_srv_Inside_Outside:http}</p>
%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> }	<p>A link to the specified service, <i>service</i>.</p> <p>For example, %SRV{smtp} would be replaced by "smtp" and linked to the definition of this service, as defined on this device.</p>
%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.

**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-header is 'Schedule Dashboard E-Mail'. The form is divided into several sections:

- Job Details:**
  - Job name:** A text field containing 'Dash 3'.
  - Select dashboard:** A dropdown menu showing 'Compliance Dashboard (11 charts)'.
- Email Details:**
  - Recipients (separated by commas - ,):** A text field containing 'example@domain.net;someone@someplace.com'.
  - Email Subject (defaults to dashboard name):** A text field.
  - Email Body (optional. Cannot contain special characters):** A text area.
- Recurrence:**
  - Radio buttons for frequency: ☒ Daily, ☐ Weekly, ☐ Monthly, ☐ Quarterly, ☐ Yearly.
- Recurrence Pattern:**
  - Set time:** Two dropdown menus showing '19' and '30'.

At the bottom right of the form 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](https://192.168.2.5/~demo/fa_reports/demo-12/index.html)  
Report summary:

Findings	
<b>Risks Found:</b> 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 all new)
3. R02	Implicit Check Point Rules (DNS/TCP) (x1)
7. D02	TCP on all ports between internal networks (x1 all new)

### 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 all new)
D02	TCP on all ports between internal networks (x1 all new)
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/](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.

1 Firewall Analyzer

Analysis StatusAlgoSec Administrator

Administration

DEVICES SETUPUSERS/ROLESCHEDULERCOMPLIANCEOPTIONSMONITORINGDOMAINSARCHITECTURE

GeneralLanguageDisplayLog analysisProxyMailStorageWorkFlowAuthenticationBackup/RestoreAdvanced Configuration

SMTP server

Server name:

☐ Use name and password

Username:

Password:

☐ Use SSL

Email notification FROM address

Email address:

demo-fireflow@algosec.com

Test E-Mail message

Email greeting

Dear %NAME%,

[From the AlgoSec Firewall Analyzer demo server]

Default

CancelOK

- 4. Complete the fields using the information in Mail Fields (see [Mail Fields](#)).
- 5. Click OK.

Mail Fields

In this field...	Do this...
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.

In this field...	Do this...
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.

## 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.

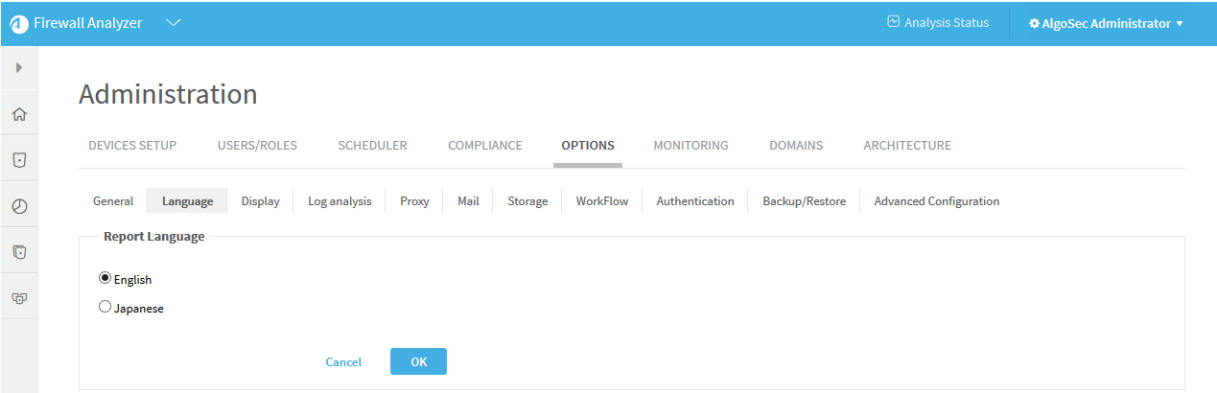
## General Fields

In this field...	Do this...
<b>Comprehensive mode - analyze every service defined on the device (slow)</b>	<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' <b>Policy</b> tab, particularly when comparing different reports.</p> <p><b>Note:</b> Checking this option will result in longer analysis time and will require more disk space.</p>
<b>With IP address name lookups (slow)</b>	<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>
<b>Include traffic changes analysis in Change History (slow)</b>	<p>Select this option to specify that the <b>Changes</b> 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>
<b>Timed rules: only apply rules active at analysis time</b>	<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>
<b>Use public key authentication in data collection</b>	<p>Select this option to use public key authentication in SSH connections to a Check Point management, Juniper Netscreen devices, or NSMs.</p> <p><b>Note:</b> When this option is enabled, the password defined for the device(s) in AFA must be the local private key passphrase.</p>
<b>Simulation timeout (seconds)</b>	<p>Type the maximum amount of time in seconds that a traffic simulation query can run.</p>

In this field...	Do this...
<b>Data collection timeout (seconds)</b>	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.
<b>Days before expiration alerts</b>	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.
<b>Report rules whose comment field...</b>	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 <b>does not match</b> , 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 <b>Details</b> button for more information and examples of regular expressions.  If this field is left empty, rule comment detection will be disabled.
<b>Run device analysis</b>	Select <b>Only if the policy/topology changed</b> 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 <b>Always</b> to specify that AFA will always run a full analysis, regardless of whether the policy has changed or not.  <b>Note:</b> Selecting the <b>Always</b> option will result in longer analysis time and will require more disk space.

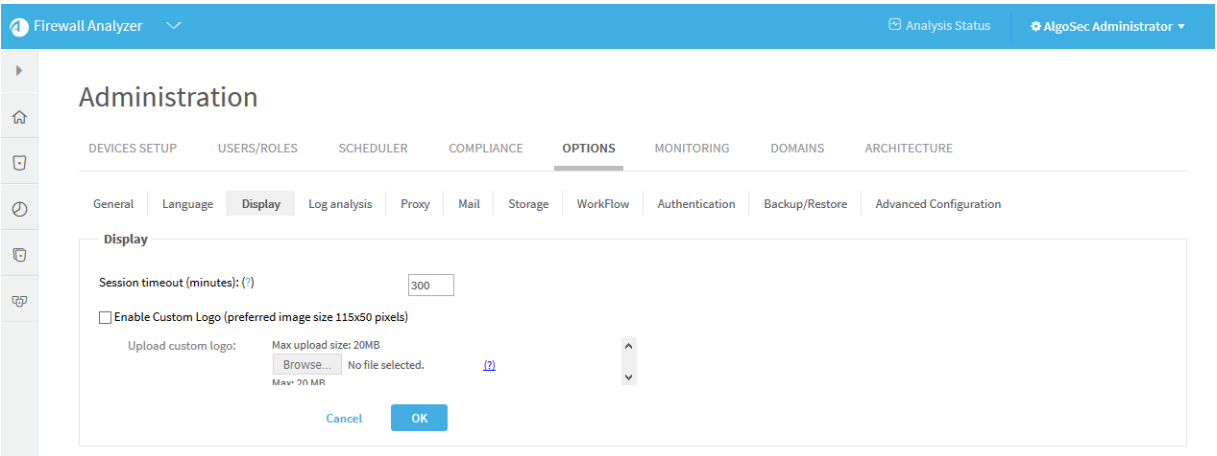
## Language

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...
<b>Session timeout (minutes)</b>	Enter the number of minutes of inactivity before a user is logged out of the Web interface.

In this field...	Do this...
<b>Enable Custom Logo</b>	<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 BusinessFlow 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 'Administration' section of the Firewall Analyzer interface. 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' with a value of 500 and 'Timeout for log analysis is' with a value of 900. Below these fields are 'Cancel' and 'OK' buttons. A 'Syslog Collection for BusinessFlow Discovery' section is also visible, with a 'Define' button.

## Log analysis fields

In this field...	Do this...
<b>Use log starting <i>n</i> days before the report date</b>	<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 <b>Define</b> to define log collection for BusinessFlow 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 'Administration' section of the Firewall Analyzer interface. The 'OPTIONS' tab is selected, and the 'Proxy' sub-tab is active. The interface includes a sidebar with navigation icons and a top header with 'Firewall Analyzer' and 'AlgoSec Administrator'.

**Administration**

DEVICES SETUP   USERS/ROLES   SCHEDULER   COMPLIANCE   **OPTIONS**   MONITORING   DOMAINS   ARCHITECTURE

General   Language   Display   Log analysis   **Proxy**   Mail   Storage   WorkFlow   Authentication   Backup/Restore   Advanced Configuration

**Proxy**

☐ Use proxy server

Proxy:  Port:

☐ Use proxy authentication

Username:  Password:

[Cancel](#) [OK](#)

## Proxy fields

In this field...	Do this...
<b>Use proxy server</b>	<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"> <li>You want to connect to cloud devices defined in AFA (such as AWS or Azure) via a proxy server.</li> <li>You want to validate your AFA "Online" license via a proxy server. Defining the proxy server enables AFA to access the license server.</li> </ul> <p><b>Note:</b> This only applies if you received an "Online" license from AlgoSec.</p> <p><b>Note:</b> Only one proxy server can be defined.</p>
<b>Proxy</b>	Type the proxy server's IP address.
<b>Port</b>	Type the port number used by the proxy server.
<b>Use proxy authentication</b>	<p>Select this option if the proxy server requires authentication.</p> <p>If you select this option, you must complete the <b>Username</b> and <b>Password</b> fields.</p>
<b>Username</b>	Type the username to use for authenticating to the proxy server.
<b>Password</b>	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 web interface. The 'Mail' tab is selected under the 'OPTIONS' category. The configuration is divided into three sections: SMTP server, Email notification FROM address, and Email greeting.

**SMTP server**

- Server name:
- ☐ Use name and password
- Username:
- Password:
- ☐ Use SSL

**Email notification FROM address**

- Email address:
- [Test E-Mail message](#)

**Email greeting**

Buttons at the bottom: [Cancel](#), [OK](#), [Default](#)

## 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: 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 'Administration' page in the Firewall Analyzer interface. The 'Options' tab is selected, and the 'Analysis Options' section is visible. The 'General' sub-tab is active, showing various configuration options for analysis. The 'Default Scheduled Analysis Options' section is also visible at the bottom.

**Administration**

DEVICES SETUP   USERS/ROLES   SCHEDULER   COMPLIANCE   **OPTIONS**   MONITORING   DOMAINS   ARCHITECTURE

General   Language   Display   Log analysis   Proxy   Mail   Storage   Workflow   Authentication   Backup/Restore   Advanced Configuration

**Analysis Options**

- ☒ 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](#)

**Default Scheduled Analysis Options**

Run device analysis:

[Cancel](#) [OK](#)

3. Click **Storage**.

The **Storage** tab appears.

The screenshot shows the 'Administration' page in the Firewall Analyzer interface, with the 'Storage' sub-tab selected under the 'Options' tab. The 'Automatic Report Deletion' section is visible, showing retention policies and cleanup options.

**Administration**

DEVICES SETUP   USERS/ROLES   SCHEDULER   COMPLIANCE   **OPTIONS**   MONITORING   DOMAINS   ARCHITECTURE

General   Language   Display   Log analysis   Proxy   Mail   **Storage**   Workflow   Authentication   Backup/Restore   Advanced Configuration

**Automatic Report Deletion**

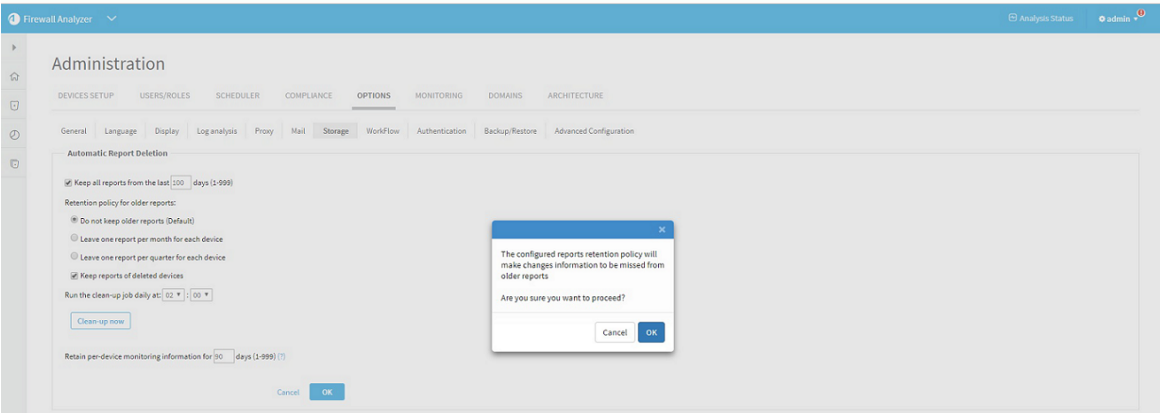
- ☒ Keep all reports from the last  days (1-999)
- Retention policy for older reports:
  - ☒ Do not keep older reports (Default)
  - ☐ Leave one report per month for each device
  - ☐ Leave one report per quarter for each device
  - ☒ Keep reports of deleted devices
- Run the clean-up job daily at:  :
- [Clean-up now](#)
- Retain per-device monitoring information for  days (1-999) (?)

[Cancel](#) [OK](#)

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 <b>Keep all reports from the last <i>n</i> days</b> 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.  <b>Important:</b> If you made changes to the deletion criteria that you want to apply to the clean-up, click <b>OK</b> 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><Change_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 panel includes the following elements:

- Enable integration with external Change Management System:** A checked checkbox.
- Integration System:** A dropdown menu set to 'AlgoSec FireFlow' with a 'Details' button next to it.
- Server:** An empty text input field.
- URL Template:** A text area containing the template: `/FireFlow/Ticket/Display.html?id=__REQUEST_ID__`.
- Change Request Id Format:** A section with 'Before' and 'After' labels and input fields. The 'Before' field contains 'FireFlow #'.
  - Change Request Id:** A dropdown menu set to '\d+'.
  - After:** An empty text input field.
- Buttons:** 'Cancel', 'OK', 'Show Full URL', and 'Details' buttons are present.

- **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.

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. Under the 'OPTIONS' tab, the 'WorkFlow' sub-tab is selected. The 'WorkFlow' configuration area includes a checkbox for 'Enable integration with external Change Management System', which is checked. Below this, a dropdown menu shows 'HP ServiceManager (Peregrine)'. There are input fields for 'Server:', 'File:', 'Query:' (containing 'name'), and 'URL Template:' (containing 'http://\_\_SERVER\_NAME\_\_/sc/index.do?ctx'). To the right of the 'Server' field is a 'Details' button. Below the 'URL Template' field is a 'Show Full URL' button. Further down, there are fields for 'Change Request Id Format:' with sub-fields for 'Before:', 'Change Request Id:' (containing 'd+'), and 'After:'. There is another 'Details' button to the right of these fields. At the bottom 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**.

The screenshot displays the 'WorkFlow' configuration page in the Firewall Analyzer. The page includes a sidebar with navigation icons and a top header with 'Firewall Analyzer' and 'AlgoSec Administrator'. The main area is titled 'Administration' and contains tabs for various settings. The 'WorkFlow' tab is active, showing options to enable integration with an external Change Management System, a dropdown for the system type, a text field for the server URL, and a text area for the URL template. Below these are fields for 'Change Request Id' format, 'Before' and 'After' values, and buttons for 'Show Full URL', 'Details', 'Cancel', and 'OK'.

- **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. Refer to [Configuring User Authentication](#) (see [Configure user authentication](#)) or [Configuring CyberArk Integration](#) (see [Integrate AFA and CyberArk](#)) for more details.

**Firewall Analyzer** Analysis Status AlgoSec Administrator

## Administration

DEVICES SETUP USERS/ROLES SCHEDULER COMPLIANCE **OPTIONS** MONITORING DOMAINS ARCHITECTURE

General Language Display Log analysis Proxy Mail Storage WorkFlow **Authentication** Backup/Restore Advanced Configuration

### 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:

## 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:

<b>User roles</b>	You must be an administrator to perform the backup or restore.
<b>Version</b>	<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>
<b>System processes</b>	<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>
<b>System requirements</b>	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. When restoring an environment with a distributed architecture, the data is restored to each node, but topological relationships are not changed.

The settings and device definitions configured on the source node overwrite the data on each target node.

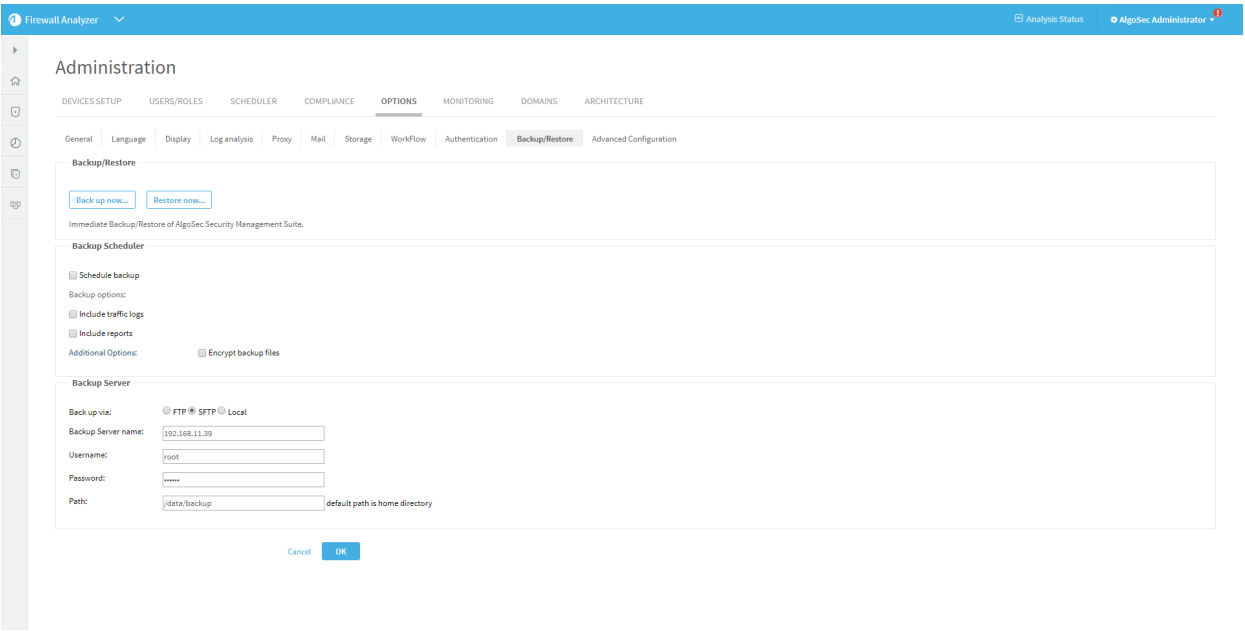
For this reason, run your backup and restore only on the Central Manager or Master Appliance.

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 slaves than existed on the backup environment will impact performance.

## 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](#).



## Backup Scheduler options

Define the following options to schedule a regular system backup:

<b>Schedule backup</b>	Select to schedule a regular backup process. Define the daily, weekly, or monthly backup schedule in the <b>Scheduling Options</b> area that appears below.
------------------------	--

<b>Backup options</b>	<p>Select either of the following:</p> <ul style="list-style-type: none"> <li>• <b>Include traffic logs.</b> Includes traffic logs in the backup.</li> <li>• <b>Include reports.</b> Includes AFA reports in the backup. This option includes all reports created since the last scheduled backup.</li> </ul>
<b>Additional options</b>	<p>Select <b>Encrypt backup files</b> to configure encryption for the backup file.</p> <p>In the <b>Password</b> and <b>Retype password</b> 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:

<b>Back up via</b>	<p>Select one of the following to determine how backup files are sent to the backup server:</p> <ul style="list-style-type: none"> <li>• <b>FTP</b></li> <li>• <b>SFTP</b></li> <li>• <b>Local</b></li> </ul>
<b>Backup server name</b>	<p>Enter the name of the backup server.</p> <p>This field is not relevant for local backups.</p>
<b>Username / Password</b>	<p>Enter the credentials used to access the backup server.</p> <p>These fields are not relevant for local backups.</p> <p><b>Note:</b> Public key authentication is supported for SFTP. In such cases, enter the private key's passphrase in the <b>Password</b> field.</p>

<b>Path</b>	<p>Enter the path where you want to store the backup files. The <b>afa</b> 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"> <li>• <b>Local paths.</b> When testing the connection</li> <li>• <b>Remote paths.</b> Only when performing a backup, either manual or automatic.</li> </ul> <p><b>Note:</b> 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.

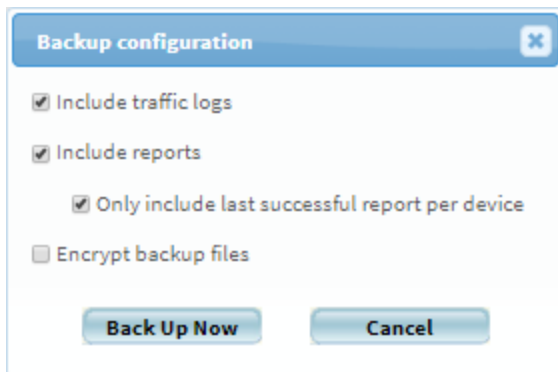
Do the following:

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:

<b>Include traffic logs</b>	<b>Include traffic logs.</b> Includes traffic logs in the backup
-----------------------------	--

<b>Include reports</b>	<p>Includes AFA reports in the backup. By default, this includes all reports created since the last scheduled backup.</p> <p><b>Tip:</b> To save disk space, select <b>Only include last successful report per device</b>.</p> <p>Including all existing reports may require a significant amount of disk space</p>
<b>Encrypt backup files</b>	<p>Select to configure encryption specifically for this backup file.</p> <p>In the <b>Password</b> and <b>Retype password</b> fields that appear, enter and confirm the password you want to use to secure the backup file.</p>

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:

<b>File name</b>	Enter the filename of the backup file you want to use.
<b>Backup file requires password</b>	<p>Select if the backup file is encrypted. Enter the required password in the <b>Password</b> field that appears.</p> <p><b>Note:</b> 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.</p>

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.

## Special Considerations for Distributed Architecture Environments

The backup and restore functionality handles the information / settings on the appliance, only. When restoring an environment with a distributed architecture, the information will be restored to each node, but the topological relationships will not be changed. Any settings and device definitions from each source node will overwrite the settings and device definitions on each target node.

- A backup or restore can be executed only on the Central Manager / Master Appliance.

- In geographic distribution environments, the target appliance for the restore must have the same number of Remote Agents with the same names as the appliance from which the backup was taken.
- In a load distribution there is no such limitation, but restoring to an environment with fewer load slaves will impact performance.

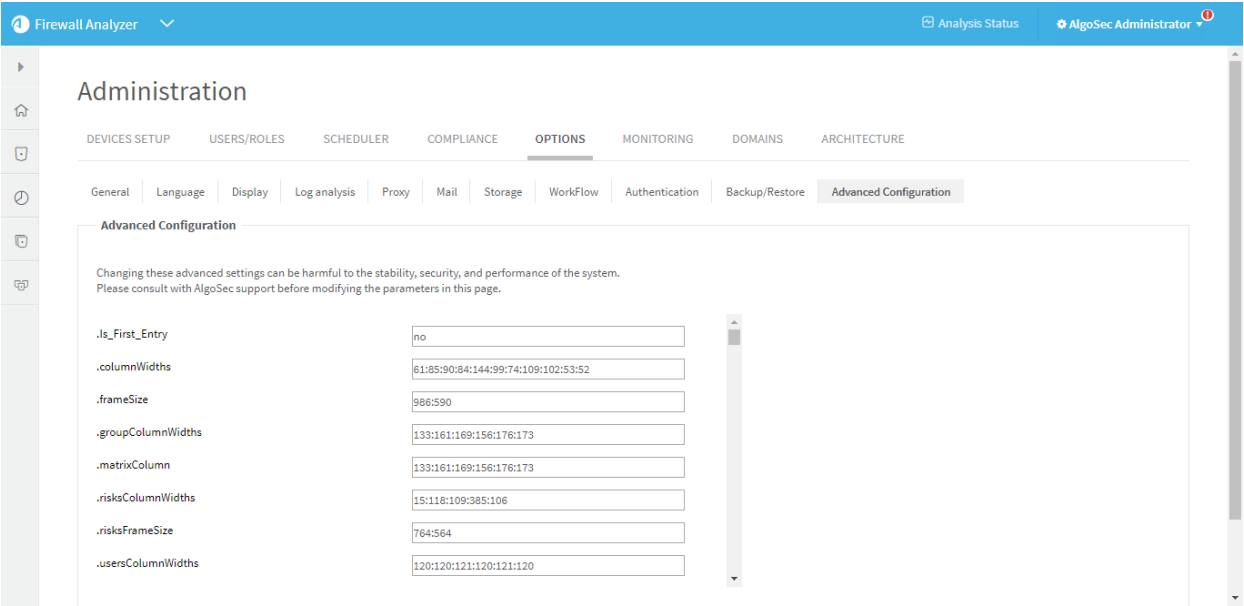
## Limitations

- Before restoring to an HA/DR cluster, it is necessary to break the cluster.
- Only one backup or restore process can run at a time.
- During the restore process, the entire system will be unresponsive. To view information during the restore process, see the `/data/algosec-ms/logs/ms-backuprestore.log` file.
- If the password for backup files has been changed, not all reports will be restored. Only reports that were not encrypted and the reports encrypted with the specified password will be restored. The restore process will not fail, but error messages in the log will contain all the names of reports that failed to restore.
- It is recommended to restore to an appliance with the same number of cores as the appliance from which the backup was taken.

## Advanced Configuration

In the **Advanced Configuration** tab, set advanced configuration parameters, using the procedure below.

**Note:** For information about specific configuration parameters to set, see [Override AFA system defaults](#).



1. Click **Add**.  
  
The **Add New Configuration Parameter** dialog box appears.
2. In the **Name** field, type the name of the configuration parameter you want to set.
3. In the **Value** field, type the value to which you want to set the parameter.
4. Click **OK**.

# Override AFA system defaults

This section explains how to override the AFA system defaults.

For details, see:

- [Configure the device tree view](#)
- [Configure group traffic query results](#)
- [Enable IPT rule recommendations](#)
- [Configure IPT rule recommendations](#)
- [Disable sort/filters in tables](#)
- [Configure change detail display](#)
- [Enable custom report pages](#)
- [Define chart threshold](#)
- [Define default dashboard](#)
- [Configure subnet prioritization](#)

## Configure the device tree view

By default, the AFA device tree is collapsed upon logging in to AFA. Each device defined in AFA appears with its individual components hidden. If desired, you can configure the the device tree to appear fully expanded upon logging in to AFA.

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** page appears.

4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

5. In the **Name** field, type `CollapseDevicesTreeOnLogin`.
6. In the **Value** field, type one of the following:
  - Type `true` to set the default device view to collapsed. This is the default setting.
  - Type `false` to set the default device view to expanded.
7. Click **OK**.
8. Click **OK**.

## Configure group traffic query results

By default, group traffic simulation query results include all devices in the group. You can choose to display group query results grouped by policy, with only one representative device per policy.

**Note:** This setting affects group traffic simulation query results and batch traffic simulation query results. It also affects initial plan query results in FireFlow.

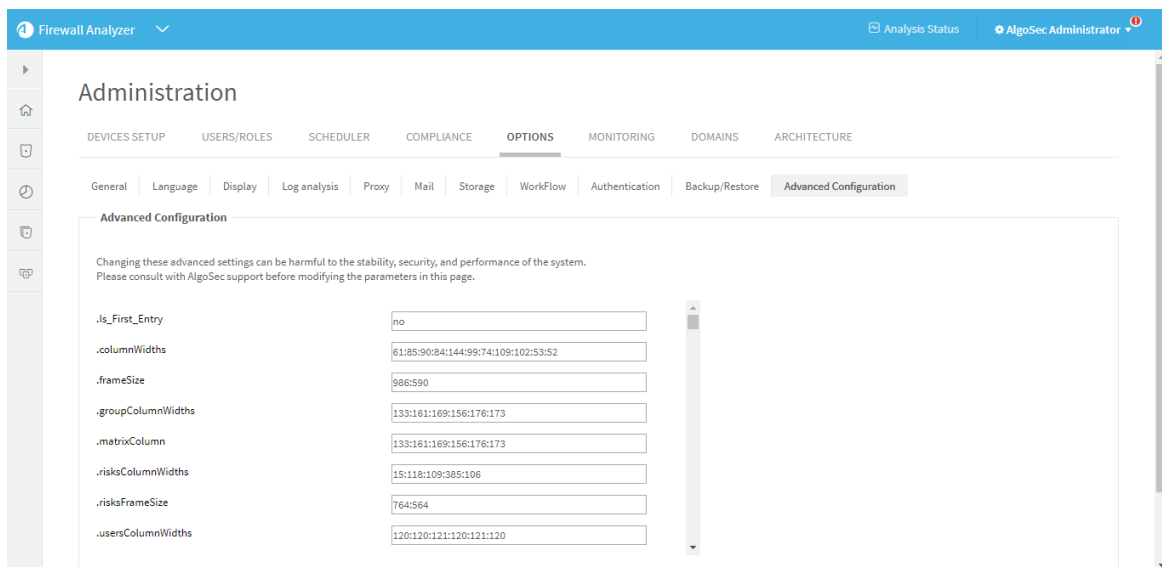
Do the following:

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** page appears.



4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.



5. In the **Name** field, type `QueryByPolicy`.

6. In the **Value** field, type one of the following:

- Type `no` to disable group query results by policy.
- Type `yes` to enable group query results by policy.

7. Click **OK**.

8. Click **OK**.

## Enable IPT rule recommendations

The **Policy Optimization** page's Intelligent Policy Tuner (IPT) provides recommendations for replacing permissive rules with new, tighter rules. However, generating these recommendations may take a while, thus extending the report generation time. If desired, you can disable this feature using the following procedure.

**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".

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** page appears.

4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

5. In the **Name** field, type `Disable_IPT_Recommendations`.

6. In the **Value** field, type one of the following:

- Type `yes` to disable IPT rule replacement recommendations.
- Type `no` to enable IPT rule replacement recommendations.

7. Click **OK**.

8. Click **OK**.

## Configure IPT rule recommendations

The **Policy Optimization** page's Intelligent Policy Tuner (IPT) provides recommendations for replacing permissive rules with new, tighter rules, as well as recommendations for new objects to be used in the rules.

For each sparse object, IPT generates recommendations as follows:

1. IPT searches the device configuration for an existing object that contains the exact same IP addresses, services, and applications as the original object. If such an object is found, IPT suggests it as a replacement.
2. If no such object is found, IPT suggests a new object as follows:
  - **Host objects:** If the number of used IP addresses/ranges is smaller than a certain number (`IPT_Recommendation_Max_Subnets_Per_Range`), then IPT recommends creating a new object that contains these IP addresses/ranges. If the number is larger, IPT searches for a set of CIDR blocks that covers all of the used IP addresses/ranges contained in the original object, and is composed of no more than a certain number of CIDR blocks (`IPT_Recommendation_Max_Ranges`). If such a set is found, IPT suggests a new object that contains the set.
  - **Service/application objects:** If the number of services/application is less than a certain number (`IPT_Recommendation_Max_Services`), IPT suggests a new object that contains these services/applications. If the number is larger, IPT does not suggest a new object.
3. IPT's recommendations are saved in an XML file and then displayed in the **Policy Optimization** page.

If desired, you can change the values used in IPT's calculations, by using the following procedure.

**Note:** For information on disabling IPT rule replacement recommendations altogether, see [Enabling/Disabling IPT Rule Replacement Recommendations](#) (see [Enable IPT rule recommendations](#)).

To configure IPT rule replacement recommendations:

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. Add the desired items specified in the following table, 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 the configuration item.

c. In the **Value** field, type the item's value.

d. Click **OK**.

Repeat these steps as needed.

5. Click **OK**.

### **IPT Rule Replacement Configuration Items**

<b>Item</b>	<b>Description</b>
<b>IPT_Recommendation_Max_Subnets_Per_Range</b>	The maximum number of CIDR blocks into which IPT will recommend splitting a host object. The default value is 4.
<b>IPT_Recommendation_Max_Ranges</b>	The maximum number of CIDR blocks into which IPT will recommend splitting a host object, if the original object contains more than the number of IP addresses/ranges specified in <code>IPT_Recommendation_Max_Subnets_Per_Range</code> . The default value is 20.
<b>IPT_Recommendation_Max_Services</b>	The maximum number of services or applications from which IPT will recommend composing a new object. The default value is 20.

Item	Description
IPT_Density_Action_Limit	The maximum density of a sparse object. When this limit is exceeded, the object is considered semi-dense.  The default value is 50.

## Disable sort/filters in tables

AFA allows sorting and filtering of tables in reports; however, performing these actions for tables with a large number of rows many take time. If desired, you can disable sorting and filtering for large tables.

Do the following:

1. In the toolbar, click your username.

A drop-down menu appears.

2. Select **Administration**.

3. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

4. Click the **Advanced Configuration** tab.

The **Advanced Configuration** page appears.

5. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

6. In the **Name** field, type `Max_Rows_To_Sort`.

7. In the **Value** field, type one of the following:

- Type the maximum number of rows for which sorting and filtering should be performed.
- Type 0 to disable sorting and filtering entirely.

The default value is 10,000.

8. Click **OK**.
9. Click **OK**.

## Configure change detail display

AFA allows you to omit change details from emails about new reports and from change alerts, and includes only the device name and a link to the AFA Web interface. You can configure this setting for individual users by selecting the **Hide change details** check box for each user or you can configure this setting globally for all users by using the following procedure.

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

To globally hide/display change details:

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 `hide_change_details`.

6. In the **Value** field, type one of the following:

- Type `yes` to hide change details for all users. This global setting overrides individual users' Hide change details setting.
- Type `no` to display change details for all users. It is possible to override this setting on a per-user basis.

7. Click **OK**.

8. Click **OK**.

## Enable custom report pages

Creating and installing a custom report page automatically enables custom report pages. If desired, you can disable custom report pages, using the following procedure. The custom report page will no longer appear in AFA reports.

For more details, see [Custom report pages](#).

To enable/disable custom report pages:

1. In the toolbar, click your username.

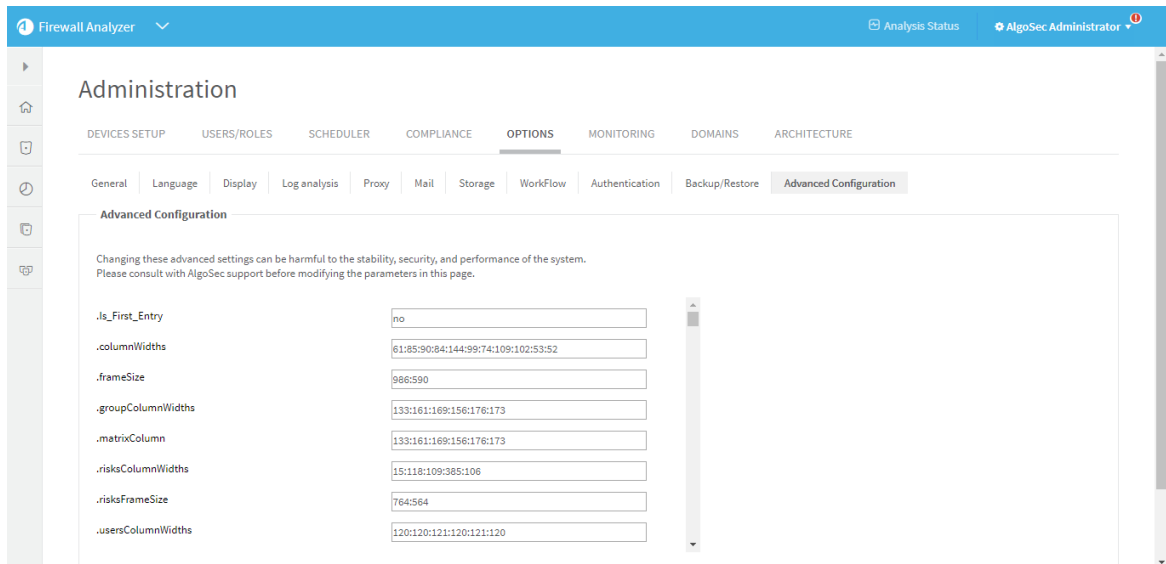
A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

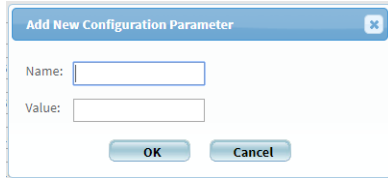
3. Click the **Advanced Configuration** sub-tab.

The **Advanced Configuration** page appears.



4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

A screenshot of a dialog box titled "Add New Configuration Parameter". It has a blue header bar with a close button (X) in the top right corner. Below the header, there are two text input fields. The first is labeled "Name:" and the second is labeled "Value:". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

5. In the **Name** field, type `Use_Custom_Report`.
6. In the **Value** field, do one of the following:
  - Type `no` to disable custom report pages.
  - Type `yes` to enable custom report pages.
7. Click **OK**.
8. Click **OK**.

## Define chart threshold

**Note:** Changing this configuration item will affect all charts of the type `condition`. This includes the built-in compliance charts. By default, this parameter is set to 23.

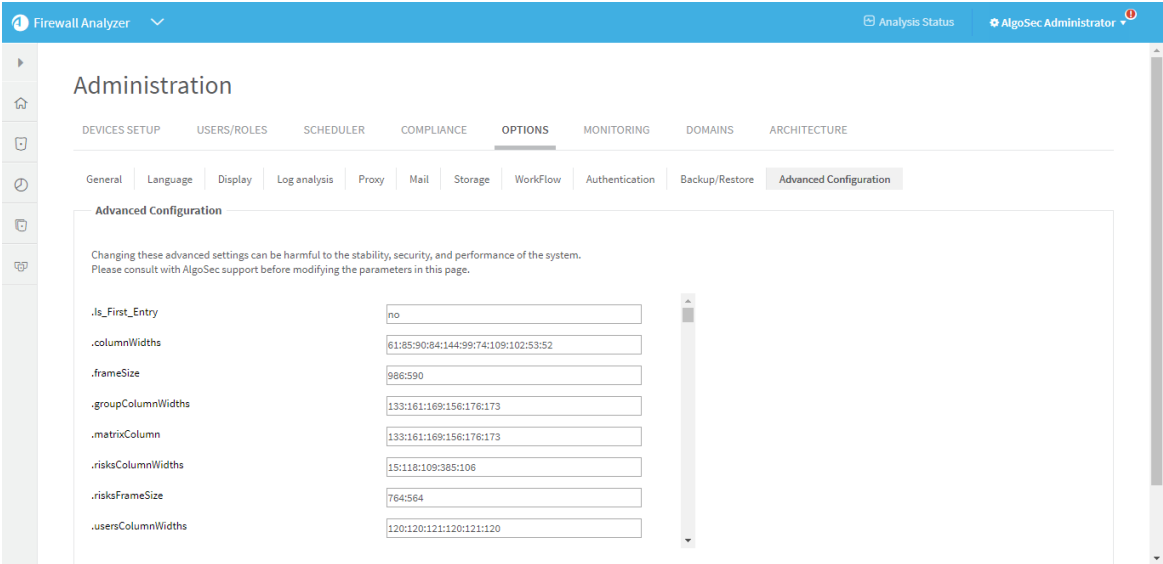
To set the `Chart_Threshold_Val` configuration item:

1. In the toolbar, click your username.

A drop-down menu appears.
2. Select **Administration**.

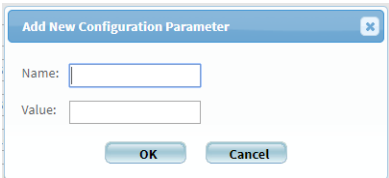
The **Administration** page appears, displaying the **Options** tab.
3. Click the **Advanced Configuration** sub-tab.

The **Advanced Configuration** page appears.



4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.



5. In the **Name** field, type `Chart_Threshold_Val`.

6. In the **Value** field, type the threshold you want for your chart(s).

7. Click **OK**.

8. Click **OK**.

## Define default dashboard

When you log in to AFA, the default dashboard is displayed in the workspace. By default, the default dashboard is the **Optimizations** dashboard. To change the default dashboard, complete the following procedure.

To set the default dashboard:

1. In the toolbar, click your username.

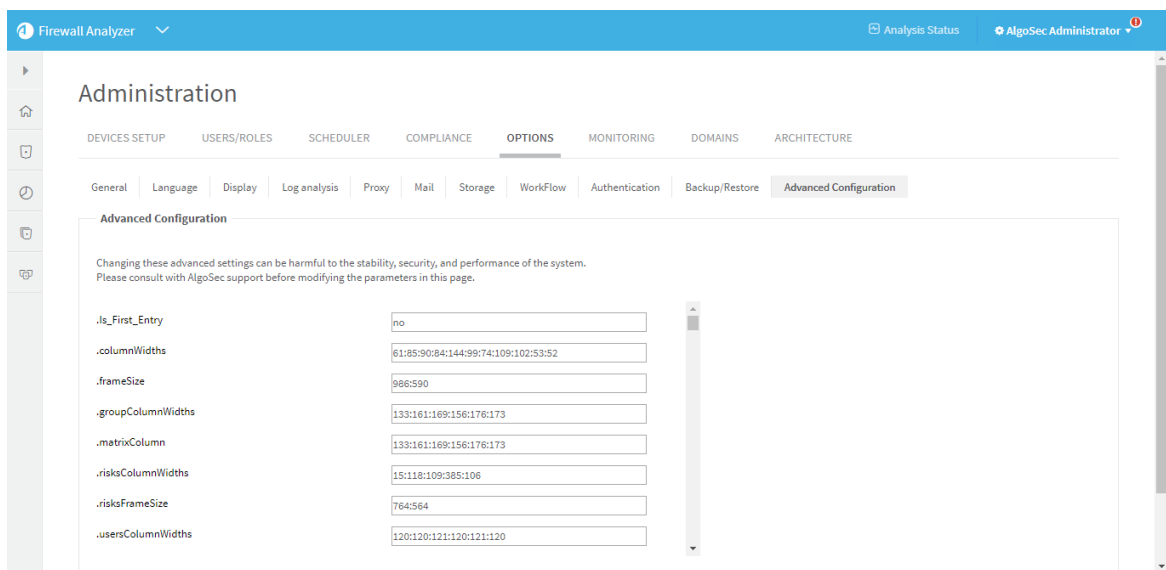
A drop-down menu appears.

2. Select **Administration**.

The **Administration** page appears, displaying the **Options** tab.

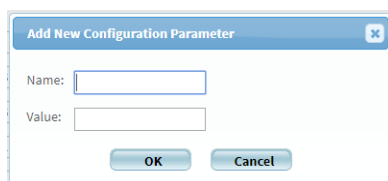
3. Click the **Advanced Configuration** sub-tab.

The **Advanced Configuration** page appears.



4. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.



5. In the **Name** field, type `default_dashboard`.

6. In the **Value** field, do one of the following:

- Type the name of the XML file describing the dashboard that you wish to be the default.

For example, type `compliance.xml` to set the compliance dashboard as the default dashboard.

- Type `none` to specify no dashboard should load at login.

7. Click **OK**.

8. Click **OK**.

## Configure subnet prioritization

By default, routing queries and traffic simulation queries prioritize paths that begin and end with a subnet (and not a cloud). If desired, you can disable this preference for sources and/or destinations.

To enable/disable prioritization of subnets in queries:

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. To change the setting for sources, do the following:

5. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

6. In the **Name** field, type `PrioritizeFIPSources`.

7. In the **Value** field, type one of the following:

- Type `yes` to enable a preference for subnets. This is the default setting.
- Type `no` to disable the preference for subnets.

8. Click **OK**.

9. To change the setting for destinations, do the following:

a. Click **Add**.

The **Add New Configuration Parameter** dialog box appears.

b. In the **Name** field, type `PrioritizeFIPDestination`.

c. In the **Value** field, type one of the following:

- Type `yes` to enable a preference for subnets. This is the default setting.
- Type `no` to disable the preference for subnets.

d. Click **OK**.

10. Click **OK**.

# 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: Note:** Only one custom report page is supported.

**Note: 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. See [Enabling/Disabling Custom Report Pages](#) (see [Enable custom report pages](#)).

## Custom report configuration file parameters

Parameter	Description
report_name	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
<b>-f</b> <i>zip_file</i>	<p>The name of the <code>.zip</code> file.</p> <div> <b>Note:</b> The file must be located in the current directory. </div>
<b>-d</b> <i>domain_number</i>	<p>The number of the domain in the <code>.fa</code> directory, where the <code>.zip</code> file should be extracted.</p> <p>This flag is optional.</p>
<b>-u</b> <i>user_name</i>	<p>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.</p> <p>This flag is optional. If it is not included, the contents of the <code>.zip</code> file will be installed using the "afa" user.</p>

## 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**

title	<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"><li>• <code>__GROUP_NAME__</code>. The name of the device group that is analyzed by the chart (as defined in the dashboard XML file).</li><li>• <code>__THRESHOLD__</code>. The value set as the "Chart_Threshold_Val" configuration item.</li><li>• <code>__COUNT__</code>. The number of devices the chart displays.</li></ul>
-------	---

**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><b>Note:</b> 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><b>Note:</b> 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...
<code>baseline_score</code>	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.
<code>risks_per_risk_level</code>	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.
<code>total_changes</code>	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	<p>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.</p> <p>For information regarding setting this threshold, see Setting the Chart Threshold Value Configuration Item (see <a href="#">Define chart threshold</a>).</p>
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	<p>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.</p> <p>For information regarding setting this threshold, see Setting the Chart Threshold Value Configuration Item (see <a href="#">Define chart threshold</a>).</p>
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
<b>DASHBOARD</b>	<p>Identifies the dashboard and specifies how charts are oriented. Includes the <a href="#">CHARTS</a> sub-tag.</p> <p>Parameters include:</p> <ul style="list-style-type: none"> <li>• <b>name</b>. String. The dashboard name. This name appears at the top of the dashboard.</li> <li>• <b>columns</b>. The number of charts that appear in each row of the dashboard.</li> </ul> <p>The charts will be filled in order of appearance, from left to right and top to bottom.</p>
<b>CHARTS</b>	<p>Defines all the charts that appear in the dashboard. Includes several <a href="#">CHART</a> sub-tags.</p>
<b>CHART</b>	<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"> <li>• <b>group</b>. String. The name of the AFA device group that is analyzed in the chart.</li> <li>• <b>definition_file</b>. String. The name of the chart XML file.</li> </ul> <p>Specify a custom chart that you created and saved in the <b>&lt;AFA home dir&gt;/.fa/dashboards/charts</b> directory, or a built-in chart.</p> <p>For more details, see <a href="#">Custom dashboards and charts</a>.</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\_templ\_*reportname*.html**
- For group device reports: **compliance\_rep\_templ\_group\_*reportname*.html**
- For matrix device reports: **compliance\_rep\_templ\_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
<code>id</code>	Internal key necessary for report creation.
<code>title</code>	Title of the report. This title will appear as a link on the <b>Regulatory Compliance</b> page of the device report. The link leads to the compliance report.
<code>template_file</code>	HTML template file for a single device. This template will be used to create a single device compliance report.

Attribute	Description
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:

<b>Stop/Start/Restart services</b>	Users may need to stop/start/restart the following services: <ul style="list-style-type: none"><li>• httpd</li><li>• apache-tomcat</li><li>• crond</li><li>• syslog-ng</li><li>• iptables</li></ul>
<b>Files and folders</b>	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: <ul style="list-style-type: none"><li>• /usr/share/fa/* (all sub-tree)</li><li>• /home/afa/algosec/syslog_processor/*</li><li>• /home/afa</li><li>• /home/afa/.fa</li><li>• /home/afa/.fa/firewalls/*</li></ul>

<p><b>Run various commands</b></p>	<p>Users may be required to run the following commands:</p> <ul style="list-style-type: none"> <li>• <b>crontab -e -u afa</b></li> <li>• <b>vi /etc/ntp.conf</b></li> <li>• <b>vi /etc/hosts</b></li> <li>• <b>vi /etc/security/limits.conf</b></li> <li>• <b>kill -9 / pkill -9</b></li> <li>• <b>screen</b></li> <li>• <b>strace</b></li> </ul> <p>In addition, they may be required to modify the <b>iptables</b> configuration on the AlgoSec appliance/VM.</p>
<p><b>Sync AFA and FireFlow DB passwords</b></p>	<p>Some support cases may require performing a sync between the Firewall Analyzer and FireFlow DB passwords.</p> <p>To do this, run the following commands from the root user SSH CLI:</p> <pre>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&gt;/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</pre>

## Entering and exiting debug mode

AlgoSec Support may request that you enter **Debug** mode.

<b>Enter Debug mode</b>	Click your username in the toolbar and then click <b>Info</b> . In the <b>Info</b> dialog, click <b>Enter Debug Mode</b> .
<b>Exit Debug mode</b>	Click your username in the toolbar and then click <b>Info</b> . In the <b>Info</b> dialog, click <b>Exit Debug Mode</b> .

## 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:

<b>GUI-related issues</b>	<p><b>algosec-support-gui.zip</b></p> <p>For details, see <a href="#">Download general log files</a></p> <p>If the <b>algosec-support-gui.zip</b> file is unavailable, send the following files instead:</p> <ul style="list-style-type: none"> <li>• <b>.fa-history</b></li> <li>• <b>fa-install.log</b></li> <li>• <b>.ht-fa-history</b></li> </ul> <p>For more details, see <a href="#">Access log and configuration files</a>.</p>
<b>All other issues</b>	<p><b>algosec-support.zip</b></p> <p>For details, see <a href="#">Download report log files</a></p> <p>If the <b>algosec-support.zip</b> file is unavailable, send the following files instead:</p> <ul style="list-style-type: none"> <li>• <b>fa-install.log</b></li> <li>• <b>.fa-history</b></li> <li>• <b>log.html</b></li> <li>• <b>index.html</b></li> <li>• <b>.ht-fa-history</b></li> </ul> <p>For more details, see <a href="#">Access log and configuration files</a>.</p>

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
<b>algosec-support.zip</b>	<p>An archive file that includes the following report and general log files:</p> <ul style="list-style-type: none"> <li>• <b>fa-history</b></li> <li>• <b>fa-install.log</b></li> <li>• <b>ht-fa-history</b></li> <li>• <b>log.html</b></li> <li>• <b>fwa_monitor.history</b></li> </ul> <p><b>Note:</b> The <b>fwa_monitor.history</b> 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><b>\$HOME/algosec/firewalls/&lt;job-name&gt;/</b></p> <p>Where <b>&lt;job-name&gt;</b> is the <b>Job Name</b> of the report.</p> <p>The <b>Job Name</b> consists of the user login name followed by a hyphen and an integer.</p> <p><b>Example:</b> afa-3</p>
<b>algosec-support-gui.zip</b>	<p>An archive file that includes:</p> <ul style="list-style-type: none"> <li>• <b>fa-history</b></li> <li>• <b>fa-install.log</b></li> <li>• <b>ht-fa-history</b></li> <li>• <b>map.sqlite</b></li> <li>• <b>dump_nat_data</b></li> </ul>	<p>Download from AFA.</p> <p>For details, see <a href="#">Download general log files</a>.</p>

File Name	Description	Location
log.html	The report log file. <b>Note:</b> This file may be missing if the file report has a status of FAILED.	<b>\$HOME/algosec/firewalls/&lt;job-name&gt;/</b> For details, see: <ul style="list-style-type: none"> <li>• <a href="#">View report log files</a></li> <li>• <a href="#">Download report log files</a></li> </ul>
algosec-support-full-ENTITY_NAME.zip	Full support data files which include: <ul style="list-style-type: none"> <li>• report log files</li> <li>• full firewall configuration</li> </ul>	Download from the device report. For details, see <a href="#">Download full support files</a> .
algosec-support-full-ENTITY_NAME-withlogs.zip	Full support data files which include: <ul style="list-style-type: none"> <li>• report log files</li> <li>• full firewall configuration</li> <li>• traffic logs</li> </ul>	Download from the device report. For details, see <a href="#">Download full support files</a> .
messages	All syslog messages.	/var/log/
fa-install.log	The AFA installation log	/var/log/
fa-history	The AFA application's history file.	<b>\$HOME/</b> This file is hidden by default. To view, run: <b>ls -a \$HOME/.fa-history</b>
ht-fa-history	The Web interface's log file.	<b>\$HOME/public_html/algosec/</b> This file is hidden by default. To view, run: <b>ls -a \$HOME/public_html/algosec/.ht-fa-history</b>
map.sqlite	The database of the map.	<b>\$HOME/.fa/map.sqlite</b>
dump_nat_data	Dump of NAT related tables.	

File Name	Description	Location
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.

Severity Level	Description
<b>Warning</b>	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 <a href="#">Contact technical support</a> .
<b>Error</b>	A problem that prevented the report from being generated occurred. Contact AlgoSec Technical Support. For more details, see <a href="#">Contact technical support</a> .
<b>Fatal</b>	A severe error condition required an immediate halt to the report generation process. Contact AlgoSec Technical Support. For more details, see <a href="#">Contact technical support</a> .

## 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 **algosec-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`

➔ **See also:**

- [Static support troubleshooting](#)

# Send us feedback

Let us know how we can improve your experience with the Administration Guide.

Email us at: [techdocs@algosec.com](mailto:techdocs@algosec.com)

**Note:** For more details not included in this guide, see the online [ASMS Tech Docs](#).