Forcepoint

Security Appliance Manager

2.x

Installation Guide

Contents

Introduction

Use these instructions to complete a typical installation of the Forcepoint™ Security Appliance Manager (FSAM). For information about this version and its use, see:

- Forcepoint Security Manager Installation Guide
- Forcepoint Security Manager Help
- Forcepoint Security Appliance Manager User Guide
- Forcepoint Security Appliance Manager Release Notes
- FSAM Known Issues (Knowledge Base article)

Contact Forcepoint Technical Support for assistance with installation problems.

System Requirements

The Forcepoint Security Appliance Manager must be installed on the machine that hosts the Forcepoint Security Manager (named Forcepoint TRITON Manager in versions 8.3.0 and earlier). The Forcepoint Management Server must meet the system requirements listed in the Deployment and Installation Center.

FSAM version	Appliance version	Forcepoint Security Manager version
1.0.0	v8.3	v8.3.0
1.1.0	v8.3, v8.4	v8.4.0
1.2.0	v8.3, v8.4	v8.4.0
1.2.1	v8.3, v8.4, v8.5	v8.5.0
2.0.0	v8.3, v8.4, v8.5, v8.5.3	v8.5.3
2.0.1	v8.3, v8.4, v8.5.x*	v8.5.x

Browser requirements

The Security Appliance Manager is certified or supported on the following browsers.

Browser	Version
Microsoft Internet Explorer	11 (certified)
Microsoft Edge	44 (supported)
Mozilla Firefox	76 (certified) 66 through 75 (supported)
Google Chrome	81 (certified) 57 through 62, 79, 80 (supported)

Note

- The recommended screen resolution is 1920 x 1080 or higher.
- Installing the FSAM on a mapped network drive is not supported.

Hotfix requirements

To download a hotfix:

1) On the Forcepoint home page, log on to **My Account**.

2) Click **Downloads**. On the **My Downloads** page, click **All Downloads**.

3) Appliance hotfixes are available under the Appliance heading of the Email Security or Web Security sections.

See the hotfix ReadMe file for more information.

v8.3 appliances

For version 8.3.x appliances, the Security Appliance Manager requires Appliance-Hotfix-App-8.3.0-018.rpm to be installed in the target V Series, X Series, and Virtual appliances.

Note

Hotfix APP-8.3.0-018 requires the installation of hotfix APP-8.3.0-009

> **Note**
>
> Hotfix APP-8.3.0-009 requires the installation of all dependencies:
>
> - APP-8.3.0-001
> - APP-8.3.0-005
> - APP-8.3.0-008
> - APP-8.3.0-010
> - APP-8.3.0-011
>
> It is not necessary to reboot the appliance after each dependency. Reboot the appliance after installing hotfix APP-8.3.0-018.

v8.4 appliances

For version 8.4.x appliances, the Security Appliance Manager requires Appliance-Hotfix-App-8.4.0-004.rpm to be installed in the target V Series, X Series, and Virtual appliances.

Installing the Forcepoint Security Appliance Manager

Installing the Forcepoint Security Appliance Manager is a 9-step process that takes less than 5 minutes.

Downloading the installer

To download the Security Appliance Manager Installer:

Steps

1) On the Forcepoint home page, log on to **My Account**.

2) Click **Downloads**. On the **My Downloads** page, click **All Downloads**.

3) The Security Appliance Manager is available under the Appliance heading of the Email Security or Web Security sections.

4) Click on the entry for the Security Appliance Manager Installer.

## Installation steps

> **Note**
>
> If a version of FSAM is already present, a dialogue box will display, asking you if you would like to uninstall the existing FSAM version.

Steps

1) Double-click the Installer (.exe) file to begin the installation. A progress dialog box appears as files are extracted.

2) When the welcome screen displays, click **Next**.

3) Read the Subscription Agreement. To accept the terms, click **I Agree**.
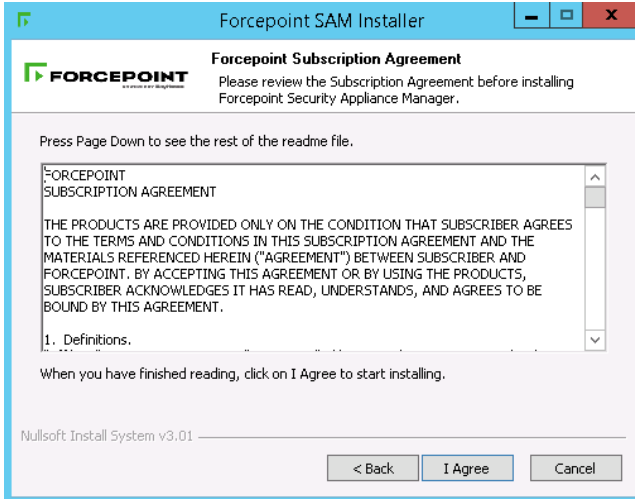
4) On the **Choose Components** screen:

a) Verify that the required space for installation is available.

b) Click **Next**.
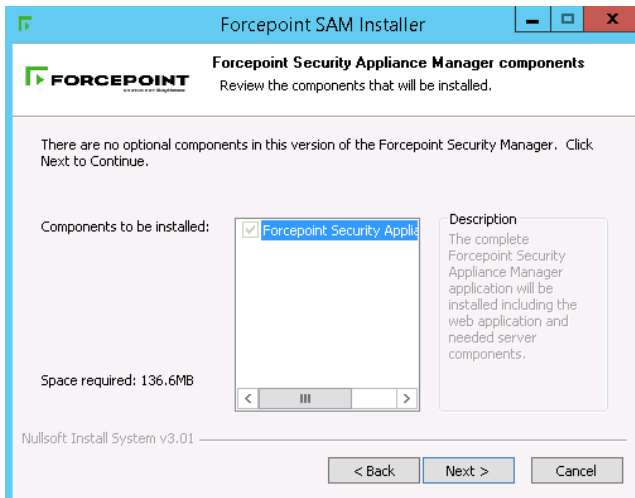
5) On the **Choose Install Location** screen, accept the default location or specify the location where you want the Security Appliance Manager to be installed.

- To accept the default location (recommended), click **Install**.
- To specify a different location, click **Browse**. Browse to the desired location and click **Install**.
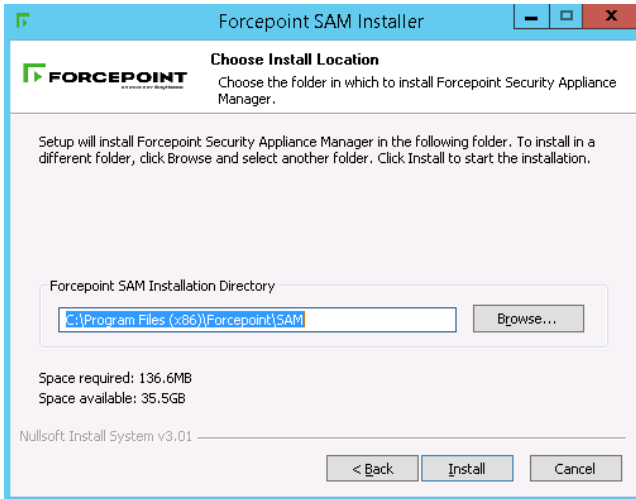

A progress bar displays.

6) On the **Port Selection** screen, accept the default port or modify the port number. Click **Install**.
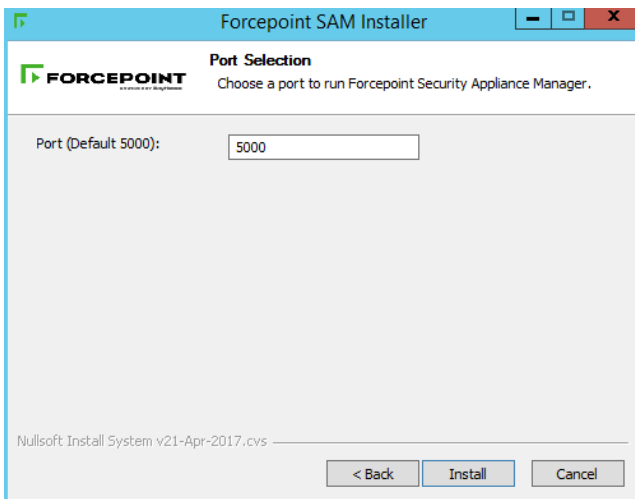
7) Once the installation is complete, a restart message displays. The TRITON Web Server must be restarted before the Security Appliance Manager will function.

> **Note**
>
> It is recommended that you restart the Web Server immediately. Restarting the Web Server takes several seconds.
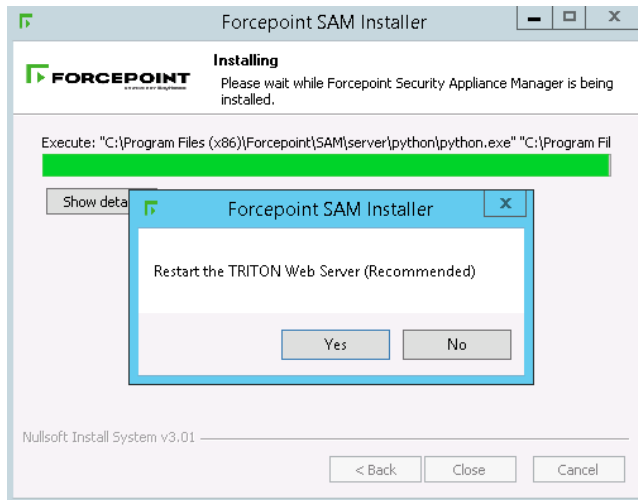
- Click **Yes** to restart the Web Server (recommended). A message displays, confirming that the Web Server has been restarted. Click **OK**.

- Click **No** to continue without restarting the Web Server. You must restart the Web Server before using the Security Appliance Manager.

8) A message displays, confirming that the Security Appliance Manager has been installed successfully. Click **Show details** for more information or click **Close** to exit the installer.

9) Ensure that appliances are registered within the Forcepoint Security Manager (formerly named TRITON Manager) and that Single Sign-On (SSO) is enabled.

Uninstalling the Security Appliance Manager

> **Note**
>
> During an uninstall of FSAM v2.0 or later, a dialogue box displays, asking if you would like to keep your settings.

To uninstall the Forcepoint Security Appliance Manager from Windows clients:

Steps

1) Go to **Start** > **Control Panel** > **Add/Remove Programs** on the client machine.

2) Select **Forcepoint Security Appliance Manager**, and then click **Remove**.

Upgrading to Security Appliance Manager v2.x

To upgrade to FSAM v2.0.1, uninstall the older FSAM version using Windows Control Panel, and then install FSAM v2.0.1 using the installer tool. See the Forcepoint Security Appliance Manager Installation Guide.

Beginning with FSAM v2.x, upgrades can be done through the FSAM itself. See the Forcepoint Security Appliance Manager User Guide for more information.

> **Note**
>
> When upgrading to a new version of FSAM, it is recommended that you clear the client browser cache to avoid unexpected behavior.