



FORCEPOINT

POWERED BY **Raytheon**

Forcepoint Security Appliance Manager

Administrator Help

Version v1.2

CONTENTS



Copyrights and Trademarks

| | |
|-----------------------------|---|
| Other acknowledgments | 5 |
|-----------------------------|---|

CHAPTER 1 Getting Started

| | |
|--|----|
| Overview | 8 |
| Related documents | 9 |
| Launching the Security Appliance Manager | 10 |
| Embedded help | 11 |
| Technical support | 12 |

CHAPTER 2 Navigating the Security Appliance Manager

| | |
|---------------------------------------|----|
| Icons | 14 |
| Banner | 16 |
| Filtering panel | 17 |
| Appliances table | 18 |
| Adding or deleting an appliance | 18 |
| Status tab | 19 |
| Appliance status information | 19 |
| Service status information | 21 |
| Software Updates tab | 24 |
| Available Items | 24 |
| Installed Items | 25 |
| Upload (8.5 and later) | 26 |
| Interfaces tab | 27 |
| Interface settings | 27 |
| DNS settings | 28 |
| Routing tab | 29 |
| Static IPv4 Routes table | 29 |
| Static IPv6 Routes table | 30 |
| Component Routes table | 31 |

| | |
|-----------------------------|----|
| Toolbox tab | 33 |
| Remote SSH Access | 33 |
| Remote Assistance | 33 |
| Configuration Summary | 33 |
| Backup and Restore | 34 |
| SNMP tab | 37 |
| SNMP Setup | 37 |
| SNMP Events | 37 |

Copyrights and Trademarks

Security Appliance Manager Help | Forcepoint Appliances | v1.2

© 2017 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA

All rights reserved.

Published 11/30/2017 Revision C

Printed in the United States and Ireland

D080216830

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint LLC.

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint LLC, makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint LLC shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Forcepoint is a registered trademark and TRITON is a trademark of Forcepoint LLC, in the United States and certain international markets. Forcepoint has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

eDirectory and Novell Directory Services are a registered trademarks of Novell, Inc., in the U.S and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (<http://www.apache.org>).

Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Other acknowledgments

Portions of this Forcepoint product includes or may include the following components:

CLICK, © 2014 Armin Ronacher, is distributed under the BSD 3-Clause License (opensource.org/licenses/BSD-3-Clause) ■ FLASK, © 2015 Armin Ronacher and contributors, is distributed under the BSD 3-Clause license (opensource.org/licenses/BSD-3-Clause) ■ ITSDANGEROUS, © 2011 Armin Ronacher and the Django Software Foundation, is distributed under the BSD 3-Clause license (opensource.org/licenses/BSD-3-Clause) ■ JINJA, © 2009 the Jinja Team, is distributed under the BSD 3-Clause license (opensource.org/licenses/BSD-3-Clause) ■ JYTHON 2.7.0, © 2001-2017 Python Software Foundation, is distributed under the Python Software Foundation License Version 2 (python.org/license.html) ■ PSYCOPG2 2.6.2, © 2007 Free Software Foundation, Inc., is distributed under the GNU Lesser General Public License (<http://www.gnu.org/licenses/lgpl-3.0-standalone.html>) ■ PYTHON 3.5.3, © 2001-2017 Python Software Foundation, is distributed under the Python Software Foundation License (

docs.python.org/3/license.html) ■ PYTHONNET, © 2006-2017 the contributors of the “Python for .NET” project, is distributed under the MIT License (opensource.org/licenses/mit-license) ■ PYWIN32, © 1996-2008 Greg Stein and Mark Hammond, is distributed under the BSD 3-Clause license (opensource.org/licenses/BSD-3-Clause) ■ WERKZEUG, © 2014 the Werkzeug Team, is distributed under the BSD 3-Clause license (opensource.org/licenses/BSD-3-Clause)



Getting Started

Security Appliance Manager Help | Forcepoint Appliances | v1.2

CHAPTER 1

Overview

The Forcepoint™ Security Appliance Manager is a browser-based console that provides a central, graphical interface for the configuration and management of your Forcepoint appliances.

The Forcepoint Security Appliance Manager allows you to configure appliance settings, monitor system performance, manage services, perform system backups, apply hotfixes and upgrade patches, and perform diagnostic tasks.

To learn to use the Forcepoint Security Appliance Manager, browse this guide or select one of the following topics as a launch point.

| Navigating the Security Appliance Manager | Configuring your appliances |
|---|---|
| "Launching the Security Appliance Manager" on page 10 "Banner" on page 16 "Filtering panel" on page 17 "Appliances table" on page 18 "Status tab" on page 19 "Software Updates tab" on page 24 "Interfaces tab" on page 27 "Routing tab" on page 29 "Toolbox tab" on page 33 "SNMP tab" on page 37 | "Adding or deleting an appliance" on page 18 "Interface settings" on page 27 "DNS settings" on page 28 "Static IPv4 Routes table" on page 29 "Static IPv6 Routes table" on page 30 "Component Routes table" on page 31 "SNMP Setup" on page 37 and Configuration "Remote SSH Access" on page 33 "Remote Assistance" on page 33 "Configuration Summary" on page 33 "Backup and Restore" on page 34 |
| Monitoring your appliances | Troubleshooting |
| "Appliance status information" on page 19 | "Related documents" on the facing page "Embedded help" on page 11 "Technical support" on page 12 |

Related documents

The Forcepoint Security Appliance Manager must be installed on the machine that hosts the Forcepoint Security Manager (named TRITON Manager in versions 8.3.0 and earlier). For more information about the Forcepoint Security Manager, refer to the [Security Manager Help](#) document.

To install the Forcepoint Security Appliance Manager, refer to the [Forcepoint Security Appliance Manager Installation Guide](#).

For release information, refer to the [Forcepoint Security Appliance Manager Release Notes](#).

Launching the Security Appliance Manager

To launch the Forcepoint Security Appliance Manager:

- ▶ Open a supported browser on any machine in your network and enter the following:

```
https://<IP_address_or_hostname>:9443/cm/
```

Substitute the IP address or hostname of the Security Manager machine. It is recommended that you use the IP address, especially when launching the Forcepoint Security Appliance Manager from a remote machine.

At the logon screen, enter your **User name** and **Password**, then click **Log On**.

The user name is **admin**. The password was set when the firstboot script was run, and can be changed via the Forcepoint Security Manager.

If you are unable to connect to the Forcepoint Security Manager from a remote machine, make sure that your firewall allows communication on that port.

 **Note:** After 10 minutes of idle time, a messages displays, warning that your session will expire in 5 minutes.

Embedded help

Access embedded help from the **Help** drop-down at the top right area of the screen, in the Forcepoint Security Appliance Manager banner.

Click **Help > Explain This Tab** to open context-sensitive help for the active configuration tab.

Click **Help > Filtering Panel** to open help information for the filtering panel on the left side of the screen.

Click **Help > All Appliances Table** to open help information for the All Appliances table in the middle of the screen.

Click **Help > Help Contents** to display the complete embedded help contents. To find a topic, select one of the following tabs:

- ▶ **Contents**

- Double-click a book icon to expand that book's topics.

- Click a table of contents entry to display the corresponding topic.

- ▶ **Search**

- Enter a word or phrase and click **Go**.

Click an entry in the results list to display the corresponding topic.

Click **Help > Support Portal** to access the Forcepoint online [support site](#). For more information, refer to the "Getting Started" on page 7 section of this document.

Click **Help > About** for product information.

Many user interface features, such as buttons and icons, have tooltips. Hover over an item to display the tooltip.

Technical support

Click **Help > Support Portal** in the Forcepoint Security Appliance Manager to access the Forcepoint online [support site](#). Technical information about Forcepoint software and services is available 24 hours a day, including:

- ▶ a searchable Knowledge Base
- ▶ product documentation
- ▶ answers to frequently asked questions

For additional questions, click the **Contact Support** tab at the top of the page.

The contact page includes information for finding solutions, opening an online support case, and calling Technical Support.

For faster phone response, please use your Account ID, which you can find in the Profile section on the [My Account](#) page.

For telephone requests, please have ready:

- ▶ Product subscription key
- ▶ Access to the management console for your solutions
- ▶ Familiarity with your network's architecture, or access to a specialist



CHAPTER 2

Navigating the Security Appliance Manager

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The Forcepoint™ Security Appliance Manager interface can be divided into several main areas:

- ▶ "Navigating the Security Appliance Manager" above
- ▶ "Filtering panel" on page 17
- ▶ "Appliances table" on page 18
- ▶ Configuration tabs
 - "Status tab" on page 19
 - "Software Updates tab" on page 24
 - "Interfaces tab" on page 27
 - "Routing tab" on page 29
 - "Toolbox tab" on page 33
 - "SNMP tab" on page 37

The filtering pane and the configuration tabs pane can be collapsed or expanded using the left and right arrow buttons.

Icons

The following icons are used throughout the Forcepoint Security Appliance Manager:

| Navigation/Operations | |
|---|--|
| Icon | Description |
|  | Information |
|  | Collapse/expand panel |
|  | Collapse/expand panel |
|  | Settings |
|  | Idle |
|  | Loading |
|  | Restart/restarting |
| Status | |
| Icon | Description |
|  | OK Appliance is connected; services are running. |

| | |
|---|---|
|  | <p>Degraded Appliance is connected; one or more services are down.</p> |
|  | <p>Disconnected Appliance is disconnected OR appliance is connected but all services are down.</p> |
|  | <p>Unsupported Appliance is pre-v8.3 and unsupported in FSAM.</p> |
|  | <p>Hotfix & SSO Required Appliance is v8.3 and does not have the required hotfix(es) installed and/or does not have SSO enabled OR appliance is v8.4 or later and does not have SSO enabled.</p> |

Banner

The banner, located at the top of the browser page, shows:

- ▶ The **Help** drop-down menu, which provides access to ["Getting Started" on page 7](#), Technical Support resources, and product information.
- ▶ The user name drop-down menu, which displays your logon account user name, and a **Log Off** option, which allows you to end your session.
- ▶ The refresh button, which allows you to refresh the information in the active tab.

Filtering panel

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The filtering panel allows you to filter the appliances that display in the **Appliances** table in the appliance window.

- ▶ Click **Version** to filter on a software version.
- ▶ Click **Mode** to filter on a deployment mode.
- ▶ Click **Status** to filter on an alert status.
- ▶ Click on **All Appliances** to display all registered appliances in the table.

 **Note:** Unsupported appliances and appliances requiring a hotfix or SSO enabled will display in the Appliance table, but will not be selectable. Information for these appliances will not display in the right panel. When no active appliances are displayed in the Appliance table (for example, when filtering on unsupported appliances), the tab in the right panel will display as inactive, but will show the most recent valid information.

Appliances table

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The **Appliances** table displays information about all appliances that are registered through the Forcepoint Security Manager (named TRITON Manager in versions 8.3.0 and earlier), including:

- ▶ Status (appliance status "[Navigating the Security Appliance Manager](#)" on page 13)
- ▶ Hostname (hostname of the appliance)
- ▶ C IP Address (IP address of the C interface)
- ▶ Version (software version number)
- ▶ Mode (Web or Email mode)
- ▶ Hardware or virtual platform
- ▶ Description (this is a user-added field, accessible through the Status tab)

To change the sort order of a column, click the column header to display the sorting arrow, and click the arrow.

To change the width of the a column, drag the column edges to the desired width.

To select the columns that display in the **Appliances** table, click the column icon in the upper right of the table, and select the columns to display. Custom column selections are retained in subsequent FSAM sessions.

To filter the appliances that display in this table, use the "[Filtering panel](#)" on the previous page.

Adding or deleting an appliance

To add or delete (register or unregister) an appliance, please go to the Appliance page in the Forcepoint Security Manager (TRITON Manager). Refer to the [Security Manager Help](#) document.

Status tab

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The **Status** tab displays general information for each registered appliance and related services. This tab also allows you to edit appliance information, view resource usage data stop, restart, and restart services

This tab uses appliance status icons to indicate connectivity status.

Appliance status information

General section

The **General** section of the **Status** tab displays appliance connectivity status and uptime data, and allows you to edit appliance information and restart the appliance.

Appliance Info window

Click on or hover over the **Appliance Info** link to display the **Appliance Info** window. The **Appliance Info** window displays additional appliance information, including:

- ▶ Hostname
- ▶ Description
- ▶ Time zone
- ▶ Date and time
- ▶ Security mode
- ▶ Software version
- ▶ Installed hotfixes (listed by ID)
- ▶ Hardware platform
- ▶ Service tag

Editing Appliance Information

The **Edit Appliance Info** window allows you to edit the appliance hostname, description, time zone, and date and time.

To edit your appliance information:

1. Select the appliance you want to edit in the **Appliances** table by clicking in the appropriate table row.
2. Click **Appliance Info** at the top of the **Status** tab.
The **Appliance Info** window displays.
3. Click the **Edit** button in the **Appliance Info** window.
The **Edit Appliance Info** window displays.
4. Edit the appliance information:
 - a. To edit the appliance hostname or description, enter the information into the **Hostname** or **Description** field.
 - b. To edit the time zone, use the **Time zone** drop-down menu to select the desired time zone.
5. To edit the date and time, you can either automatically synchronize with an NTP server or manually set the date and time:
 - a. To synchronize with an NTP server, select the **Automatically synchronize...** radio button and enter the NTP server IP address(es).
 - b. To manually set the date and time, select the **Manually set...** radio button and enter the desired date (yyyy/mm/dd or use the date picker) and time (hh:mm:ss).
6. Click the **Save** button.

When the appliance information is saved, a confirmation message displays in the Security Appliance Manager banner.

If the appliance information cannot be saved, an error message displays at the top of the **Edit Appliance Info** window, indicating the error.

Restarting the appliance

To restart the appliance:

1. Click the restart icon in the upper right corner of the **General** section of the **Status** tab.
Select **Restart appliance** from the drop-down menu.
A **Restart Appliance** dialog box displays.
2. Click the **Yes** button in the dialog box.
A **Restarting appliance** status message displays.
3. When the appliance has been restarted successfully, the **Connectivity status** field will display a green **Connected** icon. See the "[Navigating the Security Appliance Manager](#)" on [page 13](#) section for more information about the icons used in the Forcepoint Security Appliance Manager.

Service status information

Web Security Services (TRITON AP-WEB in versions 8.3 and earlier)

The **Web Services** section of the **Status** tab displays the status of related services, including:

- ▶ Bridge Service
- ▶ Cloud App Agent
- ▶ Control Service
- ▶ Event Message Broker
- ▶ Filtering Service
- ▶ Message Broker Handler
- ▶ Multiplexer
- ▶ Policy Broker
- ▶ Policy Database
- ▶ Policy Server
- ▶ SIEM Connector
- ▶ Usage Monitor
- ▶ User Service

For more information about Web services, refer to the [Web Security Administrator Help](#) document.

Proxy Services

The **Proxy Services** section of the **Status** tab displays the status of related services, including:

- ▶ Analytics Server
- ▶ Content Cop
- ▶ Content Gateway
- ▶ Content Gateway Manager
- ▶ Endpoint Authentication Server

For more information about the Proxy services, refer to the [Content Gateway Manager Help](#) document.

Network Agent Services

The **Network Agent Services** section of the Status tab displays the status of related services, including:

- ▶ Control Service
- ▶ Network Agent

For more information about the Network Agent services, refer to the [Web Security Administrator Help](#) document.

Email Security Services (TRITON AP-EMAIL in versions 8.3 and earlier)

The Email Security Services section of the Status tab displays the status of related services, such as:

- ▶ Authentication Service
- ▶ Configuration Service
- ▶ Filtering Service
- ▶ Log Service
- ▶ Mail Transfer Agent
- ▶ Quarantine Service
- ▶ Update Service

For more information about the Email Security services, refer to the [Email Security Administrator Help](#) document.

Stopping, starting, or restarting services

The **Status** tab allows you to stop, start, or restart Proxy, Web Security, Network Agent, or Email Security services.

To stop services:

1. Click the restart icon in the upper right corner of the appropriate section of the **Status** tab. Select **Stop services** from the drop-down menu. A **Stop Services** confirmation message displays.
2. Click the **Yes** button. A **Services stopped** status message displays.

When the services have been stopped successfully, the service fields will display the appropriate status icons. See the ["Navigating the Security Appliance Manager" on page 13](#) section for more information about the icons used in the Forcepoint Security Appliance Manager.

To start services (when the service is in a "stopped" state):

1. Click the restart icon in the upper right corner of the appropriate section of the **Status** tab. Select **Start services** from the drop-down menu. A **Starting services** status message displays.
2. When the services have been started successfully, the service fields will display the appropriate status icons. See the ["Navigating the Security Appliance Manager" on page 13](#) section for more information about the icons used in the Forcepoint Security Appliance Manager.

To restart services:

1. Click the restart icon in the upper right corner of the appropriate section of the **Status** tab. Select **Restart service** from the drop-down menu. A **Restart Services** confirmation message displays.
2. Click the **Yes** button. A **Restarting service** status message displays.

When the services have been restarted successfully, the service fields will display the appropriate status icons. See the ["Navigating the Security Appliance Manager" on page 13](#) section for more information about the icons used in the Forcepoint Security Appliance Manager.

Usage section

The **Usage** section of the **Status** tab displays CPU and memory usage, including the total, used, and free resources, and the percentage being used.

This section also displays information about disk space usage, including:

- ▶ Email: system disk and email spool data
- ▶ Web: system disk, fingerprinting, and proxy cache data
- ▶ URL Filtering: system disk data

Software Updates tab

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The **Software Updates** tab displays available and installed hotfixes and upgrades, and allows you to upload hotfixes and upgrades to your appliances.

Available Items

The **Available Items** section displays the available hotfixes and upgrades that are applicable to the selected appliance. Once installed, the hotfix or upgrade is removed from the list of available items.

To view available hotfixes and upgrades:

1. Expand the **Hotfixes** or **Upgrades** section using the arrow to the left of the section.
A list of available hotfixes or upgrades displays, including the hotfix ID or upgrade filename, as well as the description, available actions, and severity (hotfixes only).
2. To view more information about a hotfix or upgrade, click the plus sign to the left of the item.

To download a hotfix or upgrade:

1. Expand the **Hotfixes** or **Upgrades** section using the arrow to the left of the section.
A list of available hotfixes or upgrades displays.
2. Click **Download** to the right of the item.
A **Downloads** status window displays.

To install a hotfix:

1. Expand the **Hotfixes** section using the arrow to the left of the section.
A list of available hotfixes displays.
2. Click **Install** to the right of the item.
A confirmation window displays.
3. Click **Yes**.
An installation status window displays.

 **Note:** Some hotfix installations require you to restart the appliance.

 **Note:** During the installation and restart process, the application will not be available through the FSAM. All other appliances are available.

To install an upgrade:

1. Expand the **Upgrades** section using the arrow to the left of the section.
A list of available upgrades displays.
2. Click **Install** to the right of the item.
A subscription agreement window displays.
3. Click **I Agree**.
A confirmation window displays.
4. Click **Yes**.
A progress window displays.
Once the installation is complete, a confirmation message displays.

 **Note:** Upgrade installations require you to restart the appliance.

 **Note:** During the installation and restart process, the application will not be available through the FSAM. All other appliances are available.

To delete a hotfix or upgrade:

1. Expand the **Hotfixes** or **Upgrades** section using the arrow to the left of the section.
A list of available hotfixes or upgrades displays.
2. Click **Delete** to the right of the item.
A confirmation window displays.
3. Click **Yes**.
A progress window displays.
Once the deletion is complete, a confirmation message displays.

Installed Items

The **Installed Items** section displays hotfix and upgrade history.

To view history:

1. Expand the **Hotfix History** or **Upgrade History** section using the arrow to the left of the section.
A list of installed hotfixes or upgrades displays.
2. To view more information about a hotfix or upgrade, click the plus sign to the left of the item.

To uninstall a hotfix:

1. Expand the **Hotfix History** section using the arrow to the left of the section.
A list of installed hotfixes displays.
2. Click **Uninstall** to the right of the item.
A confirmation window displays.
3. Click **Yes**.
Once the hotfix is uninstalled, a confirmation message displays.

Upload (8.5 and later)

The **Upload** section allows you to manually upload a hotfix or upgrade to the appliance, once it has been downloaded locally. To upload a hotfix or upgrade:

1. Be sure that the hotfix or upgrade to be uploaded has already been downloaded locally.
2. In the **Upload** section of the **Software Updates** tab, select **Hotfix** or **Upgrade**.
3. Browse to the hotfix or upgrade location.
4. Click **Upload**.

A progress window displays. Once the upload is complete, a confirmation message displays.

Interfaces tab

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The **Interfaces** tab displays and allows you to edit network interface and domain name system (DNS) setting information.

Interface settings

The **Network Interface Settings** section of the **Interfaces** tab displays interface settings for Appliance Controller, Network Agent, Proxy, and Email.

Click the right arrow to expand each section and display its information, including:

- ▶ State (Enabled/Disabled)
- ▶ MAC address
- ▶ Interface speed
- ▶ Interface status
- ▶ IPv4 or IPv6 address
- ▶ Subnet mask
- ▶ Subnet prefix
- ▶ Default gateway
- ▶ Interface bonding (On/Off)

Editing Interface settings

 **Note:** The C interface IP address cannot be changed through FSAM. It can only be changed through the CLI, but this is not recommended. Changing the C interface IP address will affect communication with other TRITON components.

To edit the interface settings:

1. Expand the section for which you want to edit the settings.
The interface settings display.
2. Click the **Edit** button at the bottom of the section.
The interface settings display as editable.
3. Edit the settings using the toggle buttons, drop-down menus, or editable fields.
4. Click the **Save** button.

For more information about interface settings, refer to the [Forcepoint Appliances Getting Started Guide](#).

DNS settings

The **DNS Settings** section of the **Interfaces** tab displays the DNS settings for the Appliance Controller, Network Agent, Proxy, and Web Security.

Click the right arrow to expand each section and display DNS information.

Editing DNS settings

To edit the DNS settings:

1. Expand the section for which you want to edit the settings.
The DNS settings display.
2. Click the **Edit** button at the bottom of the section.
The DNS settings display as editable.
3. Edit the primary, secondary, and tertiary DNS settings by entering the information in the appropriate fields.
4. Click the **Save** button.

Routing tab

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The **Routing** tab displays static and component route information and allows you to add or delete static and component routes from your appliance. This tab also allows you to import and export status routes.

Static IPv4 Routes table

The **Static IPv4 Routes** table displays IPv4 static route information, including:

- ▶ Destination network
- ▶ Subnet mask
- ▶ Gateway
- ▶ Interface

Adding a static IPv4 route

To add a static IPv4 route:

1. Click the **Add Route** button below the **Static IPv4 Routes** table.
An **Add Static IPv4 Routes** dialog box displays.
2. Enter the destination network address in the **Destination network** field (the machine to route all traffic through the interface).
3. Enter the subnet mask address in the **Subnet mask** field.
4. Enter the gateway address in the **Gateway** field.
5. Select the interface from the **Interface** drop-down menu.
6. Click the **Save** button.
A confirmation message displays in the Security Appliance Manager banner.

Importing static IPv4 routes

To import static IPv4 routes:

1. Click the **Import** link below the **Static IPv4 Routes** table.
An **Import Static IPv4 Routes** dialog box displays.
2. Click the **text template** link to download the IPv4 route template file.
3. Populate the file with routes to be imported. Save the file.
4. Click the **Browse** button to navigate to the populated file.

5. Click the **Import** button.

When the routes are imported, a confirmation message displays in the Security Appliance Manager banner.

If the import fails, an error message displays in the **Import IPv4 Routes** dialog box, indicating the error(s).

Exporting static IPv4 routes

To export IPv4 static routes to a file, click the **Export** link below the **Static IPv4 Routes** table. The exported file downloads to the local downloads location.

Deleting a static IPv4 route

To delete a static IPv4 route:

1. Highlight the route you want to delete in the **Static IPv4 Routes** table.
2. Click the **Delete** button below the table.
3. A **Delete Route** dialog box displays, confirming that you want to delete the route.
4. Click the **Delete** button in the dialog box to delete the route.
A “route deleted” confirmation message displays.

Multiple routes can be selected for deletion using the **Ctrl** and **Shift+Ctrl** keys.

Static IPv6 Routes table

The **Static IPv6 Routes** table displays static IPv6 route information, including:

- ▶ Destination network
- ▶ Prefix
- ▶ Gateway
- ▶ Interface

Adding a static IPv6 route

To add a static IPv6 route:

1. Click the **Add** button below the **Static IPv6 Routes** table.
An **Add Static IPv6 Routes** dialog box displays.
2. Enter the destination network address in the **Destination network** field (the machine to route all traffic through the interface).
3. Enter the prefix in the **Prefix length** field.

4. Enter the gateway address in the **Gateway** field.
5. Select the interface from the **Interface** drop-down menu. Only interfaces with IPv6 enabled will be listed.
6. Click the **Save** button.
A confirmation message displays in the Security Appliance Manager banner.

Importing static IPv6 routes

To import static IPv6 routes:

1. Click the **Import** link below the **Static IPv6 Routes** table.
An **Import Static IPv6 Routes** dialog box displays.
2. Click the **text template** link to download the IPv6 route template file.
3. Populate the file with routes to be imported. Save the file.
4. Click the **Browse** button to navigate to the populated file.
5. Click the **Import** button.

When the routes are imported, a confirmation message displays in the Security Appliance Manager banner.

If the import fails, an error message displays in the **Import Static IPv6 Routes** dialog box, indicating the error(s).

Exporting static IPv6 routes

To export IPv6 static routes to a file, click the **Export** link below the **Static IPv6 Routes** table. The exported file downloads to the local downloads location.

Deleting a static IPv6 route

To delete a static IPv6 route:

1. Highlight the route you want to delete in the **Static IPv6 Routes** table.
2. Click the **Delete** button below the table.
3. A **Delete Route** dialog box displays, confirming that you want to delete the route.
4. Click the **Delete** button in the dialog box to delete the route.
A “route deleted” confirmation message displays.

Multiple routes can be selected for deletion using the **Ctrl** and **Shift+Ctrl** keys.

Component Routes table

The **Component Routes** table displays component route information, including:

- ▶ Module
- ▶ Destination network
- ▶ Subnet mask

Adding a component route

To add a component route:

1. Click the **Add** button below the **Component Routes** table.
An **Add Component Route** dialog box displays.
2. Enter the destination network address in the **Destination network** field (the machine to route all traffic through interface C).
3. Enter the subnet mask ID in the **Subnet mask** field.
4. Select the module from the **Module** drop-down menu.
5. Click the **Save** button.
A confirmation message displays in the Security Appliance Manager banner.

Deleting a component route

To delete an component route:

1. Highlight the route you want to delete in the **Component Routes** table.
2. Click the **Delete** button below the table.
3. A **Delete Route** dialog box displays, confirming that you want to delete the route.
4. Click the **Delete** button in the dialog box to delete the route.
A “route deleted” confirmation message displays.

Toolbox tab

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The **Toolbox** tab allows you to:

- ▶ Enable/disable remote SSH access to the appliance command line interface
- ▶ Enable/disable remote access for Technical Support
- ▶ Generate a configuration summary report for Technical Support
- ▶ Create backup files
- ▶ Create backup schedules
- ▶ Restore from backup files

Remote SSH Access

To enable access to the appliance command line interface (CLI) using a remote SSH client, toggle the **ON/OFF** button in the **Remote SSH Access** section to ON. For more information about the CLI, refer to the [Forcepoint Appliances CLI Guide](#).

Remote Assistance

To enable remote access for Technical Support assistance, toggle the **ON/OFF** button in the **Remote Assistance** section to ON.

 **Note:** Enable remote access only at the request of Technical Support. When remote access is enabled, a passcode is automatically generated and displays in the **Remote Assistance** section. Provide the passcode to the Technical Support technician.

Configuration Summary

The configuration summary tool gathers data from the appliance and generates a file that can be sent to Forcepoint Technical Support for analysis and debugging. The file will take approximately 3-5 minutes to generate.

To generate a configuration summary file:

1. Click the **Generate** button in the **Configuration Summary** section.
A status message displays.
When the file has been generated, a confirmation message and download link displays.
2. Click the **Download file** link to download the configuration summary file.

Backup and Restore

The **Backup & Restore** section allows you to view the most recent backup files, create backup files and schedules, and restore from backup files.

 **Note:** Restoring the appliance from a backup can take up to 20 minutes, and requires the appliance to be rebooted.

The most recent backup file displays in the **Backup & Restore** section.

To view previous backup files:

- ▶ Expand the **Backup Files** section. A table listing the previous backup files displays, including file name, version number, creation date, description, storage location, backup type, and any available actions (restore or delete).

To delete a locally stored backup file:

 **Note:** Only locally stored backup files can be deleted through the FSAM. Backups stored elsewhere must be deleted through the Command Line Interface (CLI).

1. Expand the **Backup Files** section.
2. In the **Available Actions** drop-down menu, select **Delete**.
A **Confirm Backup Delete** window displays.
3. Click **Yes**.
A confirmation message displays.

To view current backup schedules:

- ▶ Expand the **Backup Schedules** section. Backup schedules display, including schedule type, frequency, location, last backup time, next backup time, and any available actions (cancel).

To create a backup file:

1. Click the icon at the top of the **Backup & Restore** section.
2. Select "Create backup now".
The **Create Backup Now** window displays.
3. Select the backup type.
4. Select the backup location.
If you select "Create new filestore" editable fields display:

- a. Enter the filestore description, host, path, and port.
 - b. Select the filestore type (FTP, Samba, or TFTP).
 - c. Enter the filestore alias, user name, and password.
5. Enter a description for the backup file.

To restore from a backup file:

 **Note:** All existing backup files for this hostname display in the file list. Only backups which match the current appliance's version and type can be restored.

1. Expand the **Backup Files** section.
2. Click **Restore** to the right of the backup file from which you want to restore.
The **Confirm Backup Restore** confirmation message displays.
3. Click **Yes**.
The appliance will restart.

To create a backup schedule:

1. Click the icon at the top of the **Backup & Restore** section.
2. Select "Schedule backup".
The **Schedule Backup** window displays.
3. Select the backup frequency.
For a weekly schedule, also select the day of the week.
For a monthly schedule, also select the day of the month.
4. Select the backup type.
5. Enter the time of day for the backup to occur.
6. Select the backup location. If you select "Create new filestore" editable fields display:
 - a. Enter the filestore description, host, path, and port.
 - b. Select the filestore type (FTP, Samba, or TFTP).
 - c. Enter the filestore alias, user name, and password.
7. Enter a description for the backup file.

To cancel a backup schedule:

1. Expand the **Backup Schedules** section.
2. Click **Cancel** to the right of the backup schedule you want to cancel.
The **Confirm Backup Schedule Cancel** confirmation message displays.

3. Click **Yes**.

The backup schedule will be removed and cannot be resumed.

SNMP tab

Security Appliance Manager Help | Forcepoint Appliances | v1.2

The **SNMP** tab allows you to view and edit Simple Network Management Protocol (SNMP) setup and event specifications.

For more information about SNMP, refer to the [Forcepoint Appliance Getting Started Guide](#).

SNMP Setup

The **SNMP Setup** section displays SNMP monitor and trap server information.

To edit SNMP monitor and trap server information:

1. Click the **Edit** button in the **SNMP Setup** section.
The section fields display as editable.
2. Toggle the monitor or trap server on or off using the **ON/OFF** buttons.
3. Select the SNMP version from the **SNMP version** drop-down menus.
4. Enter the community name in the **Community name** field.
5. Enter the IP address in the **IP address** field (trap server only).
6. Enter the Port in the **Port** field (trap server only).
7. Click **Save**.

A test trap can be sent by clicking the **Send Test Trap** button.

SNMP Events

The **SNMP Events** section of the **SNMP** tab allows you to view SNMP events tables for each module: Appliance Controller, Proxy, Web Security, Network Agent, and Email Security. Click the right arrow to expand each section and display its table.

Each SNMP event table indicates which events are enabled or disabled, and lists the notification thresholds and event types.

To edit an SNMP event table:

1. Click the **Edit** button at the bottom of the event table.
The enable/disable check boxes and the notification threshold fields display as editable.
2. Edit which events you would like to enable or disable by selecting or deselecting the check boxes.
3. Edit the notification thresholds by using the drop-down menus in the **Threshold** column.
4. Click **Save**.