



Network Security Platform

7.5

Installation Guide

© 2026 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.

Published 15 June 2026

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint 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.

Contents

| | |
|--|-----|
| Preface | 7 |
| Introduction to the Forcepoint Network Security Platform solution | 9 |
| 1 Introduction to Forcepoint Network Security Platform | 11 |
| Components in the Forcepoint Network Security Platform solution..... | 12 |
| Forcepoint Security Management Center..... | 13 |
| 2 Preparing for installation | 15 |
| Installation security considerations..... | 15 |
| Supported platforms..... | 16 |
| Clustering..... | 19 |
| Deployment options for Security Engines..... | 20 |
| Cable connection guidelines..... | 22 |
| Speed and duplex settings for Security Engines..... | 26 |
| Obtain installation files..... | 26 |
| Licensing Security Engine components..... | 28 |
| Installation overview..... | 32 |
| Forcepoint Security Management Center deployment | 33 |
| 3 Installing the SMC | 35 |
| SMC installation options..... | 35 |
| SMC installation overview..... | 38 |
| Install the SMC..... | 38 |
| Install the SMC in Demo Mode..... | 44 |
| Install the SMC in Linux from the command line..... | 46 |
| Install the SMC Appliance..... | 51 |
| Start the SMC after installation..... | 54 |
| Post-installation SMC configuration..... | 59 |
| 4 Configuring the SMC | 61 |
| Configuring NAT addresses for SMC components..... | 61 |
| Install additional Management Servers for high availability..... | 64 |
| Using the SMC Client in a web browser..... | 67 |
| SMC Client downloads from the Management Server..... | 69 |
| Forcepoint Security Engine deployment | 73 |
| 5 Configuring Forcepoint Security Engine with Layer 3 Interfaces | 75 |
| Types of interfaces for Security Engines with Layer 3 Interfaces..... | 75 |
| Interface numbering..... | 76 |
| Install licenses for Security Engines..... | 77 |
| Configuring Single Engines..... | 78 |
| Configuring Engine Clusters..... | 105 |

| | |
|---|-----|
| 6 Configuring Security Engine for the IPS role | 125 |
| Types of interfaces for Security Engines in the IPS and Layer 2 Engine roles..... | 125 |
| Interface numbering..... | 126 |
| Install licenses for Security Engines..... | 127 |
| Configuring IPS engines..... | 127 |
| Bind engine licenses to IPS elements..... | 141 |
| 7 Configuring Security Engine for the Layer 2 Engine role | 143 |
| Types of interfaces for Security Engines in the IPS and Layer 2 Engine roles..... | 143 |
| Install licenses for Security Engines..... | 144 |
| Configuring Layer 2 Engines..... | 144 |
| Bind engine licenses to Layer 2 Engine elements..... | 157 |
| 8 Configuring Security Engines as Master Engines and Virtual Engines | 159 |
| Master Security Engine and Virtual Security Engine configuration overview..... | 159 |
| Install licenses for Security Engines..... | 160 |
| Add Master Security Engine elements..... | 160 |
| Create Virtual Engines..... | 169 |
| Create Virtual IPS engines..... | 174 |
| Add Virtual Layer 2 Engine elements..... | 176 |
| 9 Configuring routing | 179 |
| Getting started with routing..... | 179 |
| Add routers..... | 180 |
| Add or view the default route..... | 181 |
| Add static routes..... | 181 |
| 10 Initial configuration of Security Engine software | 183 |
| Options for initial configuration..... | 183 |
| Using plug-and-play configuration..... | 184 |
| Using automatic configuration..... | 188 |
| Using the Security Engine Configuration Wizard..... | 190 |
| 11 Creating and installing policies | 205 |
| Create and install a Engine Policy..... | 205 |
| Install a predefined policy on IPS engines and Layer 2 Engines..... | 206 |
| Maintenance | 209 |
| 12 Upgrading licenses | 211 |
| Getting started with upgrading licenses..... | 211 |
| Upgrade licenses manually..... | 211 |
| Install licenses..... | 212 |
| Check Security Engine licenses..... | 212 |
| 13 SMC maintenance | 215 |
| Upgrading the SMC..... | 215 |
| Uninstall the SMC..... | 219 |
| 14 SMC Appliance maintenance | 221 |
| Getting started with SMC Appliance maintenance..... | 221 |
| Patching and upgrading the SMC Appliance..... | 222 |
| Roll back the SMC Appliance to the previous version on the command line..... | 226 |





| | |
|--|-----|
| 15 Upgrading Security Engines | 227 |
| How engine upgrades work..... | 227 |
| Obtain Security Engine upgrade files..... | 229 |
| Prepare Security Engine upgrade files..... | 230 |
| Upgrade Security Engines remotely..... | 231 |
| Upgrade engines locally..... | 233 |
| Appendices | 237 |
| A Default communication ports | 239 |
| Forcepoint Security Management Center ports..... | 239 |
| Security Engine ports..... | 242 |
| Security Engine in the Factory Default State..... | 246 |
| B Command line tools | 247 |
| Security Management Center commands..... | 247 |
| Security Engine commands..... | 263 |
| Server Pool Monitoring Agent commands..... | 273 |
| C Installing SMC Appliance software on a virtualization platform | 275 |
| Hardware requirements for installing SMC Appliance software on a virtualization platform..... | 275 |
| Install SMC Appliance software using an <code>.iso</code> file..... | 275 |
| D Installing Forcepoint Security Engine on a virtualization platform | 277 |
| Hardware requirements for installing Forcepoint Security Engine software on a virtualization platform..... | 277 |
| Install Forcepoint Security Engine software using an <code>.iso</code> file..... | 277 |
| E Installing Forcepoint Security Engine software on third-party hardware | 281 |
| Hardware requirements for installing Security Engine on third-party hardware..... | 281 |
| Start the Forcepoint Security Engine installation on third-party hardware..... | 286 |
| Install Forcepoint Security Engine in expert mode..... | 287 |
| F Installing the SMC with external certificate management | 289 |
| External SMC certificate management configuration overview..... | 290 |
| Install the SMC Appliance with external certificate management..... | 290 |
| Create a certificate for the Management Server using external certificate management..... | 291 |
| Create a certificate for the Log Server using external certificate management..... | 292 |
| Create certificates for Security Engines using external certificate management..... | 296 |
| G Example network (Security Engines with Layer 3 Interfaces) | 301 |
| Example Engine Cluster..... | 301 |
| Example Single Engine..... | 304 |
| Example headquarters management network..... | 305 |
| H Example network (IPS) | 307 |
| Example network overview (IPS)..... | 307 |
| Example headquarters intranet network..... | 309 |
| HQ IPS Cluster..... | 309 |
| Example headquarters DMZ network..... | 310 |
| I Cluster installation worksheet instructions | 311 |
| Cluster installation worksheet..... | 311 |

Preface

This guide provides the information you need to work with your Forcepoint product.

Conventions

The following typographical conventions and icons are used.

| | |
|---|---|
| <i>Book title, term, emphasis</i> | Title of a book, chapter, or topic; a new term; emphasis. |
| Bold | Text that is strongly emphasized. |
| User input, code, message | Commands and other text that the user types; a code sample; a displayed message. |
| Interface text | Words from the product interface like options, menus, buttons, and dialog boxes. |
| Hypertext | A link to a topic or to an external website. |
|  | Note: Additional information, like an alternate method of accessing an option. |
|  | Tip: Suggestions and recommendations. |
|  | Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data. |
|  | Warning: Critical advice to prevent bodily harm when using a hardware product. |

Find product documentation

In the Forcepoint Customer Hub, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product in the Forcepoint Customer Hub at <https://support.forcepoint.com>. There, you can access product documentation, release notes, Knowledge Base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint Customer Hub. If you do not yet have credentials, create a customer account. To create a customer account, navigate to the Customer Hub Home page, and then click the **Create Account** link.

Part I

Introduction to the Forcepoint Network Security Platform solution

Contents

- Introduction to Forcepoint Network Security Platform on page 11
- Preparing for installation on page 15

Before setting up Forcepoint Network Security Platform, it is useful to know what the different components do and what Security Engine roles are available. There are also tasks that you must complete to prepare for installation.

Chapter 1

Introduction to Forcepoint Network Security Platform

Contents

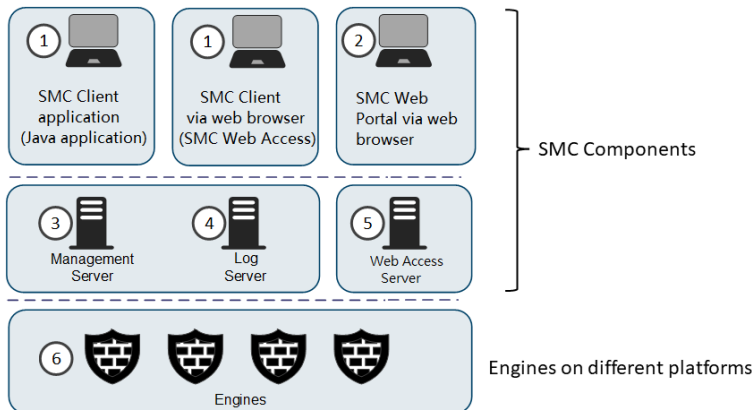
- Components in the Forcepoint Network Security Platform solution on page 12
- Forcepoint Security Management Center on page 13

The Forcepoint Network Security Platform solution consists of Security Engines and the Forcepoint Security Management Center (SMC). The SMC is the management component of the Forcepoint Network Security Platform solution.

Components in the Forcepoint Network Security Platform solution

The Forcepoint Network Security Platform solution includes Security Engines, SMC server components, and SMC user interface components.

Components in the Forcepoint Network Security Platform solution



- 1 The **SMC Client** is the user interface for the SMC, used for all configuration and monitoring tasks. You can install the SMC Client as an application on your local workstation or access it on Management Server or Web Access Server using a web browser. You can have an unlimited number of SMC Clients.
- 2 The **SMC Web Portal** is a browser-based, read-only user interface that provides limited access to configuration, logs, and reports on the Management Server. Configuring and using the Web Portal is optional.
- 3 The **Management Server** is the central component for system administration. A single Management Server can manage different types of Security Engines and Log Servers.
- 4 The **Log Server** stores traffic logs that can be managed and compiled into reports. In addition, Log Servers also:
 - Correlate events
 - Monitor the status of Security Engines
 - Displays real-time statistics
 - Forward logs to third-party devices

In smaller installations, the Log Server can run on the same server as the Management Server. For larger environments, it is recommended to install the Log Server on a separate server. There can be multiple Log Server instances.
- 5 The **Web Access Server** provides additional scalability for administrators using SMC Client via web browser. Configuring and using this component is optional.
- 6 **Security Engines** process and inspects traffic. A single Security Engine installation can be used for multiple purposes, depending on its configuration:
 - Layer 3 Firewall with VPN and SD-WAN capabilities
 - IPS or Layer 2 Firewall with Layer 2 Interfaces
 - IDS with a capture interface

Forcepoint Security Management Center

The basic SMC components are the Management Server, Log Server, and one or more SMC Clients.

The SMC Client is the user interface for the SMC. You can use the same SMC installation to manage multiple Security Engines in different roles.

The SMC can optionally include multiple Management Servers, multiple Log Servers, and multiple Web Access Servers. Your licenses specify the type and number of optional components and engines that your environment can include. You can install the SMC components separately on different computers or on the same computer, depending on your performance requirements. The SMC all-in-one appliance is shipped with the Management Server and a Log Server pre-installed on it.

Chapter 2

Preparing for installation

Contents

- Installation security considerations on page 15
- Supported platforms on page 16
- Clustering on page 19
- Deployment options for Security Engines on page 20
- Cable connection guidelines on page 22
- Speed and duplex settings for Security Engines on page 26
- Obtain installation files on page 26
- Licensing Security Engine components on page 28
- Installation overview on page 32

Before installing Forcepoint Network Security Platform, identify the components of your installation and how they integrate into your environment.

Installation security considerations

Physical security

All Forcepoint Network Security Platform components including SMC components and Security Engines, whether in physical or virtual form factors, must always be setup in secured and access controlled physical premises where only trusted administrators can physically access the appliances running the platform components.

If appliances are to be in general office space, it is recommended to place appliances in a locked room or cabinet where access is available only to trusted administrators. Do not place platform components in public areas such as hallways, reception areas, or shared spaces where tampering risk is higher.

Upgrade appliances

When installing physical appliances, upgrade appliance to the latest recommended version as part of installation procedure. Important functionality and security updates may have become available between the time the appliance was manufactured and when the appliance is deployed. See the *Upgrading Security Engines* chapter for Security Engine upgrade options and the *Patching and upgrading the SMC Appliance* chapter for SMC Appliance upgrade options.

Supported platforms

Several platforms are supported for deploying Security Engine and SMC components.

Supported platforms for SMC deployment

SMC server components can be installed on third-party hardware or they are available as a dedicated Forcepoint Network Security Platform Security Management Center Appliance (SMC Appliance).

Third-party hardware



CAUTION

Do not install the SMC components on Security Engine hardware.

- You can install the SMC on third-party hardware that meets the hardware and operating system requirements. For information about hardware requirements, see the [Release Notes](#).
- You can install all SMC server components on the same computer, or install separate components on different computers.
- In a large or geographically distributed deployment, we recommend installing the Management Server, Log Server, and optional Web Access Server on separate computers.

Physical Forcepoint SMC Appliance

The Management Server and a Log Server are integrated with the hardware operating system as a dedicated server appliance.

Virtual Forcepoint SMC Appliance

The Management Server and a Log Server are integrated with the operating system and provided as `.iso` image for installation to your own hypervisor as a virtual machine.

Supported platforms for Security Engine deployment

You can run Security Engines on various platforms.

The following general types of platforms are available for Security Engines:

- Purpose-built Security Engine appliances



Note

For information about supported appliance models, see Knowledge Base article [9743](#).

- VMware ESX and KVM virtualization platforms
- Microsoft Hyper-V virtualization platform (Security Engine with Layer 3 Interfaces only)
- Microsoft Azure cloud-based virtualization platform (Security Engine with Layer 3 Interfaces only)
- Amazon Web Services (AWS) cloud-based virtualization platform (Security Engine with Layer 3 Interfaces only)
- Third-party hardware that meets the hardware requirements

**Note**

When Security Engine is running on a virtualization platform or a cloud virtualization platform, Master Engines and Virtual Engines are not supported.

For supported versions of virtualization platforms, see the [Release Notes](#).

The Security Engine software includes an integrated, hardened Linux operating system. The operating system eliminates the need for separate installation, configuration, and patching.

Deploying Security Engines on cloud-based virtualization platforms

You can deploy Security Engines on cloud-based virtualization platforms, such as the Amazon Web Services (AWS) cloud and the Microsoft Azure cloud.

Security Engines on cloud-based virtualization platforms provide VPN connectivity, access control, and inspection for services hosted on cloud-based virtualization platforms.

For information about deploying Security Engines in the AWS cloud, see the document *How to deploy Forcepoint Network Security Platform in the Amazon Web Services cloud* and Knowledge Base article [10156](#).

For information about deploying Security Engines in the Azure cloud, see the document *How to deploy Forcepoint Network Security Platform in the Azure cloud* and Knowledge Base article [14485](#).

After deployment, you can manage Security Engines on cloud-based virtualization platforms using the SMC Client in the same way as other Security Engines. If you deploy Security Engines that use the scaling feature, you can only preview the Security Engines and make changes to the Engine policies.

**Note**

Only Single Security Engine with Layer 3 Interfaces are supported. Master Engines and Virtual Engines are not supported.

Licensing

Two licensing models are supported.

- **Bring Your Own License** — You pay only the AWS or Azure standard runtime fee for the Security Engine instance. You must install a license for the Security Engine in the SMC.
- **Hourly** (pay as you go license) — You pay the AWS or Azure standard runtime fee for the Security Engine instance plus an hourly license fee based on the runtime of the Security Engine. No license installation is needed for the Security Engine in the SMC.

For features that require separate licenses, the SMC automatically detects which licensing model the Security Engine uses.

Support for scaling in cloud-based virtualization platforms

When Security Engines are deployed from the Microsoft Azure or AWS cloud environment, additional instances can be created and removed, depending on traffic load.

You deploy the Cloud Auto-Scaled Engines from the cloud environment, and in the SMC Client, the Cloud Auto-Scaled Engine are automatically added to Cloud Auto-Scaled Group elements. You can monitor the Cloud Auto-Scaled Engines on the dashboard, for example.

Limitations

- Cloud Auto-Scaled Engines cannot be edited in the SMC Client.
- The automatic scaling feature is only supported in the Azure cloud. In the AWS cloud, you must add and remove instances manually.

Running Security Engines as Master Security Engines

There are some hardware requirements and configuration limitations when you use an Security Engine as a Master Security Engine.

Running the Security Engine as a Master Security Engine does not require a third-party virtualization platform. When you run Security Engine as a Master Security Engine, the Security Engine hardware provides the virtual environment and resources for the hosted Virtual Security Engines. You must always install the Security Engine software on a hardware device to run the Security Engine as a Master Security Engine.

You can run Master Security Engines on the following types of hardware platforms:

- Purpose-built Security Engine appliances with 64-bit architecture
- Third-party hardware with 64-bit architecture that meets the hardware requirements

For information about system requirements, see the [Release Notes](#).

The following limitations apply when you use an Security Engine as a Master Security Engine:

- Each Master Security Engine must run on a separate 64-bit physical device.
- All Virtual Security Engines hosted by a Master Security Engine or Master Security Engine cluster must have the same role and the same Failure Mode (*fail-open* or *fail-close*).
- Master Security Engines can allocate VLANs or interfaces to Virtual Security Engines. If the Failure Mode of the Virtual IPS engines or Virtual Layer 2 Engines is *Normal* (*fail-close*) and you want to allocate VLANs to several engines, you must use the Master Security Engine cluster in standby mode.

Clustering

There are special considerations when you deploy an Security Engine as a Engine Cluster, IPS Cluster, or Layer 2 Engine Cluster.

Heartbeat connection and state synchronization for clusters

The nodes in a cluster use a heartbeat connection to monitor the other nodes' operation and to synchronize their state tables.

The nodes in a cluster exchange status information through a heartbeat network using multicast transmissions. If a node becomes unavailable, the other nodes of the cluster immediately notice the change, and connections are reallocated to the available nodes. A dedicated network is recommended for at least the primary heartbeat communications.

The heartbeat connection is essential for the operation of the cluster. Make sure that these conditions are true:

- The heartbeat network works correctly and reliably.
- You are using the correct type of network cables (after testing that they work).
- The network interface cards' duplex and speed settings match.
- Any network devices between the nodes are correctly configured.

It is possible to authenticate and encrypt the heartbeat traffic.

Problems in the heartbeat network might seriously degrade the performance and operation of the cluster.

In the Security Engine with Layer 3 Interfaces, the nodes of a Engine Cluster periodically exchange synchronization messages to synchronize state data.

Hardware for Engine Cluster nodes

You can run different nodes of the same cluster on different types of hardware.


The hardware the cluster nodes run on does not need to be identical. Different types of equipment can be used as long as all nodes have enough network interfaces for your configuration. Engine Clusters can run on a Security Engine appliance, on a standard server with an Intel-compatible processor, or as a virtual machine on a virtualization platform.

If equipment with different performance characteristics is clustered together, the load-balancing technology automatically distributes the load so that lower performance nodes handle less traffic than the higher performance nodes. However, when a node goes offline, the remaining nodes must be able to handle all traffic on their own to ensure high availability. For this reason, it is usually best to cluster nodes with similar performance characteristics.

Deployment options for Security Engines

There are several ways to deploy Security Engines depending on how you want to inspect and respond to traffic.

Deployment options for Security Engine

| Security Engine role | Deployment type | Description |
|---|-------------------------|---|
| Security Engine with Layer 3 Interfaces | Layer 3 deployment only | Security Engines with Layer 3 Interfaces have only Layer 3 Physical Interfaces. The Security Engine provide only the features and traffic inspection that are available for Security Engines with Layer 3 Interfaces. |
| | Multi-layer deployment | <p>Security Engines with Layer 3 Interfaces have both Layer 2 Physical Interfaces and Layer 3 Physical Interfaces. Layer 2 Physical Interfaces on Security Engines with Layer 3 Interfaces allow the engine to provide the same kind of traffic inspection that is available for Security Engines in the IPS and Layer 2 Engine roles.</p> <p>The Security Engine also supports the features and traffic inspection that are available for Security Engines with Layer 3 Interfaces.</p> <div data-bbox="565 919 620 974" style="float: left; margin-right: 10px;">  </div> <div data-bbox="662 926 1471 1094" style="background-color: #f0f0f0; padding: 10px;"> <p>Note</p> <p>Multi-layer deployment requires advanced configuration that is outside the scope of this guide. For configuration steps, see the <i>Forcepoint Network Security Platform Product Guide</i>.</p> </div> |
| IPS | Inline | The traffic flows through the IPS engine. The IPS engine has full control over the traffic flow and can automatically block any traffic. An inline IPS engine can also enforce block listing commands from other components. Fail-open network cards can ensure that traffic flow is not disrupted when the IPS engine is offline. An inline IPS engine also provides access control and logging for any Ethernet traffic (layer 2). |
| | Capture | External equipment duplicates the traffic flow for inspection, and the IPS engine passively monitors traffic. The IPS engine does not have direct control over the traffic flow, but it can respond to selected threats by sending packets that reset the connections. An IDS-only IPS engine can send block listing requests to other IPS engines, Layer 2 Engines, or Engines, but it cannot enforce block listing requests from other components. |
| Layer 2 Engine | Inline | The traffic flows through the Layer 2 Engine. The Layer 2 Engine has full control over the traffic flow and can automatically block any traffic. An inline Layer 2 Engine can also enforce block listing commands received from other components. An inline Layer 2 Engine also provides access control and logging for any Ethernet traffic (layer 2). |

| Security Engine role | Deployment type | Description |
|----------------------|--------------------------|--|
| | Capture (Passive Engine) | <p>In a Capture (Passive Engine) installation, external equipment duplicates the traffic flow for inspection to the Layer 2 Engine, and the Layer 2 Engine passively monitors traffic.</p> <p>The Layer 2 Engine does not have direct control over the traffic flow, but it can respond to selected threats by sending packets that reset the connections. A Layer 2 Engine in Passive Engine mode can send block listing requests to other Layer 2 Engine, IPS engines, or Engines. It cannot enforce block listing requests from other components.</p> |
| | Passive Inline | <p>In a Passive Inline installation, the traffic flows through the Layer 2 Engine, but the Layer 2 Engine only logs connections. A Layer 2 Engine in Passive inline mode can send block listing requests to other Layer 2 Engines, IPS engines, or Engines. It cannot enforce block listing requests from other components.</p> |

There are two ways to connect Capture Interfaces on Engines, IPS engines, and Layer 2 Engines to your networks to capture network traffic.

Network connection options for Capture Interfaces

| Option | Description |
|------------------------------------|--|
| Switched Port Analyzer (SPAN) port | A SPAN port captures network traffic to a defined port on an external switch. This action is also known as port mirroring. The capturing is passive, so it does not interfere with the traffic. All traffic to be monitored must be copied to this SPAN port. |
| Network Test Access Port (TAP) | A network TAP is a passive device at the network wire between network devices. The capturing is done passively, so it does not interfere with the traffic. With a network TAP, the two directions of the network traffic are divided to separate wires. For this reason, the IPS engine or Layer 2 Engine needs two capture interfaces for a network TAP; one capture interface for each direction of the traffic. The two related capture interfaces must have the same logical interface that combines the traffic of these two interfaces for inspection. You could also use the pair of capture interfaces to monitor traffic in two separate network devices. |

Cable connection guidelines

Follow these cable connection guidelines when connecting cables to Security Engine hardware and the SMC Appliance.

Cable connection guidelines for SMC Appliance

For an SMC Appliance, make sure that all copper cables are correctly rated (CAT 5e or CAT 6 in gigabit networks).

Cable connection guidelines for Engines

The cabling of Engines depends on the engine type and the installation.

Make sure that all Ethernet cables are correctly rated (CAT 5e or CAT 6 in gigabit networks).

If you have a two-node Engine Cluster, it is recommended to use a crossover cable without any intermediary devices between the nodes. If you use an external switch between the nodes, follow these guidelines:

- Make sure that portfast is enabled on the external switches.
- Make sure that the speed/duplex settings of the external switches and the Engine devices are set to Auto.
- Configure the external switches to forward multicast traffic.

For layer 2 physical interfaces on Engines, follow these cable connection guidelines:

- Capture interfaces — Follow the cable connection guidelines for IPS and Layer 2 Engines.
- Inline IPS interfaces — Follow the cable connection guidelines for IPS.
- Inline Layer 2 Engine interfaces — Follow the cable connection guidelines for Layer 2 Engines.

Cable connection guidelines for IPS and Layer 2 Engines

The cabling of IPS engines and Layer 2 Engines depends on the engine type and the installation.

Make sure that all Ethernet cables are correctly rated (CAT 5e or CAT 6 in gigabit networks).

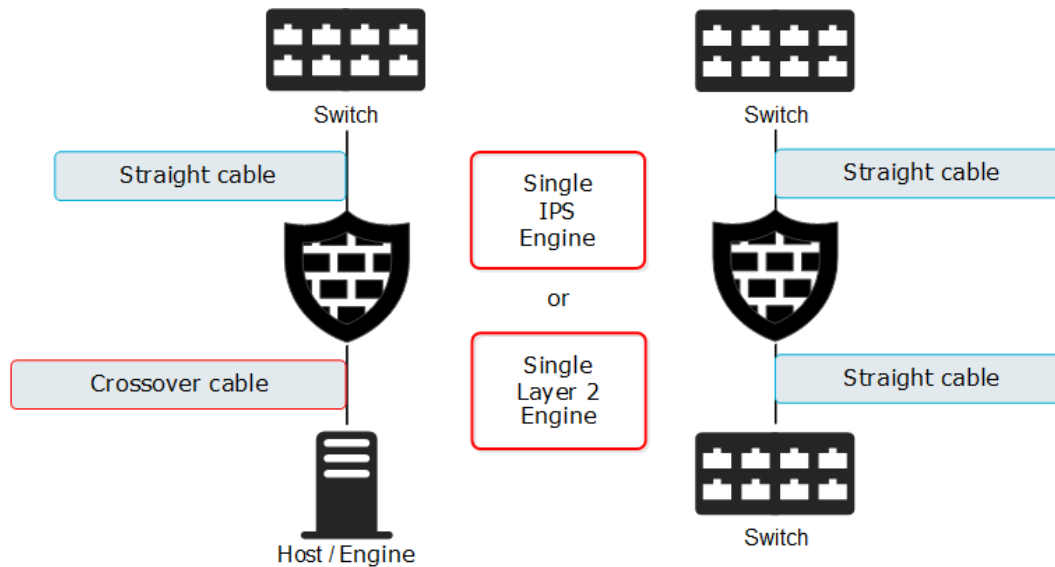
Follow standard cable connections with inline IPS engines and Layer 2 Engines:

- Use straight cables to connect the IPS engines and Layer 2 Engines to external switches.
- Use crossover cables to connect the IPS engines and Layer 2 Engines to hosts (such as routers or Engines).

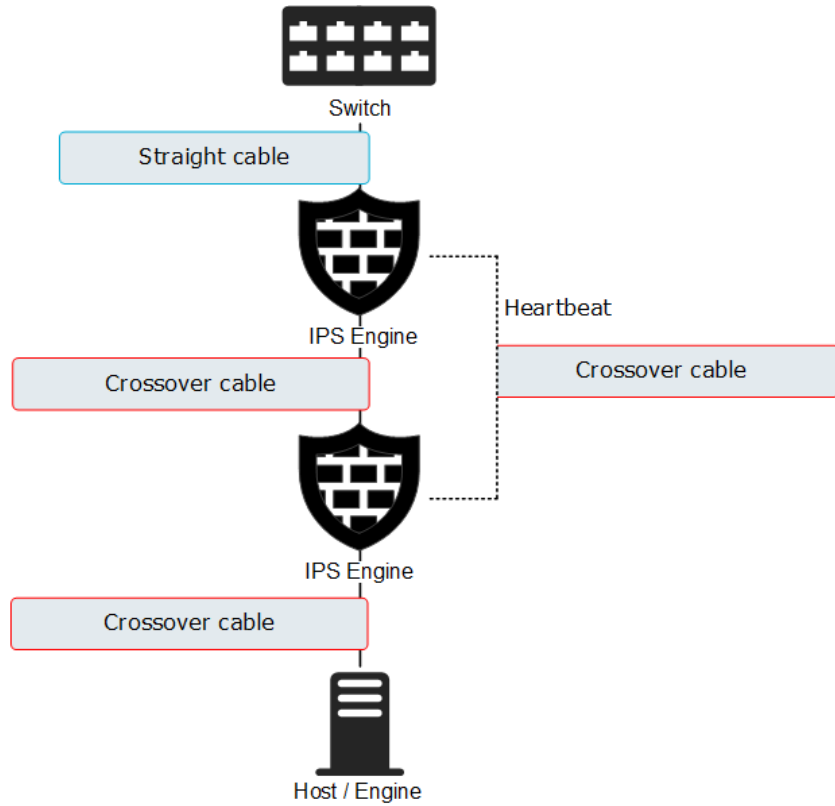
**Note**

Fail-open network interface cards support Auto-MDIX, so both crossover and straight cables might work when the IPS engine is online. However, only the correct type of cable allows traffic to flow when the IPS engine is offline and the fail-open network interface card is in bypass state. It is recommended to test the IPS deployment in offline state to make sure that the correct cables are used.

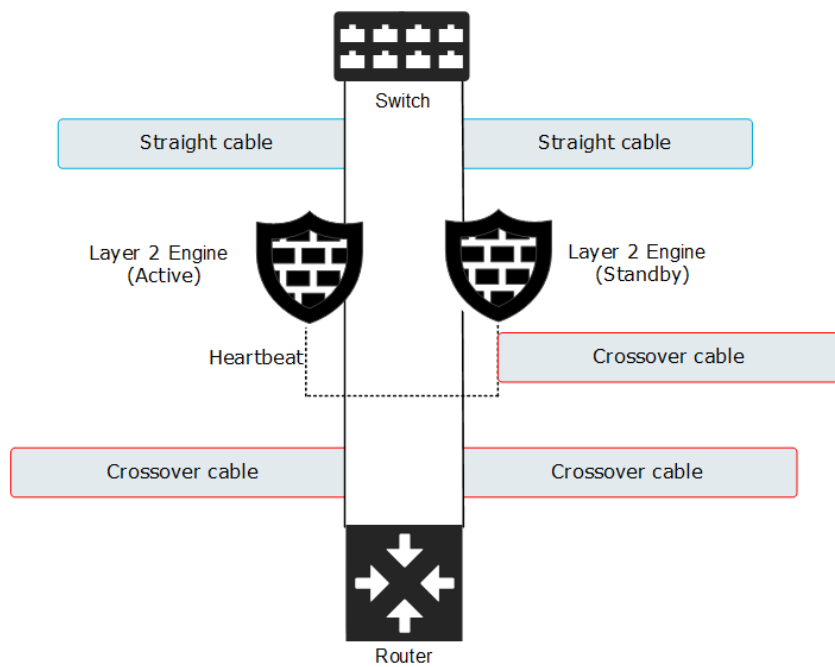
Cable connections for Master Engines that host Virtual IPS engines or Virtual Layer 2 Engines follow the same principles as the connections for inline IPS engines and Layer 2 Engines.

Correct cable types for Single IPS engines and Single Layer 2 Engines

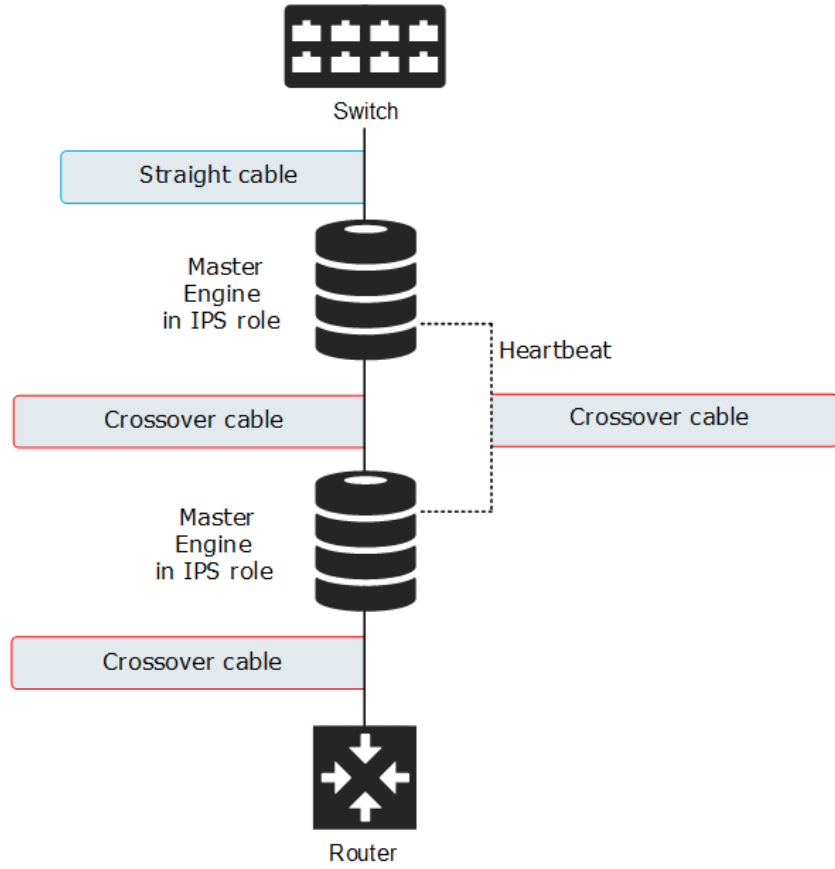
Correct cable types for Serial IPS Clusters



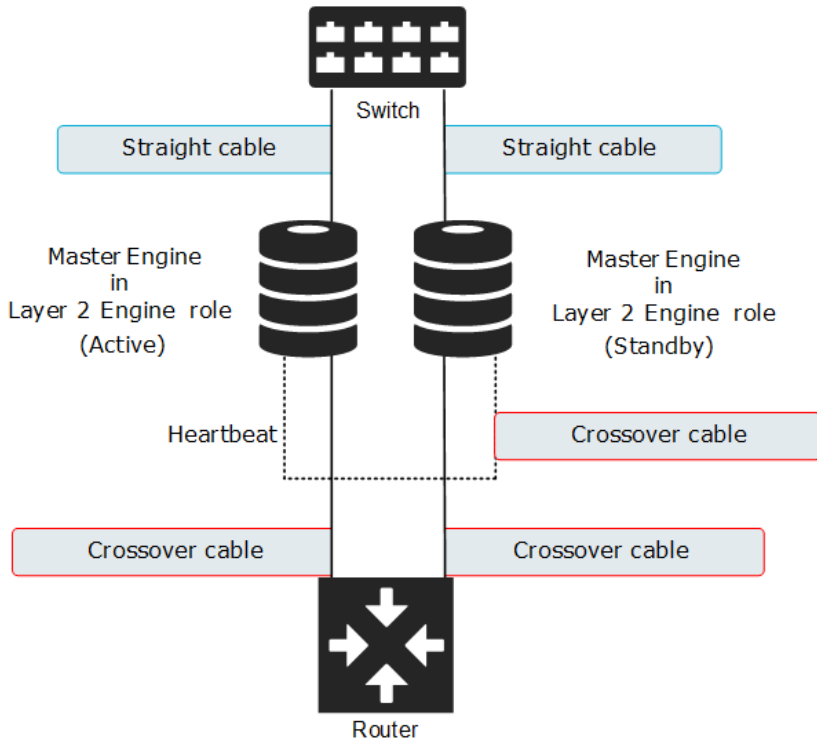
Correct cable types for Active/Standby Layer 2 Engine Clusters



Correct cable types for Serial Virtual IPS Clusters



Correct cable types for Active/Standby Virtual Layer 2 Engine Clusters



Speed and duplex settings for Security Engines

Mismatched speed and duplex settings are a frequent source of networking problems.

The basic principle for speed and duplex settings is that network cards at both ends of each cable must have identical settings. This principle also applies to the automatic negotiation setting: if one end of the cable is set to auto-negotiate, the other end must also be set to auto-negotiate and not to any fixed setting. Gigabit standards require interfaces to use auto-negotiation. Fixed settings are not allowed at Gigabit speeds.

For Inline Interfaces, the settings must be identical on both links within each Inline Interface pair. Use identical settings on all four interfaces, instead of just matching settings at both ends of each cable (two + two interfaces). If one of the links has a lower maximum speed than the other link, the higher-speed link must be set to use the lower speed.

Obtain installation files

If you did not receive an installation DVD for the Security Engine software or the SMC, download installation files.

You do not have to download installation files under these circumstances:

- Security Engine appliances and the SMC Appliance are delivered with the necessary software pre-installed on them. You do not need to download installation files for these appliances.

- You might have received ready-made installation DVDs of the Security Engine software and the SMC software.

Download installation files

Download the files you need to install the Security Engine software and the SMC components.

Installation files for the SMC components are available only as `.zip` files. Installation files for the Security Engine software are available as `.zip` files or `.iso` image files.

Steps

- 1) Go to <https://support.forcepoint.com>.
- 2) Log on using an existing user account.
- 3) Select **Downloads**.
- 4) Under **Network Security**, click the version of the SMC software that you want to download, then download the `.zip` file installation file.
- 5) Under **Network Security**, click the version of the Security Engine software that you want to download, then select the type of installation file to download.
 - The `.zip` file is used in the remote upgrade on all supported platforms. It can also be used for a local upgrade from a USB drive or a non-bootable DVD.
 - The `.iso` file allows you to create a bootable installation DVD for a local upgrade on platforms that have an optical drive.

Check file integrity

Before installing the Security Engine software from downloaded files, check that the installation files have not become corrupt or been changed.

Using corrupt files might cause problems at any stage of the installation and use of the system. Check file integrity by generating a file checksum of the files. Compare the checksum of the downloaded files with the checksum for the software version in the [Release Notes](#) or on the download page at the Forcepoint website.



Note

In Windows environments, you can use Windows PowerShell to generate checksums. Several third-party programs are also available.

Steps

- 1) Look up the correct checksum at <https://support.forcepoint.com>.
- 2) Change to the directory that contains the files to be checked.
- 3) Generate a checksum of the file using one of the following commands, where `filename` is the name of the installation file:

- `sha1sum filename`
- `sha256sum filename`
- `sha512sum filename`

- 4) Compare the displayed output to the checksum for the software version. They must match.

**CAUTION**

Do not use files that have invalid checksums. If downloading the files again does not help, contact [Forcepoint Customer Hub](#) to resolve the issue.

Next steps

If you downloaded the installation files as a `.zip` file, unzip the contents at the installation location.

Create an installation DVD for Security Engine software

To use the installation DVD successfully, it must have the correct structure stored in the `.iso` images. Otherwise you cannot use it for installing the Security Engine software.

Steps

- 1) Use a DVD burning application that can correctly read and burn the DVD structure stored in the `.iso` image for the Security Engine software.
For instructions, see the documentation that came with your application.

Licensing Security Engine components

Generate and download a license for each SMC server and Security Engine node before you start installing the Security Engine.

You install the SMC server license when you start the SMC after installation. You install the Security Engine licenses when you start configuring the Security Engines.

Types of licenses for SMC servers and Security Engines



Each SMC server and Security Engine node must have its own license.

- Some Security Engines use an Security Engine Node license. Other Security Engines use role-specific licenses. The correct type of license for each Security Engine is generated based on your Management Server proof-of-license (POL) code or the appliance proof-of-serial (POS) code.

- If there is no connection between the Management Server and the License Center, a Security Engine appliance can be used without a license for 30 days. After this time, you must generate the licenses manually at the License Center webpage and install them using the SMC Client.
- Virtual Security Engines do not require a separate license. However, the Master Security Engine license limits the number of Virtual Resources that can be created. The limit for the number of Virtual Resources defines how many Virtual Security Engines can be created.
- The Management Server's license might be limited to managing only a specific number of Security Engines.
- Security Engines deployed in the AWS cloud with the Bring Your Own License image must have a license in the SMC. Security Engines deployed in the AWS cloud with the Hourly (pay as you go) image do not require a separate license in the SMC.

Licenses can be bound to a component in several different ways. The possible binding methods depend on the licensed component and the software version.

License binding methods

| License binding | Description |
|---|---|
| IP address binding | <p>The license is statically bound to the IP address of the licensed component.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Only licenses for SMC servers can be bound to an IP address. Existing IP-address-bound licenses for other components continue to work and can be upgraded. Any new licenses for other components must be bound to the Management Server's proof-of-license (POL) code.</p> </div> |
| UUID binding | <p>The license is statically bound to the unique installation identifier (UUID) for the SMC. The UUID is automatically generated when you install the SMC. The UUID is also shown in the properties of the Management Server or Log Server elements.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Only licenses for SMC servers can be bound to the UUID for the SMC.</p> </div> |
| Management Server proof-of-license (POL) code binding | <p>Licenses are dynamically bound to the Management Server's proof-of-license (POL) code. You must manually bind Management Server POL-bound licenses to the correct element. Licenses are valid only for components that are managed by the Management Server that has the same POL code.</p> |
| Appliance proof-of-serial (POS) code binding | <p>The license is bound to the unique POS code of a pre-installed Forcepoint Network Security Platform appliance. The appliance identifies itself when contacting the Management Server. The Management Server allows the use of the appliance if the license POS code matches the reported code. The Management Server automatically binds the correct license to the Security Engine element based on the POS code. For the Management Server and pre-installed appliances, the Management Server can use this licensing method automatically with new appliances.</p> |

The license types that are available depend on the SMC server or type of Security Engine.

| License binding | Description |
|--------------------|---|
| Management Servers | A static IP-address-bound license or a static UUID-bound license. |

| License binding | Description |
|---|---|
| Log Servers | A static IP-address-bound license, a static UUID-bound license, or a dynamic license bound to the Management Server's POL code |
| Pre-installed Forcepoint Network Security Platform appliances | A license bound to the POS code of the appliance (all current models) or a dynamic license bound to the Management Server's POL code (older models) |
| Security Engines installed on your own hardware | Always a dynamic license bound to the Management Server's POL code |
| Security Engines installed on a virtualization platform | Always a dynamic license bound to the Management Server's POL code |
| Feature-specific licenses | A dynamic license bound to the Management Server's POL code or a license bound to the POS code of the appliance depending on the feature |

After the Security Engines and the SMC are fully installed, the SMC can automatically download and install future Security Engine licenses. For more information about automatic downloading and installation of licenses, see the *Forcepoint Network Security Platform Product Guide*.

Obtain license files

Generate the licenses based on your Management Server proof-of-license (POL) code or the appliance proof-of-serial-number (POS) code.

If you are licensing several components of the same type, remember to generate a license for each component.


Evaluation licenses are also available. Evaluation license requests might need manual processing. See the license page for current delivery times and details.

All licenses include the latest version for which they are valid. Automatic upgrade and installation of licenses is enabled by default. If you have disabled automatic license upgrades, you must upgrade the licenses when you upgrade to a new major release of the software.

Steps

- 1) Go to <https://stonesoftlicenses.forcepoint.com>.
- 2) In the **License Identification** field, enter the POL or POS code, as follows.
 - Proof-of-license (POL) code — Identifies the license. For previously licensed components, the POL code is shown in the Licenses tree in the **Administration Configuration** view.
 - Proof-of-serial (POS) number — The Forcepoint Network Security Platform appliances additionally have a proof-of-serial number that you can find on a label attached to the appliance hardware.
- 3) Click **Submit**.
- 4) Check which components are listed as included in this license, then click **Register**.
- 5) Read the instructions on the page, then fill in the required fields for all included components.

6) Enter the details that bind each license to a component, as follows:

| Component | Details for license binding |
|-------------------------|--|
| Management Servers | <ul style="list-style-type: none"> ■ IP-address-bound license — Enter the IP address that you plan to use on the server. If your license allows several Management Servers in the same SMC for high availability, enter a comma-separated list of the IP addresses of all Management Servers. ■ UUID-bound license — Enter the UUID of the SMC. The UUID is automatically generated when you install the SMC. The UUID is also shown in the properties of the Management Server or Log Server elements. |
| Other SMC servers | <ul style="list-style-type: none"> ■ IP-address-bound license — Enter the IP address that you plan to use on the server. ■ Management Server POL-bound license — Enter the Management Server's POL code. ■ UUID-bound license — Enter the UUID of the SMC. The UUID is automatically generated when you install the SMC. The UUID is also shown in the properties of the Management Server or Log Server elements. |
| Master Security Engines | Enter the POS code of a Forcepoint Network Security Platform appliance (see the label attached to the appliance). |
| Security Engines | <ul style="list-style-type: none"> ■ For Forcepoint Network Security Platform appliances, enter the POS code of the appliance (see the label attached to the appliance). ■ For Forcepoint Network Security Platform software installed on your own hardware or on a virtualization platform, enter the POL code of the Management Server that you use to manage the Security Engine. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Note POS binding is always recommended when the option is available.</p> </div> |

**Note**

If the binding information is incorrect, the license is unusable. If you accidentally generated a license with the wrong binding information, request a license change through the License Center.

7) Click **Submit Request**.

The license file available for download at the License Center.

Related tasks

[Install licenses for SMC servers on page 56](#)

[Install licenses for Security Engines on page 77](#)

Installation overview

The process of installing Security Engine consists of several high-level steps.

- 1) Install and configure the SMC and a SMC Client.
- 2) Download licenses for the SMC components and the Security Engines, and install the licenses in the SMC Client.
- 3) If network address translation (NAT) is applied to communications between system components, define contact addresses for the SMC components in the SMC Client.
- 4) Define the Security Engines with required interfaces and interface types in the SMC Client. You can optionally define Master Security Engines and Virtual Security Engines.
- 5) Configure interfaces and routing for the Security Engines in the SMC Client.
- 6) In the SMC Client, generate the initial configuration for Security Engines and Master Security Engines. You do not need an initial configuration for Virtual Security Engines.
- 7) If you are not using a Forcepoint appliance that has pre-installed Security Engine software, install the Security Engine software on virtualization platforms or third-party hardware.
- 8) Configure the Security Engine software and apply the initial configuration to the Security Engines.
- 9) Create and install a policy on the Security Engines.

Part II

Forcepoint Security Management Center deployment

Contents

- Installing the SMC on page 35
- Configuring the SMC on page 61

SMC is the management component of the Security Engine system. SMC must be installed and running before you can deploy the Security Engines.

Installing the SMC

Contents

- SMC installation options on page 35
- SMC installation overview on page 38
- Install the SMC on page 38
- Install the SMC in Demo Mode on page 44
- Install the SMC in Linux from the command line on page 46
- Install the SMC Appliance on page 51
- Start the SMC after installation on page 54
- Post-installation SMC configuration on page 59

The SMC is the management component of the Forcepoint Network Security Platform solution. The SMC manages and controls the other components in the system. You must install the SMC before you can install Security Engines.

SMC installation options

You can install SMC server components on your own hardware or use an all-in-one SMC Appliance.



CAUTION

Make sure that the operating system version you plan to install on is supported. The supported operating systems for running the SMC are listed in the [Forcepoint Security Management Center Release Notes](#).

There are several ways to install the SMC server components:

- (Recommended) You can install the SMC server components using the Installation Wizard.



Tip

To evaluate the Forcepoint Network Security Platform system in a simulated network environment, you can install the SMC in demo mode.

- In Linux, you can install the SMC server components from the command line.



Note

You need a graphical environment to use the SMC Client. Only the SMC server components can run in a command line-only environment.

- The Management Server and a default Log Server are pre-installed on the SMC Appliance. When you start the appliance, the installation wizard includes the configuration of these components.

During the installation, certificates can be generated for the SMC server components. The certificates are needed for authentication in establishing the secure encrypted communication channel between system components.

You can optionally install the SMC with external certificate management if you want to use certificates issued by an external CA instead of certificates generated by the internal CA on the Management Server for internal TLS communication between system components. For more information, see *Installing the SMC with external certificate management*.

After the installation, you can install the SMC Client on other computers. You can also run the SMC Client in a web browser.

Related tasks

[Install the SMC in Demo Mode](#) on page 44

[Install the SMC in Linux from the command line](#) on page 46

Related information

[Installing the SMC with external certificate management](#) on page 289

Requirements for running SMC on third-party hardware

There are some minimum requirements and recommendations when you run the SMC on third-party hardware. For more information, see the [Release Notes](#).

Security considerations for SMC deployment

The information stored in the SMC Manager is highly valuable to anyone conducting or planning malicious activities in your network. Someone who gains administrator rights to the Management Server can change the configurations.

An attacker can gain access by exploiting operating system weaknesses or other services running on the same computer to gain administrator rights in the operating system.



Important

Secure the Management Server computer. Anyone who has administrator rights to the operating system can potentially view and change any SMC configurations.

Consider at least the following points to secure the Management Server and Log Server:

- Prevent any unauthorized access to the servers. Restrict access to the minimum required both physically and with operating system user accounts.
- We recommend allowing access only to the required ports.
- Never allow SMC Client connections from insecure networks.
- Take all necessary steps to keep the operating system secure and up to date.
- We recommend that you do not run any third-party server software on the same computer with the SMC servers.
- We recommend placing the servers in a separate, secure network segment without third-party servers and limited network access.

You can optionally install the SMC with external certificate management. Using certificates issued by an external CA allows you to use your own established internal CA infrastructure to generate certificates for internal TLS communication between system components. Certificate revocation checking is also supported. If any devices are compromised, the certificates associated with them can be revoked and replaced centrally using the external certificate management system.

Related reference

[Security Engine ports](#) on page 242

[Forcepoint Security Management Center ports](#) on page 239

Related information

[Installing the SMC with external certificate management](#) on page 289

Basic system settings for the SMC components

Check these operating system settings on the computers that you use as a platform for the SMC components.

Date and time settings for SMC components

Make sure that the date, time, and time zone settings are correct on any computer that you use as a platform for any SMC component, including the SMC Client workstations. The time settings of the Security Engines do not need to be adjusted, as they are automatically synchronized with the Management Server's time setting. For this operation, the time is converted to UTC time according to the Management Server's time zone setting. The SMC always uses UTC internally.

Hosts file for SMC servers

Due to a restriction of the Java platform, the Management Server and Log Server host names must be resolvable on the computer running the SMC Client. This restriction applies even if the SMC Client is running on the same computer as the servers.

To guarantee that the host names can be resolved, add the IP address and host name pairs to the local hosts file on the client computer:

- In Windows: `\\%SystemRoot%\system32\drivers\etc\hosts`
- In Linux: `/etc/hosts`

Installing on Linux

The installation creates `sgadmin` user and group accounts.

If there is a pre-existing `sgadmin` account, the installation fails. All shell scripts belong to `sgadmin` and are executed either by root or the `sgadmin` user. The shell scripts are executed with `sgadmin` rights. After the installation, the `sgadmin` account is disabled. The `sgadmin` account is deleted at uninstallation.

SMC installation overview

The process of installing SMC consists of several high-level steps.

- 1) Install the SMC components or start the SMC Appliance.
If you are installing components on separate computers, install the Management Server first.
- 2) Start the SMC.
- 3) Install licenses for SMC servers.
- 4) (Optional) Install additional Management Servers.

Install the SMC

You can install the SMC using a graphical user interface installation wizard in Windows and Linux.
For information about installing the all-in-one appliance, see the topic about installing the SMC Appliance.

Related tasks

[Obtain installation files](#) on page 26

[Install the SMC in Linux from the command line](#) on page 46

[Install the SMC Appliance](#) on page 51

Start the installation

Start the Installation Wizard on the computer where you want to install the SMC components.

Steps

- 1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.
- 2) Start the Installation Wizard from a `.zip` file or the Installation DVD.
Decompress the `.zip` file.
 - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
 - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

If the DVD is not automatically mounted in Linux, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

- 3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the SMC Client.

- 4) Read the information on the **Introduction** page, then click **Next**.

**Tip**

Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

- 5) Select **I accept the terms of the License Agreement**, then click **Next**.

- 6) (Optional) Select where to install the SMC, then click **Next**.

The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.

**Note**

If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

- 7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.

- 8) Select where to create shortcuts, then click **Next**.

These shortcuts can be used to manually start components and to run some maintenance tasks.

- 9) Select the installation type, then click **Next**.

- **Typical** — Installs a Management Server, a Log Server, and the SMC Client.
- **SMC Client Only** — Use to install additional SMC Clients on administrators' workstations.
- **Demo Mode** — For more information, see the section about installing in Demo mode.
- **Custom** — Select individual components to install. Use this option to:
 - Install individual SMC components. For example, you can install the Management Server on one computer, and the Log Server on another.
 - Install the Web Access Server.
 - Install only a Management Server if you want to install an additional Management Server for high availability.

- 10) If you selected a custom installation, select the components to install, then click **Next**.

**Important**



Make sure that you have a license for any separately licensed components before installing them.

Install a Management Server

Continue the installation in the Installation Wizard to configure the options for the Management Server.

Steps

- 1) Configure the settings, then click **Next**.

| Option | Description |
|---|---|
| Select Management Server IP Address | Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding. |
| Log Server IP Address | Enter the IP address of the Log Server to which this server sends its log data. |
| Advanced Management Server Options | When selected, you can configure additional options on another page. Select this option if you want to: <ul style="list-style-type: none"> ■ Disable the use of 256-bit encryption for communication between the Management Server and the Security Engines. ■ Enable the use of Web Access to run the SMC Client in a web browser. |
| Install as an Additional Management Server for High Availability | When selected, you can configure additional options on another page. For more information, see the section about adding a Management Server for high availability. |
| Enable FIPS Configuration Restrictions | When selected, restrictions for a FIPS-compatible environment are enabled. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>This option only is for environments that are required to follow FIPS standards. Do not enable this option unless you have a specific reason to do so.</p> </div> |
| Use External Certificate Authority | When selected, the SMC uses certificates issued by an external CA instead of certificates generated by the internal CA on the Management Server for internal TLS communication between system components. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>Using this option requires additional configuration after installation. For more information, see <i>Installing the SMC with external certificate management</i> .</p> </div> |
| Install the Management Server as a Service | When selected, the server starts automatically. |

- 2) If you selected **Advanced Management Server Options** on the previous page, select the features to enable, then click **Next**.

| Option | Description |
|--|---|
| Enable and Configure Web Access | When enabled, administrators can access the SMC in a web browser. You can run the SMC Client in a web browser instead of installing the SMC Client locally. On Linux platforms, <code>xvfb-run</code> must be installed under <code>/usr/bin</code> . You can specify another path in the Management Server properties after the installation has completed. |
| Enable OWASP encoding | When enabled, the SMC API uses the OWASP encoder in responses. Using the OWASP encoder reduces the risk of cross site scripting (XSS) attacks when you use the SMC API in a web browser. <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Note</p> <p>When you enable this option, some strings in data returned by the SMC API, such as special characters inside JSON payloads, are also encoded. We recommend enabling this option only if you use the SMC API in a web browser.</p> </div> |
| 256-bit Security Strength | When enabled, 256-bit encryption is used for communication between the Management Server and the Security Engines. This option is selected by default. |

- 3) If you enabled Web Access, configure the settings, then click **Next**.

| Option | Description |
|---------------------------------------|--|
| Port Number | Enter the TCP port number that the service listens to. By default, port 8085 is used when Web Access is enabled on the Management Server and port 8083 when enabled on the Web Access Server. <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Note</p> <p>Make sure that the listening port is not in use on the server.</p> </div> |
| Host Name (Optional) | Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names. |
| Certificate Distinguished Name | Administrators must use an HTTPS connection to access and use the SMC Client. Enter the distinguished name in LDAP string format for the certificate used to secure the HTTPS connection. Example: <code>dn=smc,dc=demo,dc=com</code> |
| Certificate Algorithm | Select the algorithm and key length for the certificate used to secure the HTTPS connection. |
| Certificate Signer | Select the signer for the certificate used to secure the HTTPS connection. You can use the Internal Certificate Authority or the certificate can be self-signed. |

- 4) Enter a user name and password to create a superuser account, then click **Next**.



Important

This is the only account that an administrator can use to log on after the installation has been completed.

Related information


Installing the SMC with external certificate management on page 289

Install a Log Server

Continue the installation in the Installation Wizard to configure the options for the Log Server.

Steps

- 1) Configure the settings, then click **Next**.

| Option | Description |
|--|---|
| Select Log Server IP Address | Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding. |
| IP Address(es) of the Management Server(s) that will control this Log Server | Enter the IP address of the Management Server that controls this server. If there are multiple Management Servers, enter the IP addresses as a comma-separated list. |
| Certify the Log Server during the installation | When selected, the server is automatically certified. If the components are installed on different computers and the Management Server is not immediately contactable, deselect this option to avoid connection attempts after installation. Certifying is mandatory for running the server. |
| Port on which the Log Server will receive data | Enter the port number that the server receives data on. |
| Enable FIPS Configuration Restrictions | When selected, restrictions for a FIPS-compatible environment are enabled. <div data-bbox="495 976 548 1029" style="float: left; margin-right: 10px;"></div> <div data-bbox="592 976 1469 1102" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Note</p> <p>This option only is for environments that are required to follow FIPS standards. Do not enable this option unless you have a specific reason to do so.</p> </div> |
| Install the Log Server as a Service | When selected, the server starts automatically. |

- 2) (Optional) Click **Choose** to browse to a different storage folder for log data.



Note

Remote locations are not suitable for active storage, as quick and reliable access is required.


- 3) Click **Next**.

Install a Web Access Server

Continue the installation in the Installation Wizard to configure the options for the Web Access Server. The Web Access Server provides restricted access to log data, reports, and policy snapshots.

Steps

- 1) Configure the settings, then click **Next**.

| Option | Description |
|---|---|
| Select Web Access Server IP Address | Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding. |
| IP Address(es) of the Management Server(s) that will control this Web Access Server | Enter the IP address of the Management Server that controls this server. If there are multiple Management Servers, enter the IP addresses as a comma-separated list. |
| Certify the Web Access Server during the installation | When selected, the server is automatically certified. If the components are installed on different computers and the Management Server is not immediately contactable, deselect this option to avoid connection attempts after installation. Certifying is mandatory for running the server. |
| Log Server IP Address | Enter the IP address of the Log Server to which this server sends its log data. |
| Enable FIPS Configuration Restrictions | When selected, restrictions for a FIPS-compatible environment are enabled. <div data-bbox="495 1008 548 1060" style="float: left; margin-right: 10px;">  </div> <div data-bbox="592 1018 657 1045" style="border-bottom: 1px solid black; padding-bottom: 5px;"> Note </div> <div data-bbox="592 1060 1437 1123" style="padding: 5px;"> This option only is for environments that are required to follow FIPS standards. Do not enable this option unless you have a specific reason to do so. </div> |
| Install the Web Access Server as a Service | When selected, the server starts automatically. |

Finish the installation

Review the configuration options that you set in the Installation Wizard, then finish the installation.

Before you begin

If you are installing any server components as a service on a Windows system, make sure that the Services window is closed before you proceed.



Important

This is the last chance to cancel the installation or make changes. Click **Previous** to adjust your selections.

Steps

- 1) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.
Depending on the options, you selected, you might be prompted to generate certificates during the installation.

When the installation has completed, the unique installation identifier (UIID) for the SMC is shown. If you plan to use UIID-bound licenses for SMC servers, make a note of the UIID for the SMC. You will need the UIID to generate licenses.

- 2) When the installation has completed, click **Done**.



Note

If any Log Server or Web Access Server certificate was not retrieved during the installation, retrieve a certificate manually before starting the server.

Related tasks

[Generate SMC server certificates](#) on page 58

Install the SMC in Demo Mode

The Demo Mode installation creates a simulated network environment for evaluation.

Demo Mode installation is for evaluation only. The SMC in Demo mode cannot be used for traffic inspection and cannot be upgraded.

Steps

- 1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.
- 2) Start the Installation Wizard from a `.zip` file or the Installation DVD.

Decompress the `.zip` file.

- On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
- On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

If the DVD is not automatically mounted in Linux, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

- 3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the SMC Client.
- 4) Read the information on the **Introduction** page, then click **Next**.



Tip

Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

- 5) Select **I accept the terms of the License Agreement**, then click **Next**.

- 6) (Optional) Select where to install the SMC, then click **Next**.

The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.



Note

If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

- 7) (Linux only) Read the instructions about the hosts file, make any necessary configuration changes, then click **Next**.
- 8) Select where to create shortcuts, then click **Next**.
These shortcuts can be used to manually start components and to run some maintenance tasks.
- 9) Select **Demo Mode** as the installation type, then click **Next**.
- 10) Select the **Standard** demo backup to simulate a standard preconfigured environment, then click **Next**.
You can also use the **Select your own backup file** option to create the simulation based on your environment.
- 11) Read the description of the Demo Mode installation, then click **Next**.
- 12) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.
- 13) When the installation has completed, click **Done**.

Result

The SMC Client starts automatically, and the simulated environment is now ready for testing.

Related tasks

[Log on to the SMC on page 55](#)

Install the SMC in Linux from the command line

In Linux, you can install the Security Management Center on the command line.

Before you begin

Check the installation package integrity using the file checksums.



Important

You need a graphical environment to use the SMC Client. It cannot be run on the command line. Only the SMC server components can be run in a command line-only environment.

Related tasks

[Check file integrity](#) on page 27

Start the installation on the command line

Start the command line installer to install SMC components from the command line.

Steps

- 1) Log on to the operating system as the root user.
- 2) Start the Installation Wizard from a `.zip` file or the Installation DVD.
Decompress the `.zip` file.
If the DVD is not automatically mounted, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

The path to the installer is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`. Run the script with the `- nodisplay` parameter.
When using the installer, enter `back` to return to the previous step or `quit` to cancel the installation.
- 3) Select the language for the installation.
To use the default option, press **Enter**. You can also select another option, then press **Enter**.
- 4) Read the information in the introduction, then press **Enter**.
- 5) Press **Enter** to scroll through the license agreement, then enter `y` to accept the license agreement.
- 6) Specify the installation directory.
To use the default option, press **Enter**. You can also enter a different directory, then press **Enter**.

- 7) Read the instructions about the hosts file, make any necessary configuration changes, then press **Enter**.
- 8) Create links to the most commonly used command-line tools.
To use the default option, press **Enter**. You can also select another option, then press **Enter**.
- 9) Select the type of installation.
 - **Typical** — Installs a Management Server, a Log Server, and the SMC Client.
 - **SMC Client Only** — Use to install additional SMC Clients on administrators' workstations.
 - **Demo Mode** — For more information, see the section about installing in Demo mode.
 - **Custom** — Select individual components to install. Use this option to:
 - Install individual SMC components. For example, you can install the Management Server on one computer, and the Log Server on another.
 - Install the Web Access Server.
 - Install only a Management Server if you want to install an additional Management Server for high availability.
- 10) If you selected a custom installation, enter a comma-separated list of numbers that represent the components you want to install, then press **Enter**.
 - Enter the number of a *selected* component to *deselect* the component.
 - Enter the number of a component that is *not* selected to *select* the component.
 - By default, the Management Server, Log Server, and SMC Client are selected.For example, to install only the Web Access Server, enter `1,2,3,4`, then press **Enter**.
- 11) Review the component selection, then press **Enter**.

Install a Management Server on the command line

Configure the Management Server settings in a command line installation.

Steps

- 1) Specify the IP address for the server.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.
If IP address binding is used, the server's license must be generated with this IP address as the binding.
- 2) Specify the IP address for the Log Server to which the server sends its log data.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.
- 3) To install as an additional Management Server for high availability, enter `Y`.
To install as a standalone Management Server or as the primary Management Server in a high-availability environment, enter `N`.

- 4) To enable OWASP encoding for the SMC API, enter **Y**. Otherwise, enter **N**.



Note

When you enable this option, some strings in data returned by the SMC API, such as special characters inside JSON payloads, are also encoded. We recommend enabling this option only if you use the SMC API in a web browser.

- 5) To enable and configure Web Access, enter **Y**. Otherwise, enter **N**.

When enabled, administrators can access the SMC in a web browser. You can run the SMC Client in a web browser instead of installing the SMC Client locally.

On Linux platforms, `xvfb-run` must be installed under `/usr/bin`. You can specify another path in the Management Server properties after the installation has completed.

- 6) If you enabled Web Access, configure the settings.

Administrators must use an HTTPS connection to access and use the SMC Client.

- a) Enter the TCP port number that the service listens to.

By default, port 8085 is used when Web Access is enabled on the Management Server and port 8083 when enabled on the Web Access Server.



Note

Make sure that the listening port is not in use on the server.

- b) Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names.

- c) Enter the distinguished name in LDAP string format for the certificate used to secure the HTTPS connection.

Example: `dn=smc,dc=demo,dc=com`

- d) Select the algorithm and key length for the certificate used to secure the HTTPS connection.

To use the default option, press **Enter**. You can also select another option, then press **Enter**.

- e) Select the signer for the certificate used to secure the HTTPS connection.

You can use the Internal Certificate Authority or the certificate can be self-signed. To use the default option, press **Enter**. You can also select another option, then press **Enter**.

- 7) To enable 256-bit security strength for communication between the Management Server and Security Engines, enter **Y**. Otherwise, enter **N**.

- 8) (256-Bit Security Strength only) If you are shown a compatibility warning, press **Enter** to continue, or type `back` to restart the Management Server configuration and disable 256-bit security strength.

- 9) To enable FIPS restrictions, enter **Y**. Otherwise, enter **N**.



Note

This option only is for environments that are required to follow FIPS standards. Do not enable this option unless you have a specific reason to do so.

- 10) To install the server as a service, enter **Y**. Otherwise, enter **N**.
When installed as a service, the server starts automatically.
- 11) To create a superuser account, enter a user name, then enter and confirm the password.

Related information

Default communication ports on page 239

Install a Log Server on the command line

Configure the Log Server settings in a command line installation.

Steps

- 1) Specify the IP address for the server.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.
If IP address binding is used, the server's license must be generated with this IP address as the binding.
- 2) Specify the IP address of the Management Server that controls this server.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**. If there are multiple Management Servers, enter the IP addresses as a comma-separated list.
- 3) Specify the port on which the Log Server receives data.
To use the default option, press **Enter**. You can also enter a different port, then press **Enter**.
- 4) To install the server as a service, enter **Y**. Otherwise, enter **N**.
When installed as a service, the server starts automatically.
- 5) Specify the directory for storing log files.
To use the default option, press **Enter**. You can also enter a different directory, then press **Enter**.

Install a Web Access Server on the command line

Configure the Web Access Server settings in a command line installation.

Steps

- 1) Specify the IP address for the server.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.
If IP address binding is used, the server's license must be generated with this IP address as the binding.

- 2) Specify the IP address of the Management Server that controls this server.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**. If there are multiple Management Servers, enter the IP addresses as a comma-separated list.
- 3) Specify the IP address for the Log Server to which the server sends its log data.
To use the default option, press **Enter**. You can also enter a different IP address, then press **Enter**.
- 4) To install the server as a service, enter **Y**. Otherwise, enter **N**.
When installed as a service, the server starts automatically.

Finish the installation on the command line

Review the configuration options that you set in the command line installer, then finish the installation.



Important

This is the last chance to cancel the installation or make changes. Enter `back` to adjust your selections, or enter `quit` to cancel the installation.

Steps

- 1) Check that the information in the **Pre-Installation Summary** is correct, then press **Enter**.

Result

The components that you selected are installed.

When the installation has completed, the unique installation identifier (UIID) for the SMC is shown. If you plan to use UIID-bound licenses for SMC servers, make a note of the UIID for the SMC. You will need the UIID to generate licenses.

Install the SMC Appliance

The SMC Appliance ships with the Management Server and a Log Server pre-installed on it. Starting the SMC Appliance initiates an installation wizard.

Before you begin

Prepare the appliance for installation:

- Determine the appliance networking information:
 - IPv4 network addresses
 - IPv4 network masks
 - (Optional) Default gateway address
 - (Optional) DNS server addresses
- Mount the appliance in a rack.
- Connect the network and console cables.
- Access the appliance through a KVM or the integrated Dell Remote Access Controller (iDRAC) port.

See the *Forcepoint Hardware Guide* for complete details.

Steps

- 1) Turn on the SMC Appliance.
- 2) Accept the EULA.
- 3) Select **Begin**, then press **Enter**.
- 4) Select the keyboard layout for accessing the SMC Appliance on the command line.
- 5) Enter the administrator account name and password.



Note

The administrator account and password are used for command line access to the SMC Appliance and for access to the SMC Client. The administrator account is created with unrestricted permissions (superuser).

- a) Enter the account name.
This field is case sensitive and limited to eight characters.
- b) Enter the password.
The password is case sensitive. The password must be at least ten characters long and contain at least one number.
- c) Enter the password again.

- 6) (Optional) Configure a bootloader password.
If you configure a bootloader password, you must enter the bootloader password to edit the options that appear in the bootloader menu of the SMC Appliance.
 - a) Press the space bar to configure a bootloader password.
 - b) Enter the password.
 - c) Enter the password again.

- 7) Make your security selections.

- a) To run the appliance in FIPS mode, select **Enable FIPS configuration restrictions**.

**Note**

This option only is for environments that are required to follow FIPS standards. Do not enable this option unless you have a specific reason to do so.

- b) To use 256-bit security strength, select **Enable 256-bit security strength**.

This option is enabled by default.

**Note**

The security strength is for the connection to the Security Engines. The engines must also use 256-bit security strength.

- c) To use external certificate management for internal communication between system components, select **Use External Certificate Authority**.

When enabled, the appliance uses certificates issued by an external CA instead of certificates generated by the internal CA on the Management Server for internal TLS communication between system components.

**Note**

Using this option requires additional configuration after installation. For more information, see *Installing the SMC with external certificate management*.

- d) To encrypt the disk, select **Enable disk encryption**.
- e) To use a restricted command line shell that prevents administrators from running arbitrary commands, select **Enable restricted shell**.
The restricted shell has a limited set of commands that include patching utilities, appliance maintenance, service handling, and other basic functionality. When the restricted shell is enabled, all administrator accounts that you create in the SMC automatically use the restricted shell.

- 8) To enable network interface configuration, select **Disabled**, then press **Enter**.

- 9) Complete the network interface configuration for the primary network interface for management.

- a) Select **Enable interface**.
- b) Select **Primary**.

- c) Complete the network configuration fields for the interface.
- 10) (Optional) Complete the network interface configuration for the secondary network interface for management.
- a) Select **Enable interface**.
 - b) Select **Secondary**.
 - c) Complete the network configuration fields for the interface.

11) Enter a host name for the Management Server.

12) (Optional) Enter one or more IPv4 or IPv6 addresses in the DNS server fields.

**Note**

CIDR notation is not allowed.

13) (Optional) If you do not want to use NTP, disable it in the NTP settings.

**Note**

NTP settings that you configure in the installation wizard are not visible in the SMC Client. Configuring NTP in the SMC Client overrides the NTP settings that you configure here.

14) Select the time zone.

15) Set the date and time.
You are prompted to review the configuration.

16) Select **Confirm**, then press **Enter**.

Result

When the installation is complete, select one of the following options:

- Reboot
- Shutdown.

Related tasks

[Contact the Management Server on the command line on page 197](#)

Related information

[Installing the SMC with external certificate management on page 289](#)

Start the SMC after installation

Proceed through the following sections to start the SMC for the first time.

Start the Management Server

If the Management Server does not start automatically, you must start it.

If the Management Server has been installed as a service, it starts automatically both after the installation and during the operating system boot process. In Windows, the Security Engine Management Server service is controlled in the **Services** window, under the **Administrative Tools** category of the Windows Control Panel.

Steps

- 1) Start the Management Server manually.
 - In Windows, use the shortcut icon or run the script `<installation directory>/bin/sgStartMgtSrv.bat`.
 - In Linux, run the script `<installation directory>/bin/sgStartMgtSrv.sh`.

Next steps

When the Management Server has successfully started, start the SMC Client.

Start the SMC Client


After you have started the Management Server, start the SMC Client.

Steps

- 1) If you installed the SMC Client locally on the workstation, do the following:
 - (Windows) Use the shortcut icon or run the script `<installation directory>/bin/sgClient.bat`.
 - (Linux) Run the script `<installation directory>/bin/sgClient.sh`. A graphical environment is needed.
- 2) If you enabled Web Access to run the SMC Client in a web browser, do the following:
 - a) In a web browser, browse to the URL of the server that you configured the Web Access feature on. The URL can be the IP address of the server or the host name that you defined in the properties of the server. Make sure that you include the port number at the end of the URL.
Example where Web Access is enabled on the default port 8085 on the Management Server:
`https://127.0.0.1:8085`
 - b) Enter your user name and password, then click **Log On**.

Log on to the SMC

The SMC Client connects to the Management Server and to Log Servers.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select the Management Server in one of the following ways.
 - Select an existing Management Server IP address or DNS name.
 - Click **Add Management Server**, then enter the IP address or DNS name of the Management Server.
In Demo mode, select 127.0.0.1.
- 2) Enter the user name and password for the Administrator you defined during the Management Server or SMC Appliance installation.
In Demo Mode, both the user name and password are "demo".



Note

In FIPS mode, previously used user names are not shown in the logon dialog box.

- 3) Click **Log On**.

Result

After you log on to the SMC Client, the SMC Client shows the date and time when you last logged on to the SMC Client, and the IP address from which you last logged on. If your administrator permissions have been changed since the last time you logged on, you are notified that your permissions have been changed.

Accept the Management Server certificate

As a precaution, to make sure that you are communicating with your Management Server, check the Certificate Authority fingerprint.

The certificate dialog box that contains the fingerprint is shown when the SMC Client contacts a Management Server for the first time. You can also manually view the fingerprint.

Steps

1) View the Management Server fingerprint.

- In Windows, use the shortcut icon (default: **Start > All Programs > Forcepoint > Show Fingerprint**) or run the script `<installation directory>/bin/sgShowFingerPrint.bat`.
- In Linux, run the script `<installation directory>/bin/sgShowFingerPrint.sh`.
- On the SMC Appliance, log on to the command line with your administrator credentials, then run the following command

```
sudo smca-system fingerprint
```

On restricted shell:

```
smcasystem fingerprint
```



Note

When external certificate management is used, the Management Server certificate fingerprint is shown on the client instead of the Certificate Authority certificate fingerprint. See Appendix F *Installing the SMC with external certificate management* for more details.

2) If the fingerprint matches, click **Accept**.

Result

The SMC Client starts.

Install licenses for SMC servers

Install the SMC server licenses that you downloaded while preparing for installation.

The SMC servers require licenses to become operational. If you do not have a valid Management Server license, a message appears when you log on. If the message appears after licensing, make sure that the license binding details are correct.

- If you use IP address binding, make sure that the IP addresses are correct and active on the server when the Management Server service starts.
- If you use licenses bound to the unique installation identifier (UIID) for the SMC, make sure that the UIID that you used to generate the license matches the UIID shown in the properties of the SMC server element.



Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the SMC Client, install licenses through the License Information message.

a) Click **Continue**.

b) Select the license files in the dialog box.

If the message is not shown, install the licenses as explained in the next step. Otherwise, check that the licenses were installed correctly.

- 2) If you are not prompted to install a Management Server license, install the license files for the other SMC servers.
 - a) Select  **Settings** > **Install Licenses**.
 - b) Select the license files and click **Install**.
- 3) To check that the licenses were installed correctly, select  **Engine Configuration**, then browse to **Administration** > **Licenses** > **All Licenses**.


Related tasks

Obtain license files on page 30

Bind Management Server POL-bound licenses to servers

You must bind Management Server POL-bound licenses for Log Servers to specific Server elements.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Administration**.
- 2) Browse to **Licenses** > **Servers**.
- 3) Right-click a Management Server POL-bound license, then select **Bind**.
- 4) In the **Select License Binding** dialog box, select the correct server from the list, then click **Select**.



Tip

If you bound the license to an incorrect element, right-click the license, select **Unbind**.



Note

The license is permanently bound to the Log Server element when the server is started for the first time. A permanently bound license cannot be rebound to a different Log Server element without relicensing or deleting the element that the license is bound to. Until you do that, the unbound license is shown as **Retained**.

Result

The license is now bound to the selected Log Server element.

Start SMC servers

If the Log Server or Web Access Server does not start automatically, you must manually start them.

If a server has been installed as a service, the server starts automatically during the operating system boot process. If the operating system is restarted and the servers do not yet have a license, you might need to start them manually.

Steps

- 1) Start the Log Server or the optional Web Access Server.
 - If you installed the server as a service in Windows, start or stop the server through the **Services** window.
 - You can also run a script from the `<installation directory>/bin/` directory in a console window.

| Server type | Windows script | Linux script |
|-------------------|---|--|
| Log Server | <code>sgStartLogSrv.bat</code> | <code>sgStartLogSrv.sh</code> |
| Web Access Server | <code>sgStartWebAccessServer.bat</code> | <code>sgStartWebAccessServer.sh</code> |

Read the console messages for information about the progress. Closing the console stops the service.

- 2) If the Log Server or Web Access Server does not start, troubleshoot and resolve issues that cause starting to fail.
 - Try starting the server by running scripts in a console window to see if an error is displayed on the console.
 - Check that licenses are correctly bound to components.
 - Make sure that the server has a valid certificate for secure system communications. If there are certificate-related problems or problems you are not able to identify, try regenerating the certificate.

Generate SMC server certificates

If necessary, you can manually certify an SMC server or generate an SMC server certificate.

To manually certify a server, run one of the following scripts from the `<installation directory>/bin/` directory in a console window.

| Server type | Windows script | Linux script |
|-------------------|---|--|
| Log Server | <code>sgCertifyLogSrv.bat</code> | <code>sgCertifyLogSrv.sh</code> |
| Web Access Server | <code>sgCertifyWebAccessServer.bat</code> | <code>sgCertifyWebAccessServer.sh</code> |

To generate a server certificate, follow these steps:

Steps

- 1) Enter the user name and password for the account you created during the Management Server installation. You can also use other accounts that have unrestricted permissions.
- 2) Click **Accept** to accept the certificate fingerprint of the Management Server's Certificate Authority. As a precaution, you can make sure that the communication really is with your Management Server.

- 3) In the **Server Selection** dialog box, identify the component that you want to certify.
 - If the server element that represents the component is listed, select it.
 - If **recommended** follows the name of a server element, the component ID of the server element matches the ID of the component that you are certifying. We recommend that you select that server element.

**CAUTION**

Selecting a server element that is not the recommended server element might cause serious problems. For example, the server's log data or the monitoring status of the server might be displayed incorrectly.

- If the correct server element is not listed, select **Create a New Log Server** or **Create a New Web Access Server**, then enter a name for the server.
- 4) Click **OK**.

Post-installation SMC configuration

After installation, you can configure settings for system communication and enable more features for the SMC.

- If NAT is applied to communications between any SMC components, configure NAT addresses for SMC components.
- You can install and configure additional Management Servers for high availability.

When you are finished configuring the SMC, you are ready to use the SMC Client to configure Engine, IPS, and Layer 2 Engine elements. The elements must be configured before installing the physical appliances.

Related concepts

[Configuring NAT addresses for SMC components on page 61](#)

[Alternative methods for accessing the SMC Client](#)

Related tasks

[Install additional Management Servers for high availability on page 64](#)

Configuring the SMC

Contents

- [Configuring NAT addresses for SMC components on page 61](#)
- [Install additional Management Servers for high availability on page 64](#)
- [Using the SMC Client in a web browser on page 67](#)
- [SMC Client downloads from the Management Server on page 69](#)

After initial installation is complete, configure the SMC to allow adding the other components for your system.

Configuring NAT addresses for SMC components

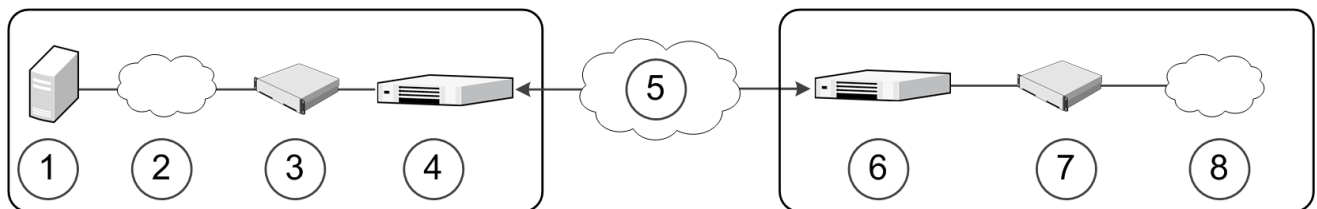
You must configure Locations and contact addresses when network address translation (NAT) is applied to the communications between any of the SMC components.

If there is NAT between communicating SMC components, the translated IP address might have to be defined for system communications.

You use Location elements to configure SMC components for NAT. There is a Default Location to which all elements belong if you do not assign them to a specific Location. If NAT is applied between two SMC components, you must separate them into different Locations and then add a contact address for the component to be contacted.

You can define a Default contact address for contacting an SMC component (defined in the **Properties** dialog box of the corresponding element). The component's Default contact address is used in communications when SMC components that belong to another Location contact the component and the component has no contact address defined for its Location.

Example scenario—using locations



| Component | Description |
|------------------------------|-----------------------|
| Headquarters Location | |
| 1 | Management/Log server |
| 2 | Internet |

| Component | Description |
|-------------------------------|-------------|
| 3 | IPS |
| 4 | Engine |
| Between locations | |
| 5 | Internet |
| Branch Office Location | |
| 6 | Engine |
| 7 | IPS |
| 8 | Internet |

In the example scenario above, the same Management Server and Log Server manage SMC components both at a company's headquarters and at the branch office.

NAT could typically be applied at the following points:

- The engine at the headquarters or an external router can provide the SMC servers external IP addresses on the Internet. The external addresses must be defined as contact addresses so that the SMC components at the branch offices can contact the servers across the Internet.
- The branch office engine or an external router can provide external addresses for the SMC components at the branch office. In this case, the external IP addresses must also be defined as contact addresses so that the Management Server can contact the components.

When contact addresses are needed, it might be enough to define a single new Location element, for example, for the branch office, and to group the SMC components at the branch office into the "Branch Office" Location. The same Location element could also be used to group SMC components at any other branch office when they connect to the SMC servers at the headquarters.

To be able to view logs, the administrators at the branch office must select the "Branch Office" Location in the SMC Client.

Configuration overview

- 1) Define Location elements.
- 2) Define contact addresses for the Management Servers and Log Servers.
- 3) Select the Location for your SMC Client.
- 4) Select the Locations for Security Engines when you create the engine elements.

Related information

[Default communication ports](#) on page 239

Add Location elements

Group the SMC components into **Location** elements based on which components are on the same side of a NAT device.

The elements that belong to the same **Location** element always use the primary IP address when contacting each other.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Administration**.
- 2) Expand the **Other Elements** branch.
- 3) Right-click **Locations** and select **New Location**.
- 4) In the **Name** field, enter a name.
- 5) Select elements from the **Resources** pane and click **Add**.
- 6) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- If your **Management Server** or **Log Server** needs a contact address, add SMC server contact addresses.
- Configure the **Engine**, **IPS**, and **Layer 2 Engine** elements in the SMC Client. You must configure the elements before configuring the Security Engine software.

Add SMC Server contact addresses

The Management Server and Log Server can have more than one contact address for each Location.

- If you have additional Management Servers or Log Servers, define two or more contact addresses for each Location. Multiple contact addresses are required so that remote components can connect to a Management Server or a Log Server even if one of the Management Servers or Log Servers fails.
- If you have configured Multi-Link, define two or more contact addresses per Location so that remote components can connect to the servers even if a NetLink goes down.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a server and select **Properties**.
- 2) From the **Location** drop-down menu, select the location to which the server belongs.

- 3) If necessary, edit the contact addresses.
 - A Default contact address is automatically entered based on the element properties.
 - If the server has multiple Default contact addresses, separate the addresses with commas.
 - If necessary, click **Exceptions** to define other contact addresses for specific Locations

**Note**

Elements that belong to the same Location element always use the primary IP address when contacting each other instead of any contact addresses. Elements that do not belong to a specific Location are considered to belong to the Default Location.

- 4) Click **OK**.

Set the SMC Client location

When there is a NAT device between the SMC Client and a Log Server, select the correct Location for your SMC Client. Make the selection in the status bar at the bottom of the SMC Client window to be able to view logs.

**Note**

You must select the SMC Client Location separately in each administrative Domain if there are multiple Domains in your environment.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, click the **Default Location** name in the status bar at the bottom of the window.
- 2) Select the Location that includes the IP address or network of the computer where you use the SMC Client.

Install additional Management Servers for high availability

You can optionally install one or more additional Management Servers for high availability.

**Note**

The SMC Appliance does not support high availability for the Management Server or the Log Server.

Additional Management Servers control the system if the active Management Server is damaged, loses power, or becomes otherwise unusable. Configuration data is automatically replicated between the Management Servers. Only one Management Server at a time can be used as an active Management Server to configure and manage the system.

To use additional Management Servers, you must have a special Management Server license that lists the IP addresses of all Management Servers within the same SMC.

**Note**

You must install the license in the SMC Client before installing the additional Management Servers. If you do not yet have the license, generate the license at the Forcepoint website after receiving the Proof-of-License, then install the license.

Steps

- 1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.
- 2) Start the Installation Wizard from a `.zip` file or the Installation DVD.
Decompress the `.zip` file.

- On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
- On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

If the DVD is not automatically mounted in Linux, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

- 3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the SMC Client.
- 4) Read the information on the **Introduction** page, then click **Next**.

**Tip**

Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.



- 5) Select **I accept the terms of the License Agreement**, then click **Next**.
- 6) (Optional) Select where to install the SMC, then click **Next**.
The default installation directory in Windows is `C:\Program Files\Forcepoint\SMC`. Click **Choose** to browse to a different installation folder.

**Note**

If you install the SMC in `C:\Program Files\Forcepoint\SMC`, the installation creates an extra `C:\ProgramData\Forcepoint\SMC` folder, which duplicates some of the folders in the installation directory and also contains some of the program data.

- 7) Select where to create shortcuts, then click **Next**.
These shortcuts can be used to manually start components and to run some maintenance tasks.
- 8) Select **Custom** as the installation type, then click **Next**.
- 9) Select **Management Server**, then click **Next**.

- 10) Configure the settings, then click **Next**.

| Option | Description |
|---|---|
| Select Management Server IP Address | Select the server's IP address from the drop-down list. If you use IP address binding, the server's license must be generated with this IP address as the binding. |
| Log Server IP Address | Enter the IP address of the Log Server to which this server sends its log data. |
| Advanced Management Server Options | Do not select this option. The options are inherited from the active Management Server. |
| Install as an Additional Management Server for High Availability | You must select this option. |
| Enable FIPS Configuration Restrictions | When selected, restrictions for a FIPS-compatible environment are enabled.  Note This option only is for environments that are required to follow FIPS standards. Do not enable this option unless you have a specific reason to do so. |
| Use External Certificate Authority | When selected, the SMC uses certificates issued by an external CA instead of certificates generated by the internal CA on the Management Server for internal TLS communication between system components.  Note Using this option requires additional configuration after installation. For more information, see <i>Installing the SMC with external certificate management</i> . |
| Install the Management Server as a Service | When selected, the server starts automatically. |

- 11) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.
- 12) When prompted during the installation, log on using an unrestricted administrator account. The Management Server Selection dialog opens.
- 13) When the Management Server Selection dialog opens, select the correct Management Server from the list, then click **OK**.
You can also select **Create a new Management Server**, then enter a name for the Management Server. The databases are synchronized.



Note

If the synchronization fails, run the `sgOnlineReplication` script on the additional Management Server when connectivity is restored.

Next steps

- If NAT is applied to communications between any SMC components, configure NAT addresses for SMC components.
- If there is a Engine or Layer 2 Engine between the first Management Server you installed and the additional Management Servers, add rules that allow the communications between the servers when you define your Engine or Layer 2 Engine Policy.

Related tasks

Install licenses for SMC servers on page 56

Install the SMC on page 38

Using the SMC Client in a web browser

To avoid installing the full Java-based SMC Client on each workstation that an administrator uses, you can run the SMC Client in a web browser.


You can enable the Web Access feature on the Management Server or Web Access Server. Administrators log on to the SMC Client on a web page, and the SMC Client runs as an HTML5 application in the web browser. The web browser is the only requirement on the workstation.


You can also connect to and manage multiple versions of the SMC. This removes the requirement to have the SMC and the locally-installed SMC Client be the same version.

You can configure Web Access in the properties of the Management Server or Web Access Server. You can also enable the Web Access feature during the installation of the Management Server.

Limitations and recommendations

- By default, the SMC allows a maximum of five sessions using Web Access at the same time. To change the maximum number of concurrent sessions, see Knowledge Base article [17248](#).
- Web browser support is limited to Google Chrome and Mozilla Firefox.
- It is not possible to log on using certificate-based authentication.
- Interacting with the local file system is limited. Each user has a folder located at `%installation%\data\%servertype%\webswing\users\admin%id%` where `%servertype%` is `datamgtserver` for the Management Server and `datawebserver` for the Web Access Server and `%id%` is the ID of the administrator in the database. Users can import or export elements to this folder, for example.
- When you copy text using Ctrl+C, you must manually allow the copy operation in the bottom-right corner of the screen.

 Copy to Clipboard (CTRL+C)

 Discard



Note

Using right-click actions to paste text from the system clipboard is not supported. You must use Ctrl+V to paste text into the SMC Client.

- Web Access can consume resources. Especially if many administrators will be using the feature, we recommend that you enable the feature on the Web Access Server.

- If the Management Server or Web Access Server is installed on a Linux platform, xvfb-run must be installed.
- If the Management Server and Web Access Server are installed on the same computer, we recommend that you do not enable Web Access on both servers.

Enable Web Access

You can enable and configure the feature in the properties of the Management Server or Web Access Server.



Note

To use Web Access for a Management Server or Web Access Server installed on a Linux platform, xvfb-run must be installed in /usr/bin.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Network Elements**.
- 2) Browse to **Servers**.
- 3) Right-click the Management Server or Web Access Server, then select **Properties**.
- 4) On the **Web Access** tab, select **Enable**.
- 5) Configure the settings, then click **OK**.


Management Server and Web Access Server Properties

| Option | Definition |
|---|--|
| Host Name (Optional) | Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names. |
| Port Number | <p>Enter the TCP port number that the service listens to.</p> <p>By default, port 8085 is used when Web Access is enabled on the Management Server and port 8083 when enabled on the Web Access Server.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>Make sure that the listening port is not in use on the server.</p> </div> |
| Listen Only on Address (Optional) | If the server has several addresses and you want to restrict access to one address, specify the IP address to use. |
| Session Timeout | Enter the timeout in seconds after which the session expires. While the session is still active, the administrator does not need to log on again if they close the web browser. |
| Server Credentials | Select the TLS Credentials element that is used for HTTPS connections. Click Select to select an element. |

| Option | Definition |
|---|--|
| Server TLS Cryptography Suite Set | Select the TLS Cryptography Suite Set element that defines the allowed algorithms for HTTPS connections. Click Select to select an element. |
| Use SSL for session ID (Optional) | Track sessions in your web application. Do not select this option if your network requires you to use cookies or URIs for session tracking. |

Start the SMC Client in a web browser

Administrators can log on to the SMC Client and perform their duties using a web browser.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In a web browser, browse to the URL of the server that you configured the Web Access feature on. The URL can be the IP address of the server or the host name that you defined in the properties of the server. Make sure that you include the port number at the end of the URL.
Example where Web Access is enabled on the default port 8085 on the Management Server:
`https://127.0.0.1:8085`
- 2) Enter your user name and password, then click **Log On**.
- 3) Use the SMC Client as you normally would.

SMC Client downloads from the Management Server

When the Management Server provides the SMC Client for download, administrators can download and install the SMC Client from the SMC Downloads page.


Enable and configure SMC Client downloads on the Management Server

To allow administrators to download and install the SMC Client from the SMC Downloads page, enable SMC Client downloads on the Management Server.

Steps

- 1) Select  **Network Elements**.

- 2) Browse to **Servers**.
- 3) Right-click the Management Server, then select **Properties**.
- 4) If it is not already selected, select **Enable** on the **Client Downloads** tab.
- 5) Select **Management Client Download**.
- 6) Configure the settings, then click **OK**.

| Management Server Properties | |
|---|---|
| Option | Definition |
| Host Name (Optional) | Enter the host name that the service uses. Leave the field blank to allow requests to any of the server's host names. |
| Port Number | <p>Enter the TCP port number that the service listens to.</p> <p>By default, port 8080 is used for new SMC installations, and port 8084 is used when you upgrade the SMC.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p> Note Make sure that the listening port is not in use on the server.</p> </div> |
| Listen Only on Address (Optional) | If the server has several addresses and you want to restrict access to one address, specify the IP address to use. |
| Server Credentials | Select the TLS Credentials element that is used for HTTPS connections. Click Select to select an element. |
| Generate Server Logs (Optional) | Select if you want to log all file load events for further analysis with external web statistics software. |

Download the SMC Client from the Management Server

Download and install the SMC Client from the SMC Downloads page.

Steps

- 1) In a web browser, browse to the URL of the Management Server.
The URL can be the IP address of the Management Server or the host name that you defined in the properties of the Management Server. Make sure that you include the port number at the end of the URL.

- 2) To download the SMC Client installation package, click **Download Management Client for <operating system>**.



Tip

The operating system is automatically detected. To download the SMC Client installation package for another operating system, click **Click here for other platforms**.

- 3) Install the SMC Client with administrator privileges.
- 4) Log on and use the SMC Client as you normally would.

Part III

Forcepoint Security Engine deployment

Contents

- [Configuring Forcepoint Security Engine with Layer 3 Interfaces on page 75](#)
- [Configuring Security Engine for the IPS role on page 125](#)
- [Configuring Security Engine for the Layer 2 Engine role on page 143](#)
- [Configuring Security Engines as Master Engines and Virtual Engines on page 159](#)
- [Configuring routing on page 179](#)
- [Initial configuration of Security Engine software on page 183](#)
- [Creating and installing policies on page 205](#)

Forcepoint Security Engine deployment consists of adding and configuring engine elements in the SMC, and configuring the Security Engine software on the engine.

Configuring Forcepoint Security Engine with Layer 3 Interfaces

Contents

- [Types of interfaces for Security Engines with Layer 3 Interfaces](#) on page 75
- [Interface numbering](#) on page 76
- [Install licenses for Security Engines](#) on page 77
- [Configuring Single Engines](#) on page 78
- [Configuring Engine Clusters](#) on page 105

Configuring engine elements in the SMC prepares the SMC to manage Security Engine with Layer 3 Interfaces.

Types of interfaces for Security Engines with Layer 3 Interfaces

You can configure several types of interfaces for Security Engines with Layer 3 Interfaces.

Types of interfaces for Security Engines with Layer 3 Interfaces

| Interface type | Purpose of interface | Limitations |
|------------------|--|--|
| Layer 3 physical | System communications and traffic inspection. | You cannot add both VLAN Interfaces and IP addresses to a Physical Interface. If an IP address is already configured for a Physical Interface, adding a VLAN Interface removes the IP address. If you plan to use VLAN Interfaces, configure the VLAN Interfaces first and then add IP addresses to the VLAN Interfaces. |
| Layer 2 physical | Traffic inspection. Layer 2 interfaces on Security Engines with Layer 3 Interfaces allow the engine to provide the same kind of traffic inspection that is available for Security Engine in the IPS and Layer 2 Engine roles. | You cannot add layer 2 physical interfaces of the Inline Layer 2 Engine type to Engine Clusters in Load Balancing mode. Only Standby mode is supported. You cannot add IP addresses to layer 2 physical interfaces on Security Engines with Layer 3 Interfaces. VLAN retagging is not supported on layer 2 physical interfaces of the inline IPS type. |

| Interface type | Purpose of interface | Limitations |
|-----------------------------------|---|---|
| VLAN | Divides a single physical interface into several virtual interfaces. | <ul style="list-style-type: none"> You cannot add VLAN interfaces on top of other VLAN Interfaces (nested VLANs). You cannot create valid VLAN Interfaces in a Virtual Engine if the Master Engine interface that hosts the Virtual Engine is a VLAN Interface. |
| Modem (Single Engines only) | Represents a mobile broadband modem connected to a USB port on a purpose-built Security Engine appliance. | <ul style="list-style-type: none"> A Modem Interface is only supported on Single Engines that run on specific Security Engine appliances. Modem Interfaces do not support VLAN tagging. |
| Tunnel | A logical interface that is used as an endpoint for tunnels in route-based VPNs. | <ul style="list-style-type: none"> Tunnel Interfaces can only have static IP addresses. Tunnel Interfaces do not support VLAN tagging. |
| VPN Broker | A specialized interface for use with the VPN Broker. For more information about VPN Broker, see the <i>Forcepoint Security Engine Manager and VPN Broker Product Guide</i> . | This type of interface is only supported for use with the VPN Broker. |
| Wireless (Single Engines only) | Represents a wireless network interface card of a purpose-built Security Engine appliance. | A Wireless Interface is only supported on Single Engines that run on specific Security Engine appliances that have a wireless network interface card. |
| Switch (Single Engines only) | Represents the switch functionality on a purpose-built Security Engine appliance. | <ul style="list-style-type: none"> The switch functionality is only supported on Single Engines that run on specific Security Engine appliances that have an integrated switch. The ports in the integrated switch do not support VLAN tagging or PPPoE. You cannot use ports on the integrated switch as the control interface. |

Interface numbering

The interfaces have their own numbering in the SMC called the interface ID. The interface IDs are mapped to the corresponding network interfaces on the Security Engine when you configure the Forcepoint Network Security Platform software.

Interface numbering for Security Engines

| Interface type | Interface numbering in the SMC |
|---|---|
| Layer 3 physical (Security Engine with layer 3 interfaces) | Each physical interface has a unique interface ID number. |

| Interface type | Interface numbering in the SMC |
|---|--|
| Layer 2 physical (Security Engine with layer 3 interfaces) | |
| Physical (IPS and Layer 2 Engine roles) | |
| VLAN | Each VLAN interface has a VLAN number. The defined VLAN interfaces are displayed, for example, as "5.202" for network interface 5 with VLAN 202. |
| Wireless | The wireless interface has a unique interface ID number. An SSID (service set identifier) interface represents an 802.11 wireless LAN. You can add several SSID interfaces to the wireless interface. |
| Modem | Modem Interfaces are identified with modem numbers. The modem number is mapped to the modem's IMEI (international mobile equipment identity) number. Each modem is assigned a unique ID when you connect the modem to the engine. You can change the mapping between the modem's IMEI number and the modem ID through the engine command line, if necessary. |
| Tunnel | Tunnel interfaces are numbered with tunnel interface ID numbers. The mapping of Tunnel Interfaces to physical network interfaces on the engine is done automatically by the engine operating system based on the routing configuration. |
| Switch | Switches are identified with switch IDs. Integrated switches have predefined switch IDs. You can add port group interfaces to switches. Port group interfaces are identified by port group IDs. The defined switches and port group interfaces are displayed, for example, as 0.1 for switch ID 0 with port group 1. |


Install licenses for Security Engines


Install the Security Engine licenses that you downloaded while preparing for installation.


Before you begin

The license files must be available to the computer that you use to run the SMC Client.

You can install all licenses at the same time even though you have not yet created all elements that the licenses are bound to.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select  **Settings** > **Install Licenses**.
- 2) Select one or more license files to install in the dialog box that opens and click **Install**.

- 3) To check that the licenses were installed correctly, select  **Administration**, then browse to **Licenses > All Licenses**.

One license is shown for each Security Engine node. You must bind POL-bound licenses manually to the correct Security Engine nodes after you have configured the Security Engine elements. POS-bound licenses are automatically bound to the Security Engine nodes when you install a policy on the Security Engine after the Security Engine makes initial contact with the Management Server.

Next steps

Define the engine elements.

Related concepts

[Types of licenses for SMC servers and Security Engines](#) on page 28

[Configuring Single Engines](#) on page 78

[Configuring Engine Clusters](#) on page 105

Configuring Single Engines

After you have the SMC installed and running, you can configure the Single Engine elements.

Little configuration is done directly on the engines. Most of the configuration is done using the SMC Client. The engines cannot be successfully installed before defining them in the SMC Client.

The tasks you must complete are as follows:

- 1) Add Single Engine elements.
- 2) Add interfaces and define their properties.
- 3) (Optional) Select system communication roles for the interfaces.
- 4) Bind Management Server POL-bound licenses to specific Single Engine elements.

Add Single Engine elements



To add a single-node engine to the SMC, add a Single Engine element that stores the configuration information related to the engine.



Note

You can also create several Single Engine elements at the same time using the [Create Multiple Single Engines](#) wizard. For more information about creating several Single Engine elements at the same time, see the *Forcepoint Network Security Platform Product Guide*.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click **Engines**, then select **New > Engine > Single Engine**.
- 3) In the **Name** field, enter a unique name.
- 4) From the **Log Server** drop-down list, select the Log Server for storing logs.
- 5) (Optional) In the **DNS IP Addresses** list, add one or more IP addresses.
The Security Engine uses the DNS servers at these IP addresses to resolve malware signature mirrors, domain names, and web filtering categorization services. There are two ways to define IP addresses:
 - To enter an IP address, select **Add > IP Address**, then enter the IP address.
 - To use an element that represents an IP address, select **Add > Network Element**, then select a Host or External DNS Server element.
- 6) (Optional) From the **Location** drop-down list, select the Location to which the Security Engine belongs.
- 7) (Optional) If you have a Security Engine appliance, copy and paste the proof-of-serial (POS) code delivered with the appliance to the **Proof-of-Serial** field.
Using the POS code allows you to configure the Single Engine using plug and play configuration.
- 8) Click  **Save**.
Do not close the Engine Editor.

Next steps

Add the interfaces.

Related tasks

[Prepare for plug-and-play configuration on page 184](#)

Add layer 3 interfaces to Single Engines

Layer 3 interfaces are used in system communications and in traffic inspection on Single Engines.

Add layer 3 physical interfaces to Single Engines

To route traffic through the engine, you must define at least two layer 3 physical interfaces.




Note


Only the interface that is used for communications between the Management Server and the Engine is required when you install the Single Engine. Although you can configure more interfaces at any time, it is recommended to add more interfaces right away.

There are three types of layer 3 physical interfaces:

- An interface that corresponds to a single network interface on the engine. In the SMC Client, the interface type is **None**.
- An *aggregated link in high availability mode* represents two interfaces on the engine. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the first interface fails. Connect the first interface in the link to one external switch and the second interface to another external switch.
- An *aggregated link in load balancing mode* represents two or more interfaces (up to eight interfaces) on the engine. All interfaces in the aggregated link are actively used and connections are automatically balanced between the interfaces.
Link aggregation in load-balancing mode is implemented based on the IEEE 802.3ad Link Aggregation standard. Connect all interfaces to a single external switch. Make sure that the switch supports the Link Aggregation Control Protocol (LACP) and that LACP is configured on the switch.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Select **Add > Layer 3 Physical Interface**.
- 3) From the **Interface ID** drop-down list, select an ID number.
This ID maps to a network interface during the initial configuration of the engine.
- 4) From the **Type** drop-down list, select the interface type.
- 5) If the type is aggregated link, select one or more other interfaces that belong to the aggregated link.
 - For an aggregated link in high availability mode, select an interface ID from the **Second Interface ID** drop-down list.
 - For an aggregated link in load balancing mode, click **Add** to add one or more interface IDs to the **Additional Interface(s)** list.
- 6) Click **OK**.

- 7) Click  **Save**.
Do not close the Engine Editor.

Result

The layer 3 physical interface is added to the interface list.

Next steps

Add VLAN interfaces or IP addresses to the layer 3 physical interface.

Related tasks


[Add VLAN interfaces to layer 3 physical interfaces of Single Engines on page 81](#)

[Add IP addresses to Single Engine interfaces on page 87](#)

Add VLAN interfaces to layer 3 physical interfaces of Single Engines

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANs to each physical interface.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface and select **New > VLAN Interface**.
- 3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).



Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

- 4) Click **OK**.
The specified VLAN ID is added to the physical interface.
- 5) Click  **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Next steps

Continue the configuration in one of the following ways:

- Add IP addresses to the VLAN interfaces.
- Add other types of interfaces.

Related tasks

[Add IP addresses to Single Engine interfaces](#) on page 87

Add wireless interfaces to Single Engines

You can add one wireless interface to a Single Engine.

Wireless interfaces are only supported on specific Security Engine appliances that have an integrated wireless network interface card.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click the empty space and select **New > Wireless Interface**.
- 3) From the **Interface ID** drop-down list, select the interface ID number.
This ID number maps to the wireless port during the initial configuration of the engine.
- 4) In the **Country** field, enter or select the country where the engine is used as a wireless access point.
- 5) From the **Band** drop-down list, select the band for the wireless interface access point.

- 6) From the **Wireless Mode** drop-down list, select the mode for transmitting the wireless traffic according to the capabilities of the connecting clients.

The wireless mode options that you can select depend on the band.

| Band | Wireless mode |
|---------|---------------|
| 2.4 GHz | 802.11b |
| | 802.11bg |
| | 802.11g |
| | 802.11n |
| | 802.11bgn |
| 5 GHz | 802.11a |
| | 802.11an |
| | 802.11n |
| | 802.11ac |
| | 802.11acn |
| | 802.11ax |



Note

Some wireless clients do not support the 802.11n, 802.11ac, 802.11acn, and 802.11ax wireless modes with the WEP security mode.

- 7) From the **Channel** drop-down list, select the channel for transmitting the wireless traffic. If there are other wireless access points nearby, use channels that are as far apart as possible to avoid interference. Security Management Center might sometimes select another channel to use the best frequency available. If you select **Automatic**, the best channel is automatically selected.
- 8) (Optional) From the **Width** drop-down list, select the width of the channel. This option is only available if the Wireless Mode is one of the following: 802.11n, 802.11bgn, 802.11an, 802.11n, 802.11ac, 802.11acn or 802.11ax.
- 9) (Optional) From the **Transmit Power** drop-down list, select the maximum power of the signal for transmitting the wireless traffic.
- The power options are shown as milliwatts (mW) and as the power ratio in decibels of the measured power referenced to 1 milliwatt (dBm).
 - The values available depend on the regulatory limits for the selected country and the channel for the wireless interface.
 - If you are not sure what value to use, leave the default value selected.
- 10) Click **OK**.
The wireless interface is added to the interface list.
- 11) Click **Save**.
Do not close the Engine Editor.


Next steps

Add SSID interfaces to the wireless interface.

Add SSID interfaces to Single Engines

A service set identifier (SSID) interface represents an 802.11 wireless LAN.

You can add several **SSID Interfaces** to the **Wireless Interface**.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.


- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click the wireless interface and select **New SSID Interface**.
- 3) In the **Wireless Network Name (SSID)** field, enter the wireless network name.
It identifies the network to the end users.
- 4) From the **Wireless SSID Broadcast** drop-down list, select one of the following options:
 - **Enabled** — The wireless network name is broadcast to anyone in range.
 - **Disabled** — Users must type the name to connect.
- 5) From the **MAC Address Type** drop-down list, select one of the following options:
 - **Hardware** — The first SSID Interface that you define is automatically assigned the MAC address of the wireless card.
 - **Custom** — A custom MAC address.
- 6) (Custom MAC address only) In the **MAC Address** field, enter a MAC address.
- 7) Click the **Security** tab.
- 8) From the **Security Mode** drop-down list, select the security mode.



Tip

When you select the security mode, the options particular for that mode are enabled. We recommend using one of the WPA security modes.

- 9) If you selected **WEP Open System** or **WEP Shared Key**, configure these options.
 - a) From the **Key Length** drop-down list, select the key length.
 - b) From the **Default Key** drop-down list, select which key is used by default.
 - c) Enter 1–4 encryption keys.

- 10) If you selected **WPA Personal**, configure these options.
 - a) From the **WPA Mode** drop-down list, select the WPA mode.
 - b) In the **Pre-Shared Key** field, enter a pre-shared key of 8 to 64 ASCII characters.
- 11) If you selected **WPA Enterprise**, configure these options.
 - a) From the **WPA Mode** drop-down list, select the WPA mode.
 - b) Next to the **Authentication Method** field, click **Select**.
 - c) Select the RADIUS authentication method for authenticating users and click **Select**.
- 12) Click **OK**.
- 13) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add IP addresses to the SSID Interfaces.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.

Related tasks

[Add IP addresses to Single Engine interfaces](#) on page 87

[Select system communication roles for Single Engine interfaces](#) on page 101

[Bind engine licenses to Single Engine elements](#) on page 102

Add Switches to Single Engines

A software-based switch represents the switch functionality on purpose-built Forcepoint Network Security Platform appliances. Integrated switches eliminate the need for an external switch device and reduce costs and clutter.

The switch functionality is only supported on specific Forcepoint Network Security Platform appliances models.

- On Forcepoint Network Security Platform appliances that support software integrated switches, you can configure one or more integrated switches, and one port group interface on each integrated switch.


You can only use the integrated switch if the appliance has been configured as a Single Engine.



Note

The ports in the integrated switch do not support VLAN tagging or PPPoE. You cannot use ports on the integrated switch as the control interface.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click the empty space and select **New > Switch**.
- 3) From the **Switch ID** drop-down list, select the ID according to your switch type.
- 4) From the **Switch Type** drop-down list, select the adjustable type of your Security Engine switch.
- 5) Click **OK**.
- 6) Click  **Save**.
Do not close the Engine Editor.

Next steps

Add port group interfaces to the switch.

Add Port Group Interfaces to Single Engines

Port groups simplify port and network segment configuration. Traffic inside a port group is not inspected. The traffic between port groups is inspected by the engine in the same way as other traffic.

Before you begin

You must add the integrated switch before you can add port group interfaces.

Depending on the Forcepoint Network Security Platform appliance model, you can define one or more port group interfaces and add different types of interfaces to the port group:

- On Forcepoint Network Security Platform appliances that support software integrated switches, you can define one port group interface on each integrated switch.
You can add physical and SSID interfaces to the port group interface. You must first add the physical and SSID interfaces in the engine editor without any IP address configuration, before adding these interfaces to the port group.

For more information about the type of integrated switch that your appliance has, see the model-specific *Forcepoint Network Security Platform Hardware Guide* for your Forcepoint Network Security Platform appliance.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click the switch and select **New Port Group Interface**.
- 3) Define the port group interface properties.

4) Click **OK**.

The port group interface is added to the interface list. The defined switches and port group interfaces are displayed, for example, as “0.1” for switch ID 0 with port group 1.

5) Click  **Save**.

Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add IP addresses to the port group interfaces.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.

Related tasks

[Select system communication roles for Single Engine interfaces on page 101](#)

[Bind engine licenses to Single Engine elements on page 102](#)

Add IP addresses to Single Engine interfaces

You can add one or more IP addresses to each interface on a Single Engine.


The number and types of IP addresses that you can add depend on the interface type.

IP addresses for each interface type

| Interface type | Static IPv4 addresses | Dynamic IPv4 Addresses | Static IPv6 Addresses | Dynamic IPv6 Addresses |
|---------------------------|-----------------------|------------------------|-----------------------|------------------------|
| Physical interface | One or more | One | One or more | One |
| Aggregated Link interface | One or more | None | One or more | None |
| VLAN interface | One or more | One | One or more | One |
| Port group interface | One or more | One | One or more | One |
| SSID interface | One | None | One | None |

Add static IPv4 addresses to Single Engine interfaces

Depending on the type of interface, you can add one or more static IPv4 addresses to Single Engine interfaces.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Right-click a physical interface, VLAN interface, SSID interface, or port group interface, then select **New > IPv4 Address**.
- 3) In the **IPv4 Address** field, enter the IPv4 address.
- 4) In the **Netmask** field, adjust the automatically added netmask if necessary. The Network Address and Broadcast IP address are updated accordingly.
- 5) If the interface is used for system communications and NAT is applied, add contact addresses.
 - a) If the default contact address is not dynamic, deselect **Dynamic** and enter the static contact address.
 - b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.
- 6) If you want to use Virtual Router Redundancy Protocol (VRRP), add a virtual router.



Note

One virtual router can be configured for each physical interface, VLAN interface, or port group interface. Although VRRP support is also available, for port group interfaces, it is not normally used.

- a) Click **VRRP Settings**.
 - b) Select **Enable VRRP**.
 - c) Fill in the **ID**, **Priority**, and **IPv4 Address** fields according to the configuration of the virtual router.
 - d) Click **OK**.
- 7) Click **OK**.
The IPv4 address is added to the interface.
- 8) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more IP addresses.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.


Related tasks

[Select system communication roles for Single Engine interfaces](#) on page 101

[Bind engine licenses to Single Engine elements](#) on page 102

Add static IPv6 addresses to Single Engine interfaces

Depending on the type of interface, you can add one or more static IPv6 addresses to Single Engine interfaces.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical, VLAN, SSID, or port group interface and select **New > IPv6 Address**.
- 3) In the **IPv6 Address** field, enter the IPv6 address.



Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 4) Enter the Prefix Length (0–128).
- 5) Click **OK**.
- 6) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more IP addresses.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.

Related tasks

Select system communication roles for [Single Engine interfaces](#) on page 101

Bind engine licenses to [Single Engine elements](#) on page 102

Add dynamic IPv4 addresses to Single Engine interfaces

You can configure dynamic IPv4 addresses for physical, VLAN, and port group interfaces on Single Engines.


**Note**

Dynamic IP addresses are not supported on Aggregated Link interfaces.

You can identify interfaces that have a dynamic IPv4 address using a DHCP Index. A modem interface always has a dynamic IP address.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Right-click a physical, VLAN, or port group interface, then select **New > IPv4 Address**.
- 3) Select **Dynamic** as the type of IP address.
- 4) From the **Dynamic Index** drop-down list, select a DHCP index.
The index is used for identification in other parts of the configuration (such as Engine Policies) to represent the possibly changing IP address.
- 5) If the interface is used for system communications and NAT is applied, add contact addresses.
 - a) If the default contact address is not dynamic, deselect **Dynamic**, then enter the static contact address.
 - b) If components from some locations must use a different IP address for contact, click **Exceptions**, then define the location-specific addresses.
- 6) If the interface's dynamic IP address is assigned through point-to-point protocol, configure the settings.
PPPoE can be used with physical, or VLAN interfaces.
 - a) Click **PPP Settings**.
 - b) From the **Mode** drop-down list, select **PPPoE**.
 - c) Fill in the **User Name**, **Password**, and (optional) **Service Name** fields according to the details provided by your service provider.
If you do not have these details, contact your service provider. By default, passwords and keys are not shown in plain text. To show the password or key, deselect the **Hide** option.

- d) Click **OK**.
- 7) Click **OK**.
The dynamic IPv4 address is added to the interface.
- 8) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more IP addresses.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.

Related tasks

[Select system communication roles for Single Engine interfaces](#) on page 101

[Bind engine licenses to Single Engine elements](#) on page 102

Add dynamic IPv6 addresses to Single Engine interfaces


You can add dynamic IPv6 addresses to physical interfaces, VLAN interfaces, and port group interfaces on Single Engines.




Note

Dynamic IP addresses are not supported on Aggregated Link interfaces.

You can identify interfaces that have a dynamic IPv6 address using a DHCP Index.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface and select **New > IPv6 Address**.
- 3) In the **IP Address Properties** dialog box, select **Dynamic**.
- 4) From the **Dynamic Index** drop-down list, select a DHCP index.
The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.

- 5) If the interface is used for system communications and NAT is applied, add contact addresses.
 - a) Enter the default contact address in one of the following ways:
 - In the **Default** field, enter the contact address.
 - Select **Dynamic** and define the translated IP address of this component.
 - b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.
- 6) (Optional) If you do not want a default route to be automatically created through the interface, deselect **Automatic Default Route**.
- 7) (Optional) If you want to use DHCPv6 to get the IPv6 address, select **Use DHCPv6 to get IPv6 Address**.
- 8) Click **OK**.
The IP address is added to the interface.
- 9) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add more IP addresses.
- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.


Related tasks

[Select system communication roles for Single Engine interfaces](#) on page 101


[Bind engine licenses to Single Engine elements](#) on page 102

Add modem interfaces to Single Engines

You can use mobile broadband modems with Single Engines to provide wireless links for outbound connections.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click the empty space, then select **New > Modem Interface**.
- 3) From the **Modem Type** drop-down list, select the type of mobile broadband modem that was delivered with your appliance.

- 4) From the **Modem Number** drop-down list, select the modem number that is mapped to the modem's IMEI (international mobile equipment identity) number.
- 5) From the **DHCP index** drop-down list, select the DHCP index number.
The DHCP index is a number for your own reference to identify the DHCP interface.
- 6) In the **PIN** field, enter the PIN code if it is needed for the modem's SIM card.
- 7) Fill in the **Access Point Name** field according to the instructions that you have received from your service provider.
- 8) (3G Modem only) In the **Phone Number** field, enter the modem's phone number if it differs from the default phone number.
- 9) (3G Modem only) Fill in the **Service Name** fields according to the instructions that you have received from your service provider.
- 10) (LTE Modem only) If the service provider requires authentication, select the authentication method from the **Auth Method** drop-down list according to the instructions that you have received from your service provider.
- 11) (3G Modem or when an authentication method is selected) Fill in the **Username** and **Password** fields according to the instructions that you have received from your service provider.
- 12) If necessary, define the contact address information.
If components from some Locations cannot use the Default contact address, click **Exceptions** to define Location-specific contact addresses.
- 13) Click **OK**.
The Modem Interface is added to the interface list.
- 14) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other types of interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.

Related tasks

[Select system communication roles for Single Engine interfaces](#) on page 101

[Bind engine licenses to Single Engine elements](#) on page 102


Add layer 2 interfaces to Single Engines


Layer 2 interfaces are used in traffic inspection on Single Engines.

Add logical interfaces to Single Engines

Logical Interface elements are used in the Layer 2 Interface Policy and the traffic inspection process to represent a network segment.

The SMC contains one default Logical Interface element. A logical interface can represent any number or combination of physical interfaces and VLAN interfaces. However, the same logical interface cannot be used to represent both inline IPS interfaces and inline Layer 2 Engine interfaces on the same Single Engine. The rules in the ready-made Layer 2 Interface Template policy match all logical interfaces.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Expand the **Other Elements** branch.
- 3) Right-click **Logical Interfaces** and select **New Logical Interface**.
- 4) In the **Name** field, enter a unique name.
- 5) (Optional) If you use VLAN tagging, select **View interface as one LAN**.
By default, the Single Engine treats a single connection as multiple connections when an external switch passes traffic between different VLANs and all traffic is mirrored to the Single Engine through a SPAN port.
- 6) Click **OK**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Related tasks

- [Add reset interfaces to Single Engines on page 95](#)
- [Add capture interfaces to Single Engines on page 95](#)
- [Add inline IPS interfaces to Single Engines on page 97](#)
- [Add inline Layer 2 Engine interfaces to Single Engines on page 99](#)

Add reset interfaces to Single Engines

Reset interfaces can deliver TCP resets and ICMP destination unreachable messages to interrupt communications picked up from capture interfaces when the communications trigger a response.


VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.


The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.



Important

An interface that is used only as a reset interface must not have an IP address.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Single Engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Layer 3 Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **None**.
- 6) Click **OK**.
- 7) Click  **Save**.
Do not close the Engine Editor.

Result

This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interfaces.

Next steps


Add capture interfaces.


Add capture interfaces to Single Engines

Capture interfaces monitor traffic that external devices have duplicated for inspection to the Single Engine.

You can have as many capture interfaces as there are available physical ports on the Single Engine (there are no license restrictions regarding this interface type).

External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to an external switch SPAN port or a network TAP to capture traffic.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Single Engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Layer 2 Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Capture Interface**.
- 6) (Optional) From the **Reset Interface** drop-down list, select a TCP reset interface for traffic picked up through this capture interface.
- 7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 8) If you want the Single Engine to inspect traffic from VLANs that are not included in the Single Engine's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the Single Engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 10) Click **OK**.
- 11) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLAN interfaces to the capture interface.
- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.

Related tasks

[Add VLAN interfaces to layer 2 interfaces of Single Engines](#) on page 100

[Select system communication roles for Single Engine interfaces](#) on page 101

[Bind engine licenses to Single Engine elements](#) on page 102


Add inline IPS interfaces to Single Engines


There are two physical interfaces in an inline IPS interface. The traffic is forwarded from one interface to the other.

The traffic that the Single Engine allows goes through the inline IPS interface as if it was going through a network cable. The Single Engine drops the traffic you want to stop.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the Layer 2 Interface Engine Policies and the traffic inspection process to represent one or more inline IPS interfaces.

Fail-open network cards have fixed pairs of ports. Make sure to map these ports correctly during the initial configuration of the engine. If you use the automatic USB memory stick configuration method for the engine's initial configuration, the ports are configured automatically.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Single Engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Layer 2 Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Inline IPS Interface**.
- 6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.
- 7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 8) If you want the Single Engine to inspect traffic from VLANs that are not included in the Single Engine's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the Single Engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 10) Click **OK**.
- 11) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Define how the Single Engine handles traffic when the traffic load is too high using the **Bypass Traffic on Overload** setting.
- Add VLAN interfaces to the inline IPS interface.
- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Single Engine elements.

Related tasks

[Bypass traffic on overload on Single Engines](#) on page 98

[Add VLAN interfaces to layer 2 interfaces of Single Engines](#) on page 100

[Select system communication roles for Single Engine interfaces](#) on page 101

[Bind engine licenses to Single Engine elements](#) on page 102

Bypass traffic on overload on Single Engines


You can configure the Single Engine to bypass traffic when the traffic load becomes too high.


By default, Single Engines inspect all connections. If the traffic load is too high for the Single Engine to inspect all connections, the Single Engine can dynamically reduce the number of inspected connections. This reduction can improve performance in evaluation environments, but some traffic might pass through without any access control or inspection.



CAUTION

Using bypass mode requires a fail-open network interface card. If the ports that represent the interfaces cannot fail open, policy installation fails on the engine. Bypass mode is not compatible with VLAN retagging. In network environments where VLAN retagging is used, normal mode is automatically enforced.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Single Engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, select **General > Layer 2 Settings**.
- 3) Select **Bypass Traffic on Overload**.
- 4) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to Single Engine elements.

Related tasks

Select system communication roles for [Single Engine interfaces](#) on page 101


Bind engine licenses to [Single Engine elements](#) on page 102

Add inline Layer 2 Engine interfaces to Single Engines


There are two physical interfaces in an inline Layer 2 Engine interface. The traffic is forwarded from one interface to the other.

The traffic that the Single Engine allows goes through the inline Layer 2 Engine interface as if it was going through a network cable. The Single Engine drops the traffic you want to stop. If the Single Engine is unable to process traffic, all traffic that goes through the inline Layer 2 Engine interface is blocked.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the Layer 2 Interface Engine Policies and the traffic inspection process to represent one or more inline Layer 2 Engine interfaces.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Single Engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Layer 2 Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Inline Layer 2 Engine Interface**.
- 6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.
- 7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 8) If you want the Single Engine to inspect traffic from VLANs that are not included in the Single Engine's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the Single Engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 10) Click **OK**.

- 11) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLAN interfaces to the inline Layer 2 Engine interface.
- Select system communication roles for interfaces.
- Bind engine licenses to Single Engine elements.

Related tasks

[Add VLAN interfaces to layer 2 interfaces of Single Engines](#) on page 100


[Select system communication roles for Single Engine interfaces](#) on page 101

[Bind engine licenses to Single Engine elements](#) on page 102

Add VLAN interfaces to layer 2 interfaces of Single Engines

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANS to each physical interface.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface and select **New > VLAN Interface**.
- 3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).



Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

- 4) Click **OK**.
The specified VLAN ID is added to the physical interface.
- 5) Click  **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Next steps

Continue the configuration in one of the following ways:

- Select system communication roles for interfaces.
- Bind engine licenses to Single Engine elements.

Related tasks

Select system communication roles for Single Engine interfaces on page 101

Bind engine licenses to Single Engine elements on page 102

Select system communication roles for Single Engine interfaces

Select which IP addresses are used for particular roles in system communications.

For example, you can select which IP addresses are used in communications between the Engine and the Management Server.

The interfaces you have defined are shown as a tree-table on the Interfaces tab. Global interface options have codes in the tree-table.

Interface option codes

| Code | Description |
|------|---|
| A | The interface that has the IP address used as the identity for authentication requests. |
| C | The interfaces that have the primary and backup control IP addresses. |
| O | The default IP address for outgoing connections. |



Note

You cannot use layer 2 physical interfaces on engines for system communications.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces > Interface Options**.
- 2) Select the interface options.
 - a) From the **Primary** drop-down list, select the primary control IP address that the Engine uses for communications with the Management Server.
 - b) (Optional, recommended) From the **Backup** drop-down list, select a backup control IP address that the Engine uses for communications with the Management Server if the primary control IP address fails.

- c) If the Engine's primary control IP address and backup control IP address are dynamic or if the Engine is in an environment where only the Engine can initiate connections to the Management Server, select **Node-initiated contact to Management Server**.
When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.
- d) From the **Identity for Authentication Requests** drop-down list, select the IP address that identifies the Engine to external authentication servers.

**Note**

This selection has no effect on routing.

- e) (Optional) From the **Source for Authentication Requests** drop-down list, select the IP address that identifies the engine when it sends an authentication request to an external authentication server over a VPN.

**Note**

This selection has no effect on routing.

- f) From the **Default IP Address for Outgoing Traffic** drop-down list, select the IP address that nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

- 3) Click **Save**, then close the Engine Editor.

Next steps

Bind engine licenses to the Single Engine elements.

Bind engine licenses to Single Engine elements

After you have configured the Single Engine elements, you must manually bind Management Server POL-bound licenses to specific Single Engine elements.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct Engine element when the engine is fully installed.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Administration**.
- 2) Browse to **Licenses > Engines** depending on the type of licenses you have.
All installed licenses appear in the right pane.

- 3) Right-click a Management Server POL-bound license and select **Bind**.
- 4) Select the node and click **Select**.
The license is now bound to the selected Engine element.

**Tip**

If you bound the license to an incorrect element, right-click the license and select **Unbind**.

**CAUTION**

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses can't be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Transfer the configuration to the engines.

Related concepts

[Options for initial configuration](#) on page 183

Configure Backup Unit for Single Engine

A backup unit provides hardware redundancy for a single engine. If the primary engine fails, the backup unit automatically takes over using the same configuration, IP addresses, and policies. Hence, ensuring continuous service even if the primary engine is offline.

Configuring Backup Unit for Single Engine instead of actual cluster in active-standby or active-active modes is a simpler high-availability mechanism and also supports normal Single Engine features like interfaces that get IP address dynamically. Backup Unit configuration for Single Engine does not need additional external IP addresses or other cluster specific configuration requirements.

The tasks you must complete are as follows:

- 1) Enable Backup Unit
- 2) Bind license to the Backup Unit
- 3) Switch Active Node

Enable Backup Unit

Use this task to configure a backup unit to ensure service continuity if the primary engine fails.

Steps

- 1) Select  **Engine Configuration**.

- 2) Browse to **Engine > Engines**.
- 3) Right-click an engine, then select **Edit <element type>**.
- 4) In the navigation pane on the left, browse to **Advanced Settings > High Availability**.
- 5) In the **Backup Unit** section, select the **Enable** checkbox.
- 6) Enter the Proof of Serial (POS) of the appliance in the **Proof of Serial for Pairing** field.
- 7) Click the **Save** button.

Bind license to the Backup Unit

You must manually bind a license to the Backup unit.



Note

Both the backup unit and the primary engine must have different licenses.

Steps

- 1) Select **Administration**.
- 2) Browse to **Licenses > Engines**.
- 3) All installed licenses appear in the right pane.
- 4) Right-click the Engine and select **Bind**. The **Select License Binding** dialog box opens.
- 5) Select the backup unit and click **Select**.

Switch Active Node

In a high availability setup you can switch between nodes to make one as primary engine and the other as the backup unit.

Steps

- 1) Select **Dashboard > Engines**.
- 2) Right-click the engine, then select **Commands > Switch Active Node**.
- 3) Click **Yes**.
The active node is switched shortly.

Configuring Engine Clusters

After you have the SMC installed and running, you can configure the Engine Cluster elements.

Little configuration is done directly on the engines. Most of the configuration is done using the SMC Client. The engines cannot be successfully installed before defining them in the SMC Client.

The tasks you must complete are as follows:

- 1) Add Engine Cluster elements.
- 2) Add the necessary number of nodes to the Engine Cluster.
- 3) Add interfaces and define their properties.
- 4) (Optional) Select system communication roles for the interfaces.
- 5) Bind Management Server POL-bound licenses to specific nodes in the Engine Cluster.

Operating modes for Engine Cluster interfaces

There are several operating modes for the physical interfaces of a Engine Cluster. Packet dispatch mode is recommended for new installations.

The other modes are provided for backward compatibility. See the *Forcepoint Network Security Platform Product Guide* for more information about the other operating modes.

In packet dispatch mode:

- There is only one contact MAC address for each physical interface. The dispatcher node controls this MAC address.
- The dispatcher node forwards the packets to the other nodes for processing. Any node in the cluster can process the traffic.
- The dispatcher node is chosen separately for each physical interface.



Note

Different nodes might be selected as dispatcher nodes for different physical interfaces.

The packet dispatcher for the physical interface changes automatically if the dispatcher goes offline. When the dispatcher changes:

- The packet dispatcher MAC address is moved to another engine node.
- The engine sends an ARP message to the external switch or router.
- The switch or router updates its address table.



Note

This process is a standard network addressing operation where the switch or router learns that the MAC address is located behind a different port.

- The switch or router forwards traffic destined to the physical interface to this new packet dispatcher.

Add Engine Cluster elements

To introduce a new Engine Cluster to the SMC, you must define a Engine Cluster element that stores the configuration information related to the Engine.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Engine Configuration**.
- 2) Right-click **Engines**, then select **New > Engine > Engine Cluster**.
- 3) In the **Name** field, enter a unique name.
- 4) From the **Log Server** drop-down list, select the Log Server for storing logs.
- 5) (Optional) In the **DNS IP Addresses** list, add one or more IP addresses.
The Security Engine uses the DNS servers at these IP addresses to resolve malware signature mirrors, domain names, and web filtering categorization services. There are two ways to define IP addresses:
 - To enter an IP address, select **Add > IP Address**, then enter the IP address.
 - To use an element that represents an IP address, select **Add > Network Element**, then select a Host or External DNS Server element.
- 6) (Optional) From the **Location** drop-down list, select the Location to which the Security Engine belongs.
- 7) Click **Save**.
Do not close the Engine Editor.


Add nodes to Engine Clusters

The Engine Cluster element has two nodes when the element is created.

Engine Clusters can have up to 16 nodes. Add all nodes you plan to install before you begin configuring the interfaces.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **General > Clustering**.
- 2) (Optional) In the **Name** field, change the name.
- 3) Click **OK**.
The node is added to the Engine Cluster.

- 4) Click  **Save**.
Do not close the Engine Editor.

Add layer 3 interfaces to Engine Clusters

Layer 3 interfaces are used in system communications and in traffic inspection on Engine Clusters.

Add layer 3 physical interfaces to Engine Clusters

To route traffic through the Engine Cluster, you must define at least two layer 3 physical interfaces.

We recommend defining at least two interfaces for the Engine Cluster:


- An interface used for communications between the Management Server and the Engine.
- An interface for the heartbeat communications between the cluster nodes. The heartbeat traffic is critical to the functioning of the cluster, so it is highly recommended to have a dedicated heartbeat interface.

Although you can configure more interfaces at any later time, it is simplest to add more interfaces right away. This action allows traffic to be routed through the Engine. You can use the Cluster installation worksheet to document the interfaces.

There are three types of layer 3 physical interfaces on Engine Clusters:

- An interface that corresponds to a single network interface on each node in the Engine Cluster. In the SMC Client, the interface type is **None**.
- An *aggregated link in high availability mode* represents two interfaces on each node. Only the first interface in the aggregated link is actively used. The second interface becomes active only if the first interface fails. Connect the first interface in the link to one external switch and the second interface to another external switch.
- An *aggregated link in load balancing mode* represents two or more interfaces (up to eight interfaces) on each node. All interfaces in the aggregated link are actively used and connections are automatically balanced between the interfaces.

Link aggregation in load-balancing mode is implemented based on the IEEE 802.3ad Link Aggregation standard. Connect all interfaces to a single external switch. Make sure that the switch supports the Link Aggregation Control Protocol (LACP) and that LACP is configured on the switch.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Select **Add > Layer 3 Physical Interface**.
- 3) From the **Interface ID** drop-down list, select an interface ID number.
This ID maps to a network interface during the initial configuration of the engine.
- 4) From the **Type** drop-down list, select the interface type.
- 5) If the type is **Aggregated Link**, select one or more other interfaces that belong to the aggregated link.

- For an aggregated link in high availability mode, select an interface ID from the **Second Interface ID** drop-down list.
 - For an aggregated link in load balancing mode, click **Add** to add one or more interface IDs to the **Additional Interface(s)** list.
- 6) Leave **Packet Dispatch** selected as the CVI Mode, then enter a MAC Address with an even number as the first octet.



Important


This MAC address must not belong to any actual network card on any of the nodes.

- Packet Dispatch is the primary clustering mode in new installations.
- Different CVI modes can be used for different interfaces of a Engine Cluster without limitations.



Note

All CVI addresses that are defined for the same physical interface must use the same unicast MAC address. The dispatcher nodes use the MAC address you define here. Other nodes use their network card's MAC address.

- 7) (Optional) In the **MTU** field, enter the MTU value if this link requires a lower MTU than the Ethernet-default 1500.
- 8) Click **OK**.
- 9) Click  **Save**.
Do not close the Engine Editor.

Result

The layer 3 physical interface is added to the interface list.

Next steps

Add VLAN interfaces or IP addresses to the layer 3 physical Interface.

Related tasks

[Add VLAN interfaces to layer 3 interfaces of Engine Clusters](#) on page 108

[Add IP addresses to Engine Cluster interfaces](#) on page 109

Add VLAN interfaces to layer 3 interfaces of Engine Clusters

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANs to each physical interface.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface and select **New > VLAN Interface**.
- 3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).



Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

- 4) Click **OK**.
The specified VLAN ID is added to the physical interface.
- 5) Click  **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Next steps

Continue the configuration in one of the following ways:

- Add IP addresses to the VLAN interfaces.
- Add other types of interfaces.

Add IP addresses to Engine Cluster interfaces

To route traffic through the engine, each Engine Cluster interface must have at least two IP addresses.

Engine Clusters can have two types of IP addresses.

Types of IP addresses for Engine Clusters

| Interface type | Description | When to use it |
|----------------------------------|---|--|
| Cluster Virtual IP address (CVI) | <p>An IP address that is used to handle traffic routed through the cluster for inspection. All nodes in a cluster share this IP address.</p> <p>Allows other devices to communicate with the Engine Cluster as a single entity.</p> | Define a CVI for the interface if traffic that the engine inspects is routed to or from the interface. |


| Interface type | Description | When to use it |
|---------------------------------|--|--|
| Node Dedicated IP address (NDI) | <p>An IP address that is used for traffic to or from an individual node in a cluster. Each node in the cluster has a specific IP address that is used as the NDI.</p> <p>Used for the heartbeat connections between the engines in a cluster, for control connections from the Management Server, and other traffic to or from individual nodes.</p> | <p>Define at least two NDIs: one for management connections and one for the heartbeat traffic between the nodes.</p> <p>We recommend that you define an NDI for each interface that has a CVI, if practical. Some features might not work reliably without an NDI.</p> |

You can define several CVIs and NDIs on the same physical interface or VLAN interface. A physical interface or a VLAN interface can have only a CVI or only an NDI.

IPv6 addresses are supported on Engine Clusters with dispatch clustering mode. IPv6 and IPv4 addresses can be used together on the same Engine Cluster.

Add IPv4 addresses to Engine Cluster interfaces

Add an IPv4 address to a Engine Cluster interface.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.



- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface or VLAN interface and select **New > IPv4 Address**.
- 3) Select the types of IP addresses that you want to add using the **Cluster Virtual IP Address** and **Node Dedicated IP Address** options.
By default, both are selected. If the interface does not receive or send traffic that the Engine examines, there is no need to define a Cluster Virtual IP address (CVI). We recommend adding a Node Dedicated IP address (NDI) for each network or subnetwork that is located behind the physical interface.
- 4) To add a CVI, enter the IP address in the **IPv4 Address** field in the **Cluster Virtual IP Address** section.



Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 5) If the CVI is used for system communications and NAT is applied, define a contact address for the CVI.
 - a) Enter the default contact address in one of the following ways:
 - In the **Default** field, enter the contact address.
 - Select **Dynamic** and define the translated IP address of this component.

- b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.
- 6) To add NDIs for the nodes, enter the IP address in the **IPv4 Address** field for each node in the **Node Dedicated IP Address** table.
- 
- Tip**
- To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.
- 7) If the NDIs are used for system communications and NAT is applied, define a contact address for the NDIs.
- a) Double-click the node's **Contact Address** cell.
- b) In the **Default** field, enter the contact address.
- c) (Optional) If components from some locations must use a different IP address for contact, click **Add** and define the location-specific addresses.
- d) Click **OK**.
- 8) (Optional) In the **Netmask** field, change the automatically added netmask if necessary.
- 9) Click **OK**.
The IPv4 addresses are added to the interface.
- 10) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other IP addresses.
- Select system communication roles for interfaces.
- Bind engine licenses to the Engine Cluster elements.


Related tasks

[Select system communication roles for Engine Cluster interfaces](#) on page 120

[Bind engine licenses to Engine Cluster elements](#) on page 122

Add IPv6 addresses to Engine Cluster interfaces

Add an IPv6 address for a Engine Cluster interface.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface or a VLAN interface and select **New > IPv6 Address**.
- 3) Select the types of IP addresses that you want to add using the **Cluster Virtual IP Address** and **Node Dedicated IP Address** options.
By default, both are selected.
 - If the interface does not receive or send traffic that the engine examines, there is no need to define a Cluster Virtual IP address.
 - We recommend that you add a Node Dedicated IP address for each (sub)network that is located behind the Physical Interface.
- 4) If you are adding a Cluster Virtual IP address, in the **IPv6 Address** field, enter the IP address that is used as the Cluster Virtual IP address.



Tip


To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 5) If you are adding a Node Dedicated IP address for the nodes, double-click the **IPv6 Address** cell for each node and enter the IP address.



Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 6) (Optional) In the **Prefix Length** field, change the automatically filled in prefix length (0-128).
- 7) Click **OK**.
- 8) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other IP addresses.
- Select system communication roles for interfaces.
- Bind engine licenses to the Engine Cluster elements.

Related tasks

Select system communication roles for [Engine Cluster interfaces](#) on page 120

Bind engine licenses to [Engine Cluster elements](#) on page 122


Add layer 2 interfaces to Engine Clusters


Layer 2 interfaces are used in traffic inspection on Engine Clusters.

Add logical interfaces to Engine Clusters

Logical Interface elements are used in the Layer 2 Interface Policy and the traffic inspection process to represent a network segment.

The SMC contains one default Logical Interface element. A logical interface can represent any number or combination of physical interfaces and VLAN interfaces. However, the same logical interface cannot be used to represent both inline IPS interfaces and inline Layer 2 Engine interfaces on the same Engine Cluster. The rules in the ready-made Layer 2 Interface Template policy match all logical interfaces.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Expand the **Other Elements** branch.
- 3) Right-click **Logical Interfaces** and select **New Logical Interface**.
- 4) In the **Name** field, enter a unique name.
- 5) (Optional) If you use VLAN tagging, select **View interface as one LAN**.
By default, the Engine Cluster treats a single connection as multiple connections when an external switch passes traffic between different VLANs and all traffic is mirrored to the Engine Cluster through a SPAN port.
- 6) Click **OK**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Related tasks

[Add reset interfaces to Engine Clusters](#) on page 114

[Add capture interfaces to Engine Clusters](#) on page 115

[Add inline IPS interfaces to Engine Clusters](#) on page 116

Add reset interfaces to Engine Clusters


Reset interfaces can deliver TCP resets and ICMP destination unreachable messages to interrupt communications picked up from capture interfaces when the communications trigger a response.


VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.

The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.

**Important**

An interface that is used only as a reset interface must not have an IP address.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Engine Cluster and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Layer 3 Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **None**.
- 6) Click **OK**.
- 7) Click  **Save**.
Do not close the Engine Editor.

Result

This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interfaces.

Next steps


Add capture interfaces.


Add capture interfaces to Engine Clusters

Capture interfaces monitor traffic that external devices have duplicated for inspection to the Engine Cluster.

You can have as many capture interfaces as there are available physical ports on the Engine Cluster (there are no license restrictions regarding this interface type).

External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to an external switch SPAN port or a network TAP to capture traffic.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Engine Cluster and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Layer 2 Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Capture Interface**.
- 6) (Optional) From the **Reset Interface** drop-down list, select a TCP reset interface for traffic picked up through this capture interface.
- 7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 8) If you want the Engine Cluster to inspect traffic from VLANs that are not included in the Engine Cluster's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the Engine Cluster to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 10) Click **OK**.
- 11) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLAN interfaces to the capture interface.
- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.

- Bind engine licenses to the Engine Cluster elements.

Related tasks

[Add VLAN interfaces to layer 2 interfaces of Engine Clusters](#) on page 119

[Select system communication roles for Engine Cluster interfaces](#) on page 120

[Bind engine licenses to Single Engine elements](#) on page 102


Add inline IPS interfaces to Engine Clusters

There are two physical interfaces in an inline IPS interface. The traffic is forwarded from one interface to the other.


The traffic that the Engine Cluster allows goes through the inline IPS interface as if it was going through a network cable. The Engine Cluster drops the traffic you want to stop.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the Layer 2 Interface Engine Policies and the traffic inspection process to represent one or more inline IPS interfaces.

Fail-open network cards have fixed pairs of ports. Make sure to map these ports correctly during the initial configuration of the engine. If you use the automatic USB memory stick configuration method for the engine's initial configuration, the ports are configured automatically.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Engine Cluster and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Layer 2 Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Inline IPS Interface**.
- 6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.
- 7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 8) If you want the Engine Cluster to inspect traffic from VLANs that are not included in the Engine Cluster's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the Engine Cluster to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 10) Click **OK**.

- 11) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Define how the Engine Cluster handles traffic when the traffic load is too high using the **Bypass Traffic on Overload** setting.
- Add VLAN interfaces to the inline IPS interface.
- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to the Engine Cluster elements.

Related tasks

[Bypass traffic on overload on Engine Clusters](#) on page 117

[Add VLAN interfaces to layer 2 interfaces of Engine Clusters](#) on page 119

[Select system communication roles for Engine Cluster interfaces](#) on page 120

[Bind engine licenses to Engine Cluster elements](#) on page 122

Bypass traffic on overload on Engine Clusters


You can configure the Engine Cluster to bypass traffic when the traffic load becomes too high.


By default, Engine Clusters inspect all connections. If the traffic load is too high for the Engine Cluster to inspect all connections, the Engine Cluster can dynamically reduce the number of inspected connections. This reduction can improve performance in evaluation environments, but some traffic might pass through without any access control or inspection.



CAUTION

Using bypass mode requires a fail-open network interface card. If the ports that represent the interfaces cannot fail open, policy installation fails on the engine. Bypass mode is not compatible with VLAN retagging. In network environments where VLAN retagging is used, normal mode is automatically enforced.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Engine Cluster and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, select **General > Layer 2 Settings**.
- 3) Select **Bypass Traffic on Overload**.
- 4) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add other types of layer 2 interfaces.
- Select system communication roles for interfaces.
- Bind engine licenses to Engine Cluster elements.

Related tasks

Select system communication roles for Engine Cluster interfaces on page 120

Bind engine licenses to Engine Cluster elements on page 122

Add inline Layer 2 Engine interfaces to Engine Clusters


There are two physical interfaces in an inline Layer 2 Engine interface. The traffic is forwarded from one interface to the other.

The traffic that the Engine Cluster allows goes through the inline Layer 2 Engine interface as if it was going through a network cable. The Engine Cluster drops the traffic you want to stop. If the Engine Cluster is unable to process traffic, all traffic that goes through the inline Layer 2 Engine interface is blocked.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the Layer 2 Interface Engine Policies and the traffic inspection process to represent one or more inline Layer 2 Engine interfaces.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Engine Cluster and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New > Layer 2 Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Inline Layer 2 Engine Interface**.
- 6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.
- 7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.

- 8) If you want the Engine Cluster to inspect traffic from VLANs that are not included in the Engine Cluster's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the Engine Cluster to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 10) Click **OK**.
- 11) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLAN interfaces to the inline Layer 2 Engine interface.
- Select system communication roles for interfaces.
- Bind engine licenses to Engine Cluster elements.

Related tasks

[Add VLAN interfaces to layer 2 interfaces of Engine Clusters](#) on page 119

[Select system communication roles for Engine Cluster interfaces](#) on page 120

[Bind engine licenses to Engine Cluster elements](#) on page 122

Add VLAN interfaces to layer 2 interfaces of Engine Clusters

VLANs divide a single physical network link into several virtual links.


Steps

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface and select **New > VLAN Interface**.
- 3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).



Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.

- 4) Click **OK**.
The specified VLAN ID is added to the physical interface.
- 5) Click  **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Next steps

Continue the configuration in one of the following ways:

- Select system communication roles for interfaces.
- Bind engine licenses to Engine Cluster elements.

Related tasks

[Select system communication roles for Engine Cluster interfaces](#) on page 120

[Bind engine licenses to Engine Cluster elements](#) on page 122

Select system communication roles for Engine Cluster interfaces


Select which IP addresses are used for particular roles in system communications.

For example, you can select which IP addresses are used in communications between the Engine Cluster and the Management Server.

The interfaces you have defined are shown as a tree-table on the Interfaces tab. Global interface options have codes in the tree-table.

Interface option codes

| Code | Description |
|------|---|
| A | The interface that has the IP address used as the identity for authentication requests. |
| C | The interfaces that have the primary and backup control IP addresses. |
| H | The primary and backup heartbeat Interfaces. |
| O | The default IP address for outgoing connections. |

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces > Interface Options**.
- 2) Select the interface options.
 - a) From the **Primary** control IP address drop-down list, select the primary control IP address that the Engine Cluster uses for communications with the Management Server.
 - b) (Optional, recommended) In the **Backup** control IP address drop-down list, select a backup control IP address that the Engine Cluster uses for communications with the Management Server if the primary control IP address fails.

- c) If the Engine Cluster's primary control IP address and backup control IP address are dynamic or if the Engine Cluster is in an environment where only the Engine Cluster can initiate connections to the Management Server, select **Node-initiated contact to Management Server**.
When this option is selected, the Engine Cluster opens a connection to the Management Server and maintains connectivity.

- d) From the **Primary** heartbeat drop-down list, select the primary interface for communications between the nodes.
We recommend using a physical interface, not a VLAN interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network (without other traffic) is recommended for security and reliability of heartbeat communication.



CAUTION

Primary and backup heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information.

- e) From the **Backup** heartbeat drop-down list, select the backup heartbeat interface that is used if the primary heartbeat interface is unavailable.
It is not mandatory to configure a backup heartbeat interface, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic is disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well.
- f) From the **Identity for Authentication Requests** drop-down list, select the IP address that identifies the engine to external authentication servers.



Note

This selection has no effect on routing.

- g) (Optional) From the **Source for Authentication Requests** drop-down list, select the IP address that identifies the engine when it sends an authentication request to an external authentication server over a VPN.



Note

This selection has no effect on routing.

- h) From the **Default IP Address for Outgoing Traffic** field, select the IP address that the nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

- 3) Click **Save**.

Next steps

Continue the configuration in one of the following ways:

- If an interface used for external connections has only a Cluster Virtual IP address, add manual ARP entries for the nodes.
- Bind the engine licenses to the nodes in the Engine Cluster.

Related tasks


[Add manual ARP entries for Engine Clusters](#) on page 122


[Bind engine licenses to Engine Cluster elements](#) on page 122

Add manual ARP entries for Engine Clusters

ARP entries are normally managed automatically based on the Engine's routing configuration. However, you can also add manual ARP entries for the nodes.

If an interface used for external connections has only a cluster virtual IP address (CVI), you must add a static ARP entry. This entry gives the node a permanent reference to an IP address and MAC address.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces > ARP Entries**.
- 2) Click **Add ARP Entry**.
A new entry is added to the table.
- 3) Click **Type** and select **Static**.
- 4) Click **Interface ID** and select the interface on which the ARP entry is applied.
- 5) Double-click **IP Address** and enter the IP address information.
- 6) Double-click **MAC Address** and enter the MAC address information.
- 7) Click **OK**.
- 8) Click  **Save**, then close the Engine Editor.

Next steps


Bind the engine licenses to the nodes of the Engine Cluster.

Bind engine licenses to Engine Cluster elements

After you have configured the Engine Cluster elements, you must manually bind Management Server POL-bound licenses to specific nodes in Engine Cluster elements.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct Engine element when the engine is fully installed. Each engine is licensed separately even when the engines are clustered.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Administration**.
- 2) Browse to **Licenses > Engines** depending on the type of licenses you have.
All installed licenses appear in the right pane.
- 3) Right-click a Management Server POL-bound license and select **Bind**.
- 4) Select the node and click **Select**.
The license is now bound to the selected Engine element.



Tip

If you bound the license to an incorrect element, right-click the license and select **Unbind**.



CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses can't be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Transfer the configuration to the engines.

Related concepts

[Options for initial configuration on page 183](#)

Configuring Security Engine for the IPS role

Contents

- Types of interfaces for Security Engines in the IPS and Layer 2 Engine roles on page 125
- Interface numbering on page 126
- Install licenses for Security Engines on page 127
- Configuring IPS engines on page 127
- Bind engine licenses to IPS elements on page 141

Configuring engine elements in the SMC prepares the SMC to manage Security Engine in the IPS role.

Types of interfaces for Security Engines in the IPS and Layer 2 Engine roles

Interface definitions are an important part of IPS and Layer 2 Engine elements.

Types of interfaces for Security Engines in the IPS and Layer 2 Engine roles

| Interface type | Purpose of interface | Limitations |
|--|---|-------------|
| Physical (Normal type) | System communications. These interfaces are used when the engine is the source or the final destination of the communications. An example is control communications between the engine and the Management Server. Define at least one interface that is dedicated to system communications for each IPS engine or Layer 2 Engine. | |
| Physical (Capture Interface or Inline Interface type) | Traffic inspection. Define one or more traffic inspection interfaces for each IPS engine or Layer 2 Engine. | |

| Interface type | Purpose of interface | Limitations |
|----------------|--|---|
| VLAN | Divides a single physical interface into several virtual interfaces. | <ul style="list-style-type: none"> You cannot add VLAN Interfaces on top of other VLAN Interfaces (nested VLANs). You cannot create valid VLAN Interfaces in a Virtual Engine if the Master Engine interface that hosts the Virtual Engine is a VLAN Interface. |

Interface numbering

The interfaces have their own numbering in the SMC called the interface ID. The interface IDs are mapped to the corresponding network interfaces on the Security Engine when you configure the Forcepoint Network Security Platform software.

Interface numbering for Security Engines

| Interface type | Interface numbering in the SMC |
|--|--|
| Layer 3 physical (Security Engine with layer 3 interfaces) | Each physical interface has a unique interface ID number. |
| Layer 2 physical (Security Engine with layer 3 interfaces) | |
| Physical (IPS and Layer 2 Engine roles) | |
| VLAN | Each VLAN interface has a VLAN number. The defined VLAN interfaces are displayed, for example, as "5.202" for network interface 5 with VLAN 202. |
| Wireless | The wireless interface has a unique interface ID number. An SSID (service set identifier) interface represents an 802.11 wireless LAN. You can add several SSID interfaces to the wireless interface. |
| Modem | Modem Interfaces are identified with modem numbers. The modem number is mapped to the modem's IMEI (international mobile equipment identity) number. Each modem is assigned a unique ID when you connect the modem to the engine. You can change the mapping between the modem's IMEI number and the modem ID through the engine command line, if necessary. |
| Tunnel | Tunnel interfaces are numbered with tunnel interface ID numbers. The mapping of Tunnel Interfaces to physical network interfaces on the engine is done automatically by the engine operating system based on the routing configuration. |

| Interface type | Interface numbering in the SMC |
|----------------|--|
| Switch | Switches are identified with switch IDs. Integrated switches have predefined switch IDs. You can add port group interfaces to switches. Port group interfaces are identified by port group IDs. The defined switches and port group interfaces are displayed, for example, as <i>0.1</i> for switch ID 0 with port group 1. |

Install licenses for Security Engines



Install the Security Engine licenses that you downloaded while preparing for installation.

Before you begin

The license files must be available to the computer that you use to run the SMC Client.

You can install all licenses at the same time even though you have not yet created all elements that the licenses are bound to.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select  **Settings** > **Install Licenses**.
- 2) Select one or more license files to install in the dialog box that opens and click **Install**.
- 3) To check that the licenses were installed correctly, select  **Administration**, then browse to **Licenses** > **All Licenses**.
One license is shown for each Security Engine node. You must bind POL-bound licenses manually to the correct Security Engine nodes after you have configured the Security Engine elements. POS-bound licenses are automatically bound to the Security Engine nodes when you install a policy on the Security Engine after the Security Engine makes initial contact with the Management Server.

Next steps

Define the engine elements.

Configuring IPS engines

IPS elements are a tool for configuring nearly all aspects of your physical IPS components.

Little configuration is done directly on the engines. Most of the configuration is done using the SMC Client. You cannot successfully install the engines before defining them in the SMC as outlined.

After you have the SMC installed and running, you can configure the IPS engines.

The tasks you must complete are as follows:



- 1) Add Single IPS or IPS Cluster elements.
- 2) Add system communication interfaces.
- 3) Add traffic inspection interfaces.
- 4) Bind licenses to specific IPS elements.

Add IPS elements

To add IPS engines to the SMC, add a Single IPS element or an IPS Cluster element that stores the configuration information related to the IPS engine.

This procedure covers the basic configuration of IPS engine elements. For complete instructions about configuring IPS engines, see the *Forcepoint Network Security Platform Product Guide*.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click **Engines** and select one of the following:
 - **New > IPS > IPS Cluster**
 - **New > IPS > Single IPS**The Engine Editor opens.
- 3) In the **Name** field, enter a unique name.
- 4) From the **Log Server** drop-down list, select the Log Server for storing this IPS engine's logs. If no Log Server is selected, the engine does not make any traffic recordings.
- 5) (Optional) In the **DNS IP Addresses** list, add one or more DNS IP addresses. These addresses are the IP addresses of the DNS servers that the IPS engine uses to resolve domain names and web filtering categorization services (which are defined as URLs).
 - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog that opens.
 - To define an IP address by using a network element, click **Add** and select **Network Element**. Select a Host or External DNS Server element.
- 6) From the **Location** drop-down list, select the Location to which the IPS belongs.
- 7) Click  **Save**.
Do not close the Engine Editor.


Add system communication interfaces to IPS engines


Each IPS engine needs at least one interface for communicating with the SMC.

You can add more than one system communication interface to provide a primary and a backup interface for Management Server communications.

Add physical interfaces to IPS elements

Add a physical interface for system communications.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click the empty space and select **New Physical Interface**.
- 3) From the **Interface ID** drop-down list, select an ID number.
This ID maps to a network interface during the initial configuration of the engine.
- 4) From the **Type** drop-down list, select **Normal Interface**.
- 5) Click **OK**.
The physical interface is added to the interface list
- 6) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLANs to the physical interface.
- Add IP addresses to the physical interface.

Related tasks

[Add static IPv4 addresses to Single IPS interfaces](#) on page 130

[Add IP addresses to IPS Cluster interfaces](#) on page 133


Add VLAN interfaces to IPS elements

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANs to each physical interface.

**CAUTION**


Do not add any manual VLAN definitions to an interface you want to use for sending resets. Adding VLANs prevents selecting the interface as a reset interface and also removes the reset interface from any existing selections.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface and select **New > VLAN Interface**.
- 3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).

**Note**

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.


- 4) Click **OK**.
The specified VLAN ID is added to the physical interface.
- 5) Click  **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Add static IPv4 addresses to Single IPS interfaces


You can add one or more static IPv4 addresses to each physical or VLAN interface on a Single IPS engine.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a Physical Interface or a VLAN Interface and select **New > IPv4 Address**.
- 3) In the **IPv4 Address** field, enter the IPv4 address.

**Tip**

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.


- 4) Click **Netmask** and adjust the automatically added netmask if necessary.
The **Network Address** and **Broadcast IP Address** are updated accordingly
- 5) If the interface is used for system communications and NAT is applied, add contact addresses.
 - a) Enter the default contact address in one of the following ways:
 - In the **Default** field, enter the contact address.
 - Select **Dynamic** and define the translated IP address of this component.
 - b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.
- 6) Click **OK**.
The IP address is added to the interface.
- 7) Click  **Save**.
If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

**Tip**

Write down the networks to which each Interface ID is connected.

Add dynamic IPv4 addresses to Single IPS interfaces


You can add one dynamic IPv4 address to each physical or VLAN interface on a Single IPS engine.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a Physical Interface or a VLAN Interface and select **New > IPv4 Address**.
- 3) Select **Dynamic**.
- 4) From the **Dynamic Index** drop-down list, select a DHCP index.
The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.
- 5) If the interface is used for system communications and NAT is applied, add contact addresses.
 - a) Enter the default contact address in one of the following ways:
 - In the **Default** field, enter the contact address.
 - Select **Dynamic** and define the translated IP address of this component.

Add dynamic IPv6 addresses to Single IPS interfaces

You can add one dynamic IPv6 address to each physical or VLAN interface on a Single IPS engine.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Right-click a Physical Interface or a VLAN Interface and select **New > IPv6 Address**.
- 3) Select **Dynamic**.
- 4) From the **Dynamic Index** drop-down list, select a DHCP index.
The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.
- 5) If the interface is used for system communications and NAT is applied, add contact addresses.
 - a) Enter the default contact address in one of the following ways:
 - In the **Default** field, enter the contact address.
 - Select **Dynamic** and define the translated IP address of this component.
 - b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.
- 6) (Optional) If you do not want a default route to be automatically created through the interface, deselect **Automatic Default Route**.
- 7) (Optional) If you want to use DHCPv6 to get the IPv6 address, select **Use DHCPv6 to get IPv6 Address**.
- 8) Click **OK**.
The IP address is added to the interface.
- 9) Click  **Save**.
If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.



Tip

Write down the networks to which each Interface ID is connected.

Add IP addresses to IPS Cluster interfaces

You can add IP addresses to each node of an IPS Cluster.

You can add both IPv4 and IPv6 addresses to the same interface.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Right-click a physical interface or a VLAN interface and add the IP address in one of the following ways:
 - To add an IPv4 address, select **New > IPv4 Address**
 - To add an IPv6 address, select **New > IPv6 Address**
- 3) Click the **IPv4 Address** or **IPv6 Address** cell in the table and enter the IP address for each node.



Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 4) (IPv4 addresses only) If necessary, double-click the **Contact Address** cell in the table and define the contact address for each node.
 - In the **Default** field at the top of the dialog box, enter the default contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
 - If components from some Locations cannot use the default contact address, click **Add** to define Location-specific contact addresses.
- 5) (IPv4 addresses only) Check the automatically filled-in **Netmask** and adjust it as necessary.
- 6) (IPv6 addresses only) Check the automatically filled-in **Prefix Length** and adjust it as necessary.
- 7) Click **OK**.
- 8) Click  **Save**.

Next steps

Continue the configuration in one of the following ways:

- Select system communication roles for the interfaces.
- Add traffic inspection interfaces.

Select system communication roles for IPS interfaces


Select which interfaces are used for particular roles in system communications.

For example, you can select which IP addresses are used in communications between the IPS engine and the Management Server.

The interfaces you have defined are shown as a tree-table on the Interfaces tab. Global interface options have codes in the tree-table.

Interface option codes

| Code | Description |
|-------------------------|---|
| C | The interfaces that have the primary and backup control IP addresses. |
| (IPS Cluster only) H | The primary and backup heartbeat Interfaces. |
| O | The default IP address for outgoing connections. |

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces > Interface Options**.
- 2) Select the interface options.
 - a) From the **Primary** control IP address drop-down list, select the primary control IP address that the IPS engine uses for communications with the Management Server.
 - b) (Optional, recommended) In the **Backup** control IP address drop-down list, select a backup control IP address that the IPS engine uses for communications with the Management Server if the primary control IP address fails.

- c) (IPS Cluster only) From the **Primary** heartbeat drop-down list, select the primary interface for communications between the nodes.

We recommend using a physical interface, not a VLAN interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network (without other traffic) is recommended for security and reliability of heartbeat communication.



CAUTION

Primary and backup heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information.

- d) (IPS Cluster only) From the **Backup** heartbeat drop-down list, select the backup heartbeat interface that is used if the primary heartbeat interface is unavailable.
It is not mandatory to configure a backup heartbeat interface, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic is disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well.
 - e) (Single IPS only) If the Single IPS engine's primary control IP address and backup control IP address are dynamic or if the Single IPS engine is in an environment where only the IPS engine can initiate connections to the Management Server, select **Node-initiated contact to Management Server**.
When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.
 - f) From the **Default IP Address for Outgoing Traffic** drop-down list, select the IP address that nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

- 3) Click  **Save**.

Next steps

Add traffic inspection interfaces for the IPS engine.

Add traffic inspection interfaces to IPS engines

IPS engines pick up passing network traffic for inspection in real time.

You can define both capture interfaces and inline interfaces for the same IPS engine.

When traffic is inspected, it might be important to know the interface through which it arrives to the IPS engine. It is also important to be able to distinguish an IPS engine's capture interfaces from its inline interfaces. Logical interface elements are used for both these purposes. They allow you to group interfaces that belong to the same network segment and to identify the type of the traffic inspection interface.

Define a logical interface in the following cases:

- You want to create both capture interfaces and inline interfaces on the same IPS engine.
- You want to distinguish interfaces from each other.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Add logical interfaces to IPS engines

Logical Interface elements are used in the IPS Policy and the traffic inspection process to represent a network segment.

The SMC contains one default Logical Interface element. A logical interface can represent any number or combination of physical interfaces and VLAN interfaces. However, the same logical interface cannot be used to represent both capture interfaces and inline interfaces on the same IPS engine. The rules in the ready-made IPS Template policy match all logical interfaces.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select **Engine Configuration**.
- 2) Expand the **Other Elements** branch.
- 3) Right-click **Logical Interfaces** and select **New Logical Interface**.
- 4) In the **Name** field, enter a unique name.
- 5) (Optional) If you use VLAN tagging, select **View interface as one LAN**.
By default, the IPS engine treats a single connection as multiple connections when an external switch passes traffic between different VLANs and all traffic is mirrored to the IPS engine through a SPAN port.

- 6) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Related tasks

[Add capture interfaces to IPS engines](#) on page 138

[Add inline interfaces to IPS engines](#) on page 139

Add reset interfaces to IPS engines

Reset interfaces can deliver TCP resets and ICMP destination unreachable messages to interrupt communications picked up from capture interfaces when the communications trigger a response.


VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.


The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.



Important

An interface that is used only as a reset interface must not have an IP address.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the IPS engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Normal Interface**.
- 6) Click **OK**.
- 7) Click  **Save**.

Result


This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interfaces.


Add capture interfaces to IPS engines

Capture interfaces monitor traffic that external devices have duplicated for inspection to the IPS engine.

You can have as many capture interfaces as there are available physical ports on the IPS engine (there are no license restrictions regarding this interface type).

External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to an external switch SPAN port or a network TAP to capture traffic.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the IPS engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Capture Interface**.
- 6) (Optional) From the **Reset Interface** drop-down list, select a TCP reset interface for traffic picked up through this capture interface.
- 7) If your configuration requires you to change the logical interface from `Default_Eth`, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 8) If you want the IPS engine to inspect traffic from VLANs that are not included in the IPS engine's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the IPS engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 10) Click **OK**.
- 11) Click  **Save**.

Next steps

Continue the configuration in one of the following ways:

- Define Inline Interfaces.
- Define how the IPS engine handles traffic when the traffic load is too high using the **Bypass Traffic on Overload** setting.
- Bind engine licenses to IPS elements.

Related tasks

[Bypass traffic on overload](#) on page 140

[Bind engine licenses to IPS elements](#) on page 141


Add inline interfaces to IPS engines


There are two interfaces in an inline interface. The traffic is forwarded from one interface to the other.

The traffic that the IPS engine allows goes through the inline interface as if it was going through a network cable. The IPS engine drops the traffic you want to stop.

Inline interfaces are associated with a Logical interface element. The Logical interface is used in the IPS policies and the traffic inspection process to represent one or more IPS engine interfaces.

Fail-open network cards have fixed pairs of ports. Make sure to map these ports correctly during the initial configuration of the engine. Otherwise, the network cards do not correctly fail open when the IPS engine is offline. If you use the automatic USB memory stick configuration method for the engine's initial configuration, the ports are configured automatically.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the IPS engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Inline Interface**.
- 6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.
- 7) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 8) If you want the IPS engine to inspect traffic from VLANs that are not included in the IPS engine's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the IPS engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 10) Click **OK**.
- 11) Click  **Save**.

Next steps

Continue the configuration in one of the following ways:

- Define how the IPS engine handles traffic when the traffic load is too high using the **Bypass Traffic on Overload** setting.
- Bind engine licenses to IPS elements.

Related tasks

[Bind engine licenses to IPS elements](#) on page 141

[Configure Forcepoint Security Engine software using automatic configuration](#) on page 189

Bypass traffic on overload


You can configure the IPS engine to bypass traffic when the traffic load becomes too high.


By default, IPS engines inspect all connections. If the traffic load is too high for the IPS engine to inspect all connections, IPS engines can dynamically reduce the number of inspected connections. This reduction can improve performance in evaluation environments, but some traffic might pass through without any access control or inspection.



CAUTION

Using bypass mode requires a fail-open network interface card. If the ports that represent the interfaces cannot fail open, policy installation fails on the engine. Bypass mode is not compatible with VLAN retagging. In network environments where VLAN retagging is used, normal mode is automatically enforced.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the IPS engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, select **Advanced Settings**.
- 3) Select **Bypass Traffic on Overload**.
- 4) Click  **Save**.


Next steps


Bind engine licenses to IPS elements.

Bind engine licenses to IPS elements

After you have configured the IPS elements, you must manually bind Management Server POL-bound licenses to specific IPS elements.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct IPS element when the engine is fully installed. Each engine is licensed separately even when the engines are clustered.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Administration**.
- 2) Browse to **Licenses > Engine** or **Licenses > IPS** depending on the type of licenses you have. All installed licenses appear in the right pane.
- 3) Right-click a Management Server POL-bound license and select **Bind**.
- 4) Select the IPS element and click **Select**.
The license is now bound to the selected IPS element.



Tip

If you bound the license to an incorrect element, right-click the license and select **Unbind**.



CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses can't be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Transfer the configuration to the IPS engines.

Configuring Security Engine for the Layer 2 Engine role

Contents

- Types of interfaces for Security Engines in the IPS and Layer 2 Engine roles on page 143
- Install licenses for Security Engines on page 144
- Configuring Layer 2 Engines on page 144
- Bind engine licenses to Layer 2 Engine elements on page 157

Configuring engine elements in the SMC prepares the SMC to manage Security Engine with the Layer 2 Engine role.

Types of interfaces for Security Engines in the IPS and Layer 2 Engine roles

Interface definitions are an important part of IPS and Layer 2 Engine elements.

Types of interfaces for Security Engines in the IPS and Layer 2 Engine roles

| Interface type | Purpose of interface | Limitations |
|--|---|--|
| Physical (Normal type) | System communications. These interfaces are used when the engine is the source or the final destination of the communications. An example is control communications between the engine and the Management Server. Define at least one interface that is dedicated to system communications for each IPS engine or Layer 2 Engine. | |
| Physical (Capture Interface or Inline Interface type) | Traffic inspection. Define one or more traffic inspection interfaces for each IPS engine or Layer 2 Engine. | |
| VLAN | Divides a single physical interface into several virtual interfaces. | <ul style="list-style-type: none">■ You cannot add VLAN Interfaces on top of other VLAN Interfaces (nested VLANs).■ You cannot create valid VLAN Interfaces in a Virtual Engine if the Master Engine interface that hosts the Virtual Engine is a VLAN Interface. |


Install licenses for Security Engines



Install the Security Engine licenses that you downloaded while preparing for installation.

Before you begin

The license files must be available to the computer that you use to run the SMC Client.

You can install all licenses at the same time even though you have not yet created all elements that the licenses are bound to.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select  **Settings** > **Install Licenses**.
- 2) Select one or more license files to install in the dialog box that opens and click **Install**.
- 3) To check that the licenses were installed correctly, select  **Administration**, then browse to **Licenses** > **All Licenses**.

One license is shown for each Security Engine node. You must bind POL-bound licenses manually to the correct Security Engine nodes after you have configured the Security Engine elements. POS-bound licenses are automatically bound to the Security Engine nodes when you install a policy on the Security Engine after the Security Engine makes initial contact with the Management Server.

Next steps

Define the engine elements.

Configuring Layer 2 Engines

Layer 2 Engine elements are a tool for configuring nearly all aspects of your Layer 2 Engines.

Little configuration is done directly on the engines. Most of the configuration is done using the SMC Client. The engines cannot be successfully installed before defining them in the SMC as outlined.


After you have the SMC installed and running, you can configure the Layer 2 Engines.



The tasks you must complete are as follows:

- 1) Add Single Layer 2 Engine or Layer 2 Engine Cluster elements.
- 2) Add system communication interfaces.
- 3) Add traffic inspection interfaces.
- 4) Bind licenses to specific Layer 2 Engine elements.

Add Layer 2 Engine elements

The basic configuration of Layer 2 Engine elements begins with creating an engine element.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select  **Engine Configuration**.
- 2) Right-click **Engines** and select one of the following:
 - **New > Layer 2 Engine > Layer 2 Engine Cluster**
 - **New > Layer 2 Engine > Single Layer 2 Engine**The Engine Editor opens.
- 3) In the **Name** field, enter a unique name.
- 4) From the **Log Server** drop-down list, select the Log Server that stores the log events that the Layer 2 Engine creates.
- 5) (Optional) In the **DNS IP Addresses** field, add one or more DNS IP addresses for the Layer 2 Engine. These addresses are the IP addresses of the DNS servers that the Layer 2 Engine uses to resolve domain names and web filtering categorization services (which are defined as URLs).
 - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
 - To define an IP address by using a Network element, click **Add** and select **Network Element**. Select a predefined Alias element that represents the IP address of the DNS of a dynamic network interface, a Host element, or an External DNS Server element.
- 6) From the **Location** drop-down list, select the location for this engine if there is a NAT device between SMC components affecting this engine's communications.
- 7) Click  **Save**.
Do not close the Engine Editor.

Add system communications interfaces to Layer 2 Engines


Each Layer 2 Engine needs at least one interface for communicating with the SMC.

You can add more than one system communication interface to provide a primary and a backup interface for Management Server communications.

Add physical interfaces to Layer 2 Engines

Add a physical interface for system communications.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Right-click the empty space and select **New Physical Interface**.
- 3) From the **Interface ID** drop-down list, select an ID number.
This ID maps to a network interface during the initial configuration of the engine.
- 4) From the **Type** drop-down list, select **Normal Interface**.
- 5) Click **OK**.
The physical interface is added to the interface list.
- 6) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add VLANs to the physical interface.
- Add an IP address to the physical interface.

Related tasks

[Add static IPv4 addresses to Single Layer 2 Engine interfaces](#) on page 147

[Add IP addresses to Layer 2 Engine Cluster interfaces](#) on page 151

Add VLAN Interfaces to Layer 2 Engines

VLANs divide a single physical network link into several virtual links.

You can add up to 4094 VLANs to each physical interface.



CAUTION

Do not add any manual VLAN definitions to an interface you want to use for sending resets. Adding VLANs prevents selecting the interface as a reset interface and also removes the reset interface from any existing selections.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.


- 1) In the navigation pane on the left, select **Interfaces**.

- 2) Right-click a physical interface and select **New > VLAN Interface**.
- 3) In the **VLAN ID** field, enter a VLAN ID number (1-4094).



Note

The VLAN ID must be the same VLAN ID used in the external switch at the other end of the VLAN trunk.


- 4) Click **OK**.
The specified VLAN ID is added to the physical interface.
- 5) Click  **Save**.
Do not close the Engine Editor.

Result

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as Interface-ID.VLAN-ID, for example 2.100 for interface ID 2 and VLAN ID 100.

Add static IPv4 addresses to Single Layer 2 Engine interfaces

You can add one or more static IPv4 addresses to each physical or VLAN interface on a Single Layer 2 Engine.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a Physical Interface or a VLAN Interface and select **New > IPv4 Address**.
- 3) In the **IPv4 Address** field, enter the IPv4 address.



Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 4) Click **Netmask** and adjust the automatically added netmask if necessary.
The **Network Address** and **Broadcast IP Address** are updated accordingly.
- 5) If the interface is used for system communications and NAT is applied, add contact addresses.
 - a) Enter the default contact address in one of the following ways:
 - In the **Default** field, enter the contact address.
 - Select **Dynamic** and define the translated IP address of this component.

7) Click  Save.


If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.

**Tip**

Write down the networks to which each Interface ID is connected.

Add static IPv6 addresses to Single Layer 2 Engine interfaces


You can add one or more static IPv6 addresses to each physical or VLAN interface on a Single Layer 2 Engine.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a Physical Interface or a VLAN Interface and select **New > IPv6 Address**.
- 3) In the **IPv6 Address** field, enter the IPv6 address.

**Tip**

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.


- 4) Click **Prefix Length** and adjust the automatically added prefix length if necessary.
- 5) Click **OK**.
The IP address is added to the interface.
- 6) Click  **Save**.
If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.


**Tip**

Write down the networks to which each Interface ID is connected.

Add dynamic IPv6 addresses to Single Layer 2 Engine interfaces

You can add one dynamic IPv6 address to each physical or VLAN interface on a Single Layer 2 Engine.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface or a VLAN interface and select **New > IPv6 Address**.
- 3) Select **Dynamic**.
- 4) From the **Dynamic Index** drop-down list, select a DHCP index.
The index is used for identification in other parts of the configuration (such as IPS Policies) to represent the possibly changing IP address.
- 5) If the interface is used for system communications and NAT is applied, add contact addresses.
 - a) Enter the default contact address in one of the following ways:
 - In the **Default** field, enter the contact address.
 - Select **Dynamic** and define the translated IP address of this component.
 - b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.
- 6) (Optional) If you do not want a default route to be automatically created through the interface, deselect **Automatic Default Route**.
- 7) (Optional) If you want to use DHCPv6 to get the IPv6 address, select **Use DHCPv6 to get IPv6 Address**.
- 8) Click **OK**.
The IP address is added to the interface.
- 9) Click  **Save**.
If you plan to add more IP addresses or change the roles that interfaces have in system communications, do not close the Engine Editor.




Tip

Write down the networks to which each Interface ID is connected.

Add IP addresses to Layer 2 Engine Cluster interfaces

Add IP addresses to Layer 2 Engine Cluster interfaces.

You can add both IPv4 and IPv6 addresses to the same interface.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, select **Interfaces**.
- 2) Right-click a physical interface or a VLAN interface and add the IP address in one of the following ways:
 - To add an IPv4 address, select **New > IPv4 Address**
 - To add an IPv6 address, select **New > IPv6 Address**
- 3) Click the **IPv4 Address** or **IPv6 Address** cell in the table and enter the IP address for each node.



Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 4) (IPv4 addresses only) If necessary, double-click the **Contact Address** cell in the table and define the contact address for each node.
 - In the **Default** field at the top of the dialog box, enter the default contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
 - If components from some Locations cannot use the default contact address, click **Add** to define Location-specific contact addresses.
- 5) (IPv4 addresses only) Check the automatically filled-in **Netmask** and adjust it as necessary.
- 6) (IPv6 addresses only) Check the automatically filled-in **Prefix Length** and adjust it as necessary.
- 7) Click **OK**.
- 8) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Select system communication roles for the interfaces.
- Add traffic inspection interfaces.

Select system communication roles for Layer 2 Engine interfaces


Select which interfaces are used for particular roles in system communications.

For example, you can select which IP addresses are used in communications between the Layer 2 Engine and the Management Server.

The interfaces you have defined are shown as a tree-table on the Interfaces tab. Global interface options have codes in the tree-table.

Interface option codes

| Code | Description |
|------------------------------------|---|
| C | The interfaces that have the primary and backup control IP addresses. |
| (Layer 2 Engine Cluster only) H | The primary and backup heartbeat Interfaces. |
| O | The default IP address for outgoing connections. |

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the navigation pane on the left, browse to **Interfaces > Interface Options**.
- 2) Select the interface options.
 - a) From the **Primary** control IP address drop-down list, select the primary control IP address that the Layer 2 Engine uses for communications with the Management Server.
 - b) (Optional, recommended) In the **Backup** control IP address drop-down list, select a backup control IP address that the Layer 2 Engine uses for communications with the Management Server if the primary control IP address fails.
 - c) (Layer 2 Engine Cluster only) From the **Primary** heartbeat drop-down list, select the primary interface for communications between the nodes.



CAUTION

Primary and backup heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information.

- d) (Layer 2 Engine Cluster only) From the **Backup** heartbeat drop-down list, select the backup heartbeat interface that is used if the primary heartbeat interface is unavailable.

It is not mandatory to configure a backup heartbeat interface, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic is disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well.

- e) (Single Layer 2 Engine only) If the Single Layer 2 Engine's primary control IP address and backup control IP address are dynamic or if the Single Layer 2 Engine is in an environment where only the Layer 2 Engine can initiate connections to the Management Server, select **Node-initiated contact to Management Server**.

When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.

- f) From the **Default IP Address for Outgoing Traffic** drop-down list, select the IP address that nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

- 3) Click  **Save**.

Next steps

Add traffic inspection interfaces for the Layer 2 Engine.

Add traffic inspection interfaces to Layer 2 Engines

Layer 2 Engines pick up passing network traffic for inspection in real time.

You can define both capture interfaces and inline interfaces for the same Layer 2 Engine.

When traffic is inspected, it might be important to know the interface through which it arrives to the Layer 2 Engine. It is also important to be able to distinguish a Layer 2 Engine's capture interfaces from its inline interfaces. Logical Interface elements are used for both these purposes. They allow you to group interfaces that belong to the same network segment and to identify the type of the traffic inspection interface.


Define a logical interface in the following cases:


- You want to create both capture interfaces and inline interfaces on the same Layer 2 Engine.
- You want to create Logical Interfaces to distinguish interfaces from each other.

Add logical interfaces to Layer 2 Engines

A logical interface is used in the Layer 2 Engine Policy and the traffic inspection process to represent a network segment.

The SMC contains one default Logical Interface element. A logical interface can represent any number or combination of physical interfaces and VLAN interfaces. However, the same logical interface cannot be used to represent both capture interfaces and inline interfaces on the same Layer 2 Engine. The rules in the ready-made Layer 2 Engine Template match all logical interfaces.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Expand the **Other Elements** branch.

- 3) Right-click **Logical Interfaces** and select **New Logical Interface**.
- 4) In the **Name** field, enter a unique name.
- 5) (Optional) If you use VLAN tagging, select **View interface as one LAN**.
By default, the engine treats a single connection as multiple connections when a switch passes traffic between different VLANs and all traffic is mirrored to the IPS engine through a SPAN port.
- 6) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- If you want to use reset interfaces with capture interfaces, add reset interfaces.
- Add capture interfaces or inline interfaces.

Related tasks

[Add capture interfaces to Layer 2 Engines](#) on page 155

[Add inline interfaces to Layer 2 Engines](#) on page 156

Add reset interfaces to Layer 2 Engines

Reset interfaces can deliver TCP resets and ICMP destination unreachable messages to interrupt communications picked up from capture interfaces when the communications trigger a response.

VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.

The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.




Important

An interface that is used only as a reset interface must not have an IP address.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Layer 2 Engine element and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Normal Interface**.

- 6) Click **OK**.
- 7) Click  **Save**.
Do not close the Engine Editor.

Result

This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interfaces.

Next steps

Add capture interfaces and inline interfaces.

Add capture interfaces to Layer 2 Engines

Capture interfaces monitor traffic that external devices have duplicated for inspection to the Layer 2 Engine.

You can have as many capture interfaces as there are available network ports on the Layer 2 Engine (there are no license restrictions regarding this interface type).

External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to an external switch SPAN port or a network TAP to capture traffic.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) On the **Interfaces** pane, right-click and select **New Physical Interface**.
- 2) From the **Interface ID** drop-down list, select an ID number.
- 3) From the **Type** drop-down list, select **Capture Interface**.
- 4) (Optional) From the **Reset Interface** drop-down list, select a TCP reset interface for traffic picked up through this capture interface.
- 5) If your configuration requires you to change the logical interface from Default_Eth, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 6) If you want the Layer 2 Engine to inspect traffic from VLANs that are not included in the IPS engine's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 7) If you want the Layer 2 Engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.
- 8) Click **OK**.

9) Click  **Save**.

If you plan to add inline interfaces, do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:

- Add inline interfaces.
- Bind engine licenses to Layer 2 Engine elements.

Related tasks

[Bind engine licenses to Layer 2 Engine elements](#) on page 157

Add inline interfaces to Layer 2 Engines


There are two interfaces in an inline interface. The traffic is forwarded from one interface to the other.

The traffic that the Layer 2 Engine allows goes through the inline interface as if it was going through a network cable. The Layer 2 Engine drops the traffic you want to stop.

Inline interfaces are associated with a Logical Interface element. The Logical Interface is used in the Layer 2 Engine Policy and the traffic inspection process to represent one or more Layer 2 Engine interfaces.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Layer 2 Engine and select **Edit <element type>**.
The Engine Editor opens.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click the empty space and select **New Physical Interface**.
- 4) From the **Interface ID** drop-down list, select an ID number.
- 5) From the **Type** drop-down list, select **Inline Interface**.
- 6) (Optional) From the **Second Interface ID** drop-down list, change the automatically selected interface ID.
- 7) If your configuration requires you to change the logical interface from `Default_Eth`, select the logical interface in one of the following ways:
 - Select an existing Logical Interface element from the list.
 - Click **Select** and browse to another Logical Interface element.
 - Click **New** to create a Logical Interface element, then click **OK**.
- 8) If you want the Layer 2 Engine to inspect traffic also from VLANs that are not included in the engine's interface configuration, leave **Inspect Unspecified VLANs** selected.
- 9) If you want the Layer 2 Engine to inspect double-tagged VLAN traffic, leave **Inspect QinQ** selected.

- 10) Click **OK**.
- 11) Click  **Save**, then close the Engine Editor.

Next steps

Bind engine licenses to Layer 2 Engine elements.


Related tasks


[Bind engine licenses to Layer 2 Engine elements](#) on page 157

Bind engine licenses to Layer 2 Engine elements

After you have configured the Layer 2 Engine elements, you must manually bind Management Server POL-bound licenses to specific Layer 2 Engine elements.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct Layer 2 Engine element when the engine is fully installed. Each engine is licensed separately even when the engines are clustered.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Administration**.
- 2) Browse to **Licenses > Engine**.
All installed licenses appear in the right pane.
- 3) Right-click a Management Server POL-bound license and select **Bind**.
- 4) Select the Layer 2 Engine element and click **Select**.
The license is now bound to the selected Layer 2 Engine element.



CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses can't be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.

Next steps

Transfer the configuration to the Layer 2 Engine.

Chapter 8

Configuring Security Engines as Master Engines and Virtual Engines

Contents

- Master Security Engine and Virtual Security Engine configuration overview on page 159
- Install licenses for Security Engines on page 160
- Add Master Security Engine elements on page 160
- Create Virtual Engines on page 169
- Create Virtual IPS engines on page 174
- Add Virtual Layer 2 Engine elements on page 176

Configuring engine elements in the SMC prepares the SMC to manage Master Security Engines and Virtual Security Engines.

Master Security Engine and Virtual Security Engine configuration overview

Virtual Security Engines are logically separate virtual engine instances on a physical engine device. A Master Security Engine is a physical engine device that provides resources for Virtual Security Engines. One physical Master Security Engine can support multiple Virtual Security Engines.

Little configuration is done directly on the Master Security Engine. No installation or configuration is done on the Virtual Security Engines. Most of the configuration is done using the SMC Client. The engines cannot be successfully installed before defining them in the SMC Client as outlined in this section.

The tasks you must complete are as follows:

- 1) Add Master Security Engine elements.
 - a) Add Virtual Resource elements.
 - b) Add physical interfaces and optionally VLAN interfaces to the Master Security Engine.
 - c) Assign Virtual Resources to the interfaces that are used by the Virtual Security Engines hosted on the Master Security Engine.
- 2) Add Virtual Engine, Virtual IPS, or Virtual Layer 2 Engine elements.
 - a) Configure the automatically created physical interfaces.

- b) (Optional) Add VLAN interfaces for the Virtual Security Engines.
- 3) Bind licenses to specific nodes of the Master Security Engine.

Install licenses for Security Engines

Install the Security Engine licenses that you downloaded while preparing for installation.

Before you begin

The license files must be available to the computer that you use to run the SMC Client.

You can install all licenses at the same time even though you have not yet created all elements that the licenses are bound to.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select **Settings > Install Licenses**.
- 2) Select one or more license files to install in the dialog box that opens and click **Install**.
- 3) To check that the licenses were installed correctly, select **Administration**, then browse to **Licenses > All Licenses**.
One license is shown for each Security Engine node. You must bind POL-bound licenses manually to the correct Security Engine nodes after you have configured the Security Engine elements. POS-bound licenses are automatically bound to the Security Engine nodes when you install a policy on the Security Engine after the Security Engine makes initial contact with the Management Server.

Next steps


Define the engine elements.

Add Master Security Engine elements

To introduce a new Master Security Engine to the SMC, add a Master Security Engine element that stores the configuration information for the Master Security Engine and Virtual Security Engines.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select **Engine Configuration**.

- 2) Right-click **Engines** and select **New > Master Engine**.
- 3) Select the role for the Virtual Engines the Master Engine hosts, then click **OK**.
The Engine Editor opens.
- 4) In the **Name** field, enter a unique name.
- 5) Select the **Log Server** to which the Master Security Engine sends its log data.
- 6) (Optional) Define one or more **DNS IP Addresses**.
These addresses are the IP addresses of the DNS servers that the Master Security Engine uses to resolve domain names. There are two ways to define IP addresses.
 - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
 - To define an IP address using a network element, click **Add** and select **Network Element**.
- 7) Select the **Location** for this Master Security Engine if there is a NAT device between this Master Security Engine and other SMC components.
- 8) (Optional) If you do not need to use clustering on the Master Security Engine:
 - a) In the navigation pane on the left, browse to **General > ARP Entries**.
 - b) Select one of the nodes, then click **Remove Node**.
 - c) When prompted to confirm that you want to delete the selected node, click **Yes**.
- 9) Click  **Save**.
Do not close the Engine Editor.

Next steps

Continue the configuration in one of the following ways:


- Add more nodes to the Master Security Engine.
- Add Virtual Resource elements.

Add nodes to Master Security Engines

Add all nodes you plan to install before you begin configuring the interfaces.

The Master Security Engine has placeholders for two nodes when the element is created. A Master Security Engine can have up to 16 nodes.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.



- 1) Right-click the Master Engine element and select **Edit Master Engine**.
The Engine Editor opens.
- 2) In the navigation pane on the left, select **General > Clustering**.
- 3) Click **Add Node**.
- 4) (Optional) Change the **Name**.
- 5) Click **OK**.
The node is added to the Master Security Engine.
- 6) Click  **Save**.

Create Virtual Resource elements

Virtual Resources associate Virtual Engines with Physical Interfaces or VLAN Interfaces on the Master Security Engine.

When you select the same Virtual Resource for a Physical Interface or VLAN Interface on the Master Engine and for a Virtual Security Engine, the Virtual Engine is automatically associated with the Master Security Engine. Create one Virtual Resource for each Virtual Engine that you plan to add.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click the Master Engine element, then select **Edit Master Engine**.
- 3) Browse to **Interfaces > Virtual Resources**.
- 4) Click **Add**.
- 5) Configure the settings.
- 6) Click **OK**.
- 7) Click  **Save**.

Next steps

Continue the configuration in one of the following ways:

- Configure Master Engine interfaces.

- Associate the Virtual Resource with a Master Engine interface and with a Virtual Engine.

Types of interfaces for Master Security Engines with Layer 3 Interfaces

You can configure several types of interfaces for Master Security Engines with Layer 3 Interfaces.

Types of interfaces for Master Security Engines with Layer 3 Interfaces

| Interface type | Purpose of interface | Limitations |
|------------------|--|--|
| Layer 3 physical | System communications and traffic inspection. | You cannot add both VLAN Interfaces and IP addresses to a Physical Interface. If an IP address is already configured for a Physical Interface, adding a VLAN Interface removes the IP address. If you plan to use VLAN Interfaces, configure the VLAN Interfaces first and then add IP addresses to the VLAN Interfaces. |
| Layer 2 physical | Traffic inspection. Layer 2 interfaces on Master Security Engines with Layer 3 Interfaces allow the engine to provide the same kind of traffic inspection that is available for Master Engines in the IPS and Layer 2 Engine roles. | <ul style="list-style-type: none"> ■ You cannot add IP addresses to layer 2 physical interfaces on Master Security Engines with Layer 3 Interfaces. ■ VLAN retagging is not supported on layer 2 physical interfaces of the inline IPS type. |
| VLAN | Divides a single physical interface into several virtual interfaces. | <ul style="list-style-type: none"> ■ You cannot add VLAN interfaces on top of other VLAN Interfaces (nested VLANs). |

Add layer 3 physical interfaces to Master Security Engines

Master Security Engines can have two types of physical interfaces: interfaces for the Master Security Engine's own communications, and interfaces that are used by the Virtual Security Engines hosted on the Master Security Engine.

You must add at least one physical interface for the Master Security Engine's own communications.

For Master Security Engine clusters, it is recommended to add at least two physical interfaces:

- An interface used for communications between the Management Server and the Master Security Engine.
- An interface for the heartbeat communications between the cluster nodes. The heartbeat traffic is critical to the functioning of the cluster, so it is highly recommended to have a dedicated heartbeat interface.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click the Master Engine element, then select **Edit <element type>**.

- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Click **Add**, then select **Layer 3 Physical Interface**.
- 4) (Interface for Master Security Engine communications only) Define the physical interface properties.
 - a) From the **Type** drop-down list, select the interface type according to the engine role.
 - b) Do not select a Virtual Resource for an interface that is used for the Master Security Engine's own communications.
 - c) In the **Cluster MAC Address** field, enter the MAC address for the Master Security Engine.

**Note**

Do not use the MAC address of any actual network card on any of the Master Security Engine nodes.

**Note**

Make sure that you set the interface speed correctly. When the bandwidth is set, the Master Security Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

- 5) (Interface for hosted Virtual Security Engine communications only) Define the physical interface properties.
 - a) From the **Type** drop-down list, select the interface type according to the engine role.
 - b) (Virtual IPS only) From the **Failure Mode** drop-down list, select how traffic to the inline interface is handled if the Virtual IPS engine goes offline.

**Note**

If there are VLAN interfaces under the inline interface, select **Bypass**.

**CAUTION**


Using Bypass mode requires the Master Security Engine appliance to have a fail-open network interface card. If the ports that represent the pair of inline interfaces on the appliance cannot fail open, the policy installation fails on the Virtual IPS engine. Bypass mode is not compatible with VLAN retagging. In network environments where VLAN retagging is used, normal mode is automatically enforced.

- c) From the **Virtual Resource** drop-down list, select the Virtual Resource element associated with the interface.
Select the same Virtual Resource in the properties of the Virtual Security Engine to add the **Virtual IPS engine** to the Master Security Engine.



Note

Only one Virtual Resource can be selected for each physical interface. If you want to add multiple Virtual Resources, add VLAN interfaces to the physical interface and select the Virtual Resource in the VLAN interface properties.

- 6) Click **OK**.
The physical interface is added to the interface list.
- 7) Click  **Save**.

Next steps

Continue the configuration in one of the following ways:


- Add VLANs to physical interfaces.
- Add IP addresses to the physical interfaces used for Master Security Engine communications.

Add VLAN interfaces to layer 3 interfaces of Master Security Engines

Master Security Engines can have two types of VLAN interfaces: VLAN interfaces for the Master Security Engine's own traffic, and VLAN interfaces that are used by the Virtual Security Engines hosted on the Master Security Engine.

The maximum number of VLANs for a single physical interface is 4094. The VLANs must also be defined in the configuration of the external switch or router to which the interface is connected.

On Master Security Engines that host Virtual IPS engines or Virtual Layer 2 Engines, the Virtual Security Engines can inspect traffic from VLAN interfaces without configuring VLAN tagging.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Master Engine, then select **Edit <element type>**.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click a physical interface, then select **New > VLAN Interface**.
- 4) To associate the VLAN interface with a Virtual Security Engine, select a Virtual Resource from the **Virtual Resource** drop-down list.

- 5) Define the VLAN interface properties.

**CAUTION**


The throughput for each VLAN interface must not be higher than the throughput for the physical interface to which the VLAN interface belongs.

**CAUTION**

Make sure that you set the interface speed correctly. When the bandwidth is set, the Master Security Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

**CAUTION**

The MTU for each VLAN interface must not be higher than the MTU for the physical interface to which the VLAN interface belongs.


- 6) Click **OK**.
The specified VLAN ID is added to the physical interface.
- 7) Click  **Save**.
Do not close the Engine Editor.

Next steps

Add IP addresses to the physical interfaces or VLAN interfaces for Master Security Engine system communications.

Add IPv4 and IPv6 addresses to Master Security Engine interfaces

You can add several IPv4 addresses to each Physical Interface or VLAN Interface that does not have a Virtual Resource associated with it.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Master Engine, then select **Edit <element type>**.
- 2) In the navigation pane on the left, browse to **Interfaces**.
- 3) Right-click a physical interface or a VLAN interface, then select **New > IPv4 Address** or **New > IPv6 Address**.

- 4) Click the **IPv4 Address** or **IPv6 Address** cell in the table, then enter the IP address for each node.

**Tip**

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 5) (IPv4 addresses only) If necessary, double-click the **Contact Address** cell in the table, then define the contact address for each node.
 - In the **Default** field at the top of the dialog box, enter the default contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
 - If components from some Locations cannot use the default contact address, click **Add** to define Location-specific contact addresses.
- 6) (IPv4 addresses only) Check the automatically filled-in **Netmask**, and adjust it as necessary.
- 7) (IPv6 addresses only) Check the automatically filled-in **Prefix Length**, and adjust it as necessary.
- 8) Click **OK**.
- 9) Click  **Save**.


Next steps

Continue the configuration in one of the following ways:

- If you are configuring a new Master Security Engine, or if you want to change the roles the different interfaces have in the configuration, select system communication roles for Master Security Engine interfaces.
- Otherwise, refresh the policy to transfer the configuration changes.

Select system communication roles for Master Engine interfaces

Select which Master Engine interfaces are used for particular roles in system communications.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Security Engine, then select **Edit <element type>**.
- 2) Browse to **Interfaces > Interface Options**.

3) In the **Interface Options** pane:

- a) From the **Primary** control IP address drop-down list, select the primary control IP address that the Master Engine uses for communications with the Management Server.



Note

We recommend that you do not use the IP address of an Aggregated Link interface as the primary or secondary control IP address of the Engine.

- b) (Optional, recommended) From the **Backup** control IP address drop-down list, select a backup control IP address that the Master Engine uses for communications with the Management Server if the primary control IP address fails.
- c) (Optional, Security Engine with Layer 3 Interfaces only) If the Master Engine is behind a device that applies dynamic NAT to outbound connections or in some other way blocks incoming connections, select **Node-Initiated contact to Management Server**.
When this option is selected, the engine opens a connection to the Management Server and maintains connectivity.
- d) (Master Engine Cluster Only) From the **Primary** heartbeat drop-down list, select the primary interface for communications between the nodes.
We recommend using a physical interface, not a VLAN interface. We strongly recommend that you do not direct any other traffic through this interface. A dedicated network helps guarantee reliable and secure operation.



CAUTION

Primary and backup heartbeat networks exchange confidential information. If dedicated networks are not possible, configure the cluster to encrypt the exchanged information.

- e) (Master Engine Cluster Only) From the **Backup** heartbeat drop-down list, select the backup heartbeat interface that is used if the primary heartbeat interface is unavailable.
It is not mandatory to configure a backup heartbeat interface, but we strongly recommend it. If heartbeat traffic is not delivered, the cluster cannot operate and traffic is disturbed. We strongly recommend that you use a dedicated interface for the backup heartbeat as well.
- f) In the **Default IP Address for Outgoing Traffic** field, select the IP address that the nodes use if they have to initiate connections through an interface that has no Node Dedicated IP address.

4) Click  **Save and Refresh**.

Next steps


Bind licenses to Master Engine elements.

Bind Master Security Engine licenses to Master Security Engine elements

You must manually bind Management Server POL-bound licenses to a specific Master Security Engine element.

Licenses are created based on the Management Server's proof-of-license (POL) code or based on the appliance's proof-of-serial (POS) code. POS-bound appliance licenses are automatically bound to the correct Master Security Engine element when the engine is fully installed. Virtual Security Engines do not require a separate license.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Administration**.
- 2) Browse to **Licenses > Engines**.
All installed licenses appear in the right pane.
- 3) Right-click a Management Server POL-bound license and select **Bind**.
The **Select License Binding** dialog box opens.
- 4) Select the node and click **Select**.
If you made a mistake, right-click the license and select **Unbind**.



CAUTION

When you install or refresh the policy on the engine, the license is permanently bound to that engine. Permanently bound licenses cannot be rebound to another engine without relicensing or deleting the engine element the license is bound to. Until you do that, the unbound license is shown as Retained.


Next steps


Add Virtual Security Engine elements.

Create Virtual Engines

Virtual Engine elements store the configuration information related to the Virtual Engines.

Selecting a Virtual Resource for the Virtual Engine automatically adds the Virtual Security Engine to the Master Engine where the Virtual Resource is used.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click **Engines** and select **New > Engine > Virtual Engine**.


- 3) In the **Name** field, enter a unique name.
- 4) Next to the **Virtual Resource** field, click **Select** and select a Virtual Resource on the Master Security Engine to which you want to add the Virtual Engine.
- 5) (Optional) In the **DNS IP Addresses** field, add one or more IP addresses.

DNS IP addresses are IP addresses of external DNS servers. Virtual Engines use these DNS servers to resolve Domain names to IP addresses. Virtual Engines need DNS resolution to contact services that are defined using URLs or domain names, and to resolve fully qualified domain names (FQDNs) used in policies. When DNS relay is configured, these DNS servers are used unless domain-specific DNS servers are specified in a DNS Relay Profile element.



Note

If you have defined NetLink-specific DNS IP addresses, adding DNS IP addresses overrides the NetLink-specific DNS IP addresses.

- To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
 - To define an IP address using a network element, click **Add** and select **Network Element**.
- 6) (Optional) Next to the **Category** field, click **Select** and select one or more categories.
 - 7) Click  **Save**.
Do not close the Engine Editor.

Next steps

Configure interfaces for the Virtual Engine.

Configuring physical interfaces for Virtual Engines

Physical interfaces for Virtual Security Engines represent interfaces allocated to the Virtual Security Engine in the Master Security Engine.

When you select the Virtual Resource for the Virtual Security Engine, physical interfaces are automatically created based on the interface configuration in the Master Security Engine properties. The number of physical interfaces depends on the number of interfaces allocated to the Virtual Security Engine in the Master Security Engine. You cannot create new physical interfaces for Virtual Engines. You can optionally change the automatically created physical interfaces. For detailed instructions, see the *Forcepoint Network Security Platform Product Guide*.

You can optionally change the automatically created physical interfaces in the Virtual IPS engine properties. For detailed instructions, see the *Forcepoint Network Security Platform Product Guide*.

If the configuration of the Master Security Engine allows it, you can add VLANs to physical interfaces on the Virtual Engine. If you do not want to add VLANs, add IP addresses to the physical interfaces.

Add VLAN interfaces to Virtual Security Engine interfaces

VLANs divide a single physical network link into several virtual links.

VLAN interfaces can only be added for Virtual Security Engines if the creation of VLAN interfaces for Virtual Engines is enabled in the Master Security Engine Properties. The maximum number of VLANs for a single physical interface is 4094. The VLANs must also be defined in the configuration of the external switch or router to which the interface is connected.



Note

You cannot add VLAN interfaces on top of other VLAN interfaces. Depending on the configuration of the Master Security Engine, you might not be able to create valid VLAN interfaces for the Virtual Security Engine. Contact the administrator who configured the Master Security Engine.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Virtual Engine, Virtual IPS engine, or Virtual Layer 2 Engine and select **Edit <element type>**.
- 2) In the navigation pane on the left, select **Interfaces**.
- 3) Right-click a physical interface and select **New > VLAN Interface**.
- 4) Define the VLAN interface properties.



CAUTION

The throughput for the Virtual Engine physical interface must not be higher than the throughput for the Master Security Engine interface that hosts the Virtual Engine. Contact the administrator of the Master Security Engine before changing this setting.



CAUTION

Make sure that you set the interface speed correctly. When the bandwidth is set, the Virtual Security Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

- 5) Click **OK**.
The specified VLAN ID is added to the physical interface.

Next steps

Continue the configuration in one of the following ways:


- (Virtual Engine only) If you do not want to add tunnel interfaces for a route-based VPN, add IP addresses directly to the physical interfaces.
- Otherwise, click **Save and Refresh** to transfer the configuration changes.

Add IP addresses for Virtual Engines

You can add one or more IPv4 and IPv6 addresses to a Physical Interface or VLAN Interface on a Virtual Engine. You can add both IPv4 and IPv6 addresses to the same interface.

Add IPv4 addresses to Virtual Engine interfaces

You can add one or more static IPv4 addresses for Virtual Engine interfaces.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Virtual Engine and select **Edit Virtual Engine**.
The Engine Editor opens.
- 2) In the navigation pane on the left, select **Interfaces**.
The **Interfaces** pane opens on the right.
- 3) Right-click a Physical Interface, VLAN Interface, or Tunnel Interface and select **New > IPv4 Address**.



Note

If you have added VLAN Interfaces to Physical Interfaces, add the IPv4 Addresses to the VLAN Interfaces.

- 4) Enter the **IPv4 Address**.




Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 5) If necessary, define the contact address information.
 - Enter the **Default** contact address. The default contact address is used by default whenever a component that belongs to another Location connects to this interface.
 - If components from some Locations cannot use the Default contact address, click **Exceptions** to define Location-specific contact addresses.
- 6) Check the automatically filled-in **Netmask** and adjust it as necessary.
- 7) Click **OK**.


Next steps

Continue the configuration in one of the following ways:

- Add IPv6 addresses.
- If you are creating a new Virtual Engine, or if you want to change the roles the different interfaces have in the configuration, select interface options for Virtual Engine interfaces.
- Otherwise, click  **Save and Refresh** to transfer the configuration changes.

Add IPv6 addresses to Virtual Engine interfaces

You can add one or more static IPv6 addresses for Virtual Engine interfaces.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Virtual Engine and select **Edit Virtual Engine**.
The Engine Editor opens.
- 2) In the navigation pane on the left, select **Interfaces**.
The **Interfaces** pane opens on the right.
- 3) Right-click a Physical interface and select **New > IPv6 Address** or right-click a VLAN Interface and select **New IPv6 Address**.
The **IP Address Properties** dialog box opens.



Note

If you have added VLAN Interfaces to Physical Interfaces, add the IPv6 Addresses to the VLAN Interfaces.

- 4) Enter the **IPv6 Address**.




Tip

To resolve the IP address from a DNS name, right-click the field, then select **Resolve From DNS Name**.

- 5) Check the automatically filled-in **Prefix Length** and adjust it if necessary by entering a value between 0-128.
The Network Address is automatically generated.
- 6) Click **OK**.

Next steps

Continue the configuration in one of the following ways:

- If you are creating a new Virtual Engine, or if you want to change the roles the different interfaces have in the configuration, select interface options for Virtual Engine interfaces.
- Otherwise, click  **Save and Refresh** to transfer the configuration changes.

Select additional options for Virtual Engine interfaces

In the Virtual Engine's interface options, you can select which IP addresses are used in particular roles.



Interface Options can only be configured for Virtual Engines. All communication between Virtual Engines and the SMC is proxied by the Master Engine. Virtual Engines do not have any interfaces for system communication.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Security Engine, then select **Edit <element type>**.
- 2) Browse to **Interfaces > Interface Options**.
- 3) Configure the settings.

Next steps

Continue the configuration in one of the following ways:


- Add loopback IP addresses for the Virtual Engine.
- If you are configuring a new Virtual Engine, click  **Save**, close the Engine Editor, then add routes for the Master Engine.
- Otherwise, click  **Save and Refresh** to transfer the configuration changes.


Create Virtual IPS engines

Virtual IPS elements store the configuration information related to the Virtual IPS engines.

Selecting a Virtual Resource for the Virtual Engine automatically adds the Virtual Security Engine to the Master Engine where the Virtual Resource is used.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click **Engines** and select **New > IPS > Virtual IPS**.
- 3) In the **Name** field, enter a unique name.
- 4) Next to the **Virtual Resource** field, click **Select** and select a Virtual Resource on the Master Security Engine to which you want to add the Virtual IPS.
- 5) (Optional) In the **DNS IP Addresses** field, add one or more IP addresses.
DNS IP addresses are IP addresses of external DNS servers. Virtual IPS engines use these DNS servers to resolve Domain names to IP addresses. Virtual IPS engines need DNS resolution to contact services that are defined using URLs or domain names, and to resolve fully qualified domain names (FQDNs) used in policies.
 - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.
 - To define an IP address using a network element, click **Add** and select **Network Element**.
- 6) (Optional) Next to the **Category** field, click **Select** and select one or more categories.

- 7) Click  **Save**.
Do not close the Engine Editor.

Next steps

Configure interfaces for the Virtual IPS engine.

Configuring physical interfaces for Virtual IPS engines

Physical interfaces for Virtual IPS engines represent interfaces allocated to the Virtual IPS engine in the Master Security Engine.

When you select the Virtual Resource for the Virtual IPS engine, physical interfaces are automatically created based on the interface configuration of the Master Security Engine. The number of physical interfaces depends on the number of interfaces allocated to the Virtual IPS engine in the Master Security Engine. It is not recommended to create new physical interfaces in the Virtual IPS engine properties, as they might not be valid.

You can optionally change the automatically created physical interfaces in the Virtual IPS engine properties. For detailed instructions, see the *Forcepoint Network Security Platform Product Guide*.

If the configuration of the Master Security Engine allows it, you can add VLANs to physical interfaces on the Virtual IPS engine. If you do not want to add VLANs, add IP addresses to the physical interfaces.

Add VLAN interfaces to Virtual Security Engine interfaces


VLANs divide a single physical network link into several virtual links.

VLAN interfaces can only be added for Virtual Security Engines if the creation of VLAN interfaces for Virtual Engines is enabled in the Master Security Engine Properties. The maximum number of VLANs for a single physical interface is 4094. The VLANs must also be defined in the configuration of the external switch or router to which the interface is connected.



Note

You cannot add VLAN interfaces on top of other VLAN interfaces. Depending on the configuration of the Master Security Engine, you might not be able to create valid VLAN interfaces for the Virtual Security Engine. Contact the administrator who configured the Master Security Engine.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Virtual Engine, Virtual IPS engine, or Virtual Layer 2 Engine and select **Edit <element type>**.
- 2) In the navigation pane on the left, select **Interfaces**.
- 3) Right-click a physical interface and select **New > VLAN Interface**.

- 4) Define the VLAN interface properties.

**CAUTION**

The throughput for the Virtual Engine physical interface must not be higher than the throughput for the Master Security Engine interface that hosts the Virtual Engine. Contact the administrator of the Master Security Engine before changing this setting.


**CAUTION**

Make sure that you set the interface speed correctly. When the bandwidth is set, the Virtual Security Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

- 5) Click **OK**.
The specified VLAN ID is added to the physical interface.

Next steps


Continue the configuration in one of the following ways:


- (Virtual Engine only) If you do not want to add tunnel interfaces for a route-based VPN, add IP addresses directly to the physical interfaces.
- Otherwise, click  **Save and Refresh** to transfer the configuration changes.


Add Virtual Layer 2 Engine elements

Virtual Layer 2 Engine elements store the configuration information related to the Virtual Layer 2 Engines.

Selecting a Virtual Resource for the Virtual Layer 2 Engine automatically adds the Virtual Layer 2 Engine to the Master Security Engine where the Virtual Resource is used.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click **Engines** and select **New > Layer 2 Engine > Virtual Layer 2 Engine**.
The Engine Editor opens.
- 3) In the **Name** field, enter a unique name.
- 4) Next to the **Virtual Resource** field, click **Select** and select a Virtual Resource on the Master Security Engine to which you want to add the Virtual Engine.
- 5) (Optional) In the **DNS IP Addresses** field, add one or more IP addresses of DNS servers that the Virtual Engine uses to resolve domain names. There are two ways to define IP addresses.
 - To enter a single IP address manually, click **Add** and select **IP Address**. Enter the IP address in the dialog box that opens.

- To define an IP address using a network element, click **Add** and select **Network Element**.
- 6) (Optional) Next to the **Category** field, click **Select** and select one or more categories.
 - 7) Click  **Save**.
Do not close the Engine Editor.

Next steps

Configure interfaces for the Virtual Layer 2 Engine.

Configuring Physical Interfaces for Virtual Layer 2 Engines

Physical interfaces for Virtual Layer 2 Engines represent interfaces allocated to the Virtual Layer 2 Engine in the Master Security Engine.

When you select the Virtual Resource for the Virtual Layer 2 Engine, physical interfaces are automatically created based on the interface configuration of the Master Security Engine. The number of physical interfaces depends on the number of interfaces allocated to the Virtual Layer 2 Engine in the Master Security Engine. It is not recommended to create new physical interfaces in the Virtual Layer 2 Engine properties, as they might not be valid.

You can optionally change the automatically created physical interfaces in the Virtual Layer 2 Engine properties. For detailed instructions, see the *Forcepoint Network Security Platform Product Guide*.

Add VLAN interfaces to Virtual Security Engine interfaces


VLANs divide a single physical network link into several virtual links.

VLAN interfaces can only be added for Virtual Security Engines if the creation of VLAN interfaces for Virtual Engines is enabled in the Master Security Engine Properties. The maximum number of VLANs for a single physical interface is 4094. The VLANs must also be defined in the configuration of the external switch or router to which the interface is connected.



Note

You cannot add VLAN interfaces on top of other VLAN interfaces. Depending on the configuration of the Master Security Engine, you might not be able to create valid VLAN interfaces for the Virtual Security Engine. Contact the administrator who configured the Master Security Engine.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Right-click a Virtual Engine, Virtual IPS engine, or Virtual Layer 2 Engine and select **Edit <element type>**.
- 2) In the navigation pane on the left, select **Interfaces**.

- 3) Right-click a physical interface and select **New > VLAN Interface**.
- 4) Define the VLAN interface properties.

**CAUTION**

The throughput for the Virtual Engine physical interface must not be higher than the throughput for the Master Security Engine interface that hosts the Virtual Engine. Contact the administrator of the Master Security Engine before changing this setting.


**CAUTION**

Make sure that you set the interface speed correctly. When the bandwidth is set, the Virtual Security Engine always scales the total amount of traffic on this interface to the bandwidth you defined. The bandwidth is scaled even if there are no bandwidth limits or guarantees defined for any traffic.

- 5) Click **OK**.
The specified VLAN ID is added to the physical interface.

Next steps

Continue the configuration in one of the following ways:

- (Virtual Engine only) If you do not want to add tunnel interfaces for a route-based VPN, add IP addresses directly to the physical interfaces.
- Otherwise, click  **Save and Refresh** to transfer the configuration changes.

Chapter 9

Configuring routing

Contents

- [Getting started with routing](#) on page 179
- [Add routers](#) on page 180
- [Add or view the default route](#) on page 181
- [Add static routes](#) on page 181

After creating the Security Engine elements and defining the interfaces, you can configure the basic routing.

Getting started with routing

Routes to directly connected networks are automatically added according to the interfaces defined for each Security Engine. You must manually add other routes or configure dynamic routing.

When the Security Engine reads routing definitions, it selects the most specific route and antispoofing definition it finds for each packet. The Security Engine:

- 1) Checks if there is a route defined for the specific destination IP address of the packet (Host elements).
- 2) Checks routes to the defined networks (Network elements).
- 3) Uses the default route (the Any network element) if no other route matches the packet's destination address. The default route typically leads to the Internet if the site has Internet access.

If there are overlapping definitions, the more specific one is considered first.

Engines

You must add the default route and routes through next-hop gateways to networks that are not directly connected to the Security Engine.

IPS engines and Layer 2 Engines

The routing information for IPS engines and Layer 2 Engines is only used for system communications. The inspected traffic is not routed. Inline interfaces are always fixed as port pairs: traffic that enters through one port is automatically forwarded to the other port. For Security Engines in the IPS and Layer 2 Engine roles, you only need to add a default route or additional routes if one or more SMC components are not directly connected and cannot be reached through the default gateway. If needed, you can add the default route and routes to internal networks that are not directly connected to the IPS or Layer 2 Engine if the networks cannot be reached through the default gateway.

Master Security Engines and Virtual Security Engines

Master Security Engines proxy all communication between Virtual Security Engines and other SMC components. You do not need to configure routing for Virtual Engines, Virtual IPS engines, or Virtual Layer 2 Engines in order for them to be managed by the SMC.

Antispoofing

Spoofing an IP address means using the IP address of a legitimate (internal) host to gain access to protected resources. The antispoofing configuration is automatically generated based on the routing information of Security Engines. By default, connection attempts with a source IP address from a certain internal network are only allowed through if they are coming from the correct interface as defined in the routing configuration. As the routing entry is needed for the communications to work, antispoofing rarely needs additional modifications. For more information, see the *Forcepoint Network Security Platform Product Guide*.


Elements used to configure routing


- Network elements represent a group of IP addresses.
- Router elements represent next-hop routers.
- NetLink elements are used for configuring Multi-Link routing. For more information, see the *Forcepoint Network Security Platform Product Guide*.

When interfaces are aggregated as one interface, those interfaces work together as a single interface. For aggregated interfaces in load-balancing mode, make sure that the connected switch supports the link aggregation control protocol (LACP), and that LACP is configured on the switch.

Add routers

A Router element represents a next-hop gateway's IP address in routing configurations.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.


- 1) Select  **Engine Configuration**.
- 2) Right-click a Security Engine, then select **Edit <element type>**.
- 3) Browse to **Routing**.
- 4) Right-click a Network element that is beneath an interface, then select **Add Router**.
- 5) Select **⋮ More actions > New > Router**.
- 6) Enter a name and the IP address of the router, then click **OK**.
- 7) Select the Router you created, then select **Add**.

- 8) Click **OK**.
- 9) Click  **Save**.

Add or view the default route


You can check which route is currently set as the default route for traffic leaving the Security Engine and set a new default route.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click a Security Engine, then select **Edit <element type>**.
- 3) Browse to **Routing**.




Tip


To view the full routing information for all interfaces, click  **Expand All**.

- 4) To show the default route, click **Show Default Route** in the **Routing Tools** pane.
The current default route or routes are shown in bold font.
- 5) To set the default route, right-click a router or NetLink, then select **Set as Default Route**.
The Any network element is added beneath the router and is set as the default route.
- 6) Click  **Save and Refresh**.

Add static routes

You can add a static route to a network in the routing configuration.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click a Security Engine, then select **Edit <element type>**.

3) Browse to **Routing**.



Tip

To view the full routing information for all interfaces, click  **Expand All**.

4) Right-click the router or NetLink through which you want to route traffic, select **Add**, then select a Network element.

For a route through a tunnel interface, add the Network element directly to the tunnel interface.

5) Click  **Save and Refresh**.

Initial configuration of Security Engine software

Contents

- Options for initial configuration on page 183
- Using plug-and-play configuration on page 184
- Using automatic configuration on page 188
- Using the Security Engine Configuration Wizard on page 190

After configuring the Security Engines in the SMC Client, apply the initial configuration of the Security Engine and contact the Management Server.

Options for initial configuration

You can configure the Security Engine software using plug-and-play configuration, automatic configuration, or the Security Engine Configuration Wizard.

Security Engine appliances come with Security Engine software installed. If you have an Security Engine license, you can configure the engine in any of the three Security Engine roles. If you have a license for a specific type of Security Engine with multiple purposes depending on the detailed configuration, you can only use the engine in that specific role.

There are three ways to configure the Security Engine software.

- **Plug-and-play configuration** — The Security Engine appliance automatically connects to the Installation Server, downloads the initial configuration file, then contacts the Management Server. You must have Security Engine appliances and proof-of-serial codes to use plug-and-play configuration. Plug-and-play configuration is only supported for single Security Engines with Layer 3 Interfaces that have a dynamic control IP address.



Note

There are special considerations when using plug-and-play configuration. For example, both the SMC and the Security Engines must be registered for plug-and-play configuration before you configure the engines. See Knowledge Base article [9662](#).

- **Automatic configuration** — You can configure Security Engine appliances automatically with a USB drive that contains the initial configuration files.
- **Security Engine Configuration Wizard** — If it is not possible to use plug-and-play configuration or automatic configuration, or you do not want to use them, you can use the Security Engine Configuration Wizard. You can use the Security Engine Configuration Wizard in two ways:
 - Connect a serial cable to the appliance and use the Security Engine Configuration Wizard on the command line.
 - Connect an Ethernet cable to the appliance and use the Security Engine Configuration Wizard in a web browser.

Before a policy can be installed on the appliance, you must configure some permanent and some temporary network settings for the engine.

To successfully complete the initial configuration:

- 1) The SMC must be installed.
- 2) The Security Engine elements (Engine, IPS, or Layer 2 Engine elements) must be defined in the SMC Client.
- 3) Engine-specific configuration information must be available from the Management Server. The required information depends on the configuration method.
 - For plug-and-play configuration, the initial configuration file for the Security Engine must be uploaded to the Installation Server.
 - For automatic configuration, you must have saved the initial configuration file on a USB drive.
 - For the Security Engine Configuration Wizard, you must have a one-time password for the engine.

The appliance must contact the Management Server before it can be operational.

Using plug-and-play configuration

In plug-and-play configuration, the Security Engine appliance automatically connects to the Installation Server, downloads the initial configuration file, then contacts the Management Server.

Prepare for plug-and-play configuration

To use plug-and-play-configuration, save the initial configuration file, then upload it to the Installation Server.

Steps

- 1) Register the SMC and Security Engine for plug-and-play configuration.
 - a) Go to <https://stonesoftlicenses.forcepoint.com>.
 - b) In the **License Identification** field, enter your SMC POL code, then click **Submit**.
 - c) Click **Register your appliances for Plug & Play installation on NGFW Installation Cloud**.
 - d) Enter your Security Engine appliance POS codes and your contact information, then click **Submit**.
- 2) In the SMC Client, select **Engine Configuration**.
- 3) Right-click the Engine for which you want to save the initial configuration, then select **Configuration > Save Initial Configuration**.

- 4) (Optional) If you already have a policy you want to use for the engine, click **Select**, then select a policy as the initial security policy.
The selected policy is automatically installed after the Security Engine has contacted the Management Server.
- 5) (Optional) Select **Enable SSH Daemon** to allow remote access to the Security Engine command line.
 - Enabling SSH in the initial configuration gives you remote command-line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server.
 - After the Security Engine is fully configured, you can enable or disable SSH access using the SMC Client. We recommend that you enable SSH access in the SMC Client when needed and disable the access again when you are finished. Make sure that your Access rules allow SSH access to the engines from the administrators' IP addresses only.

**CAUTION**

If you enable SSH, set the password for command-line access after the initial configuration either through the SMC Client or by logging on to the command line. When the password is not set, anyone with SSH access to the engine can set the password.

- 6) From the **Local Time Zone** drop-down list, select the time zone.
The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server's time after the engine is configured. For external operations, engines use the time zone of their geographical location.
- 7) From the **Keyboard Layout** drop-down list, select the keyboard layout used for the engine command line.
- 8) Select **Upload to Installation Server** to upload the initial configuration file automatically to the Installation Server.
- 9) Click **Close**.

Next steps

Configure the Security Engine software using plug-and-play configuration.

Configure Forcepoint Security Engine software using plug-and-play configuration

Connect the Security Engine to the network to start the plug-and-play configuration.

Before you begin

The SMC and Security Engine must be registered for plug-and-play configuration.

The initial configuration file for the Security Engine must be uploaded to the Installation Server.

The Security Engine appliance uses specific ports in a specific order when it tries to connect to the Installation Server.



Note

Use these default port settings in the properties of the corresponding engine interfaces that you have defined in the SMC Client. The initial configuration fails if the port settings on the physical appliance and the interface definitions in the engine element properties are not the same.

The Security Engine appliance first tries to contact the Installation Server through the mobile broadband modem if one is connected to a USB port. The mobile broadband modem and the corresponding Modem interface in the SMC Client must have the following settings:

- **Access Point Name** — internet
- **Phone number** — *99#
- **PIN Code** — <empty value>



Note

PIN code must also be disabled on the mobile broadband modem.

If attempts to connect to the Installation Server through the mobile broadband modem fail, the appliance tries to connect to the Installation Server through Ethernet port 0. If no mobile broadband modem is connected to the appliance, Ethernet port 0 is the only port that can be used.

Steps

- 1) (Optional) If you want to view the progress of the plug-and-play configuration, connect the appliance to a computer using the serial cable supplied with the appliance, and use a terminal console program to connect to the Security Engine appliance with these settings:
 - **Bits per second** — 115,200
 - **Data bits** — 8
 - **Parity** — None
 - **Stop bits** — 1.



Note

The serial console port speed is 115,200 bps in most Security Engine appliances. The speed is 9600 bps in older Security Engine appliance models. See the hardware guide for your Security Engine appliance model for more information.

- 2) (Optional) Plug an empty USB drive into one of the USB ports on the appliance if you want to save information about the progress of the plug-and-play configuration on a USB drive.
Saving the progress information on a USB drive can be useful, for example, for troubleshooting purposes.
- 3) Connect the network cables to the appliance. On specific Security Engine appliance models with wireless support, connect the antennas.

**Note**

The wireless port on Security Engine appliances cannot be used for connecting to the Installation Server.

- 4) Turn on the Security Engine appliance.

Result

The appliance automatically contacts the Installation Server. When the contact succeeds, the appliance downloads the initial configuration file from the Installation Server, then contacts the Management Server.

If plug-and-play configuration fails

If the plug-and-play configuration fails, check for possible causes and solutions.

**Note**

There are special considerations when using plug-and-play configuration. For example, both the SMC and the Security Engines must be registered for plug-and-play configuration before you configure the engines. See Knowledge Base article [9662](#).

If you plugged in a USB drive to the appliance, check the `sg_autoconfig.log` file on the USB drive.

If you see a connection refused error message, make sure that the Management Server IP address is reachable from the engine. Also check the settings that you have defined for the engine's interfaces in the SMC Client. The port numbers and settings must match the interface IDs and other interface settings in the SMC Client.

If attempts to connect to the Installation Server through the mobile broadband modem and Ethernet port 0 have failed, the appliance starts the connecting process again. It retries the ports in the same order (mobile broadband modem, then Ethernet port 0). If necessary, you can run the command `sg-reconfigure --stop-autocontact` on the engine command line to stop this process.

If plug-and play-configuration continues to fail, save the initial configuration file on a USB drive, then configure the engine using the automatic configuration method.

Using automatic configuration

In automatic configuration, you configure the engine automatically using a USB drive that contains the initial configuration files.

Prepare for automatic configuration

To use automatic configuration, save the initial configuration files on a USB drive.

When you save the initial configuration for an Security Engine cluster, the Management Server generates initial configuration files for all nodes at the same time. You can save all the initial configuration files on the same USB drive. When you apply the initial configuration to individual nodes, each node uses the initial configuration files on the USB drive in order.



Note

If you are configuring multiple Security Engine clusters, you must save the initial configuration files for each cluster on a separate USB drive.

Steps For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select **Engine Configuration**.
- 2) Right-click the Security Engine for which you want to save the initial configuration, then select **Configuration** > **Save Initial Configuration**.
- 3) (Optional) If you already have a policy you want to use for the engine, click **Select**, then select a policy as the initial security policy.
The selected policy is automatically installed on the engine after the engine has contacted the Management Server.
- 4) From the **Local Time Zone** drop-down list, select the time zone.
The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server's time after the engine is configured. For external operations, engines use the time zone of their geographical location.
- 5) From the **Keyboard Layout** drop-down list, select the keyboard layout used for the engine command line.

- 6) (Optional) Select **Enable SSH Daemon** to allow remote access to the engine command line.
 - Enabling SSH in the initial configuration gives you remote command-line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server.
 - After the engine is fully configured, you can set SSH access on or off using the SMC Client. We recommend that you enable the SSH access in the SMC Client when needed and disable the access again when you are finished. Make sure that your access rules allow SSH access to the engines from the administrators' IP addresses only.

**CAUTION**

If you enable SSH, set the password for command-line access after the initial configuration either through the SMC Client or by logging on to the command line. When the password is not set, anyone with SSH access to the engine can set the password.

- 7) Click **Save As**, then save the configuration file or files to the root directory of a USB drive. Do not change the default file name. Use a separate USB drive for each single Security Engine or Security Engine cluster.

**CAUTION**

Handle the configuration files securely. They include the one-time password that allows establishing trust with your Management Server.

- 8) Click **Close**.

Next steps

Configure the Security Engine software using automatic configuration.

Configure Forcepoint Security Engine software using automatic configuration

Automatic configuration is primarily intended to be used with Security Engine appliances, and might not work in all environments when you use your own hardware.

Before you begin

Connect a network cable to the interface that you have configured as the control interface.

If the automatic configuration does not work, use the Security Engine Configuration Wizard and import or enter the information manually.

When automatic configuration is used, Interface IDs are mapped to network interfaces on the engine in sequential order: Physical Interface ID 0 is mapped to eth0, Physical Interface ID 1 is mapped to eth1, and so forth.

**Note**

The imported configuration does not contain a password for the root account. You must set the password after the configuration has been successfully completed.

Steps

- 1) Make sure that you have a physical connection to the Security Engine appliance using a monitor and keyboard or a serial cable.
If you use a serial cable, use a terminal console program to connect to the Security Engine appliance with these settings:

- **Bits per second** — 115,200
- **Data bits** — 8
- **Parity** — None
- **Stop bits** — 1.



Note

The serial console port speed is 115,200 bps in most Security Engine appliances. The speed is 9600 bps in older Security Engine appliance models. See the hardware guide for your Security Engine appliance model for more information.

- 2) Insert the USB drive, then turn on the Security Engine appliance.
The Security Engine appliance starts, applies the initial configuration file that is saved on the USB drive, then makes initial contact to the Management Server.
 - If the automatic configuration fails, and you do not have a monitor connected, check `sg_autoconfig.log` on the USB drive.
 - If you see a connection refused error message, make sure that the Management Server IP address is reachable from the node.
- 3) When you see the prompt that indicates that the installation is finished, remove the USB drive, then press **Enter**.
The console opens and you are prompted to set the password for the root account.
- 4) Enter and confirm the password.

Result

When the appliance successfully contacts the Management Server, the configuration is complete.

Using the Security Engine Configuration Wizard

You can import or manually configure the settings for the Security Engine using either the command line or the web browser version of the Security Engine Configuration Wizard.

There are some limitations for the web browser version of the Security Engine Configuration Wizard.

- Only IPv4 addresses are supported.
- You must configure the SMC to use 256-bit security for communications.
- You cannot connect the appliance to the network through a mobile broadband modem.
- You cannot configure PPPoA interfaces.

- You cannot make the appliance follow FIPS standards.



Note

After completing the web browser version of the Security Engine Configuration Wizard, to make any changes to the configuration, you must start the configuration from the beginning. If you only want to make minor changes to the configuration, use the command-line version of the Security Engine Configuration Wizard.

Prepare for Security Engine Configuration Wizard configuration

To use the Security Engine Configuration Wizard, save the initial configuration file or write down the configuration information for manual configuration.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select ⓘ **Engine Configuration**.
- 2) Right-click the engine for which you want to save the initial configuration, then select **Configuration > Save Initial Configuration**.
- 3) To see the one-time passwords and fingerprints, click **View Details**.
If you plan to import the configuration information, you do not need to write down or copy these details.
 - a) From the **One-Time Password** field, write down or copy the one-time password for each engine node. Make a note of which password belongs to which engine node.
 - b) From the **Management Server Addresses** field, write down or copy the IP addresses of the Management Server.
 - c) (Optional) From the **Management Server Certificate Fingerprint (MD5)** or **Management Server Certificate Fingerprint (SHA-512)** field, write down or copy the fingerprint of the Management Server's certificate.
 - d) Click **Close**.
- 4) Select the other configuration options.
 - a) (Optional) If you already have a policy you want to use for the engine, click **Select**, then select a policy. The selected policy is automatically installed on the engine after the engine has contacted the Management Server.
 - b) From the **Local Time Zone** drop-down list, select the time zone.
The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server's time once the engine is configured. For external operations, engines use the time zone of their geographical location.

- c) From the **Keyboard Layout** drop-down list, select the keyboard layout used for the engine command line.
- d) Select **Enable SSH Daemon** to allow remote access to the engine command line.

Enabling SSH in the initial configuration gives you remote command-line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server. After the engine is fully configured, you can set SSH access on or off using the SMC Client. We recommend that you enable the SSH access in the SMC Client when needed and disable the access again when you are finished. Make sure that your Access rules allow SSH access to the engines from the administrators' IP addresses only.

**CAUTION**

If you enable SSH, set the password for command-line access after the initial configuration either through the SMC Client or by logging on to the command line. When the password is not set, anyone with SSH access to the engine can set the password.

- e) Under **Manual Installation**, click **Save As**, then save the configuration file.

**CAUTION**

Handle the configuration files securely. They include the one-time password that allows establishing trust with your Management Server.

**Tip**

Keep the **Save or Upload Initial Configuration** dialog box open while you configure the Security Engine software.

Next steps

Start the Security Engine Configuration Wizard.

Start the Security Engine Configuration Wizard on the command line

Start the Security Engine Configuration Wizard to configure settings for the Security Engine.

**Tip**

You can run the Security Engine Configuration Wizard at any time using the `sg-reconfigure` command on the engine command line.

Steps

- 1) If you are configuring a physical device, connect to the Security Engine appliance.
 - a) Connect the Security Engine appliance to a laptop or other client device using a serial cable.

- b) On the client device, use a terminal console program to connect to the Security Engine appliance with these settings:
- **Bits per second** — 115,200
 - **Data bits** — 8
 - **Parity** — None
 - **Stop bits** — 1.

**Note**

The serial console port speed is 115,200 bps in most Security Engine appliances. The speed is 9600 bps in older Security Engine appliance models. See the hardware guide for your Security Engine appliance model for more information.

- c) Connect the network cables to the Security Engine appliance.
- 2) Turn on the Security Engine appliance.
- 3) Start the Security Engine Configuration Wizard.

**Note**

On some appliance models, the Security Engine Configuration Wizard starts automatically.

- a) Press **Enter** to activate the console.
- b) When you are prompted to start the Security Engine Configuration Wizard, type **Y**, then press **Enter**.

- 4) Select **Exit**, and then press **Enter**:



Note

This step can be skipped, if `sg-reconfigure` command was run on the engine command line.

- a) For SMC managed engines, you can select one of the following options:
- i) **Import configuration via USB**
 - ii) **Manual configuration with sg-reconfigure**
- b) If you have selected the **Import configuration via USB** option, do the following:
- i) Select the USB drive, and then press **Enter**.
 - ii) Select the correct configuration file.
-
- #### Note
- The files are specific to each engine.
- iii) Highlight **Next**, then press **Enter**.
- c) If you have selected the **Manual configuration with sg-reconfigure** option, highlight **Next**, then press **Enter**.

Related tasks

[Configure general settings on the command line on page 194](#)

[Configure network interfaces on the command line on page 196](#)

[Contact the Management Server on the command line on page 197](#)

Configure general settings on the command line

The settings include console keyboard layout, time zone, and other optional settings.

Some of the settings might be filled in if you imported the configuration from a USB drive.

Steps

- 1) Set the console keyboard layout.
 - a) Highlight the entry field for **Keyboard Layout**, then press **Enter**.

- b) Highlight the correct layout, then press **Enter**.

The keyboard layout setting only applies to hardware that you connect to using a directly connected keyboard and monitor. This setting has no effect if you connect to the appliance through the serial console port or over the network using SSH.

If the keyboard layout that you want to use is not listed, select the best-matching available layout or select **US_English**.

**Tip**

Type the first letter of the keyboard layout to skip ahead in the list.

- 2) Set the time zone.

- a) Highlight the entry field for **Local Timezone**, then press **Enter**.

- b) Select the time zone from the list.

The time zone setting affects only the way the time is displayed on the engine command line. The actual operation always uses UTC time. The engine's clock is automatically synchronized with the Management Server's clock.

- 3) Set the rest of the settings.

- a) Enter the host name of the engine.

- b) Enter and confirm the password for the root user account.

This account is the only one with command-line access to the engine.

- c) (Optional) Highlight **Enable SSH Daemon**, then press the spacebar to allow remote access to the engine command line using SSH.

**Note**

Unless you have a specific reason to enable SSH access to the engine command line, we recommend leaving it disabled.

- d) (Optional) If you are required to follow FIPS standards, select **Restricted FIPS-compatible operating mode**.

This option enables the FIPS 140-3 cryptographic module.

**Note**

These options are only for environments that are required to follow FIPS standards. Do not enable these options unless you have a specific reason to do so.

- e) (Optional) Enter and confirm a bootloader password.

If you configure a bootloader password, you must enter the bootloader password to edit the options that appear in the bootloader menu of the Security Engine appliance.

- f) Highlight **Next**, then press **Enter**.

Configure network interfaces on the command line

The Security Engine Configuration Wizard can automatically detect which network cards are in use. You can also add interfaces manually.

Steps

- 1) Define the network interface drivers.

If the list is not populated automatically, use auto-detect.

- a) Highlight **Autodetect**, then press **Enter**.
- b) Check that the autodetected information is correct and that all interfaces have been detected.



Tip

You can use the Sniff option for troubleshooting the network interfaces. Select **Sniff** to run a network sniffer on that interface.

If autodetection fails, add network drivers manually.

- a) Highlight **Add**, then press **Enter**.
- b) Select the correct driver for your network card, then press **Enter**.

- 2) Map interfaces to the IDs you defined.

- a) Change the IDs as necessary to define how the interfaces are mapped to the interface IDs you defined for the engine element in the SMC Client.

For bypass interface modules, map the interface IDs of inline interfaces to even-odd pairs of ports on the appliance. For example, map Interface ID 1 to port eth2_0 and Interface ID 2 to port eth2_1.

- b) If necessary, highlight the **Media** column, then press **Enter** to change the settings to match those used by the device at the other end of the link.

Make sure that the speed/duplex settings of network cards are identical at both ends of each cable. For IPS and Layer 2 Engines, also make sure that the speed/duplex settings of the inline interfaces match the speed/duplex settings of both links within each inline interface pair.

- c) In the **Mgmt** column, highlight the correct interface for contact with the Management Server, then press the spacebar.



Important

The Management interface must be the same interface on which the control IP address for the corresponding element is configured in the SMC.

- d) (Optional, IPS only) Highlight **Initial Bypass**, then press **Enter** to temporarily set the IPS engine to the initial bypass state and define one or more soft-bypass interface pairs through which traffic flows.
Setting the appliance to the initial bypass state can be useful during IPS appliance deployment if bypass network interface pairs on the appliance are in Normal mode. Initial bypass allows traffic to flow through the IPS appliance until the initial configuration is ready and an IPS policy is installed on the appliance. Do not set the initial bypass state when the bypass network interface pairs are in Bypass mode.
- 3) (Modem interfaces only) Map the modem number to the IMEI of the modem.
 - a) Select **Setup modems**.
The first modem number is automatically mapped to the IMEI of the modem. You can optionally change the modem number.
 - b) Select **Stored**, then select **OK**.

Contact the Management Server on the command line

Provide the necessary information to allow the Security Engine to establish contact with the Management Server.

Before the engine can make initial contact with the Management Server, you activate the initial configuration on the engine. The initial configuration contains the information that the engine requires to connect to the Management Server for the first time.

If the initial configuration was imported from a USB drive, most of the options on the **Prepare for Management Contact** page are filled in.



Important

If there is a firewall between this engine and the Management Server, make sure that the intermediate engine's policy allows the initial contact and all subsequent communications.

Steps

- 1) If the control IP address is dynamic, select **DHCPv4**, **SLAAC (IPv6)**, or **DHCPv6**.



Note

The same protocol must be selected in the IP address properties in the SMC Client.

- 2) If the Security Engine uses PPP for management contact, define the PPPoE settings.
 - a) Highlight the **PPPoE v4 Settings** or **PPPoE v6 Settings** as required, and then press **Enter**.
 - b) On the **PPPoE Settings** dialog-box, fill in the account details according to the information you have received from your service provider.
 - c) Highlight **OK**, then press **Enter**.

- 3) If the Security Engine uses a modem for management contact, define the modem settings.
 - a) Highlight **Settings**, then press **Enter**.
 - b) On the **Modem Settings** page, enter the PIN code, then select **OK**.
The same PIN code must be configured in the properties of the modem interface in the SMC Client.
 - c) Highlight **OK**, then press **Enter**.
- 4) If the control IP address is static, select **Enter node IP address manually**, then define the IP address of the Security Engine node.
 - a) In the **IP Address** field, enter the IP address.
 - b) In the **Netmask/Prefix Length** field, enter the netmask (IPv4) or prefix length (IPv6) of the network.
 - c) If the Management Server is not in a directly connected network, enter the IP address of the next-hop gateway in the **Gateway to management** field.
- 5) If the control IP address is on a VLAN interface, select **Use VLAN, Identifier**, then enter the VLAN ID.
- 6) Select **Contact** or **Contact at Reboot**, then press the spacebar.
- 7) Enter the Management Server IP address or FQDN in the **IP address/FQDN** field.
- 8) (Optional) Enter the DNS server IP address for engine to use if Management Server was specified using FQDN.
- 9) Enter the Management Server one-time password.

**Note**

The one-time password is engine-specific and can be used only for one initial connection to the Management Server. After initial contact has been made, the engine receives a certificate from the SMC for identification. If the certificate is deleted or expires, repeat the initial contact using a new one-time password.

- 10) (Optional) To use 256-bit encryption for the connection to the Management Server, select **256-bit Security Strength**, then press the spacebar.

**Note**

256-bit encryption must also be enabled for the Management Server in the SMC.

- 11) (Optional) Highlight **Edit Fingerprint**, then press **Enter**. Fill in the Management Server's certificate fingerprint (also shown when you saved the initial configuration).
Filling in the certificate fingerprint increases the security of the communications.
- 12) Highlight **Finish**, then press **Enter**.
The engine now tries to make initial contact with the Management Server. The progress is displayed on the command line. If you see a connection refused message, make sure that the one-time password is correct

and the Management Server IP address is reachable from the node. Save a new initial configuration if you are unsure about the password.



Note

If the initial management contact fails for any reason, you can start the configuration again with the `sg-reconfigure` command.

Result

After you see notification that Management Server contact has succeeded, the engine installation is complete and the engine is ready to receive a policy.

The engine element's status changes in the SMC Client from **Unknown** to **No Policy Installed**. The connection state is **Connected**, indicating that the Management Server can connect to the node.

Next steps

Install a policy on the engine using the SMC Client

Related information

[Default communication ports](#) on page 239

Start the Security Engine Configuration Wizard in a web browser

Start the Security Engine Configuration Wizard to configure settings for the Security Engine.

Steps

- 1) If you are configuring a physical Security Engine appliance, connect the appliance to a laptop or other client device.
 - a) Connect an Ethernet cable from the client device to the physical port labeled LAN (generally port number 2) on the Security Engine appliance. If the appliance does not have the port labeled LAN, then use the port `eth0_1`. Also, you can do the following:
 - If the Security Engine appliance does not have the port `eth0_1`, then use the port `eth1_0`.
 - If you use a non-modular interfaces, then use the port `eth1`.
 - b) Connect the other network cables to the Security Engine appliance.
- 2) Turn on the Security Engine appliance.
- 3) To start the web browser version of the Security Engine Configuration Wizard, open a web browser on the client device, then connect to `https://169.254.169.169`. It might take some time for the web page to load.
- 4) When the Security Engine Configuration Wizard offers a web browser client certificate, accept the certificate.

Configure general settings in a web browser

The settings include keyboard layout, timezone, and other optional settings.

Steps

- 1) On the **Welcome** screen, select **Start**.
- 2) Select **I agree to the terms and conditions**, then select **Next**.
- 3) Enter and confirm a password for the root user account, then select **Next**.
- 4) Select the configuration method, then select **Next**.
 - If you have a .cfg configuration file, select **Import**.
 - If you want to enter the settings manually, select **Manual**.
- 5) If you selected **Import**, import the .cfg configuration file.
 - a) Select **Select File**, browse for the .cfg configuration file, then select the file.
 - b) Select **Import Configuration**.
 - c) After the file has been imported, select **Next**.
- 6) On the **Basic Information** screen, enter the required information, then select **Next**.



Note

If you imported a configuration file, some of the information might be filled in automatically.

- a) Enter the host name for the appliance.
- b) Select the time zone to use on the appliance.

The time zone setting affects only the way the time is displayed on the engine command line. The actual operation always uses UTC time. The engine's clock is automatically synchronized with the Management Server's clock.
- c) Select the keyboard layout to use when working on the command line of the engine.

The keyboard layout setting only applies to hardware that you connect to using a directly connected keyboard and monitor. This setting has no effect if you connect to the appliance through the serial console port or over the network using SSH.
- d) To allow connections to the engine using SSH, select **Enable SSH Access**.



Note

Unless you have a specific reason to enable SSH access to the engine command line, we recommend leaving it disabled.

Configure network interfaces in a web browser

The Security Engine Configuration Wizard can automatically detect which network cards are in use.



Note

If you imported a configuration file, the information is filled in automatically.

Steps

- 1) To change the mapping of the interface IDs, select **Change the Mapping**.
 - a) Change the IDs as necessary to define how the interfaces are mapped to the interface IDs that you defined for the engine element in the SMC Client.

For bypass interface modules, map the interface IDs of inline interfaces to even-odd pairs of ports on the appliance. For example, map Interface ID 1 to port eth2_0 and Interface ID 2 to port eth2_1.
 - b) If necessary, select the **Speed/Duplex** column to change the settings to match those used by the device at the other end of the link.

Make sure that the speed/duplex settings of network cards are identical at both ends of each cable. For IPS and Layer 2 Engines, also make sure that the speed/duplex settings of the inline interfaces match the speed/duplex settings of both links within each inline interface pair.
- 2) (Modem interfaces only) Map the modem number to the IMEI of the modem.
 - a) Select **Setup modems**.

The first modem number is automatically mapped to the IMEI of the modem. You can optionally change the modem number.
 - b) Select **Stored**, then select **OK**.
- 3) Select **Save**, then select **Next**.
- 4) Select the interface to use for management connectivity.

The Management interface must be the same interface on which the control IP address for the corresponding element is configured in the SMC.
- 5) If the Management interface is on a VLAN interface, enter the VLAN ID.
- 6) Set the interface type.
 - If the interface is a dynamic interface that receives its IP address from a DHCP Server, select **Dynamic IPv4 Address (DHCP)**.
 - If the interface is dynamic interface that receives its IP address from a PPPoE Server, select **Dynamic IPv4 Address or Dynamic IPv6 Address (PPPoE Server)**, select **PPPoE Settings**, then fill in the account details according to the information you have received from your service provider.
 - If the interface is a static interface, select **Static**, then enter the IP address and netmask.
- 7) Select **Next**.
- 8) Enter the IP address of the Management Server.

- 9) If the Management Server is not located in a directly-connected network, enter the IP address of the next-hop gateway in the **Default Gateway** field.
- 10) Select **Next**.

Contact the Management Server in a web browser

Provide the necessary information to allow the Security Engine to establish contact with the Management Server.



Note

If you imported a configuration file, the information is filled in automatically.



Important

If there is a firewall between this engine and the Management Server, make sure that the intermediate engine's policy allows the initial contact and all subsequent communications.

Steps

- 1) Select when you want the appliance to make contact with the Management Server.
 - **At the end of this session** — The appliance makes contact after you confirm the entered information.
 - **After the appliance restarts** — The appliance makes contact after you confirm the entered information and the appliance restarts.
- 2) Enter the one-time password generated by the SMC.



Note

The one-time password is engine-specific and can be used only for one initial connection to the Management Server. After initial contact has been made, the engine receives a certificate from the SMC for identification. If the certificate is deleted or expires, repeat the initial contact using a new one-time password.

- 3) (Optional if you set the appliance to attempt to make contact at the end of this session) Enter the SHA-512 fingerprint generated by the SMC.

Filling in the certificate fingerprint increases the security of the communications.
- 4) If the Security Engine uses a modem for management contact, define the modem settings.
 - a) Highlight **Settings**, then press **Enter**.
 - b) On the **Modem Settings** page, enter the PIN code, then select **OK**.

The same PIN code must be configured in the properties of the modem interface in the SMC Client.
 - c) Highlight **OK**, then press **Enter**.
- 5) Select **Next**.

- 6) Review the configuration summary, then continue the configuration in one of the following ways:
 - If you set the initial contact to be made at the end of this session, select **Finish and Contact the Management Server**.
 - If you set the initial contact to be made after the appliance restarts, select **Apply Configuration and Finish**.
- 7) If you set the initial contact to be made after the appliance restarts, after the configuration has been applied, select **Finish and Turn Off**.
When you turn the appliance back on, the appliance makes the initial contact.
- 8) If you set the initial contact to be made at the end of this session, and if you did not previously enter the SHA-512 fingerprint generated by the SMC, verify that the fingerprint shown matches, then select **Finish and Proceed**.



Note

If you do not select **Finish and Proceed** within the timeout, the **Reject** option is used, and you must make the initial contact again.

Result

After the initial contact has been made successfully, the Security Engine Configuration Wizard shuts down and the Ethernet port used to connect to the appliance is released for regular use.

If you set the initial contact to be made at the end of this session, a notification is shown in the web browser. If you set the initial contact to be made after the appliance restarts, the notification is not shown.

The engine element's status changes in the SMC Client from **Unknown** to **No Policy Installed**. The connection state is **Connected**, indicating that the Management Server can connect to the node.



Note

If the status remains **Unknown**, run the Security Engine Configuration Wizard again, and review the settings. All settings can be changed, except for the engine role. To change the engine role, you must first reset the appliance to factory default settings.

Next steps


After the appliance has been configured, install a policy on the engine using the SMC Client.

Troubleshoot using the Security Engine Configuration Wizard in a web browser

If you are unable to make contact with the Management Server, you can generate an sglInfo file to send to [Forcepoint Customer Hub](#), or you can reset the appliance to factory default settings and try configuring the appliance again.

Steps

- 1) Generate an sglInfo file that contains information for [Forcepoint Customer Hub](#) to use.
 - a) In the top right corner of the screen, select **⚙ > Information for support**.

- b) Select **Get Information for support**.
 - c) Select **Download**, then save the `sginfo.tar.gz` file to your client device.
- 2) Reset the appliance to factory default settings.
- a) In the top right corner of the screen, select  > **Reset to factory default settings**.



Note

This option is available only after you get to the **Configuration Method** screen.

- b) Select **Confirm Reset**.



Note

You do not receive confirmation that the reset has completed.

Creating and installing policies

Contents

- Create and install a Engine Policy on page 205
- Install a predefined policy on IPS engines and Layer 2 Engines on page 206



After successfully applying the initial configuration and establishing contact between the Security Engines and the Management Server, the Security Engine is in the initial configuration state. Now you can create and install policies for access control or inspecting traffic.

In addition to the rules in the policy, other configuration information, such as interface definitions and routing information, is also transferred to the Security Engine when you install a policy.

Create and install a Engine Policy

Create a basic policy for engines.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Right-click **Policies**, then select **New > Engine Policy**.
- 3) Enter a name for the Policy.
- 4) Select **Firewall Template** as the template.
Only the Firewall Template is available because you have not created other templates yet.
- 5) Click **OK**.
- 6) Configure the Access and NAT rules as required for your environment.
To add a rule, right-click the green row, then select **Rule > Add Rule**. Add the matching criteria and the action to be taken for matching traffic. For more information, see the *Forcepoint Network Security Platform Product Guide*.
- 7) Click  **Save and Install** to save the policy and transfer the changes to the Security Engine.
- 8) Select one or more Security Engines, then click **Add**.
- 9) Leave **Validate Policy Before Upload** selected to validate the rules in the policy.
Issues found in the policy are displayed in the tab that shows the progress of the policy installation.

- 10) Click OK.

Install a predefined policy on IPS engines and Layer 2 Engines


To be able to inspect traffic, the Security Engine must have a policy installed. Installing a predefined policy provides an easy way to begin using the system. You can then fine-tune the policy as needed.


Default Policy elements for IPS engines and Layer 2 Engines

| Element type | Default element name | Description |
|--------------------------------|--|---|
| IPS Template Policy | High-Security IPS Template | <p>IPS Template Policy that uses Inspection rules from the High-Security Inspection Template.</p> <p>A Template Policy containing the predefined Access rules necessary for the IPS engine to communicate with the SMC and some external components.</p> <p>The High-Security IPS Template Policy provides an easy starting point for determining what kinds of rules your system needs.</p> |
| | Medium-Security IPS Template | IPS Template Policy that uses Inspection rules from the Medium-Security Inspection Policy. |
| IPS Policy | Customized High-Security Inspection IPS Policy | Example of a customized IPS Policy that uses Inspection rules from the Customized High-Security Inspection Template. Used in testing Security Engine in the IPS role at ICSA Labs and NSS Labs. |
| | Default IPS Policy | <p>Basic IPS Policy that uses Inspection rules from the High-Security Inspection Template. Can be used as a starting point for creating a customized IPS Policy.</p> <p>The Default IPS Policy does not add any rules to the rules defined in the IPS Template. It allows you to install the predefined rules in the IPS Template on the IPS engine right after installation. (Template Policies cannot be installed on the Security Engine.)</p> |
| Layer 2 Engine Template Policy | Layer 2 Engine Template | <p>A Template Policy that contains the predefined Access rules necessary for the Layer 2 Engine to communicate with the SMC and some external components.</p> <p>The Layer 2 Engine Template uses Inspection rules from the No Inspection Policy. The rules in the No Inspection Policy do not enforce inspection.</p> |
| | Layer 2 Engine Inspection Template | <p>A Template Policy that is based on the Layer 2 Engine Template.</p> <p>The Layer 2 Engine Inspection Template uses Inspection rules from the High-Security Inspection Template. The Layer 2 Engine Inspection Template enables deep inspection for all traffic.</p> |

| Element type | Default element name | Description |
|-------------------|--|--|
| Inspection Policy | No Inspection Policy | Suitable for Engine deployments, in which only packet filtering is needed. Disables deep packet inspection. |
| | Medium-Security Inspection Template | For Engines, Layer 2 Engines, inline IPS deployments in asymmetrically routed networks, and IPS deployments in IDS mode. Terminates reliably identified attacks and logs Situations that have some degree of inaccuracy. Low risk of false positives. |
| | High-Security Inspection Template | For Engine, Layer 2 Engine, and inline IPS use. Extended inspection coverage and evasion protection. Not for asymmetrically routed networks. Terminates reliably identified attacks, and Situations that have some inaccuracy. Moderate false positive risk. |
| | Customized High-Security Inspection Policy | This policy is an example of a highly customized Inspection Policy for network environments in which unconditional inspection coverage and evasion protection are required. The risk of false positives is high in production use. |

The default policy elements might change when you import and activate a dynamic update package. You cannot modify any of the default policy elements, but you can make your own policies based on a copy of a default policy. For more information, see the *Forcepoint Network Security Platform Product Guide*.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Engine Configuration**.
- 2) Browse to **Policies > IPS Policies** or **Policies > Layer 2 Engine Policies**.
- 3) Right-click a predefined policy, then select **Install Policy**.
- 4) Select one or more Security Engines, then click **Add**.
- 5) Click **OK**.
A new tab opens to show the progress of the policy installation.
- 6) Check that the policy installation is successful.

Part IV

Maintenance

Contents

- [Upgrading licenses on page 211](#)
- [SMC maintenance on page 215](#)
- [SMC Appliance maintenance on page 221](#)
- [Upgrading Security Engines on page 227](#)

To maximize the benefit of Security Engine, upgrade the SMC and Security Engine regularly.

Chapter 12

Upgrading licenses

Contents

- Getting started with upgrading licenses on page 211
- Upgrade licenses manually on page 211
- Install licenses on page 212
- Check Security Engine licenses on page 212

You must upgrade licenses if you upgrade the SMC, the SMC Appliance, or the Security Engines to a new major release.

Getting started with upgrading licenses

When you installed the SMC, the SMC Appliance, or the Security Engines for the first time, you installed licenses that work with all versions up to that particular version. Each license indicates the highest version for which the license is valid, but the license is also valid for all lower software versions.


A change in the first two digits of the version number indicates a major release (for example, from 1.2.3 to 1.3.0, or from 1.2.3 to 2.0.0). If only the last number changes, the existing license is also valid for the higher software version.


You can view and download your current licenses online at <https://stonesoftlicenses.forcepoint.com>. You can also upgrade the licenses.

Upgrade licenses manually

If you have not enabled automatic license upgrades, upgrade licenses manually through the SMC Client.

Licenses are valid for any older software versions in addition to the version indicated on the license. You can upgrade the licenses at any time without affecting the system's operation.


Steps  For more details about the product and how to configure features, click **Help** or press **F1**.



- 1) Select  **Administration**.
- 2) Select **Licenses**, then browse to the type of licenses that you want to upgrade.
- 3) Select the license that you want to upgrade.
Details about the selected license open in the **Info** pane.
- 4) In the **Info** pane, copy the license information to the clipboard in one of the following ways:

- From the **Proof of License** field, copy the POL code.
 - From the **Proof of Serial** field, copy the POS code.
- 5) Go to <https://stonesoftlicenses.forcepoint.com>.
 - 6) In the **License Identification** field, paste the POL or POS code, then click **Submit**.
 - 7) Under the license information, click **Update**.
 - 8) Enter any information needed for the upgrade request, then select the license files to update.
 - 9) To send the license request, click **Submit**.
A confirmation page opens, showing the details of your request. The licenses are available for download on the license page.

Install licenses

After you have upgraded the licenses, install the license in the SMC Client.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, select  **Settings** > **Install Licenses**.
- 2) Select the license files and click **Install**.
- 3) Select  **Administration**.
- 4) Browse to **Licenses** > **All Licenses**.
- 5) Check that the licenses have now been correctly upgraded to the new version.



Tip


When you only upgrade the software version in the license, old licenses are automatically replaced.

Check Security Engine licenses

After installing the upgraded Security Engine licenses, check the license information.

When you upgrade licenses, the old licenses are automatically replaced with the new licenses.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Administration**.
- 2) Browse to **Licenses > Engines**, depending on the type of licenses you have.
The licenses and their status are displayed.
- 3) Verify that all Security Engines are correctly licensed.
- 4) If any Security Engines are not correctly licensed, you might need to upgrade or generate the licenses again.

Next steps

Continue the upgrade in one of the following ways:

- Upgrade the Security Engines remotely through the Management Server.
- Upgrade the Security Engines on the engine command line.

Chapter 13

SMC maintenance

Contents

- [Upgrading the SMC](#) on page 215
- [Uninstall the SMC](#) on page 219

When there is a new version available, upgrade the SMC before upgrading Security Engines.



Note

For information about SMC Appliance maintenance, see the SMC maintenance chapter.

Upgrading the SMC

You can upgrade SMC components without uninstalling the previous version.

Before upgrading, read the [Release Notes](#).

It is important to upgrade the SMC components before upgrading Security Engines. An older SMC version might not be able to recognize the newer Security Engine version and can generate an invalid configuration for them. The Management Server can control several older versions of the Security Engine. See the release notes for version-specific compatibility information.



CAUTION

All SMC components (Management Server, SMC Client, Log Server, and the optional Web Access Server) must use the same software version to be able to work together. Plan ahead before upgrading the components. If you have multiple Management Servers and Log Servers, you must upgrade each server separately.

The Security Engines do not require a continuous connection to the SMC and they continue to operate normally during the SMC upgrade. The Security Engines temporarily store their logs locally if the Log Server is unavailable and then send them to the Log Server when it is available again.

For more detailed instructions, see the *Forcepoint Network Security Platform Product Guide*.

Configuration overview

Follow these general steps to upgrade the SMC.

- 1) Obtain the installation files and check the installation file integrity.
- 2) (If automatic license upgrades have been disabled) Upgrade the licenses.
- 3) Upgrade all components that work as parts of the same SMC.

- 4) (Multiple Management Servers only) Synchronize the management database between the Management Servers.
- 5) Upgrade the SMC Clients that are installed locally on workstations.
If you are using the SMC Client in a web browser through Web Access, there is no need to upgrade.

Related concepts

Getting started with upgrading licenses on page 211

Related tasks

Upgrade SMC servers on page 216

Upgrade SMC servers

You can upgrade SMC servers without uninstalling the previous version. A change in the Management platform, such as a new operating system or different hardware, requires reinstalling the SMC.




CAUTION

All SMC components (Management Server, SMC Client, Log Server, and the optional Web Access Server) must use the same SMC software version to work together. If you have multiple Management Servers or Log Servers, you must upgrade each server separately.

The same installer works with all SMC components, including locally-installed SMC Clients.

If you have multiple Management Servers or Log Servers, you can upgrade them in any order. Management Servers are automatically isolated from database replication during the upgrade. There is no need to explicitly isolate the Management Servers before upgrading.

If you are upgrading from a very old version of the SMC, you might have to upgrade to an intermediate version first before upgrading to the latest version. See the [Release Notes](#).

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Log on to the operating system with administrator rights in Windows or as the root user in Linux.
- 2) Start the Installation Wizard from a `.zip` file or the Installation DVD.
Decompress the `.zip` file.
 - On Windows, the executable is `\Forcepoint_SMC_Installer\Windows-x64\setup.exe`
 - On Linux, the executable is `/Forcepoint_SMC_Installer/Linux-x64/setup.sh`

If the DVD is not automatically mounted in Linux, use the following command:

```
mount /dev/cdrom /mnt/cdrom
```

- 3) Select the language for the installation, then click **OK**.
The language that you select is also set as the default language of the SMC Client.

- 4) Read the information on the **Introduction** page, then click **Next**.

**Tip**

Click **Previous** to go back to the previous page, or click **Cancel** to close the wizard.

- 5) Select **I accept the terms of the License Agreement**, then click **Next**.
- 6) To accept the installation directory that was automatically detected, click **Next**.
The Installation Wizard displays the components to be upgraded.
- 7) (Management Server only, optional) To save a copy of the current installation that you can revert to after the upgrade, select **Save Current Installation**, then click **Next**.
- 8) (Management Server only) Select whether to back up the server, then click **Next**.
 - To create a backup that can be used and viewed without a password, select **Yes**.
 - To create a password-protected backup, select **Yes, encrypt the backup**. You are prompted for the password as you confirm the selection.
 - If you already have a recent backup of the Management Server, select **No**.
- 9) Check that the information in the **Pre-Installation Summary** is correct, then click **Install**.
- 10) (Optional) When the upgrade is complete, click the links in the notification to view the reports of changes the installer has made.
The report opens in your web browser.
- 11) When the installation has completed, click **Done**.

Next steps

- 1) Upgrade any SMC components that run on other computers (for example, additional Management Servers or Log Servers).
- 2) (Multiple Management Servers only) Synchronize the management database between the Management Servers.


Synchronize databases between the active Management Server and additional Management Servers


You must synchronize the configuration information manually through the SMC Client after upgrading the Management Servers or after restoring a backup.

Before you begin

There must be a route between the SMC Client and the Management Servers. If there is no route between the SMC Client and the Management Servers, you cannot send a command through the SMC Client HA Administration dialog box.

Manual management database synchronization is primarily meant for resynchronizing the databases after upgrading the SMC. We do not recommend using manual database synchronization unless you have a specific need to do so.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Connect to the active Management Server using the SMC Client.
- 2) Select  **Dashboard > Servers / Devices Dashboard**.
- 3) Browse to **Management Server**.
- 4) Right-click the management server, and then select **SMC Client HA Administration**.
- 5) If the SMC Client is in a different network than the additional Management Server, select the **Location** from which to send the command.
- 6) For each additional Management Server that you want to synchronize:
 - a) Right-click the Management Server, then select **Replication > Full Database Replication**.
 - b) When prompted to confirm the replication, click **Yes**.
All existing configurations on the additional Management Server are overwritten.
 - c) Click **OK** to acknowledge the completion of the synchronization, then wait for the Management Server to restart.

Result

After the Management Server has restarted, its Replication Status is updated in the **SMC Client HA Administration** dialog box. Click **Close** to close the **SMC Client HA Administration** dialog box.

Uninstall the SMC

Usually, it is not necessary to uninstall the SMC, but you can do so if needed.



Note

If you have several SMC components installed on the same computer, you cannot uninstall the SMC components one by one.

By default, the SMC is installed in the following directories:

- Windows — `C:\Program Files\Forcepoint\SMC`
- Linux — `/usr/local/forcepoint/smc`

There is a `.stonegate` directory in each user's home directory in the operating system, which contains the SMC Client configuration files. These files are not automatically deleted. You can delete them manually after the uninstallation.

The `sgadmin` account is deleted during the uninstallation of the SMC.



Tip

Back up the Management Server and the Log Server to an external system before uninstalling the SMC if you want to preserve the stored data.

Uninstall the SMC in Windows

Use this process to uninstall the SMC in a Windows environment.

Steps

- 1) Open the list of installed programs through the Windows Control Panel, right-click **Forcepoint Security Management Center**, then select **Uninstall/Change**.
You can also run the script `<installation directory>\uninstall\uninstall.bat`
- 2) When the uninstaller opens, click **Uninstall**.

Result

All SMC components are uninstalled.

Uninstall the SMC in Linux

Use this process to uninstall the SMC in a Linux environment.

You can uninstall the SMC in graphical mode or in non-graphical mode.

Steps

- 1) Stop the Security Management Center components on the computer.

- 2) Run the uninstaller script.
 - To uninstall in graphical mode, run the script `<installation directory>/uninstall/uninstall.sh`.
 - To uninstall in non-graphical mode, run the script the script `<installation directory>/uninstall/uninstall.sh -nodisplay`.
- 3) (Graphical mode only) When the uninstaller starts, click **Uninstall**.

Result

All SMC components are uninstalled.

SMC Appliance maintenance

Contents

- Getting started with SMC Appliance maintenance on page 221
- Patching and upgrading the SMC Appliance on page 222
- Roll back the SMC Appliance to the previous version on the command line on page 226

The SMC Appliance has a specific patching process that keeps the SMC software, operating system, and appliance firmware up-to-date.

Getting started with SMC Appliance maintenance

SMC Appliance patches can include improvements, enhancements, and upgrades for the SMC software, the operating system, and the appliance firmware.

The SMC Appliance patch (SAP) format is specific to the SMC Appliance. The SAP numbering is appended to the version number. Patch digests are calculated using an SHA-512 hash and signed with an ECDSA key.

There are two kinds of SMC Appliance patches:

- Hotfix patches include improvements and enhancements for the current SMC Appliance version. Hotfix patch files use the letter P as a separator between the version number and the patch number. Example: 7.3.0.1P01
- Upgrade patches upgrade the SMC Appliance to a new version. Upgrade patch files use the letter U as a separator between the version number and the patch number. Example: 7.3.0.1U01

When you install a patch, a configuration backup and a file system snapshot are automatically created for the SMC Appliance. The backup and snapshot allow you to roll back the SMC Appliance to its previous configuration if needed. If the patch activation fails, the appliance reverts to the snapshot automatically. The file system of the SMC Appliance has two partitions: an active partition and an alternative partition. Some patches update the alternative partition. You can toggle between the partitions to roll back the SMC Appliance upgrade.



Note

SMC Appliance patches apply only to the SMC Appliance hardware or to SMC Appliance software installed on a virtualization platform. SMC components installed on third-party platforms do not offer a patching and rollback feature that includes the SMC software, the operating system, and the appliance firmware.

You can patch and upgrade the SMC Appliance remotely using the SMC Client or using the appliance maintenance and bug remediation (AMBR) patching utility on the command line.

Configuration overview

- 1) Check for new SMC Appliance patches.
There is no automatic notification when new SMC Appliance patches are available. We recommend checking for new SMC Appliance patches once a month.
- 2) Obtain the patch files.
 - You can use the SMC Client or the AMBR utility to automatically download patch files directly into the SMC Client or onto the SMC Appliance.
 - In environments without Internet connectivity, you must manually download patch files, then import them into the SMC Client or transfer them to the SMC Appliance.
- 3) (If automatic license upgrades have been disabled) Upgrade the licenses.
- 4) Upgrade the SMC Clients that are installed locally on workstations.
If you are using the SMC Client in a web browser through Web Access, there is no need to upgrade.

Related concepts

[Getting started with upgrading licenses](#) on page 211

Patching and upgrading the SMC Appliance

To introduce improvements and enhancements for the current SMC Appliance version, install a hotfix patch. To upgrade the SMC Appliance, install an SMC Appliance upgrade patch.

Before upgrading, read the [Release Notes](#).

It is important to upgrade the SMC Appliance before upgrading the engines. An old SMC version might not be able to recognize the new version engines and can generate an invalid configuration for them. The Management Server can control several older versions of engines. See the release notes for version-specific compatibility information.

Patch or upgrade the SMC Appliance in the SMC Client


You can use the SMC Client to patch or upgrade the SMC Appliance. In some certified environments, you must use the SMC Client to install SMC Appliance patches.

Before you begin

In environments without Internet connectivity, you must download the SMC Appliance patch file from <https://update.stonesoft.com/download/appliance/patches/>, then transfer the file to a location that is accessible from the SMC Client.

Installing some SMC Appliance patches might restart the SMC Appliance. The Restart Required column in the SMC Client indicates whether the appliance must restart as part of the installation. You can use the SMC Client to install SMC Appliance patches regardless of whether the installation requires restarting the SMC Appliance.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Administration**.
- 2) Browse to **SMC Appliance Patches**.
- 3) Download or import SMC Appliance patches.
 - To download an individual patch, right-click a patch for which the **State** column shows Available, then select **Download SMC Appliance Patch**.
 - To automatically download all available SMC Appliance patches, right-click **SMC Appliance Patches**, then select **Download SMC Appliance Patches**.
 - To import SMC Appliance patches that you manually downloaded, right-click **SMC Appliance Patches**, select **Import SMC Appliance Patches**, browse to the SMC Appliance patch file, then click **Import**.
- 4) Install a hotfix patch or an upgrade patch.
 - To patch the current SMC Appliance version, right-click a hotfix patch file, then select **Activate**.
 - To upgrade the SMC Appliance to a new version, right-click an upgrade patch file, then select **Activate**.

Result

The SMC Appliance patch is installed on the SMC Appliance.

If you installed an SMC Appliance upgrade patch, the installation process restarts the appliance and installs the patch. When the upgrade is finished, the appliance restarts again.

Patch or upgrade the SMC Appliance on the command line

You can use the appliance maintenance and bug remediation (AMBR) patching utility to patch or upgrade the SMC Appliance on the command line.

Before you begin

In environments without Internet connectivity, you must download the SMC Appliance patch file from <https://update.stonesoft.com/download/appliance/patches/>, then transfer the files to the SMC Appliance.

If you do not have physical access to the SMC Appliance, use SSH to access the SMC Appliance remotely.



Note

In FIPS mode, SSH access to the SMC Appliance command line is not supported.

You must have SMC Appliance Superuser permissions to log on to the SMC Appliance command line. Administrators with unrestricted permissions (superusers) are allowed to log on to the SMC Appliance command line only if there are no administrators with Console Superuser permissions.

Use `sudo` if you need elevated privileges. For a list of available `sudo` commands, enter the following command:

```
sudo -l
```

Steps

- 1) From the command line, log on to the SMC Appliance.
- 2) To update the list of available remote patches from the download server, enter the following command:

```
sudo ambr-query -u
```

- 3) To show all local and remote patches, enter the following command:

```
sudo ambr-query -a
```

- 4) To automatically download a patch, or to load a patch that you manually downloaded, enter the following command:

```
sudo ambr-load <patch>
```



Note

If you manually downloaded the patch and transferred it to the SMC Appliance, append the command with the `-f` option and specify the full path to the patch file.

Example:

```
sudo ambr-load -f /var/tmp/7.3.0.0P001.sap
```

- 5) To activate the patch, enter the following command:

```
sudo ambr-install <patch>
```

Result

The SMC Appliance patch is installed on the SMC Appliance.

If you installed an SMC Appliance upgrade patch, the installation process restarts the appliance and installs the patch. When the upgrade is finished, the appliance restarts again.

Related reference

[Security Management Center commands on page 247](#)

Unload SMC Appliance patches on the command line

When you load patches, they are copied to the patch storage on the SMC Appliance. Use the unload command to remove patches that have been loaded but not installed from the patch storage on the SMC Appliance.



Note

To revert changes made by a patch that has been installed, roll back the SMC Appliance to the previous version.

Steps

- 1) From the command line, log on to the SMC Appliance.
- 2) To unload the patch, enter the following command:

```
sudo ambr-unload <patch>
```

Result

The patch is removed from the patch storage on the SMC Appliance. To verify that it has been removed, enter the following command:

```
ambr-query
```



Note

Patch files that you manually transferred to the SMC Appliance are removed from the patch storage, but are not deleted from the file system of the SMC Appliance. You must manually delete these patch files.

Roll back the SMC Appliance to the previous version on the command line

To revert changes made by a patch that has been installed, you can roll back the SMC Appliance to the previous configuration if needed.



Note

When you roll back the SMC Appliance, configuration changes made after the current version was installed are lost. We recommend rolling back as a recovery option only for a short time after an upgrade.

Steps

- 1) From the command line, log on to the SMC Appliance.
- 2) Enter the following command:

```
sudo smca-system toggle
```

- 3) Restart the SMC Appliance.

Result

When the SMC Appliance restarts, the previous SMC Appliance configuration is in use.

Upgrading Security Engines

Contents

- [How engine upgrades work](#) on page 227
- [Obtain Security Engine upgrade files](#) on page 229
- [Prepare Security Engine upgrade files](#) on page 230
- [Upgrade Security Engines remotely](#) on page 231
- [Upgrade engines locally](#) on page 233

When a new version of Forcepoint Network Security Platform introduces features that you want to use, upgrade the Security Engines.

How engine upgrades work

You can remotely upgrade engines using the SMC Client or locally on the engine command line.

The upgrade package is imported to the Management Server manually or automatically. Upgrade package digests are calculated using an SHA-512 hash and signed with an ECDSA key.

Before the import, the Management Server verifies the digital signature of the upgrade package using a valid Trusted Update Certificate. The signature must be valid for the import to succeed. Verification might fail for the following reasons:

- The SMC version is out of date. Upgrade the SMC before upgrading the engines.
- A signature is invalid or missing in the upgrade files. Obtain an official upgrade package.

After the upgrade package has been imported, you can apply it to selected engines through the SMC Client. Before the upgrade is installed on the engines, the Management Server again verifies the digital signature of the upgrade package. The engines also verify the digital signature of the upgrade package before the upgrade is installed.

The engines have two alternative partitions for the software. When you install a new software version, it is installed on the inactive partition and the current version is preserved. This configuration allows rollback to the previous version in case there are problems with the upgrade. If the engine is not able to return to operation after the upgrade, it automatically changes back to the previous software version at the next restart. You can also change the active partition manually.

You can upload and activate the new software separately. For example, you can upload the upgrade during office hours but activate it during a service window.

The currently installed working configuration (routing, policies) is stored separately and is not changed in an upgrade or a rollback. Although parts of the configuration can be version-specific (for example, if system communications ports are changed), the new software version can use the existing configuration. Possible version-specific adjustments are made when you refresh the policy after the upgrade.

Lifecycle models

There are two types of Forcepoint Network Security Platform releases:

- Long-Term Support (LTS) — Long-Term Support versions are major versions of Forcepoint Network Security Platform that are maintained for at least two years from the release date.
- Feature Stream (FS) — Feature Stream versions are major versions of Forcepoint Network Security Platform that introduce new features and enhancements. Support for Feature Stream versions is discontinued when a new major version of Forcepoint Network Security Platform is available.

We recommend using the most recent Long-Term Support version of Forcepoint Network Security Platform if you do not need any features from a later Feature Stream version.

For more information about the Forcepoint Network Security Platform lifecycle policy, see Knowledge Base article [10192](#).

Limitations

It is not possible to upgrade between a 32-bit version and a 64-bit version of the software. If you are running the software on third-party hardware, you can reinstall the software using the other version. In clusters, 32-bit and 64-bit nodes cannot be online simultaneously. Appliances support only the software architecture version that they are preinstalled with.

You cannot upgrade Virtual Security Engines directly. To upgrade Virtual Security Engines, you must upgrade the Master Security Engine that hosts the Virtual Security Engines.

What do I need to know before I begin?

The SMC must be up to date before you upgrade the engines. An old SMC version might not be able to recognize the new version engines and can generate an invalid configuration for them. The Management Server can control several older versions of engines. See the [Release Notes](#) for version-specific compatibility information.

During a cluster upgrade, it is possible to have the upgraded nodes online and operational side by side with the older version nodes. This way, you can upgrade the nodes one by one while the other nodes handle the traffic. However, you must upgrade all nodes to the same version as soon as possible, as prolonged use with mismatched versions is not supported.

The current engine version is displayed on the **General** tab in the **Info** pane when you select the engine. If the **Info** pane is not shown, select **≡ Menu > View > Panels > Info**.

Beginning from version 5.9, all Forcepoint Network Security Platform licenses include the anti-malware feature by default.

Configuration overview

Follow these general steps to upgrade engines:

- 1) (Manual download of engine upgrade files) Prepare the installation files.
- 2) (Manual license updates) Update the licenses.
- 3) Upgrade the engines.

Obtain Security Engine upgrade files

If the Management Server is not set up to download engine upgrades automatically or if you want to upgrade engines locally, download the installation files manually.

Check the installation file integrity using the MD5 or SHA-1 file checksums. Windows does not have MD5 or SHA-1 checksum programs by default, but there are several third-party programs available.

Steps

- 1) Go to <https://support.forcepoint.com>.
- 2) Enter your license code or log on using an existing user account.
- 3) Select **Downloads**.
- 4) Under **Network Security**, click the version of the Security Engine software that you want to download, then select the type of installation file to download.
 - The `.zip` file is used in the remote upgrade on all supported platforms. It can also be used for a local upgrade from a USB drive or a non-bootable DVD.
 - The `.iso` file allows you to create a bootable installation DVD for a local upgrade on platforms that have an optical drive.
- 5) On your local computer, change to the directory that contains the files to be checked.
- 6) (Linux only) Generate a checksum of the file using one of the following commands, where `filename` is the name of the installation file:
 - `sha1sum filename`
 - `sha256sum filename`
 - `sha512sum filename`

For Windows, see the documentation for the third-party checksum program.

Example:

```
$ sha1sum sg_engine_1.0.0.1000.iso
869aec7dc39321aa2e0cfaf7fafdb8f sg_engine_1.0.0.1000.iso
```

- 7) Compare the displayed output to the checksum on the website.



CAUTION

Do not use files that have invalid checksums. If downloading the files again does not help, contact [Forcepoint Customer Hub](#) to resolve the issue.


Next steps

Prepare Security Engine upgrade files.

Related tasks[Upgrade Security Engines remotely](#) on page 231[Upgrade engines locally](#) on page 233

Prepare Security Engine upgrade files

Prepare the Security Engine upgrade files depending on the type of files you downloaded and how you plan to upgrade.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) To prepare a downloaded `.zip` file for a remote upgrade, follow these steps.
 - a) Log on to the SMC Client and select **Menu > File > Import > Import Engine Upgrades**.
 - b) Select the engine upgrade (`sg_engine_version_platform.zip`) file and click **Import**.

**Note**

The Management Server verifies the digital signature of the `.zip` file before importing it. The signature must be valid for the import to succeed. If the verification fails, an error message is shown. Verification failure can result from an out-of-date SMC version or an invalid or missing signature.

The status bar at the bottom of the SMC Client window shows the progress of the import.

- 2) To prepare a downloaded `.zip` file for a local upgrade, copy the file to the root directory of a USB drive or a DVD.
- 3) To prepare a downloaded `.iso` file for a local upgrade, create the installation DVD for the engines with a DVD burning application that can correctly read and burn the DVD structure stored in the `.iso` images. If the end result is a DVD file with the original `.iso` file on it, the DVD cannot be used for installation.

Next steps

Continue in one of the following ways:

- If your license does not support the version that you are upgrading to, upgrade or generate licenses.
- Upgrade the engines remotely through the Management Server.
- Upgrade the engine locally at the engine site.

Upgrade Security Engines remotely

The Management Server can remotely upgrade Security Engine components that it manages.

Before you begin


Read the [Release Notes](#) for the new version, especially the required SMC version and any other version-specific upgrade issues that might be listed. To access the release notes, select **Administration > Other Elements > Engine Upgrades**. Select the type of Security Engine you are upgrading. A link to the release notes is included in the upgrade file's information. If the Management Server has no Internet connectivity, you can find the release notes at <https://support.forcepoint.com/s/article/Documentation-Featured-Article>.




CAUTION

If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the Engine when you upgrade to version 6.3 or later, the Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article [14093](#).

You can upgrade several Security Engines of the same type in the same operation. However, we recommend that you upgrade clusters one node at a time and wait until an upgraded node is back online before you upgrade the other nodes. Clusters operate normally throughout the upgrade when the upgrade is done in stages. However, it is recommended to upgrade all nodes in the cluster to the same version as soon as possible. Prolonged use with mismatched versions is not supported. It is not possible to have 32-bit and 64-bit Security Engines online in the cluster at the same time.

Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Select  **Dashboard > Engines Dashboard**.
- 2) Expand the nodes of the Security Engine that you want to upgrade.
- 3) Right-click the node that you want to upgrade, then select **Commands > Go Offline**.
- 4) (Optional) Enter an **Audit Comment** to be shown in the audit log entry that is generated when you send the command to the Security Engine.
- 5) When prompted to confirm that you want to set the node offline, click **Yes**.
The node goes offline shortly.

- 6) When the node is offline, right-click the node, then select **Upgrade Software** or **Configuration > Upgrade Software** depending on your selection.

**Note**

You cannot upgrade Virtual Engines directly. To upgrade Virtual Engines, you must upgrade the Master Engine that hosts the Virtual Engines.

- 7) From the **Operation** drop-down list, select the type of operation that you want to perform:
 - Select **Remote Upgrade (transfer + activate)** to install the new software and reboot the node with the new version of the software.
 - Select **Remote Upgrade (transfer)** to install the new software on the node without an immediate reboot and activation. The node continues to operate with the currently installed version until you choose to activate the new version.
 - Select **Remote Upgrade (activate)** to reboot the node and activate the new version of the software that was installed earlier.

**CAUTION**

To avoid an outage, do not activate the new configuration simultaneously on all nodes of a cluster. Activate the new configuration one node at a time, and proceed to the next node only after the previous node is back online.

- 8) If necessary, add or remove Security Engines in the **Target** list.
All Security Engines in the same Upgrade Task must be of the same type.

- 9) Click **Select** next to the **Engine Upgrade** field, select the upgrade file, then click **OK**.

If you choose to activate the new configuration, you are prompted to acknowledge a warning that the node will be rebooted. A new tab opens showing the progress of the upgrade. The time the upgrade takes varies depending on the performance of your system and the network environment. The Security Engine is automatically rebooted and brought back online.

The upgrade overwrites the inactive partition and then changes the active partition. To undo the upgrade, use the `sg-toggle-active` command or the Security Engine's boot menu to change back to the previous software version on the other partition. This change can also happen automatically at the next reboot if the Security Engine is not able to successfully return to operation when it boots up after the upgrade.

**Note**

The Management Server verifies the digital signature of the upgrade package before installing it. The signature must be valid for the upgrade to succeed. If the verification fails, an error message is shown. Verification failure can result from an out-of-date SMC version or an invalid or missing signature.

Upgrade engines locally

You can upgrade the engines on the engine command line.

Before you begin

Upgrading locally requires a physical connection to the engine using a monitor and keyboard or a serial cable.



CAUTION

If McAfee Endpoint Intelligence Agent (McAfee EIA) is configured on the Engine when you upgrade to version 6.3 or later, the Engine node is returned to the initial configuration state and stops processing traffic. You must remove the McAfee Endpoint Intelligence Agent (McAfee EIA) configuration and refresh the policy before you upgrade to version 6.3 or later. For more information, see Knowledge Base article [14093](#).

During a Engine Cluster or Master Security Engine cluster upgrade, the upgraded nodes can be online and operational side by side with the older version nodes. However, you must upgrade all nodes to the same version as soon as possible, as prolonged use with mismatched versions is not supported.

There are two ways to upgrade engines locally:

- If the hardware has a DVD drive (a USB DVD drive can be used) and you have an installation DVD, you can upgrade from an installation DVD.
- You can upgrade from a `.zip` file on a USB drive or on a DVD.

Upgrade from an installation DVD

You can upgrade the engines to the latest version from a DVD that was shipped to you, or from a DVD that you have created from an `.iso` image that you downloaded from the Forcepoint website.

Steps

- 1) Log on to the node as root with the password you set for the engine (you can set the password through the SMC Client).
- 2) Insert the DVD into the engine's DVD drive.
- 3) Restart the node from the DVD with the command `reboot` (recommended) or by cycling the power (if you cannot log on).
You are promoted to select the upgrade type.
- 4) Enter `1` to upgrade the existing installation and press **Enter** to continue.
The upgrade process starts.
- 5) When the process is finished, eject the DVD and press **Enter** to restart.

- 6) If the command-line version of the Security Engine Configuration Wizard opens, configure the engine in the same way as after the first installation.
You can also use the web browser version of the Security Engine Configuration Wizard.
- 7) When the upgrade is finished, right-click the node in the SMC Client and select **Commands > Go Online**.
A confirmation dialog box opens.
- 8) (Optional) Enter an **Audit Comment** to be shown in the audit log entry that is generated when you send the command to the engine.
- 9) Click **Yes**.

**Note**

If you are upgrading a cluster, start the upgrade on the next node only when the upgraded node is back online.

Related tasks

[Using the Security Engine Configuration Wizard on page 190](#)

Upgrade from a `.zip` file

You can use a `.zip` file to upgrade the engine software locally on the engine command line.

Steps

- 1) Log on to the node as root with the password set for the engine (you can set the password through the SMC Client).
- 2) Insert the USB drive or the DVD.
- 3) Run the command `sg-reconfigure`.
The Security Engine Configuration Wizard opens.
- 4) Select **Upgrade** and press **Enter**.
- 5) Select the source media where the upgrade file is located.
- 6) Select **OK**.
The software is upgraded.

**Note**

The Security Engine verifies the digital signature of the upgrade package before installing it. The verification can take several minutes. The signature must be valid for the upgrade to succeed. If the verification fails, an error message is shown. Verification failure can result from an out-of-date Security Engine software version or an invalid or missing signature.

- 7) When prompted, press **Enter**.
The engine restarts with the new version.

Appendices

Contents

- [Default communication ports on page 239](#)
- [Command line tools on page 247](#)
- [Installing SMC Appliance software on a virtualization platform on page 275](#)
- [Installing Forcepoint Security Engine on a virtualization platform on page 277](#)
- [Installing Forcepoint Security Engine software on third-party hardware on page 281](#)
- [Installing the SMC with external certificate management on page 289](#)
- [Example network \(Security Engines with Layer 3 Interfaces\) on page 301](#)
- [Example network \(IPS\) on page 307](#)
- [Cluster installation worksheet instructions on page 311](#)

Default communication ports

Contents

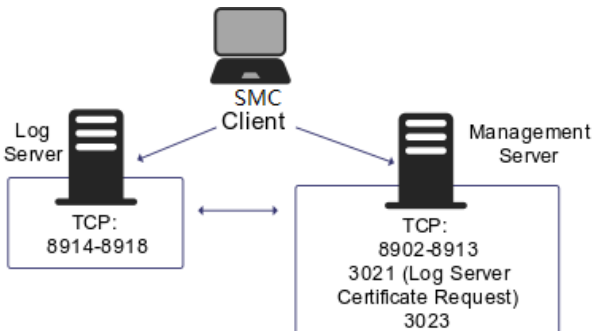
- Forcepoint Security Management Center ports on page 239
- Security Engine ports on page 242
- Security Engine in the Factory Default State on page 246

There are default ports used in connections between SMC components and default ports that SMC components use with external components.

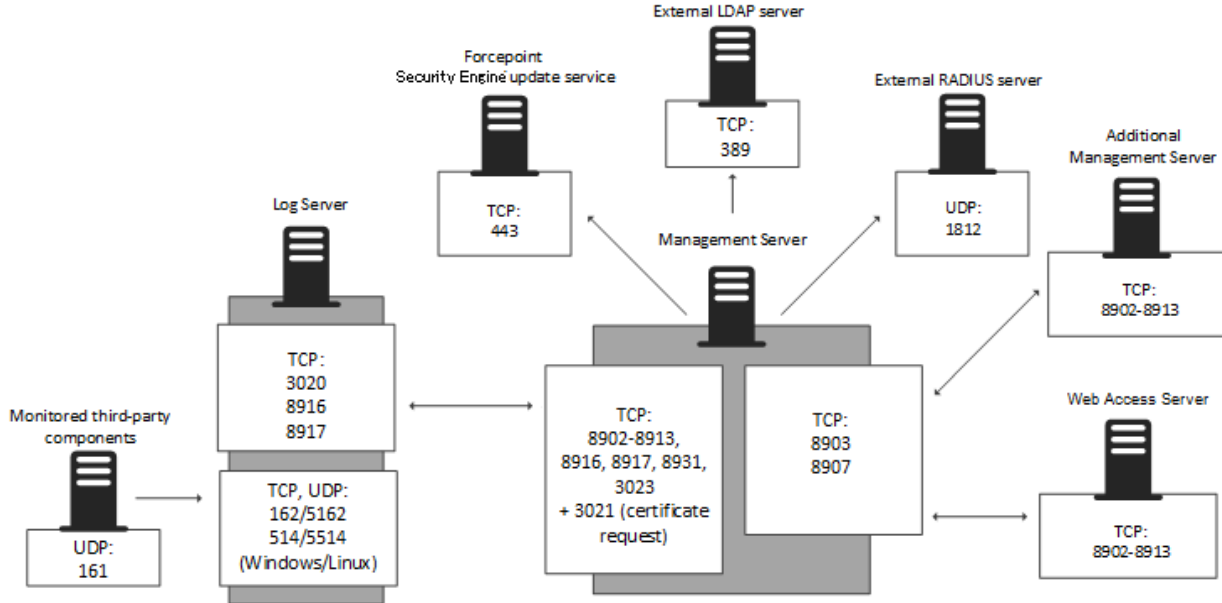
Forcepoint Security Management Center ports

The most important default ports used in communications to and from SMC components are presented in the following illustrations.

Destination ports for basic communications within the SMC



Default destination ports for optional SMC components and features





This table lists the default ports SMC uses internally and with external components. Many of these ports can be changed. The names of corresponding default Service elements are also included for your reference.

SMC default ports

| Listening host | Port/protocol | Contacting hosts | Service description | Service element name |
|-------------------------------|--------------------------------------|---|--|------------------------------|
| Additional Management Servers | 8902- 8913/TCP | Management Server | Database replication (push) to the additional Management Server. | SG Control |
| DNS server | 53/UDP, 53/TCP | SMC Client, Management Server, Log Server | DNS queries. | DNS (UDP) |
| LDAP server | 389/TCP | Management Server | External LDAP queries for display/editing in the SMC Client. | LDAP (TCP) |
| Log Server | 162/UDP, 5162/UDP | Monitored third-party components | SNMPv1 trap reception from third-party components. Port 162 is used if installed on Windows, port 5162 if installed on Linux. | SNMP (UDP) |
| Log Server | 514/TCP, 514/UDP, 5514/TCP, 5514/UDP | Monitored third-party components | Syslog reception from third-party components. Port 514 is used if installed on Windows, port 5514 if installed on Linux. | Syslog (UDP) [Partial match] |
| Log Server | 2055/UDP | Monitored third-party components | NetFlow or IPFIX reception from third-party components. Port 2055 is used in both Windows and Linux. | NetFlow (UDP) |

| Listening host | Port/protocol | Contacting hosts | Service description | Service element name |
|----------------------------------|----------------|--|---|--------------------------------------|
| Log Server | 3020/TCP | Log Server, Web Access Server, Security Engines | Alert sending from the Log Server and Web Access Server. Log and alert messages; monitoring of block lists, connections, status, and statistics from Security Engines. | SG Log |
| Log Server | 8914-8918/TCP | SMC Client | Log browsing. | SG Data Browsing |
| Log Server | 8916-8917/TCP | Log Server, Web Access Server | Database replication (push) to the Log Server; Log browsing on the Web Access Server. | SG Data Browsing (Web Access Server) |
| Management Server | 3021/TCP | Log Server, Web Access Server | System communications certificate request/renewal. | SG Log Initial Contact |
| Management Server | 8902-8913/TCP | SMC Client, Log Server, Web Access Server | Monitoring and control connections. | SG Control |
| Management Server | 3023/TCP | Additional Management Servers, Log Server, Web Access Server | Log Server and Web Access Server status monitoring. Status information from an additional Management Server to the active Management Server. | SG Status Monitoring |
| Management Server | 8903, 8907/TCP | Additional Management Servers | Database replication (pull) to the additional Management Server. | SG Control |
| Active Management Server | 8922/TCP | Backup SMC server | PostgreSQL database replication used in SMC HA configurations. | SG HA Replication |
| Management Server | 8082/TCP | Client API | Connection from the Client API to Management Server. | - |
| Management Server | 8085/TCP | Web Access clients | Communication for using Web Access. | HTTPS |
| Monitored third-party components | 161/UDP | Log Server | SNMP status probing to external IP addresses. | SNMP (UDP) |
| NTP server | 123/TCP or UDP | SMC Appliance | Receiving NTP information. | NTP |
| RADIUS server | 1812/UDP | Management Server | RADIUS authentication requests for administrator logon. The default ports can be edited in the properties of the RADIUS Server element. | RADIUS (Authentication) |
| Security Engine update service | 443/TCP | SMC servers | Update packages, engine upgrades, and licenses. | HTTPS |
| SMC Appliance | 161/UDP | Third-party components | Requesting health and other information about the SMC Appliance. | SNMP |
| Update servers | 443/TCP | SMC Appliance | Receiving appliance patches and updates. | HTTPS |

| Listening host | Port/protocol | Contacting hosts | Service description | Service element name |
|--|-------------------|--------------------|--|------------------------------|
| SMC Appliance | 22/TCP | Terminal clients | SSH connections to the command line of the SMC Appliance.  Note SSH is not available in FIPS mode. | SSH |
| Syslog server | 514/UDP, 5514/UDP | Log Server | Log data forwarding to syslog servers. The default ports can be edited in the LogServerConfiguration.txt file. | Syslog (UDP) [Partial match] |
| Engine, Layer 2 Engine, IPS, Master Engine | 22/TCP | SMC Appliance | Contacting engines and moving SMC Appliance backups off the appliance. | SSH |
| Third-party components | 2055/UDP | Log Server | NetFlow or IPFIX forwarding to third-party components. Port 2055 is used in both Windows and Linux. | NetFlow (UDP) |
| Third-party components | 162/UDP | SMC Appliance | Sending SNMP status probing to external devices. | SNMP |
| Third-party components | 445/TCP | SMC Appliance | Moving SMC Appliance backups off the appliance.  Note You cannot use CIFS in FIPS mode. | CIFS |
| Web Access Server | 8083/TCP | Web Access clients | Communication for using Web Access. | HTTPS |

Security Engine ports

The most important default ports used in communications to and from Security Engines and Master Engines are presented in the following illustrations.

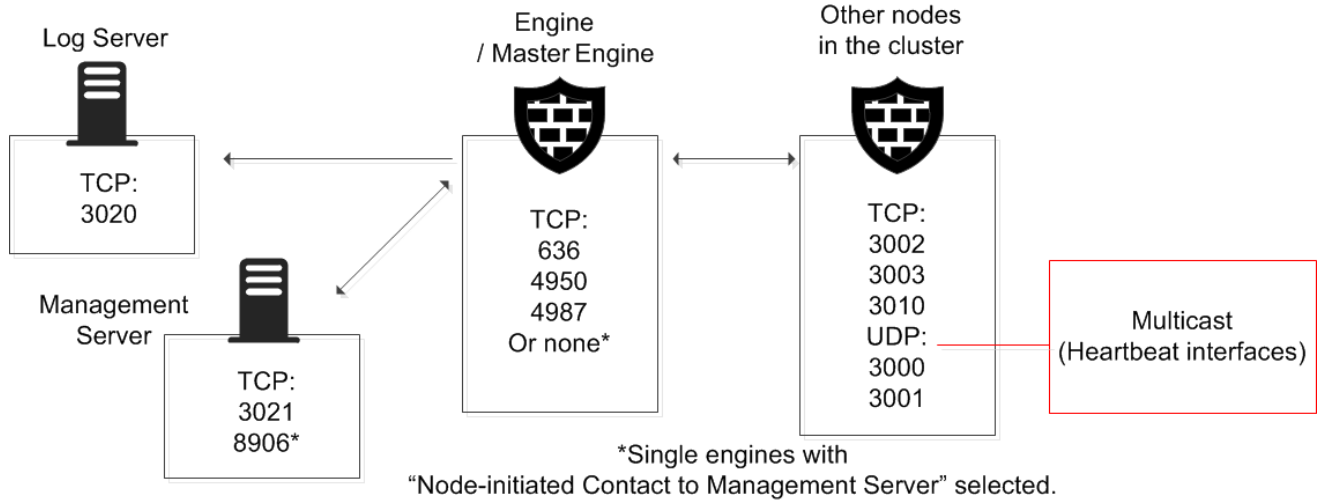
See the table for a complete list of default ports for the engines.



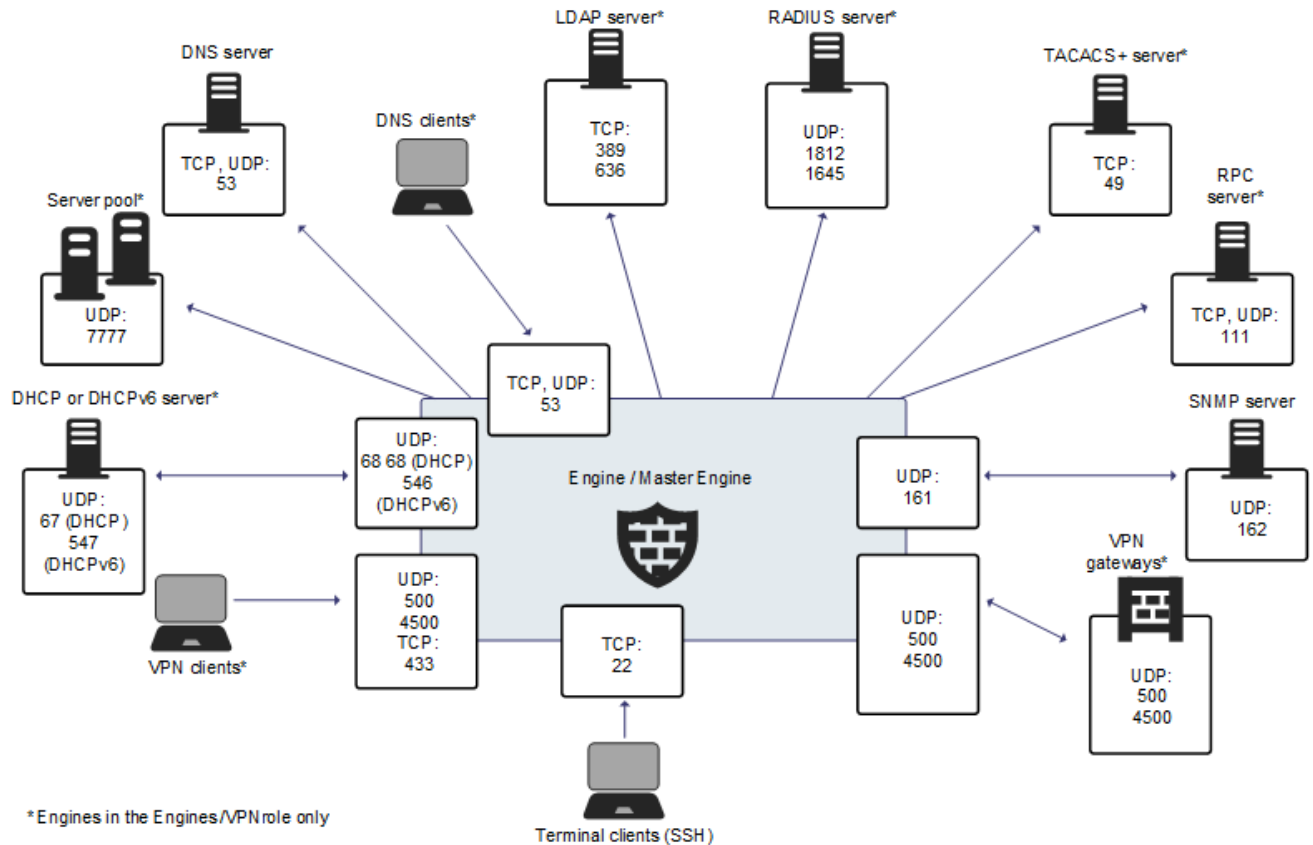
Note

Master Engines use the same default ports as clustered Security Engines. Virtual Engines do not communicate directly with other system components.

Destination ports for basic Security Engine communications




Default destination ports for Security Engine service communications



This table lists the default ports for Security Engines and Master Engines. Many of these ports can be changed. The names of corresponding default Service elements are also included for your reference.

Security Engine and Master Engine default ports

| Listening host | Port/protocol | Contacting hosts | Service description | Service element name |
|---|------------------------------------|---|--|--|
| Certificate Revocation List (CRL) server | 80/TCP | Engine | Online certificate status protocol (OCSP) queries and fetching CRLs. | HTTP |
| DHCP server | 67/UDP | Engine | Relayed DHCP requests and requests from a engine that uses dynamic IP address. | BOOTPS (UDP) |
| DHCPv6 server | 547/UDP | Engine | Requests from a engine that uses dynamic IPv6 address. | N/A |
| External DNS server | 53/UDP, 53/TCP | Engine, Master Engine | DNS resolution and dynamic DNS updates. | DNS (TCP), DNS (UDP) |
| File reputation server | 443/TCP | Engine, Layer 2 Engine, IPS, Master Engine | GTI File Reputation Server | HTTPS |
| Engine | 67/UDP | Any | DHCP relay on engine. | BOOTPS (UDP) |
| Engine | 68/UDP | DHCP server | Replies to DHCP requests. | BOOTPC (UDP) |
| Engine | 80/TCP | Clients that need to authenticate to the Engine | Browser Based User Authentication | HTTP |
| Engine | 443/TCP | Clients that need to authenticate to the Engine | Browser Based User Authentication | HTTPS |
| Engine | 443/TCP | VPN clients using SSL tunneling | VPN client SSL tunneling | TLS |
| Engine | 443/TCP | Application Access Portal users | Application Access Portal | HTTPS |
| Engine | 546/UDP | DHCPv6 server | Replies to DHCPv6 requests. | N/A |
| Engine, Master Engine | 53/UDP, 53/TCP | Clients in the internal network | DNS relay | DNS (TCP), DNS (UDP) |
| Engine, Master Engine | 500/UDP | VPN clients, VPN gateways | VPN negotiations, VPN traffic. | ISAKMP (UDP) |
| Engine, Master Engine | 636/TCP | Management Server | Internal user database replication. | LDAPS (TCP) |
| Engine, Master Engine | 4500/UDP | VPN client, VPN gateways | VPN traffic using NAT-traversal. | NAT-T |
| Engine Cluster Node, Master Engine cluster node | 3000-3001/UDP, 3002-3003, 3010/TCP | Engine Cluster Node, Master Engine cluster node | Heartbeat and state synchronization between clustered Engines. | SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync |
| Engine, Layer 2 Engine, IPS, Master Engine | 22/TCP | Terminal clients | SSH connections to the engine command line.  Note Do not use SSH in FIPS mode. | SSH |
| Engine, Layer 2 Engine, IPS, Master Engine | 4950/TCP | Management Server | Remote upgrade. | SG Remote Upgrade |

| Listening host | Port/protocol | Contacting hosts | Service description | Service element name |
|--|------------------------------------|--|--|--|
| Engine, Layer 2 Engine, IPS, Master Engine | 4987/TCP | Management Server | Management Server commands and policy upload. | SG Commands |
| Engine, Layer 2 Engine, IPS, Master Engine | 15000/TCP | Management Server, Log Server | block list entries. | SG block listing |
| Engine, Layer 2 Engine, IPS, Master Engine | 161/UDP | SNMP server | SNMP monitoring. | SNMP (UDP) |
| Engine, Layer 2 Engine, IPS | 9111/TCP | Forcepoint One Endpoint client | Endpoint information from the Forcepoint One Endpoint client. | N/A |
| Forcepoint User ID Service server | 5000/TCP | Engine, Layer 2 Engine, IPS | Information about user name and IP address mappings. | N/A |
| IPS Cluster Node | 3000-3001/UDP, 3002-3003, 3010/TCP | IPS Cluster Node | Heartbeat and state synchronization between clustered IPS engines. | SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync |
| LDAP server | 389/TCP | Engine, Master Engine | External LDAP queries, including StartTLS connections. | LDAP (TCP) |
| Layer 2 Engine Cluster Node | 3000-3001/UDP, 3002-3003, 3010/TCP | Layer 2 Engine Cluster Node | Heartbeat and state synchronization between clustered Layer 2 Engines. | SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync |
| Log Server | 3020/TCP | Engine, Layer 2 Engine, IPS, Master Engine | Log and alert messages; monitoring of block lists, connections, status, and statistics. | SG Log |
| Malware signature server | 80/TCP | Engine, Layer 2 Engine, IPS, Master Engine | Malware signature update service. | HTTP |
| Management Server | 3021/TCP | Engine, Layer 2 Engine, IPS, Master Engine | System communications certificate request/renewal (initial contact). | SG Initial Contact |
| Management Server | 8906/TCP | Engine, Layer 2 Engine, IPS | Management connection for engines with "Node-Initiated Contact to Management Server" selected. | SG Dynamic Control |
| RADIUS server | 1812, 1645/UDP | Engine, Master Engine | RADIUS authentication requests. | RADIUS (Authentication), RADIUS (Old) |
| RPC server | 111/UDP, 111/TCP | Engine, Master Engine | RPC number resolve. | SUNRPC (UDP), SunRPC (TCP) |
| Server Pool Monitoring Agents | 7777/UDP | Engine, Master Engine | Polls to the servers' Server Pool Monitoring Agents for availability and load information. | SG Server Pool Monitoring |
| SNMP server | 162/UDP | Engine, Layer 2 Engine, IPS, Master Engine | SNMP traps from the engine. | SNMP Trap (UDP) |
| TACACS+ server | 49/TCP | Engine, Master Engine | TACACS+ authentication requests. | TACACS (TCP) |
| ThreatSeeker Intelligence Cloud server | 443/TCP | Engine, Layer 2 Engine, IPS, Master Engine | ThreatSeeker Intelligence Cloud URL categorization service. | HTTPS |

| Listening host | Port/protocol | Contacting hosts | Service description | Service element name |
|----------------|---------------|-----------------------|---|----------------------|
| VPN gateways | 500, 4500/UDP | Engine, Master Engine | VPN traffic. Ports 443/TCP (or custom port) can also be used, depending on encapsulation options. | ISAKMP (UDP) |

Security Engine in the Factory Default State

The following network interfaces and services are available for the engine in the factory default state:

- **Ethernet Interface 0 (WAN):** This interface responds to ICMP Echo (Ping) requests, provided it can obtain an IP address via DHCP.
- **Ethernet Interface 2 (LAN):** This interface uses the link local IP address 169.254.169.169/16 and provides the following services:
 - Web server for Security Engine Configuration Wizard on TCP ports 80 and 443.
 - DHCP server on UDP port 67.
 - DNS server on UDP and TCP port 53.
- **Ethernet Interface 3 (HA):** This interface listens to High Availability (HA) pairing broadcasts for Backup Unit on UDP port 18770. No IP address is configured on this interface.
- **LTE Mobile Data Interface (available in certain appliances):** This interface responds to ICMP Echo (Ping) requests, provided there is a SIM card installed and a data plan that enables it to obtain an IP address from the mobile operator.

Command line tools

Contents

- Security Management Center commands on page 247
- Security Engine commands on page 263
- Server Pool Monitoring Agent commands on page 273

There are command line tools for the SMC and the Security Engines.

Security Management Center commands

SMC commands include commands for the Management Server, Log Server, and Web Portal Server.

In Windows, the command line tools are *.bat script files. In Linux, the files are *.sh scripts. Commands are found in the following locations:

- For SMC installations on Linux or Windows, commands are found in the `<installation directory>/bin` directory.
- For the SMC Appliance, general SMC commands are found in the `/usr/local/forcepoint/smc/bin` directory.
- Commands that are specific to the SMC Appliance are found in the `/usr/bin` directory.

If you enabled the restricted shell when you installed the SMC Appliance, only a limited set of commands is available. These commands include patching utilities, appliance maintenance, service handling, and other basic functionality. To show the list of allowed commands, enter `?`.



Note

When the restricted shell is enabled, all administrator accounts that you create in the SMC automatically use the restricted shell.

On the SMC Appliance, some commands must be run with elevated permissions using `sudo`. Commands in the restricted shell automatically prompt you to enter the password when required. A list of available `sudo` commands can be found by running `sudo -l` at the command line.



Note

Only administrators who have SMC Appliance Superuser administrator permissions can log on to the SMC Appliance command line.


Commands that require parameters must be run through the command line (`cmd.exe` in Windows). Commands that do not require parameters can alternatively be run through a graphical user interface, and can be added as shortcuts during installation.

**CAUTION**

login and password parameters are optional. Giving them as command-line parameters can pose a security vulnerability. Do not enter logon and password information unless explicitly prompted to do so by a command line tool.

Security Management Center commands

| Command | Description |
|---|--|
| <pre>ambr-crl (SMC Appliance only) [-a ADD --add=ADD] [-d DELETE --delete=DELETE] [-q --query] [-i IMPORT_CRL --import=IMPORT_CRL] [-v] [-l <log file path>] [-h --help]</pre> | <p>Fetches the certificate revocation lists (CRLs) for the CA certificates used by the appliance maintenance and bug remediation (AMBR) utilities.</p> <p><code>-a ADD, --add=ADD</code> adds a CRL distribution point URL in the form of <code>http://<url></code>.</p> <p><code>-d DELETE, --delete=DELETE</code> deletes a CRL distribution point URL.</p> <p><code>-q, --query</code> lists CRL distribution points.</p> <p><code>-i IMPORT_CRL, --import=IMPORT_CRL</code> imports a CRL from a file.</p> <p><code>-v</code> increases the verbosity of the command. You can repeat this command up to two times (<code>-vv</code> or <code>-v -v</code>) to further increase the verbosity.</p> <p><code>-l <log file path></code> specifies the path to a log file.</p> <p><code>-h, --help</code> shows information about the command.</p> |
| <pre>ambr-decrypt (SMC Appliance only)</pre> | <p>Decrypts an ambr patch; not normally used by administrators. <code>ambr-install</code> automatically decrypts patches.</p> |
| <pre>ambr-install <patch> (SMC Appliance only) [-F --force] [-r --skip-revocation] [--no-backup] [--no-snapshot] [--no-prompt] [-v] [-l <log file path>] [-h --help]</pre> | <p>Installs an ambr patch that has been loaded on the system.</p> <p>You can install multiple patches with a space between each patch name.</p> <p><code>-F, --force</code> forces the reinstallation of the patch or patches.</p> <p><code>-r, --skip-revocation</code> skips the certificate revocation checks.</p> <p><code>--no-backup</code> does not create a configuration backup.</p> <p><code>--no-snapshot</code> does not create a recovery snapshot.</p> <p><code>--no-prompt</code> does not prompt before restarting.</p> <p><code>-v</code> increases the verbosity of the command. You can repeat this command up to two times to further increase the verbosity.</p> <p><code>-l <log file path></code> specifies the path to a log file.</p> <p><code>-h, --help</code> shows information about the command.</p> |
| <pre>ambr-load <patch> (SMC Appliance only) [-f IN_FILES --file=IN_FILES] [-r --skip-revocation] [-v] [-l <log file path>] [-h --help]</pre> | <p>Loads an ambr patch onto the system from either the patch server or from the local file system. A loaded patch means that the file is copied to the local file system, but not installed.</p> <p>You can load multiple patches with a space between each patch name.</p> <p><code>-f IN_FILES, --file=IN_FILES</code> specifies the local file to load.</p> <p><code>-r, --skip-revocation</code> skips the certificate revocation checks.</p> <p><code>-v</code> increases the verbosity of the command. You can repeat this command up to two times to further increase the verbosity.</p> <p><code>-l <log file path></code> specifies the path to a log file.</p> <p><code>-h, --help</code> shows information about the command.</p> |

| Command | Description |
|--|--|
| <pre>ambr-query (SMC Appliance only) [-c --clean] [-u --update] [-a --all] [-j --json] [-i INFO --info=INFO <patch>] [-L <log file path>] [-v] [-h --help]</pre> | <p>Shows patch information including:</p> <ul style="list-style-type: none"> What is loaded or installed on the system A list of available updates from the patch server Detailed information about a specific patch <p><code>-u , --update</code> updates the remote patch list from a web server .</p> <p><code>-c, --clean</code> cleans the remote patch cache.</p> <p><code>-a, --all</code> shows all local and remote patches.</p> <p><code>-j, --json</code> formats output as JSON.</p> <p><code>-i INFO, --info=INFO <patch></code> shows detailed information about the patch. You can get information about multiple patches in one command by separating the patch names with a space.</p> <p><code>-v</code> increases the verbosity of the command. You can repeat this command up to two times to further increase the verbosity.</p> <p><code>-L <log file path></code> specifies the path to the file where log messages are written.</p> <p><code>-h, --help</code> shows information about the command.</p> |
| <pre>ambr-unload <patch> (SMC Appliance only) [-a --all] [-v] [-l <log file path>] [-h --help]</pre> | <p>Unloads an ambr patch from the system. The command deletes the patch file if it has not been installed, but it does not uninstall the patch.</p> <p>You can unload multiple patches with a space between each patch name.</p> <p><code>-a, --all</code> unloads all loaded patches.</p> <p><code>-v</code> increases the verbosity of the command. You can repeat this command up to two times to further increase the verbosity.</p> <p><code>-l <log file path></code> specifies the path to a log file.</p> <p><code>-h, --help</code> shows information about the command.</p> |
| <pre>ambr-verify (SMC Appliance only)</pre> | <p>Verifies the signature of a patch file; not normally used by administrators. <code>ambr-install</code> automatically verifies patches.</p> |
| <pre>revert</pre> | <p>Reverts to the previous installation saved during the upgrade process.</p> <p>The previous installation can be restored at any time, even after a successful upgrade.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>This script is located in <code><installation directory>/bin/uninstall</code>.</p> </div> |


| Command | Description |
|---|--|
| <pre>sgActivateWebswing [host=<Management Server Address[\Domain>] login=<login name> pass=<password> port=<port number> mgtserver=<name> enable=<true false> hostname=<host name> listening_address=<IP address> https=<true false> generate_logs=<true false> use_ssl=<true false> https_validity=<number of days> public_key_output=<path></pre> | <p>Configures Web Access to run the Management Client in a web browser.</p> <p><code>Host</code> specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.</p> <p><code>login</code> defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.</p> <p><code>pass</code> defines the password for the user account.</p> <p><code>port</code> specifies the port number of the Web Access service on the Management Server. The default is 8085.</p> <p><code>mgtserver</code> specifies the name of the Management Server element. The default is Management Server.</p> <p><code>enable</code> specifies whether Web Access is enabled (true) or disabled (false). The default is true.</p> <p><code>hostname</code> specifies the host name of the Web Access service.</p> <p><code>listening_address</code> specifies the listening IP address of the Web Access service if the server has several addresses. If not specified, requests to any of this server's IP addresses are allowed.</p> <p><code>https</code> specifies whether HTTPS is enabled for the Web Access service. If true, the public key is returned in the output. The default is true.</p> <p><code>generate_logs</code> specifies whether to log all file load events in Combined Log format in a file on the server for further analysis with external web statistics software. The default is false.</p> <p><code>use_ssl</code> specifies whether SSL is used to track sessions in your web application. If SSL connections are managed by a proxy or a hardware accelerator they must populate the SSL request headers. The default is false.</p> <p><code>https_validity</code> specifies the number of days for which the self-signed certificate for HTTPS is valid. The default is 365.</p> <p><code>public_key_output</code> specifies the path for the HTTPS public key.</p> |



| Command | Description |
|--|--|
| <pre>sgArchiveExport [host=<Management Server Address[\Domain>] [login=<login name>] [pass=<password>] [format=<CSV XML JSON>] i=<input files and/or directories> [o=<output file name>] [f=<filter file name>] [e=<filter expression>] [-h -help -?] [-v]</pre> | <p>Shows and exports logs from archive. Supports CEF, LEEF, and ESM formats in addition to CSV, XML, and JSON.</p> <p>This command is only available on the Log Server. The operation checks permissions for the supplied administrator account from the Management Server to prevent unauthorized access to the logs.</p> <p>Enclose details in double quotes if they contain spaces.</p> <p><code>host</code> specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.</p> <p><code>login</code> defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.</p> <p><code>pass</code> defines the password for the user account.</p> <p><code>format</code> defines the file format for the output file. If this parameter is not defined, the XML format is used.</p> <p><code>i</code> defines the source from which the logs are exported. Can be a folder or a file. The processing recurses into subfolders.</p> <p><code>o</code> defines the destination file where the logs are exported. If this parameter is not defined, the output is shown on screen.</p> <p><code>f</code> defines a file that contains the filtering criteria you want to use for filtering the log data. You can export log filters individually in the Management Client through Tools > Save for Command Line Tools in the filter's right-click menu.</p> <p><code>e</code> allows you to enter a filter expression manually (using the same syntax as exported filter files).</p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> <p><code>-v</code> shows verbose output on the command execution.</p> <p>Example (exports logs from one full day to a file using a filter): <code>sgArchiveExport login=admin pass=abc123 i= C:\Program Files\Forcepoint\SMC\data\archive\engine\year2011\month12\.sgB.day01\ f= C:\Program Files\Forcepoint\SMC\export\MyExportedFilter.flp format=CSV o=MyExportedLogs.csv</code></p> |



| Command | Description |
|---|--|
| <pre>sgBackupLogSrv [-pwd=<password>] [-path=<destpath>] [-nodiskcheck] [-comment=<comment>] [-nofsstorage] [-h --help]</pre> | <div data-bbox="591 218 649 273"></div> <div data-bbox="688 226 1474 319"> <p>Note For the SMC Appliance, use the <code>smca-backup</code> command.</p> </div> <p>Creates a backup of Log Server configuration data.</p> <p>The backup file is stored in the <code><installation directory>/backups/</code> directory.</p> <p>Twice the size of the log database is required on the destination drive. Otherwise, the operation fails.</p> <p><code>pwd</code> enables encryption.</p> <p><code>path</code> defines the destination path.</p> <p><code>nodiskcheck</code> ignores the free disk check before creating the backup.</p> <p><code>comment</code> allows you to enter a comment for the backup. The maximum length of a comment is 60 characters.</p> <p><code>nofsstorage</code> creates a backup only of the Log Server configuration without the log data.</p> <p><code>-h</code> or <code>--help</code> shows information about using the script.</p> <p>Also see <code>sgRestoreLogBackup</code>.</p> |
| <pre>sgBackupMgtSrv [pwd=<password>] [path=<destpath>] [nodiskcheck] [comment=<comment>] [-h --help]</pre> | <div data-bbox="591 921 649 976"></div> <div data-bbox="688 930 1474 1022"> <p>Note For the SMC Appliance, use the <code>smca-backup</code> command.</p> </div> <p>Creates a complete backup of the Management Server (including both the local configuration and the stored information in the configuration database). The backup file is stored in the <code><installation directory>/backups/</code> directory.</p> <p>Twice the size of the Management Server database is required on the destination drive. Otherwise, the operation fails.</p> <p><code>pwd</code> enables encryption.</p> <p><code>path</code> defines the destination path.</p> <p><code>nodiskcheck</code> ignores the free disk check before creating the backup.</p> <p><code>comment</code> allows you to enter a comment for the backup. The maximum length of a comment is 60 characters.</p> <p><code>-h</code> or <code>--help</code> shows information about using the script.</p> <p>Also see <code>sgRestoreMgtBackup</code> and <code>sgRecoverMgtDatabase</code>.</p> |
| <pre>sgCertifyLogSrv [host=<Management Server Address[\\Domain]>]</pre> | <p>Contacts the Management Server and creates a certificate for the Log Server to allow secure communications with other SMC components. Renewing an existing certificate does not require changing the configuration of any other SMC components.</p> <p><code>host</code> specifies the address of the Management Server. If the parameter is not defined, the loopback address (<code>localhost</code>) is used.</p> <p><code>Domain</code> specifies the administrative Domain the Log Server belongs to if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p>Stop the Log Server before running this command. Restart the server after running this command.</p> |

| Command | Description |
|---|--|
| <pre>sgCertifyMgtSrv [login=<login name>] [pass=<password>] [standby-server=<name of additional Management Server>] [active-server=<IP address of active Management Server>] [mode=ext-pki-init [dn=<Subject DN> dns=<SubjectAltName DNS> key-size=<256 384 521> csr-out=<path> crt-in=<path> ca-file=<path>]] [-nodisplay] [-h -help -?]</pre> | <p>Creates a certificate for the Management Server to allow secure communications between the SMC components. Renewing an existing certificate does not require changes on any other SMC components.</p> <p>In an environment with only one Management Server, or to certify the active Management Server, stop the Management Server before running the <code>sgCertifyMgtSrv</code> command. Run the command without parameters. Restart the Management Server after running this command.</p> <p>To certify an additional Management Server, stop the additional Management Server before running the <code>sgCertifyMgtSrv</code> command. The active Management Server must be running when you run this command. The management database is replicated to the additional Management Server during the certification. The additional Management Server must have a connection to the active Management Server when you run this command.</p> <p><code>[login=<login name>]</code> defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.</p> <p><code>[pass=<password>]</code> defines the password for the user account.</p> <p><code>[standby-server]</code> specifies the name of the additional Management Server to be certified.</p> <p><code>[active-server]</code> specifies the IP address of the active Management Server.</p> <p><code>[mode=ext-pki-init]</code> enables commands for external certificate management.</p> <p><code>[dn]</code> specifies the Subject DN to use in the certificate request for the Management Server.</p> <p><code>[dns]</code> specifies the SubjectAltName DNS value to use in the certificate request for the Management Server.</p> <p><code>[key-size]</code> specifies the key size to use in the certificate request for the Management Server.</p> <p><code>[csr-out]</code> specifies the output path where the certificate request is saved.</p> <p><code>[crt-in]</code> specifies the input path for importing a certificate in PEM format.</p> <p><code>[ca-file]</code> specifies the input path for importing a CA file in PEM format.</p> <p><code>-nodisplay</code> sets a text-only console.</p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> |
| <pre>sgCertifyWebPortalSrv [host=<Management Server Address[\Domain]>]</pre> | <p>Contacts the Management Server and creates a certificate for the Web Portal Server to allow secure communications with other SMC components. Renewing an existing certificate does not require changing the configuration of any other SMC components.</p> <p><code>host</code> specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.</p> <p><code>Domain</code> specifies the administrative Domain the Web Portal Server belongs to if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p>Stop the Web Portal Server before running this command. Restart the server after running this command.</p> |
| <pre>sgChangeMgtIPOnLogSrv <IP address></pre> | <p>Changes the Management Server's IP address in the Log Server's local configuration to the IP address you give as a parameter.</p> <p>Use this command if you change the Management Server's IP address. Restart the Log Server service after running this command.</p> |

| Command | Description |
|---|--|
| <code>sgChangeMgtIPOnMgtSrv <IP address></code> | <p>Changes the Management Server's IP address in the local configuration to the IP address you give as a parameter.</p> <p>Use this command if you change the Management Server's IP address. Restart the Management Server service after running this command.</p> |
| <code>sgClient</code> | Starts a locally installed Management Client. |
| <code>sgCreateAdmin</code> | <p>Creates an unrestricted (superuser) administrator account.</p> <p>The Management Server must be stopped before running this command.</p> |
| <code>sgExport</code> <code>[host=<Management Server Address[\Domain]>]</code> <code>[login=<login name>]</code> <code>[pass=password]</code> <code>file=<file path and name></code> <code>[type=<all nw ips sv rb al vpn></code> <code>[name=<element name 1, element name 2, ...>]</code> <code>[recursion]</code> <code>[-system]</code> <code>[-h -help -?]</code> | <p>Exports elements stored on the Management Server to an XML file.</p> <p>Enclose details in double quotes if they contain spaces.</p> <p><code>host</code> specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.</p> <p><code>Domain</code> specifies the administrative Domain for this operation if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p><code>login</code> defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.</p> <p><code>pass</code> defines the password for the user account.</p> <p><code>file</code> defines the name and location of the export .zip file.</p> <p><code>type</code> specifies which types of elements are included in the export file:</p> <ul style="list-style-type: none"> ■ <code>all</code> for all exportable elements ■ <code>nw</code> for network elements ■ <code>ips</code> for IPS elements ■ <code>sv</code> for services ■ <code>rb</code> for security policies ■ <code>al</code> for alerts ■ <code>vpn</code> for VPN elements. <p><code>name</code> allows you to specify by name the elements that you want to export.</p> <p><code>recursion</code> includes referenced elements in the export, for example, the network elements used in a policy that you export.</p> <p><code>-system</code> includes any system elements that are referenced by the other elements in the export.</p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> |

| Command | Description |
|--|--|
| <pre>sgHA [host=<Management Server Address[\Domain]>] [login=<login name>] [pass=<password>] [master=<Management Server used as master server for the operation>] [-set-active] [-set-standby] [-check] [-retry] [-force] [-restart] [-h -help -?]</pre> | <p>Controls active and standby Management Servers.</p> <p>If you want to perform a full database synchronization, use the <code>sgOnlineReplication</code> command.</p> <p><code>host</code> specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.</p> <p><code>Domain</code> specifies the administrative Domain for this operation if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p><code>login</code> defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.</p> <p><code>pass</code> defines the password for the user account.</p> <p><code>master</code> defines the Management Server used as a master Management Server for the operation.</p> <p><code>-set-active</code> activates and locks all administrative Domains.</p> <p><code>-set-standby</code> deactivates and unlocks all administrative Domains.</p> <p><code>-check</code> checks that the Management Server's database is in sync with the master Management Server.</p> <p><code>-retry</code> retries replication if this has been stopped due to a recoverable error.</p> <p><code>-force</code> enforces the operation even if all Management Servers are not in sync.</p> <div data-bbox="591 961 1474 1062" style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  Note This option can cause instability if used carelessly. </div> <p><code>-restart</code> restarts the specified Management Server.</p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> |
| <pre>sgImport [host=<Management Server Address[\Domain]>] [login=<login name>] [pass=<password>] file=<file path and name> [-replace_all] [-h -help -?]</pre> | <p>Imports Management Server database elements from an XML file.</p> <p>When importing, existing (non-default) elements are overwritten if both the name and type match.</p> <p><code>host</code> specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.</p> <p><code>Domain</code> specifies the administrative Domain for this operation if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p><code>login</code> defines the user name for the account that is used for this operation. If this parameter is not defined, the user name root is used.</p> <p><code>pass</code> defines the password for the user account.</p> <p><code>file</code> defines the .zip file whose contents you want to import.</p> <p><code>-replace_all</code> ignores all conflicts by replacing all existing elements with new ones.</p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> |

| Command | Description |
|--|--|
| <pre>sgImportExportUser [host=< <Management Server Address[\Domain]>>] [login=<login name>] [pass=password] action=<import export> file=<file path and name> [-h -help -?]</pre> | <p>Imports and exports a list of Users and User Groups in an LDIF file from or to a Management Server's internal LDAP database.</p> <p>To import User Groups, all User Groups in the LDIF file must be directly under the stonegate top-level group (dc=stonegate).</p> <div data-bbox="589 359 1474 485" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;">  <p>CAUTION</p> <p>The user information in the export file is stored as plaintext. Handle the file securely.</p> </div> <p>host specifies the address of the Management Server. If the parameter is not defined, the loopback address (localhost) is used.</p> <p>Domain specifies the administrative Domain for this operation if the system is divided into administrative Domains. If the Domain is not specified, the Shared Domain is used.</p> <p>login defines the user name for the account that is used for this operation. If this parameter is not defined, the user name <code>root</code> is used.</p> <p>pass defines the password for the user account.</p> <p>action defines whether users are imported or exported.</p> <p>file defines the file that is used for the operation.</p> <p>Example: <code>sgImportExportUser login=admin pass=abc123 action=export file=c:\temp\exportedusers.ldif</code></p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> |
| <pre>sgInfo SG_ROOT_DIR FILENAME [fast=<timestamp>] [list] [hprof=none limited all] [-nolog] [-client] [-h -help -?]</pre> | <p>Creates a .zip file that contains copies of configuration files and the system trace files. The resulting .zip file is stored in the logged on user's home directory. The file location is shown on the last line of screen output. Provide the generated file to support for troubleshooting purposes.</p> <div data-bbox="589 1199 1474 1381" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;">  <p>Note</p> <p>On the SMC Appliance, you must always specify the path to the directory in which the .zip file is stored. The directory must be accessible from the account that you use to log on to the command line of the SMC Appliance.</p> </div> <p>SG_ROOT_DIR SMC installation directory.</p> <p>FILENAME name of output file.</p> <p>fast collects only traces that changed after the specified time stamp. Enter the time stamp in milliseconds or in the format yyyy-MM-dd HH:mm:ss. No other information is collected, except for threaddumps.</p> <p>[list] only lists files. It does not create a .zip file or generate threaddumps.</p> <p>hprof defines whether hprof memory dump files are included.</p> <ul style="list-style-type: none"> ■ <code>none</code> does not include hprof memory dump files. ■ <code>limited</code> includes only hprof memory dump files that are created with <code>makeheap</code>. ■ <code>all</code> includes memory dump files that are created with <code>makeheap</code> and <code>java_pid</code>. <p><code>-nolog</code> extended Log Server information is not collected.</p> <p><code>-client</code> collects traces only from the Management Client.</p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> |

| Command | Description |
|---|---|
| <pre>sgOnlineReplication [active-server=<name of active Management Server>] [-nodisplay] [-h -help -?]</pre> | <p>Replicates the Management Server's database from the active Management Server to an additional Management Server.</p> <p>Stop the Management Server to which the database is replicated before running this command. Restart the Management Server after running this command.</p> <p>Use this script to replicate the database only in the following cases:</p> <ul style="list-style-type: none"> ■ The additional Management Server's configuration has been corrupted. ■ In new SMC installations if the automatic database replication between the Management Servers has not succeeded. <p>Otherwise, synchronize the database through the Management Client.</p> <div data-bbox="591 554 1474 709" style="border: 1px solid gray; padding: 5px;">  <p>CAUTION</p> <p>This script also has parameters that are for the internal use of the Management Server only. Do not use this script with any parameters other than the ones listed here.</p> </div> <p><code>active-server</code> specifies the IP address of the active Management Server from which the Management database is replicated.</p> <p><code>-nodisplay</code> sets a text-only console.</p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> |
| <pre>sgReinitializeLogServer</pre> | <p>Creates a Log Server configuration if the configuration file has been lost.</p> <div data-bbox="591 974 1474 1075" style="border: 1px solid gray; padding: 5px;">  <p>Note</p> <p>This script is located in <code><installation directory>/bin/install</code>.</p> </div> |
| <pre>sgRestoreArchive <ARCHIVE_DIR></pre> | <p>Restores logs from archive files to the Log Server.</p> <p>This command is available only on the Log Server.</p> <p><code>ARCHIVE_DIR</code> is the number of the archive directory (0–31) from where the logs will be restored. By default, only archive directory 0 is defined. The archive directories can be defined in the <code><installation directory>/data/LogServerConfiguration.txt</code> file: <code>ARCHIVE_DIR_ xx=PATH</code>.</p> |
| <pre>sgRestoreLogBackup [-pwd=<password>] [-backup=<backup file name>] [-nodiskcheck] [-overwrite-syslog-template] [-h -help]</pre> | <p>Restores the Log Server (logs or configuration files) from a backup file in the <code><installation directory>/backups/</code> directory.</p> <p><code>-pwd</code> defines a password for encrypted backup.</p> <p><code>-backup</code> defines a name for the backup file.</p> <p><code>-nodiskcheck</code> ignores the free disk check before backup restoration.</p> <p><code>-overwrite-syslog-template</code> overwrites a syslog template file if found in the backup.</p> <p><code>-h</code> or <code>-help</code> shows information about using the script.</p> |

| Command | Description |
|--|---|
| <code>sgRestoreMgtBackup</code> <code>[-pwd=<password>]</code> <code>[-backup=<backup file name>]</code> <code>[-import-license <license file name>]</code> <code>[-nodiskcheck]</code> <code>[-h -help]</code> | <p>Restores the Management Server (database or configuration files) from a backup file in the <code><installation directory>/backups/</code> directory.</p> <ul style="list-style-type: none"> <code>-pwd</code> defines a password for encrypted backup. <code>-backup</code> defines a name for the backup file. <code>-import-license</code> specifies a license file to import during the backup restoration. <code>-nodiskcheck</code> ignores the free disk check before backup restoration. <code>-h</code> or <code>-help</code> shows information about using the script. |
| <code>sgShowFingerPrint</code> <code>[-server]</code> | <p>Shows the CA certificate's fingerprint on the Management Server.</p> <ul style="list-style-type: none"> <code>-server</code> displays Management Server Certificate Fingerprint. |
| <code>sgStartLogSrv</code> | Starts the Log Server and its database. |
| <code>sgStartMgtDatabase</code> | Starts the Management Server's database. There is usually no need to use this script. |
| <code>sgStartMgtSrv</code> | Starts the Management Server and its database. |
| <code>sgStartWebPortalSrv</code> | Starts the Web Portal Server. |
| <code>sgStopLogSrv</code> | Stops the Log Server. |
| <code>sgStopMgtSrv</code> | Stops the Management Server and its database. |
| <code>sgStopMgtDatabase</code> | Stops the Management Server's database. There is usually no need to use this script. |
| <code>sgStopWebPortalSrv</code> | Stops the Web Portal Server. |
| <code>sgStopRemoteMgtSrv</code> <code>[host=<Management Server address[\Domain]>]</code> <code>[login=<login name>]</code> <code>[pass=<password>]</code> <code>[-h -help -?]</code> | <p>Stops the Management Server service when run without arguments.</p> <p>To stop a remote Management Server service, provide the arguments to connect to the Management Server.</p> <ul style="list-style-type: none"> <code>host</code> is the Management Server's host name if not localhost. <code>login</code> is an SMC administrator account for the logon. <code>pass</code> is the password for the administrator account. <code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script. |

| Command | Description |
|--|---|
| <pre>sgTextBrowser [host=<Management Server address[\Domain]>] [login=<login name>] [pass=<password>] [format=<CSV XML JSON>] [o=<output file>] [f=<filter file>] [e=<filter expression>] [m=<current stored>] [limit=<maximum number of unique records to fetch>] [-h -help -?]</pre> | <p>Shows or exports current or stored logs.</p> <p>This command is available on the Log Server.</p> <p>Enclose the file and filter names in double quotes if they contain spaces.</p> <p><code>host</code> defines the address of the Management Server used for checking the logon information. If this parameter is not defined, Management Server is expected to be on the same host where the script is run. If Domains are in use, you can specify the Domain the Log Server belongs to. If <code>domain</code> is not specified, the Shared Domain is used.</p> <p><code>login</code> defines the user name for the account that is used for this export. If this parameter is not defined, the user name root is used.</p> <p><code>pass</code> defines the password for the user account used for this operation.</p> <p><code>format</code> defines the file format for the output file. If this parameter is not defined, the XML format is used.</p> <p><code>o</code> defines the destination output file where the logs will be exported. If this parameter is not defined, the output is shown on screen.</p> <p><code>f</code> defines the exported filter file that you want to use for filtering the log data.</p> <p><code>e</code> defines the filter that you want to use for filtering the log data. Type the name as shown in the Management Client.</p> <p><code>m</code> defines whether you want to view or export logs as they arrive on the Log Server (current) or logs stored in the active storage directory (stored). If this option is not defined, the current logs are used.</p> <p><code>limit</code> defines the maximum number of unique records to be fetched. The default value is unlimited.</p> <p><code>-h</code>, <code>-help</code>, or <code>-?</code> shows information about using the script.</p> |
| <pre>smca-agent (SMC Appliance only)</pre> | <p>SMC uses it to exchange configuration data between SMC and the operating system; not normally used by administrators. The agent configures the NTP and SNMP daemons and sets the logon and SSH banners.</p> |
| <pre>smca-backup (SMC Appliance only) [-pwd <password>] [-comment <comment>] [-nodiskcheck] [-nofsstorage] [-path <destination>] [-log] [-mgt] [-h --help]</pre> | <p>Creates a configuration backup of the SMC Appliance operating system and includes an SMC backup.</p> <p><code>-pwd <password></code> enables the encryption of the backup file and sets the password.</p> <p><code>-comment <comment></code> adds a comment to the backup file name.</p> <p><code>-nodiskcheck</code> turns off the available disk space check.</p> <p><code>-nofsstorage</code> excludes the log files for the Log Server from the backup.</p> <p><code>-path <destination></code> specifies a path for backup file storage. The default directory for backups is <code>/usr/local/forcepoint/smc/backups</code>.</p> <p><code>-log</code> creates a Log Server backup.</p> <p><code>-mgt</code> creates a Management Server backup.</p> <p><code>-h</code>, <code>--help</code> shows information about the command.</p> <p>Also see <code>sgRestoreLogBackup</code> and <code>sgRestoreMgtBackup</code>.</p> |

| Command | Description |
|--|---|
| <pre>smca-backup-remove</pre> <p>(SMC Appliance only)</p> <pre>[-f --file]</pre> <pre>[--force]</pre> <pre>[--age <days>]</pre> <pre>[--log]</pre> <pre>[--mgt]</pre> <pre>[-h --help]</pre> | <p>Removes old SMC Appliance backup files.</p> <p><code>-f, --file</code> specifies the backup file to be removed.</p> <p><code>--force</code> forces backup file delete without confirmation.</p> <p><code>[--age <days>]</code> remove any backups older than the specified number of days. The default is 30 days.</p> <p><code>[--log]</code> removes Log Server backups.</p> <p><code>[--mgt]</code> removes Management Server backups.</p> <p><code>-h, --help</code> shows information about the command.</p> |
| <pre>smca-cifs</pre> <p>(SMC Appliance only)</p> <pre>[add]</pre> <pre>[remove]</pre> <pre>[-n <name>]</pre> <pre>[-s //<server>/<share>]</pre> <pre>[-u <username>]</pre> <pre>[-p <password>]</pre> <pre>[-d <domain>]</pre> | <p>Configures the mounting of remote CIFS file shares on the SMC Appliance.</p> <p><code>add</code> adds the CIFS share.</p> <p><code>remove</code> removes the CIFS share. Use with the name option.</p> <p><code>-n <name></code> specifies the name of the share.</p> <p><code>-s //<server>/<share></code> specifies the server or IP address of the share.</p> <p><code>-u <username></code> specifies the user name to authenticate with the CIFS server to get access to the share.</p> <p><code>-p <password></code> specifies the password on remote system.</p> <p><code>-d <domain></code> specifies the domain of the share.</p> |
| <pre>smca-restore</pre> <p>(SMC Appliance only)</p> <pre>[-pwd <password>]</pre> <pre>[-nodiskcheck]</pre> <pre>[-backup <filename>]</pre> <pre>[-nosmca]</pre> <pre>[-smcaonly]</pre> <pre>[-overwrite-syslog-template]</pre> <pre>[-h --help]</pre> | <p>Restores a backup on the SMC Appliance.</p> <p><code>-pwd <password></code> specifies the password for decrypting an encrypted backup file.</p> <p><code>-nodiskcheck</code> turns off the available disk space check.</p> <p><code>-backup <filename></code> specifies the backup file name. If you do not specify the backup file name, you are prompted to select the backup file.</p> <p><code>[-nosmca]</code> restores the Management Server or Log Server backup without restoring the SMC Appliance configuration</p> <p><code>[-smcaonly]</code> restores the SMC Appliance configuration without restoring the Management Server or Log Server backup.</p> <p><code>-overwrite-syslog-template</code> overwrites any existing syslog templates in the log backup file.</p> <p><code>-h, --help</code> shows information about the command.</p> |

| Command | Description |
|---|--|
| <pre>smca-rsync (SMC Appliance only) [add] [modify] [remove] [enable] [disable] [list] [run] [-t task_id] [-i <source directory>] [-o <destination directory>] [-m <mode>] [-h -help]</pre> | <p>Configures automated backup tasks. Typically used with the <code>smca-cifs</code> command to move backups off the appliance.</p> <p><code>add</code> adds a backup task. You can specify an existing source and destination directories. If not specified, the default is <code>/usr/local/forcepoint/smc/backups/</code>.</p> <p><code>modify</code> changes an existing backup task by its task ID. All attributes can be changed, except for the task ID. To change an attribute, use the appropriate option with a new value.</p> <p><code>remove</code> removes an existing backup task by its task ID.</p> <p><code>enable</code> enables an existing backup task by its task ID.</p> <p><code>disable</code> disables an existing backup task by its task ID.</p> <p><code>list</code> provides a list of all configured backup tasks.</p> <p><code>run</code> runs all enabled backup tasks.</p> <p><code>-t task_id</code> specifies the task ID. Use the list command to view the task IDs.</p> <p><code>-i <source directory></code> specifies the directory where the backups are stored when they are created. If omitted, the source directory defaults to the SMC backups directory <code>/usr/local/forcepoint/smc/backups/</code>.</p> <p><code>-o <destination directory></code> specifies the remote location to store the backups.</p> <p><code>-m <mode></code> specifies the rsync mode. You can indicate whether rsync appends or mirrors the source directory to the destination directory. Appending the directory means that existing files in the destination directory, that are not in the source directory or are newer than those files in the source directory, are not changed. If omitted, the mode defaults to append.</p> <p><code>-h, --help</code> shows information about the command.</p> |

| Command | Description |
|---|---|
| <pre>smca-system (SMC Appliance only) [ambr -p <proxy url>] [toggle] [toggle-vcdrom] [mirror [-n <name>]] [snapshot [-C --create] [-R --restore] [-D, --delete] [-n <name>]] [serial-number] [fingerprint] [toggle-console] [bootloader-password [-s --set] [-r --remove]] [netconfig] [log-view [<filename>]] [fips-config] [file-remove [filename] [-h] [-l] [--autoremove] [-a <age>] [--no-prompt]] [-f] [-h -help]</pre> | <p>Manages recovery snapshots, alternate partition mirroring, and changing system partition boot preference.</p> <p><code>ambr -p <proxy url></code> configures the appliance to use a proxy for loading SMC Appliance patches.</p> <p><code>toggle</code> restarts the appliance to the alternate partition.</p> <p><code>toggle-vcdrom</code> sets the appliance's default boot option to the vcdrom.</p> <p><code>mirror</code> mirrors the active system to the alternate system. <code>-n <name></code> specifies the name of the snapshot used for mirror operations.</p> <p><code>snapshot</code> manages recovery snapshots.</p> <ul style="list-style-type: none"> ■ <code>-C, --create</code> creates a snapshot. ■ <code>-D, --delete</code> deletes the snapshot. ■ <code>-R, --restore</code> restores the snapshot. ■ <code>-n <name></code> specifies the name of the snapshot used for snapshot operations. <p><code>[serial-number]</code> shows the hardware serial number for the SMC Appliance.</p> <p><code>[fingerprint]</code> shows the CA certificate fingerprint. If an external CA is configured, shows the Management Server certificate fingerprint instead.</p> <p><code>toggle-console</code> enables or disables the serial console on the SMC Appliance.</p> <p><code>bootloader-password</code> manages the bootloader password for the SMC Appliance.</p> <ul style="list-style-type: none"> ■ <code>-s, --set</code> sets or changes the bootloader password. ■ <code>-r, --remove</code> removes the bootloader password. <p><code>netconfig</code> sets up network-related configuration, such as IPv6 configuration.</p> <p><code>log-view <filename></code> shows the contents of the specified log file in the SMC Appliance log data directory <code>/var/log</code> or in any of the subdirectories of <code>/var/log</code>.</p> <p><code>log-view -l</code> shows a list of all available log files.</p> <p><code>fips-config</code> modifies the SMC Appliance configuration to support FIPS certification.</p> <p><code>file-remove</code> deletes the specified SMC files from the SMC Appliance.</p> <ul style="list-style-type: none"> ■ <code>filename</code> specifies the file to remove. This command can remove files in the following directories: <ul style="list-style-type: none"> ■ <code><SMC_DATA_DIR>/storage</code> ■ <code><SMC_DATA_DIR>/mgtserver</code> ■ <code><SMC_DATA_DIR>/SGInfo</code> ■ <code><SMC_DATA_DIR>/TrafficCapture</code> ■ <code><SMC_DATA_DIR>/datamgtserver/webswing/users</code> ■ <code>-h, --help</code> shows information about the remove command. ■ <code>-l, --list</code> lists the files that can be deleted. ■ <code>--autoremove</code> removes Web Swing files that are older than the number of days that are specified in the <code>-a <age></code>, <code>--age <age></code> option. ■ <code>-a <age></code>, <code>--age <age></code> specifies the age of Web Swing files to remove with the <code>--autoremove</code> option. The default is 30 days. ■ <code>--no-prompt</code> deletes the selected files without prompting for confirmation. <p><code>-f</code> forces the procedure, does not prompt for any confirmation.</p> <p><code>-h, --help</code> shows information about the command.</p> |

| Command | Description |
|--|--|
| <code>smca-user</code> (SMC Appliance only) | This utility is used by the SMC Appliance to keep user accounts in sync between the SMC and the operating system; not normally used by administrators. |

Security Engine commands

There are commands that can be run on the command line on Engine, Layer 2 Engine, IPS engines, or Master Engines.



Note

Using the SMC Client is the recommended configuration method, as most of the same tasks can be done through it.




Note

All command line tools that are available for single Security Engines are also available for Virtual Engines that have the same role. However, there is no direct access to the command line of Virtual Engines. Commands to Virtual Engines must be sent from the command line of the Master Engine using the `se-virtual-engine` command.


Some commands are only available when the Security Engine is in the Engine (FW), Layer 2 Engine (L2FW), or IPS engine (IPS) role.

Security Engine command line tools

| Command | Role | Description |
|--|----------------|--|
| <code>activate-alternative-policy</code> | FW L2FW IPS | Not supported on Master Engine or Virtual Engine. Activate alternative policies. <code>-s <number> --slot=<number></code> Use given alternative policy slot instead of prompting interactively. <code>-p <name> --policy-name=<name></code> Use policy with given name instead of prompting interactively. <code>-h --help</code> Show this help and exit. |

| Command | Role | Description |
|---|----------------|---|
| <code>remove-alternative-policy</code> <code>[options]</code> | FW L2FW IPS | <p>Not supported on Master Engine or Virtual Engine.</p> <p>Remove selected local alternative policy(s).</p> <p><code>-s <number> --slot=<number></code> Remove given alternative policy slot instead of prompting interactively.</p> <p><code>-p <name> --policy-name=<name></code> Use policy with given name instead of prompting interactively.</p> <p><code>-f --force</code> No error if specified policy does not exist.</p> <p><code>-a --all</code> Remove all alternative policies.</p> <p><code>--h --help</code> Show this help and exit.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>You can remove just one policy at a time. User must select the local alternative policy to remove.</p> </div> |
| <code>restore-alternative-policy</code> <code>[options]</code> | FW L2FW IPS | <p>Not supported on Master Security Engine or Virtual Security Engine.</p> <p>Restore selected local alternative policy(s).</p> <p>You can remove just one policy at a time. User must select the local alternative policy to remove.</p> |


| Command | Role | Description |
|---|----------------------------------|--|
| <pre>sg-blocklist show [-v] [-f FILENAME] add [[-i FILENAME] [src IP_ADDRESS/MASK] [src6 IPv6_ADDRESS/PREFIX] [dst IP_ADDRESS/MASK] [dst6 IPv6_ADDRESS/PREFIX] [proto {tcp udp icmp NUM}] [srcport PORT {-PORT}] [dstport PORT {-PORT}] [duration NUM] [ve VIRTUAL_ENGINE_ID]] del [[-i FILENAME] [src IP_ADDRESS/MASK] [src6 IPv6_ADDRESS/PREFIX] [dst IP_ADDRESS/MASK] [dst6 IPv6_ADDRESS/PREFIX] [proto {tcp udp icmp NUM}] [srcport PORT{-PORT}] [dstport PORT{-PORT}] [duration NUM] [ve VIRTUAL_ENGINE_ID]] iddel NODE_ID ID flush</pre> | <p>FW</p> <p>L2FW</p> <p>IPS</p> | <p>Used to view, add, or delete active block list entries.</p> <p>The block list is applied as defined in Access Rules.</p> <p><code>show</code> shows the current active block list entries in format: <code>engine node ID block list entry ID (internal) entry creation time (internal) address and port match originally set duration (internal) (internal)</code>. Use the <code>-f</code> option to specify a storage file to view (<code>/data/block_list/db_<number></code>). The <code>-v</code> option adds operation's details to the output.</p> <p><code>add</code> creates a block list entry. Enter the parameters or use the <code>-i</code> option to import parameters from a file.</p> <p><code>del</code> deletes the first matching block list entry. Enter the parameters or use the <code>-i</code> option to import parameters from a file.</p> <p><code>iddel</code> removes one specific block list entry on one specific Security Engine. <code>NODE_ID</code> is the ID of the Security Engine, <code>ID</code> is the block list entry's ID (as shown by the <code>show</code> command).</p> <p><code>flush</code> deletes all block list entries.</p> <p>Add/Del Parameters:</p> <p>Enter at least one parameter. The default value is used for the parameters that you omit. You can also save parameters in a text file; each line in the file is read as one block list entry.</p> <p><code>src</code> defines the source IP address and netmask to match. Matches any IP address by default.</p> <p><code>src6</code> defines the source IPv6 and prefix length to match. Matches any IPv6 address by default.</p> <p><code>dst</code> defines the destination IP address and netmask to match. Matches any IP address by default.</p> <p><code>dst6</code> defines the destination IPv6 address and prefix length to match. Matches any IPv6 address by default.</p> <p><code>proto</code> defines the protocol to match by name or protocol number. Matches all IP traffic by default.</p> <p><code>srcport</code> defines the TCP/UDP source port or range to match. Matches any port by default.</p> <p><code>dstport</code> defines the TCP/UDP destination port or range to match. Matches any port by default.</p> <p><code>duration</code> defines in seconds how long the entry is kept. Default is 0, which cuts current connections, but is not kept.</p> <p><code>ve</code> specifies the Virtual Engine on which the block list entry is created or deleted.</p> <p>Examples:</p> <pre>sg-blocklist add src 192.168.0.2/32 proto tcp dstport 80 duration 60 sg-blocklist add -i myblock list.txt sg-blocklist del dst 192.168.1.0/24 proto 47</pre> |


| Command | Role | Description |
|--|-------------------|--|
| <pre>sg-bootconfig [--primary-console=tty0 ttyS PORT,SPEED] [--secondary-console=[tty0 ttyS PORT,SPEED]] [--flavor=up smp] [--initrd=yes no] [--crashdump=yes no Y@X] [--append=kernel options] [--help] apply</pre> | FW L2FW IPS | <p>Used to edit boot command parameters for future bootups.</p> <p><code>--primary-console</code> defines the terminal settings for the primary console.</p> <p><code>--secondary-console</code> defines the terminal settings for the secondary console.</p> <p><code>--flavor</code> defines whether the kernel is uniprocessor or multiprocessor.</p> <p><code>--initrd</code> defines whether Ramdisk is enabled or disabled.</p> <p><code>--crashdump</code> defines whether kernel crashdump is enabled or disabled, and how much memory is allocated to the crash dump kernel (Y). The default is 24M. X must always be 16M.</p> <p><code>--append</code> defines any other boot options to add to the configuration.</p> <p><code>--help</code> shows usage information.</p> <p><code>apply</code> applies the specified configuration options.</p> |
| <pre>sg-clear-all [--help] [--flash-defaults] [--dry-run] [--on-boot] [--reboot --shutdown] [--fast] --wipe <number>] [--debug --verbose]</pre> | FW L2FW IPS | <p>This command restores the factory default settings on the Security Engine.</p> <p><code>--help</code> shows usage information.</p> <p><code>--flash-defaults</code> assumes that the Security Engine has a flash data partition and a RAM pool partition.</p> <p><code>--dry-run</code> exits without shutting down or restarting when command execution finishes.</p> <p><code>--on-boot</code> indicates that Security Engine is starting up. This option is not intended to be used in normal command line usage.</p> <p><code>--reboot</code> the Security Engine always restarts when command execution finishes.</p> <p><code>--shutdown</code> the Security Engine always shuts down when command execution finishes.</p> <p><code>--fast</code> runs a minimal, non-interactive clear for testing purposes.</p> <p><code>--wipe <number></code> globally specifies the number of times to wipe partitions.</p> <p><code>--debug</code> shows full debug messages during command execution.</p> <p><code>--verbose</code> shows additional informational messages during command execution.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>If you run the command without specifying any options, the Security Engine requests confirmation before restarting. When the Security Engine restarts, you are prompted to select the system restore options.</p> </div> <p>After using this command, you can reconfigure the Security Engine using the <code>sg-reconfigure</code> command.</p> |

| Command | Role | Description |
|--|-------------------|--|
| <code>sg-cluster</code> <code>[-v <Virtual Engine ID>]</code> <code>[status [-c SECONDS]]</code> <code>[versions]</code> <code>[online]</code> <code>[lock-online]</code> <code>[offline]</code> <code>[lock-offline]</code> <code>[standby]</code> <code>[safe-offline]</code> <code>[force-online]</code> <code>[move]</code> | FW L2FW IPS | <p>Shows or changes the status of the node.</p> <p><code>-v</code> (Master Engine only) specifies the ID of the Virtual Engine on which to execute the command.</p> <p><code>status</code> shows cluster status. When <code>-c SECONDS</code> is used, the status is shown continuously with the specified number of seconds between updates.</p> <p><code>version</code> shows the Security Engine software versions of the nodes in the cluster.</p> <p><code>online</code> sends the node online.</p> <p><code>lock-online</code> sends the node online and keeps it online, even if another process tries to change its state.</p> <p><code>offline</code> sends the node offline.</p> <p><code>lock-offline</code> sends the node offline and keeps it offline, even if another process tries to change its state.</p> <p><code>standby</code> sets an active node to standby.</p> <p><code>safe-offline</code> sets the node to offline only if there is another online node.</p> <p><code>force-online</code> sets the node online regardless of state or any limitations. Also sets all other nodes offline.</p> <p><code>[move]</code> (Master Engine only) moves the specified Virtual Security Engine to this node.</p> |
| <code>sg-contact-mgmt</code> | FW L2FW IPS | <p>Used for establishing a trust relationship with the Management Server as part of Security Engine installation or reconfiguration (see <code>sg-reconfigure</code>).</p> <p>The Security Engine contacts the Management Server using the one-time password created when the Security Engine's initial configuration is saved.</p> |
| <code>sg-diagnostics [-s -u] -f <facility_number></code> | FW L2FW IPS | <p>Enables or disables diagnostics for the specified facility. When enabled, diagnostic information for the specified facility is included in the log data.</p> <p><code>-f <facility_number></code> specifies the facility for which to enable diagnostics. Use the <code>sg-logger -s</code> command to get a list of facility numbers.</p> <p><code>-s</code> enables diagnostics.</p> <p><code>-u</code> disables diagnostics.</p> <p>When you run the command without <code>-s</code> or <code>-u</code>, the output shows the current value for the specified facility.</p> |

| Command | Role | Description |
|---|------|---|
| <pre>sg-dynamic-routing [start] [stop] [restart] [force-reload] [backup <file>] [restore <file>] [sample-config] [route-table] [info]</pre> | FW | <pre>start</pre> starts the Free Range Routing (FRR) routing suite. <pre>stop</pre> stops the FRR routing suite and flushes all routes made by zebra. <pre>restart</pre> restarts the FRR routing suite. <pre>force-reload</pre> forces reload of the saved configuration. <pre>backup</pre> backs up the current configuration to a compressed file. <pre>restore</pre> restores the configuration from the specified file. <pre>sample-config</pre> creates a basic configuration for FRR. <pre>route-table</pre> prints the current routing table. <pre>info</pre> shows the help information for the <code>sg-dynamic-routing</code> command, and detailed information about FRR suite configuration with <code>vtsh</code> . |
| <pre>sg-ipsec -d [-u <username[@domain]> -si <session id> -ck <ike cookie> -tri <transform id> -ri <remote ip> -ci <connection id>]</pre> | FW | Deletes VPN-related information (use the <code>vpntool</code> command to view the information). Option <code>-d</code> (for delete) is mandatory. <ul style="list-style-type: none"> <code>-u</code> deletes the VPN session of the named VPN client user. You can enter the user account in the form <code><user_name@domain></code> if there are several user storage locations (LDAP domains). <code>-si</code> deletes the VPN session of a VPN client user based on session identifier. <code>-ck</code> deletes the IKE SA (Phase one security association) based on IKE cookie. <code>-tri</code> deletes the IPSEC SAs (Phase two security associations) for both communication directions based on transform identifier. <code>-ri</code> deletes all SAs related to a remote IP address in site-to-site VPNs. <code>-ci</code> deletes all SAs related to a connection identifier in site-to-site VPNs. |

| Command | Role | Description |
|--|----------------------------------|--|
| <pre>sg-log-view -h --help -c CONFIGURATION_FILE -C --show-configuration -N --show-field-names -A --alerts -o {list table json json-pretty} --output-format {list table json json-pretty} -f --follow -t TABLE_FIELDS [TABLE_FIELDS ...] -- table-fields TABLE_FIELDS [TABLE_FIELDS ...] -a ADD_TABLE_FIELDS [ADD_TABLE_FIELDS ...] --add- table-fields ADD_TABLE_FIELDS [ADD_TABLE_FIELDS ...] -r REMOVE_TABLE_FIELDS [REMOVE_TABLE_FIELDS ...] --remove-table-fields REMOVE_TABLE_FIELDS [REMOVE_TABLE_FIELDS ...] -I --add-event-id-table-field -i EVENT_IDS [EVENT_IDS ...] --event-ids EVENT_IDS [EVENT_IDS ...] -s START_DATE --start-date START_DATE -e END_DATE --end-date END_DATE -F FILTERS [FILTERS ...] -- filters [FILTERS ...] --input-file-format {binary json} --log-files [LOG_FILES [LOG_FILES ...]] --timestamp-type {date integer} -S --show-log-counter</pre> | <p>FW</p> <p>L2FW</p> <p>IPS</p> | <p>If you have saved copies of the most recent log and alert entries locally on the Security Engine, allows you to browse log and alert entries on the command line of the Security Engine.</p> <p>-h --help shows usage information.</p> <p>-c specifies a configuration file for viewing stored log entries. If you do not specify a configuration file in this command, the <code>LOG_VIEW_CONF</code> environment variable specifies the configuration file. If no configuration file is specified in the <code>LOG_VIEW_CONF</code> variable, the default configuration is used.</p> <p>-C --show-configuration shows the active configuration.</p> <p>-N --show-field-names shows all available log field names.</p> <p>-A --alerts shows alert entries instead of log entries.</p> <p>-o --output-format specifies the output format for log entries. The default is table.</p> <p>-f --follow shows log entries in real time as they are generated.</p> <p>-t --table-fields shows the specified fields in a table view. You can specify the width and position of the field in the table using numbers and semicolons. For example, <code>situation:40:3</code>.</p> <p>-a --add-table-fields adds the specified fields to the table view. You can specify the width and position of the field in the table using numbers and semicolons. For example, <code>situation:40:3</code>.</p> <p>-r --remove-table-fields removes the specified fields from the table view.</p> <p>-I --add-event-id-table-field adds <code>event_id</code> as the first log field in the table view.</p> <p>-i --event-ids shows details about the specified events (event ids) in a list view.</p> <p>-s --start-date shows log entries starting from the specified date.</p> <p>-e --end-date shows log entries ending on the specified date.</p> <p>-F --filters specifies log filters as either a simple filter string or a complete JSON filter string.</p> <p>--input-file-format specifies the input log file format. The default is binary.</p> <p>--log-files specifies the log files to show. If you do not specify a log file, all available log files found in the specified log directories are shown.</p> <p>--timestamp-type shows timestamp values as dates or integers. The default is date.</p> <p>-S --show-log-counter shows log counters in table and list views.</p> |

| Command | Role | Description |
|---|-------------------|---|
| <code>sg-logger</code> <code>-f FACILITY_NUMBER</code> <code>-t TYPE_NUMBER</code> <code>[-e EVENT_NUMBER]</code> <code>[-i "INFO_STRING"]</code> <code>[-s]</code> <code>[-h]</code> | FW L2FW IPS | Used in scripts to create log messages with the specified properties. <code>-f</code> defines the facility for the log message. <code>-t</code> defines the type for the log message. <code>-e</code> defines the log event for the log message. The default is <code>0</code> (H2A_LOG_EVENT_UNDEFINED). <code>-i</code> defines the information string for the log message. <code>-s</code> dumps information about option numbers to stdout <code>-h</code> shows usage information. |
| <code>sg-raid</code> <code>[-status] [-add] [-re-add]</code> <code>[-force] [-help]</code> | FW L2FW IPS | Configures a new hard drive. This command is only for Security Engine appliances that support RAID (Redundant Array of Independent Disks) and have two hard drives. <code>-status</code> shows the status of the hard drive. <code>-add</code> adds a new empty hard drive. Use <code>-add -force</code> if you want to add a hard drive that already contains data and you want to overwrite it. <code>-re-add</code> adds a hard drive that is already partitioned. This command prompts for the drive and partition for each degraded array. Use <code>-re-add -force</code> if you want to check all arrays. <code>-help</code> shows usage information. |
| <code>sg-reconfigure</code> <code>[--maybe-contact]</code> <code>[--no-shutdown]</code> <code>[--stop-autocontact]</code> | FW L2FW IPS | Starts the Security Engine Configuration Wizard. Used for reconfiguring the node manually.  CAUTION This script also has parameters that are for the internal use of the Security Engine only. Do not use this script with any parameters other than the ones listed here. <code>--maybe-contact</code> contacts the Management Server if requested. This option is only available on Engines. <code>--no-shutdown</code> allows you to make limited configuration changes on the node without shutting it down. Some changes might not be applied until the node is rebooted. <code>--stop-autocontact</code> (unconfigured Security Engine appliances with valid POS codes only) prevents the Security Engine from contacting the installation server for plug-and-play configuration when it reboots. |
| <code>sg-selftest [-d] [-h]</code> | FW | Runs cryptography tests on the Security Engine. <code>-d</code> runs the tests in debug mode. <code>-h</code> shows usage information. |
| <code>sg-status [-l] [-h]</code> | FW L2FW IPS | Shows information about the Security Engine status. <code>-l</code> shows all available information about Security Engine status. <code>-h</code> shows usage information. |

| Command | Role | Description |
|---|-------------------|---|
| <pre>sg-toggle-active SHA1 SIZE --force [--debug]</pre> | FW L2FW IPS | <p>Switches the Security Engine between the active and the inactive partition.</p> <p>This change takes effect when you reboot the Security Engine.</p> <p>You can use this command, for example, if you have upgraded an Security Engine and want to switch back to the earlier Security Engine version. When you upgrade the Security Engine, the active partition is switched. The earlier configuration remains on the inactive partition. To see the currently active (and inactive) partition, see the directory listing of <code>/var/run/stonegate</code> (<code>ls -l /var/run/stonegate</code>).</p> <p>The <code>SHA1</code> option is used to verify the signature of the inactive partition before changing it to active. If you downgrade the Security Engine, check the checksum and the size of the earlier upgrade package by extracting the signature and size files from the <code>sg_engine_[version.build]_i386.zip</code> file.</p> <p><code>--debug</code> reboots the Security Engine with the debug kernel.</p> <p><code>--force</code> switches the active configuration without first verifying the signature of the inactive partition.</p> |
| <pre>sg-upgrade</pre> | FW | <p>Upgrades the node by rebooting from the installation DVD.</p> <p>Alternatively, the node can be upgraded remotely using the SMC Client.</p> |
| <pre>sg-version</pre> | FW L2FW IPS | Shows the software version and build number for the node. |
| <pre>se-virtual-engine -l --list -v <Virtual Engine ID> -e --enter -E "<command [options]>" -h --help</pre> | FW | <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Note</p> <p>Master Engine only.</p> </div> </div> <p>Used to send commands to Virtual Engines from the command line of the Master Engine.</p> <p>All commands that can be used for the Engine role can also be used for Virtual Engines.</p> <p><code>-l</code> or <code>--list</code> list the active Virtual Engines.</p> <p><code>-v</code> specifies the ID of the Virtual Engine on which to execute the command.</p> <p><code>-e</code> or <code>--enter</code> enters the command shell for the Virtual Engine specified with the <code>-v</code> option. To exit the command shell, type <code>exit</code>.</p> <p><code>-E</code> executes the specified command on the Virtual Engine specified with the <code>-v</code> option.</p> <p><code>-h</code> or <code>--help</code> shows usage information.</p> |

| Command | Role | Description |
|---|-------------------|--|
| sglinfo [-f] [-d] [-s] [-p] [--] [--help] | FW L2FW IPS | Gathers system information you can send to Forcepoint Customer Hub . Use this command only when instructed to do so by Forcepoint Customer Hub . -f forces sglInfo even if the configuration is encrypted. -d includes core dumps in the sglInfo file. -s includes slapcat output in the sglInfo file. -p includes passwords in the sglInfo file (by default passwords are erased from the output). -- creates the sglInfo file without showing the progress. --help shows usage information. |

The following table lists some general Linux operating system commands that can be useful in running your Security Engines. Some commands can be stopped by pressing **Ctrl+C**.

General command line tools on Security Engines

| Command | Description |
|---------|---|
| dmesg | Shows system logs and other information. Use the -h option to see usage. |
| halt | Shuts down the system. |
| ip | Shows IP address information. Type the command without options to see usage. Example: type ip addr for basic information about all interfaces. |
| ping | Tests connectivity with ICMP echo requests. Type the command without options to see usage. |
| ps | Reports the status of running processes. |
| reboot | Reboots the system. |
| scp | Secure copy. Type the command without options to see usage. |
| sftp | Secure FTP. Type the command without options to see usage. |
| ssh | SSH client (for opening a terminal connection to other hosts). Type the command without options to see usage. |
| tcpdump | Gives information about network traffic. Use the -h option to see usage. You can also analyze network traffic by creating tcpdump files from the SMC Client with the Traffic Capture feature. |
| top | Shows the top CPU processes taking most processor time. Use the -h option to see usage. |

| Command | Description |
|----------------------|--|
| <code>tracert</code> | Traces the route packets take to the specified destination. Type the command without options to see usage. |
| <code>vpntool</code> | Shows VPN information and allows you to issue some basic commands. Type the command without options to see usage. |

Server Pool Monitoring Agent commands

You can test and monitor the Server Pool Monitoring Agents on the command line.

Server Pool Monitoring Agent commands

| Command | Description |
|---|---|
| <code>agent</code> <code>[-v level]</code> <code>[-c path]</code> <code>[test [files]]</code> <code>[syntax [files]]</code> | <p>(Windows only) Allows you to test different configurations before activating them.</p> <p><code>-v</code> sets the verbosity level. The default level is 5. Levels 6–8 are for debugging where available.</p> <p><code>-c</code> uses the specified path as the first search directory for the configuration.</p> <p><code>test</code> runs in the test mode - status queries do not receive a response. If you specify the files, they are used for reading the configuration instead of the default files.</p> <p><code>syntax</code> checks the syntax in the configuration file. If no files are specified, the default configuration files are checked.</p> |
| <code>sgagentd [-d]</code> <code>[-v level]</code> <code>[-c path]</code> <code>[test [files]]</code> <code>[syntax [files]]</code> | <p>(Linux only) Allows you to test different configurations before activating them.</p> <p><code>-d</code> means Don't Fork as a daemon. All log messages are printed to stdout or stderr only.</p> <p><code>-v</code> sets the verbosity level. The default level is 5. Levels 6–8 are for debugging where available.</p> <p><code>-c</code> uses the specified path as the first search directory for the configuration.</p> <p><code>test</code> runs in the test mode - status queries do not receive a response. If you specify the files, they are used for reading the configuration instead of the default files. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the <code>-d</code> option.</p> <p><code>syntax</code> checks the syntax in the configuration file. If no files are specified, the default configuration files are checked. The output is directed to syslog or eventlog instead of the console where the command was run unless you use the <code>-d</code> option.</p> |

| Command | Description |
|--|---|
| <code>sgmon</code> <code>[status info proto]</code> <code>[-p port]</code> <code>[-t timeout]</code> <code>[-a id]</code> <code>host</code> | <p>Sends a UDP query to the specified host and waits for a response until received, or until the timeout limit is reached. The request type can be defined as a parameter. If no parameter is given, status is requested. The commands are:</p> <ul style="list-style-type: none"><code>status</code> queries the status.<code>info</code> queries the agent version.<code>proto</code> queries the highest supported protocol version.<code>-p</code> connects to the specified port instead of the default port.<code>-t</code> sets the timeout (in seconds) to wait for a response.<code>-a</code> acknowledge the received log messages up to the specified id. Each response message has an id, and you can acknowledge more than one message at a given time by using the id parameter. Messages acknowledged by <code>sgmon</code> will no longer appear in the engine logs. <p><code>host</code> is the IP address of the host to connect to. To get the status locally, you can give <code>localhost</code> as the host argument. This parameter is mandatory.</p> |

Installing SMC Appliance software on a virtualization platform

Contents

- Hardware requirements for installing SMC Appliance software on a virtualization platform on page 275
- Install SMC Appliance software using an .iso file on page 275

You can install the SMC Appliance software as a virtual machine on virtualization platforms such as VMware ESX. After installation, you can patch and upgrade the SMC Appliance in the same way as a purpose-built SMC Appliance.

Hardware requirements for installing SMC Appliance software on a virtualization platform

There are some hardware and software requirements when you run SMC Appliance software on a virtualization platform.

For more information, see the [Release Notes](#).

Install SMC Appliance software using an .iso file

Use an `.iso` file of the SMC Appliance software to install the SMC Appliance on the VMware ESX virtualization platform.

Steps

- 1) Create the virtual machine and configure it according to your requirements. You need to set VM options / Boot options / Firmware to "BIOS".
- 2) Download the license at <https://stonesoftlicenses.forcepoint.com>.
- 3) Download the `.iso` installation file at <https://support.forcepoint.com>.
- 4) Connect the DVD drive of the virtual machine to the `.iso` file.

- 5) Restart the virtual machine.
- 6) When the Security Engine SMC Appliance installer starts, select **Begin** and press **Enter**.
- 7) Select **Fresh Install** and press **Enter**.
A warning that all data on the disk will be erased is shown.
- 8) Select **Next** and press **Enter**.
You are prompted to review the configuration.
- 9) Select **Confirm** and press **Enter**.
- 10) When the SMC Appliance software installation is complete, select **Reboot** and press **Enter** to restart the virtual machine.

Next steps

Continue the SMC Appliance installation by configuring the operating system settings on the command line of the SMC Appliance.

Related tasks

[Install the SMC Appliance on page 51](#)

Installing Forcepoint Security Engine on a virtualization platform

Contents

- Hardware requirements for installing Forcepoint Security Engine software on a virtualization platform on page 277
- Install Forcepoint Security Engine software using an .iso file on page 277

You can install the Security Engine software as a virtual machine on virtualization platforms such as VMware ESX or KVM.

The same Security Engine software can be used in the Security Engine with Layer 3 Interfaces, IPS role, or Layer 2 Engine role. The engine role is selected during the initial configuration of the engine.

Hardware requirements for installing Forcepoint Security Engine software on a virtualization platform

There are some hardware and software requirements, and configuration limitations when you run Security Engine software on a virtualization platform.

For more information, see the [Release Notes](#).

Install Forcepoint Security Engine software using an `.iso` file

Use an `.iso` file of the Security Engine software to install Security Engine on VMware ESX, KVM, or Microsoft Hyper-V virtualization platforms.

Only Security Engines with Layer 3 Interfaces are supported on the Microsoft Hyper-V virtualization platform.

Steps

- 1) Create the virtual machine and configure it according to your requirements. You need to set VM options / Boot options / Firmware to "BIOS".



Note

It is recommended to select the highest 64bit Debian GNU/Linux version for the Guest Operating System.

- 2) (IPS and Layer 2 Engine only) Configure the virtual switches to which the IPS or Layer 2 Engine inline interfaces are connected:
 - a) Create a port group, then assign **All** (4095) as the **VLAN ID**.
 - b) Enable the use of **Promiscuous Mode**.
- 3) (Engine with Layer 3 Interfaces only) In the virtual switch settings, select **Accept** for the **MAC Address Changes** and **Forged Transmits** options.
- 4) Download the license at <https://stonesoftlicenses.forcepoint.com>.
- 5) Download the `.iso` installation file at <https://support.forcepoint.com>.
- 6) Connect the DVD drive of the virtual machine to the `.iso` file.
- 7) Restart the virtual machine.
The License Agreement appears.
- 8) Type `YES`, then press **Enter** to accept the license agreement and continue with the configuration.
- 9) Select the type of installation:
 - Type `1` for the normal **Full Install**.
 - Type `2` for the **Full Install in expert mode** if you want to partition the hard disk manually.
- 10) If the number of processors is not detected automatically, enter the number of processors:
 - For a uniprocessor system, type `1`, then press **Enter**.
 - For a multiprocessor system, type `2`, then press **Enter**.
- 11) Continue in one of the following ways:
 - If you selected **Full Install**, type `YES`, then press **Enter** to accept automatic hard disk partitioning.
 - If you selected **Full Install in expert mode**, install the engine in expert mode.

Result

The installation process starts. For more details, refer to the *Installing Forcepoint Security Engine software on third-party hardware* topic.

Related information

Installing Forcepoint Security Engine software on third-party hardware on page 281

Installing Forcepoint Security Engine software on third-party hardware

Contents

- Hardware requirements for installing Security Engine on third-party hardware on page 281
- Start the Forcepoint Security Engine installation on third-party hardware on page 286
- Install Forcepoint Security Engine in expert mode on page 287

You can install the Security Engine software on third-party hardware that meets the hardware requirements.

Hardware requirements for installing Security Engine on third-party hardware

There are some basic hardware requirements when you run Security Engine on third-party hardware.

For more information, see the [Release Notes](#).

For information about supported Ethernet interface types and adapters, see Knowledge Base article [9721](#).



CAUTION

Check that the Automatic Power Management (APM) and Advanced Configuration and Power Interface (ACPI) settings are disabled in BIOS. Otherwise, the engine might not start after installation or can shut down unexpectedly.



CAUTION

The hardware must be dedicated to the Security Engine. No other software can be installed on it.

Hardware drivers

We recommend using the listed approved drivers supported by Security Engine.

Tested network interface card drivers included in the kernel of Security Engine are listed in the following table. These drivers have been tested for use in Security Engine.

Tested network interface card drivers

| Driver | Version | Description |
|-----------------|------------|---|
| e1000e.ko | No version | Intel® PRO/1000 Network Driver |
| e1000x.ko | No version | Intel® PRO/1000 Network Driver |
| i40e.ko | 2.15.9+sg1 | Intel® 40-10 Gigabit Ethernet Connection Network Driver |
| ice.ko | 1.6.7+sg2 | Intel® Corporation Ethernet Connection E822-L 1GbE |
| igb.ko | No version | Intel® Gigabit Ethernet Linux Driver |
| igc.ko | No version | Intel® Corporation Ethernet Controller I226-V |
| ixgbe.ko | 5.2.4+sg11 | Intel® 10GbE PCI Express Linux Network Driver |
| virtio_net.ko | No version | Virtio network driver |
| vmxnet3.ko | No version | VMware vmxnet3 virtual NIC driver |
| xen-netfront.ko | No version | Xen virtual network device frontend |

Other network interface card drivers included in the kernel of Security Engine are listed in the following table. All drivers are the driver version that is included in the standard Linux 6.6.88 kernel.

**Note**

These drivers have not been tested for use in Security Engine.

Other network interface card drivers

| Driver | Description |
|-------------|---|
| 3c59x.ko | 3Com 3c59x/3c9xx Ethernet driver |
| 8139cp.ko | RealTek RTL-8139C+ series 10/100 PCI Ethernet Driver |
| 8139too.ko | RealTek RTL-8139 Fast Ethernet Driver |
| 8390.ko | No description |
| acenic.ko | AceNIC/3C985/GA620 Gigabit Ethernet Driver |
| amd8111e.ko | AMD8111 based 10/100 Ethernet Controller |
| atl1.ko | Atheros L1 Gigabit Ethernet Driver |
| atl1e.ko | Atheros 1000M Ethernet Network Driver |
| b44.ko | Broadcom 44xx/47xx 10/100 PCI Ethernet Driver |
| be2net.ko | Emulex OneConnect NIC Driver |
| bnx2.ko | QLogic BCM5706/5708/5709/5716 Driver |
| bnx2x.ko | QLogic BCM57710/57711/57711E/57712/57712_MF/57800/57800_MF/57810/57810_MF/57840/57840_MF Driver |
| tg3.ko | Broadcom Tigon3 Ethernet Driver |
| dl2k.ko | D-Link DL2000-based Gigabit Ethernet Adapter |

| Driver | Description |
|---------------|--|
| dmfe.ko | Davicom DM910X fast Ethernet Driver |
| e100.ko | Intel® PRO/100 Network Driver |
| ena_ik.ko | Elastic Network Adapter (ENA) |
| epic100.ko | SMC 83c170 EPIC series Ethernet Driver |
| fealnx.ko | Myson MTD-8xx 100/10M Ethernet PCI Adapter Driver |
| fm10k.ko | Intel® Ethernet Switch Host Interface Driver |
| forcedeth.ko | Reverse Engineered nForce Ethernet Driver |
| i40e_ik.ko | Intel® Ethernet Connection XL710 Network Driver |
| iavf.ko | Intel® Ethernet Adaptive Virtual Function Network Driver |
| ice_ik.ko | Intel® Ethernet Connection E800 Series Linux Driver |
| ixgbe_ik.ko | Intel® 10 Gigabit PCI Express Network Driver |
| ixgbev.ko | Intel® 10 Gigabit Virtual Function Network Driver |
| mlx4_core.ko | Mellanox ConnectX HCA low-level driver |
| mlx4_en.ko | Mellanox ConnectX HCA Ethernet Driver |
| mlx5_core.ko | Mellanox 5th generation network adapters (ConnectX series) core driver |
| myri10ge.ko | Myricom 10G driver (10GbE) |
| natsemi.ko | National Semiconductor DP8381x series PCI Ethernet Driver |
| ne2k-pci.ko | PCI NE2000 clone driver |
| netxen_nic.ko | QLogic/NetXen (1/10) GbE Intelligent Ethernet Driver |
| niu.ko | NIU Ethernet Driver |
| ns83820.ko | National Semiconductor DP83820 10/100/1000 driver |
| pcnet32.ko | Driver for PCnet32 and PCnetPCI based ethercards |
| qed.ko | QLogic FastLinQ 4xxxx Core Module |
| qede.ko | QLogic FastLinQ 4xxxx Ethernet Driver |
| qla3xxx.ko | QLogic ISP3XXX Network Driver v2.03.00-k5 |
| r6040.ko | RDC R6040 NAPI PCI FastEthernet driver |
| r8169.ko | RealTek RTL-8169 Gigabit Ethernet Driver |
| sc92031.ko | Silan SC92031 PCI Fast Ethernet Adapter Driver |
| sis190.ko | SiS sis190/191 Gigabit Ethernet Driver |
| sis900.ko | SiS 900 PCI Fast Ethernet Driver |
| skge.ko | SysKonnect Gigabit Ethernet Driver |
| sky2.ko | Marvell Yukon 2 Gigabit Ethernet Driver |
| starfire.ko | Adaptec Starfire Ethernet Driver |

| Driver | Description |
|-----------------|--|
| sundance.ko | Sundance Alta Ethernet driver |
| sungem.ko | Sun GEM Gbit Ethernet Driver |
| sunhme.ko | Sun HappyMealEthernet(HME) 10/100baseT Ethernet Driver |
| tehuti.ko | Tehuti Networks® Network Driver |
| tg3.ko | Broadcom Tigon3 ethernet driver |
| tulip.ko | Digital 214 Tulip Ethernet Driver |
| typhoon.ko | 3Com Typhoon Family (3C990, 3CR990, and variants) |
| uli526x.ko | ULi M5261/M5263 fast Ethernet Driver |
| via-rhine.ko | VIA Rhine PCI Fast Ethernet driver |
| via-velocity.ko | VIA Networking Velocity Family Gigabit Ethernet Adapter Driver |
| winbond-840.ko | Winbond W89c840 Ethernet driver |

SCSI drivers included in the kernel of Security Engine are listed in the following table. All drivers are the driver version that is included in the standard Linux 6.6.88 kernel.



Note

Not all included drivers have been tested for use in Security Engine.

SCSI drivers

| Driver | Description |
|--|----------------------------|
| 3Ware 9xxx SATA_RAID | [CONFIG_SCSI_3W_9XXX] |
| Adaptec / IBM ServeRAID | [CONFIG_SCSI_IPS] |
| Adaptec AACRAID | [CONFIG_SCSI_AACRAID] |
| Adaptec I2O RAID | [CONFIG_SCSI_DPT_I2O] |
| Adaptec SAS/SATA 3Gb/s | [CONFIG_SCSI_AIC94X] |
| Adaptec Ultra160 | [CONFIG_SCSI_AIC7XXX] |
| BusLogic MultiMaster and FlashPoint SCSI | [CONFIG_SCSI_BUSLOGIC] |
| Domex DMX3191D SCSI | [CONFIG_SCSI_DMX3191D] |
| Fusion MPT ScsiHost for FC/SPI/SAS | [CONFIG_FUSION_FC/SPI/SAS] |
| Initio INIA100 SCSI | [CONFIG_SCSI_INIA100] |
| Intel PIIX/ICH PATA/SATA | [CONFIG_ATA_PIIX] |
| LSI Logic MegaRAID (Legacy) | [CONFIG_MEGARAID_LEGACY] |
| LSI Logic MegaRAID (NEWGEN) | [CONFIG_MEGARAID_NEWGEN] |
| LSI Logic MegaRAID (SAS) | [CONFIG_MEGARAID_SAS] |
| NVIDIA nForce SATA | [CONFIG_SATA_NV] |
| Pacific Digital ADMA | [CONFIG_PDC_ADMA] |

| Driver | Description |
|--|---------------------------|
| Promise SATA | [CONFIG_SATA_SX4] |
| Promise SATA TX2/TX4 | [CONFIG_SATA_PROMISE] |
| QLogic IPS2x00 | [CONFIG_SCSI_QLA2XXX] |
| QLogic ISP1240/1x80/1x160/1020/1040 SCSI | [CONFIG_SCSI_QLOGIC_1280] |
| ServerWorks / Apple K2 SATA | [CONFIG_SATA_SVW] |
| Silicon Image 3124/3132 SATA | [CONFIG_SATA_SIL24] |
| Silicon Image SATA | [CONFIG_SATA_SIL] |
| Silicon Integrated Systems SATA | [CONFIG_SATA_SIS] |
| Symbios/LSI logic 53C8XX/53C101 | [CONFIG_SCSI_SYM53C8XX_2] |
| Tekram DC390(T) PCI SCSI | [CONFIG_SCSI_DC390T] |
| ULi Electronics SATA | [CONFIG_SATA_ULI] |
| VIA SATA | [CONFIG_SATA_VIA] |
| Vitesse VSC7174 SATA | [CONFIG_SATA_VITESSE] |
| Vortex GDT Disk Array / Intel Storage RAID | [CONFIG_SCSI_GDTH] |

Block device drivers included in the kernel of Security Engine are listed in the following table. All drivers are the driver version that is included in the standard Linux 6.6.88 kernel.



Note

Not all included drivers have been tested for use in Security Engine.

Block device drivers

| Driver |
|--|
| 3ware Storage controller |
| Compaq Smart Array 5xxx |
| Compaq SMART2 Array |
| Mylec DAC960 / AcceleRAID / eXtremeRAID PCI RAID |
| Serverworks OSB4 / CSB5 / CSB6 |

Start the Forcepoint Security Engine installation on third-party hardware

After configuring the engine elements in the SMC, begin installing the Security Engine software on your own hardware.

Before you begin

Before you start installing the Security Engine software, make sure that you have the initial configuration and a one-time password for management contact for each engine. These items are generated in the SMC.



CAUTION

Installing the Security Engine software deletes all existing data on the hard disk.

Depending on your order, you might have received ready-made SMC and Security Engine software DVDs. If the DVDs are not included in the order, you must first create them.

Steps

- 1) Insert the engine installation DVD into the drive and restart the system.
The License Agreement appears.
- 2) Type **YES** and press **Enter** to accept the license agreement and continue with the configuration.
- 3) Select the type of installation:
 - Type **1** for the normal **Full Install**.
 - Type **2** for the **Full Install in expert mode** if you want to partition the hard disk manually.
- 4) Enter the number of processors:
 - For a uniprocessor system, type **1** and press **Enter**.
 - For a multiprocessor system, type **2** and press **Enter**.
- 5) Continue in one of the following ways:
 - If you selected **Full Install**, type **YES** and press **Enter** to accept automatic hard disk partitioning.
 - If you selected **Full Install in expert mode**, install the engine in expert mode.

Result

The installation process starts.

Install Forcepoint Security Engine in expert mode

You can install Security Engine in expert mode if you want to partition the hard disk manually. If you are unfamiliar with partitioning hard disks in Linux, use the normal installation process.



CAUTION

When using the command prompt, use the `reboot` command to reboot and `halt` command to shut down the node. Do not use the `init` command. You can also reboot the node using the SMC Client.

Partition the hard disk in expert mode

Typically, you need five partitions for an engine.



CAUTION

Partitioning deletes all existing data on the hard disk.

Steps

- 1) If you are asked whether you want to create an empty partition table, type `y` to continue.
- 2) When prompted, press **Enter** to continue.
The partition table is displayed.
- 3) Create the partitions for the engine as follows:

| Partition | Flags | Partition type | File system type | Size | Description |
|---------------|----------|----------------|------------------|------------------------------------|---|
| Engine root A | bootable | Primary | Linux | 1000 MB | The bootable root partition for the engine element. |
| Engine root B | | Primary | Linux | 1000 MB | Alternative root partition for the engine element. Used for the engine upgrade. |
| Swap | | Logical | Linux swap | Twice the size of physical memory. | Swap partition for the engine element. |
| Data | | Logical | Linux | 500 MB or more | Used for the boot configuration files and the root user's home directory. |
| Spool | | Logical | Linux | All remaining free disk space. | Used for spooling. |

- 4) Check that the partition table information is correct.

- 5) Select **Write** to commit the changes and confirm by typing **yes**.
- 6) Select **Quit** and press **Enter**.

Allocate partitions in expert mode

After partitioning the hard disk, assign the partitions for the engine.

Steps

- 1) Check that the partition table is correct. Type `yes` to continue.
- 2) Using the partition numbers of the partition table, assign the partitions. For example:
 - For the engine root A partition, type `1`.
 - For the engine root B partition, type `2`.
 - For the swap partition, type `5`.
 - For the data partition, type `6`.
 - For the spool partition, type `7`.
- 3) Check the partition allocation and type `yes` to continue.
The engine installation starts.
- 4) When installation is complete, remove the DVD from the system and press **Enter** to reboot.

Related tasks

[Configure Forcepoint Security Engine software using automatic configuration on page 189](#)

[Using the Security Engine Configuration Wizard on page 190](#)

Appendix F

Installing the SMC with external certificate management

Contents

- External SMC certificate management configuration overview on page 290
- Install the SMC Appliance with external certificate management on page 290
- Create a certificate for the Management Server using external certificate management on page 291
- Create a certificate for the Log Server using external certificate management on page 292
- Create certificates for Security Engines using external certificate management on page 296

When you install the SMC, you can use certificates issued by an external CA for internal TLS communication between system components.

Using certificates issued by an external CA allows you to use your own established internal CA infrastructure to generate certificates for communication between components. Certificate revocation checking is also supported. If any devices are compromised, the certificates associated with them can be revoked and replaced centrally using the external certificate management system.

The following limitations apply:

- You can only configure the SMC to use external certificates when you install the SMC. It is not possible to change to using external certificates in an existing installation.
- To use certificate revocation lists (CRLs) or online certificate status protocol (OCSP) servers, you must configure a DNS server.
- We recommend that you configure an NTP server so that the time settings for the SMC are accurate when checking validity times for certificates, CRLs, and OSCP servers.
- The Management Server and Log Server services do not start immediately after installation because the components do not yet have certificates.
- You must complete the following actions after installation before you can start using the SMC:
 - Import the external CA certificate.
 - Generate and export certificate requests.
 - Sign the certificates using the external CA.
 - Import the signed certificates.
- Only the ECDSA public key algorithm is supported.

External SMC certificate management configuration overview

When you use external certificate management, the SMC configuration consists of these general tasks.

- 1) Create a certificate for the Management Server.
- 2) Create a certificate for the Log Server.
- 3) Create certificates for Security Engines.

Install the SMC Appliance with external certificate management

To use external certificate management, you must activate the feature when you install the SMC Appliance. It is not possible to change to using external certificates in an existing installation.

Steps

- 1) Start the SMC Appliance installation.
Follow the instructions in *Install the SMC Appliance*.
- 2) In the **Configure SMC security settings**, select **Use External Certificate Authority**.
- 3) Configure the other settings according to your environment.

Next steps

Create a certificate for the Management Server.

Related tasks

[Install the SMC Appliance on page 51](#)

Create a certificate for the Management Server using external certificate management

Create a certificate request for the Management Server, export and sign the certificate request using the external CA, then import the signed certificate for the Management Server.

Steps

- 1) Log in to the command line or to the restricted shell on SMC Appliance.
- 2) Create a certificate request for the Management Server.

Enter the `sgCertifyMgtSrv` command when using the restricted shell:

```
sg sgCertifyMgtSrv.sh mode=ext-pki-init dn=<Subject DN> dns=<SubjectAltName DNS> \
key-size=<Key Size (Accepted values): 256, 384, 521> \
csr-out=<output path to Certificate Request>
```

Not on restricted shell:

```
sudo <installation directory>/bin/sgCertifyMgtSrv.sh mode=ext-pki-init dn=<Subject DN> \
dns=<SubjectAltName DNS> key-size=<Key Size (Accepted values): 256, 384, 521> \
csr-out=<output path to Certificate Request>
```



Note

The value of the Subject Alternative Name (DNS) must be unique within the SMC and the external CA.

- 3) Copy the certificate request file to a remote system using SCP.
- 4) Sign the certificate request using the external CA.
- 5) Copy the signed certificate to the SMC Appliance using SCP.
- 6) Import the signed certificate for the Management Server.

Enter the `sgCertifyMgtSrv` command when using the restricted shell:

```
sg sgCertifyMgtSrv mode=ext-pki-import \
crt-in=<path to signed certificate in PEM format> \
ca-file=<path to CA file in PEM format>
```

Not on restricted shell:

```
sudo <installation directory>/bin/sgCertifyMgtSrv.sh mode=ext-pki-import \
crt-in=<path to signed certificate in PEM format> \
ca-file=<path to CA file in PEM format>
```

7) Start the Management Server.

On restricted shell:

```
daemon_ctl restart sgMgtServer
```

Not on restricted shell:

```
sudo daemon_ctl restart sgMgtServer
```

On other platforms:

```
sudo <installation directory>/bin/sgStartMgtSrv.sh
```

Next steps

Create a certificate for the Log Server.

Create a certificate for the Log Server using external certificate management

Create a certificate request for the Log Server, export and sign the certificate request using the external CA, then import the signed certificate for the Log Server.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.


- 1) Start the SMC Client.
- 2) Accept the Management Server certificate. A certificate dialog box containing the Management Server certificate fingerprint is shown when the SMC Client contacts a Management Server for the first time. Confirm that the fingerprint shown on the client matches the server certificate fingerprint.
 - a) To view the Management Server certificate fingerprint, log on to the SMC Appliance command line with your administrator credentials, then run the following command:

```
smcasystem fingerprint
```

Not on restricted shell:

```
sudo smca-system fingerprint
```


- b) If the fingerprint shown on the command line matches the one in the client dialog box, click **Accept**.
- 3) Complete the certificate request details for the Log Server.
 - a) Select **Dashboard > Servers / Devices Dashboard**.
 - b) Browse to **Log Server**.

- c) Right-click the Log Server, then select **Properties**.
 - d) On the **Certificate** tab, enter the following information:
 - **Common Name (CN)** — Enter a common name that includes the name of the Log Server element.
 - **Subject Alternative Name (DNS)** — Enter the name of the Log Server as a fully qualified domain name (FQDN).
-  **Note**

The value of the **Subject Alternative Name (DNS)** must be unique within the SMC and the external CA.
- e) Complete the other certificate request details according to your environment.
 - f) Click **OK** to close the Log Server Properties dialog box.
- 4) On the command line of the SMC Appliance, create a certificate request and a private key for the Log Server.
- a) Enter the `sgCertifyLogSrv` command on restricted shell:


```
sgCertifyLogSrv.sh
```

Not on restricted shell:

```
sudo <installation directory>/bin/sgCertifyLogSrv.sh
```
 - b) Enter the credentials for an administrator account with unrestricted permissions (superuser).
When the certification has finished, a certificate request is created for the Log Server.
- 5) In the SMC Client, export the certificate request.
- a) Select  **Dashboard > Servers / Devices Dashboard**.
 - b) Browse to **Log Server**.
 - c) Right-click the Log Server, then select **Properties**.
 - d) On the **Certificate** tab, click **Export Certificate**, browse to the location where you want to save the certificate request, then click **Save**.
Save the certificate request in a location that is accessible from your local workstation.
 - e) Click **OK** to close the Export Certificate dialog box.
 - f) Click **OK** to close the Log Server Properties dialog box.
- 6) Sign the certificate request using the external CA, then copy the signed certificate to a location that is accessible from your local workstation.

- 7) In the SMC Client, import the signed certificate for the Log Server.
 - a) Select **Dashboard > Servers / Devices Dashboard**.
 - b) Browse to **Log Server**.
 - c) Right-click the Log Server, then select **Properties**.
 - d) On the **Certificate** tab, click **Import Signed Certificate**.
 - e) Browse to the signed certificate file, then click **OK**.
 - f) Click **OK** to close the Log Server Properties dialog box.

- 8) On the command line of the SMC Appliance, transfer the signed certificate to the Log Server.
 - a) Enter the `sgCertifyLogSrv` command when using the restricted shell:

```
sgCertifyLogSrv.sh
```

Not on restricted shell:

```
sudo <installation directory>/bin/sgCertifyLogSrv.sh
```

- b) Enter the credentials for an administrator account with unrestricted permissions (superuser).

- 9) Start the Log Server.
Enter the following command on SMC Appliance:

On restricted shell:

```
daemon_ctl restart sgLogServer
```

Not on restricted shell:


```
sudo daemon_ctl restart sgLogServer
```

On other platforms:

```
sudo <installation directory>/bin/sgStartLogSrv.sh
```

Log Server Properties dialog box - Certificate tab

| Option | Definition |
|----------------------------|---|
| Current Certificate | Shows information about the current certificate of the server. Click Export Certificate to export the current certificate. Click Renew Certificate to renew the certificate. |
| Check Revocation | Checks against certificate revocation lists (CRLs or OCSP) whether the certificate of the new connection has been revoked. The certificate must be signed by a valid certificate authority. |

| Option | Definition |
|--|--|
| Ignore Revocation Check Failures if There Are Connectivity Problems | When selected, the server ignores all CRL check failures if the server cannot connect to CRL or OCSP server. This is done based on what is specified in the certificate. |
| Organization (O) (Optional) | The name of your organization as it appears in the certificate. |
| Organization Unit (OU) (Optional) | The name of your department or division as it appears in the certificate. |
| State/Province (ST) (Optional) | The name of state or province as it appears in the certificate. |
| Locality (L) (Optional) | The name of the city as it appears in the certificate. |
| Common Name (CN) | A common name that includes the name of the Log Server element. |
| Public Key Algorithm (Not editable) | The algorithm used for the public key. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> Note For Security Engine certificates, only the ECDSA public key algorithm is supported.</p> </div> |
| Key Length | The length of the key in bits. Enter <code>521</code> or <code>384</code> . |
| Signature Algorithm (Not editable) | Shows the signature algorithm according to the key length. |
| Subject Alternative Name (DNS) | Name of the Log Server as a fully qualified domain name (FQDN). |
| Generate Certificate Request | Shows the certificate request as text. |
| Export Certificate | Exports the certificate request so that you can sign it using an external certificate authority. |
| Import Signed Certificate | Imports a certificate that has been signed using an external certificate authority. |

Next steps

Create Security Engine elements, then create certificates for the Security Engines.

Create certificates for Security Engines using external certificate management

After creating an Security Engine element, create a certificate request for each Security Engine node, export and sign the certificate request using the external CA, then import the signed certificate.

Before you begin

Create an Security Engine element. For details, refer to the *Create an element for the Security Engine* topic in the *Forcepoint Network Security Platform Common Criteria Evaluated Configuration Guide*.

Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the SMC Client, edit the certificate settings for each Security Engine node.
 - a) Select ⓘ **Engine Configuration**.
 - b) Right-click an engine, then select **Edit <element type>**.
 - c) Open the certificate settings in one of the following ways:
 - For single Security Engines, click **Certificate Settings** on the **General** tab of the Engine Editor.
 - For Security Engine clusters, browse to **General > Clustering**, right-click the **Certificate** cell for a node, then select **Edit Certificate**.

- d) In the **Certificate Settings** dialog box, do the following:
 - Select the **Check Revocation** checkbox.
 - Make sure that the **Ignore Revocation Check Failures if There Are Connectivity Problems** checkbox is not selected.
 - **Common Name (CN)** — Enter a common name that includes the name of the Security Engine element.
Example: Helsinki Security Engine
 - **Subject Alternative Name (DNS)** — Enter the name of the Security Engine node as a fully qualified domain name (FQDN).
Examples:
helsinki-security-engine.example.com
helsinki-security-engine-node1.example.com

**Note**


The value of the **Subject Alternative Name (DNS)** must be unique within the SMC and the external CA.

- **Key Length** — Select 384.

**Note**

Key-size parameters of 256 bits and 521 bits are also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.

- e) Complete the other certificate request details according to your environment.
 - f) Click **OK**.
- 2) Save the initial configuration for the Security Engine.
Follow the instructions in *Prepare for Security Engine Configuration Wizard configuration*.
 - 3) On the command line of the Security Engine, make initial contact between the Security Engine and the Management Server.
Follow the instructions in *Contact the Management Server on the command line*.
A certificate request is created for the Security Engine and transferred to the Management Server.
 - 4) In the SMC Client, export the certificate request for the Security Engine.
 - a) Select **Engine Configuration**.
 - b) Right-click an Security Engine node, then select **Certificate > Export Certificate Request**.
 - c) Browse to the location to save the certificate request and name it as you want, then click **Export**.
 - d) Click **OK** to close the Certificate dialog box.
 - 5) Sign the certificate request using the external CA, then copy the signed certificate to a location that is accessible from your local workstation.



- 6) In the SMC Client, import the signed certificate for the Security Engine.
 - a) Select  **Engine Configuration**.
 - b) Right-click an Security Engine node, then select **Certificate > Import Signed Certificate**.
 - c) Browse to the signed certificate file, then click **Import**.
 - d) Click **OK** to close the Import Certificate dialog box.

**Note**

Reboot the Engine, once the Engine gets the certificate.

Result

The Security Engine node receives the signed certificate from the Management Server.

| Certificate Settings dialog box | |
|---|---|
| Option | Definition |
| Name | The name of the element. |
| Organization (O) (Optional) | The name of your organization as it appears in the certificate. |
| Organization Unit (OU) (Optional) | The name of your department or division as it appears in the certificate. |
| State/Province (ST) (Optional) | The name of state or province as it appears in the certificate. |
| Locality (L) (Optional) | The name of the city as it appears in the certificate. |
| Common Name (CN) | A common name that includes the name of the Security Engine element. |
| Public Key Algorithm (Not editable) | <p>The algorithm used for the public key.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p> Note</p> <p>For Security Engine certificates, only the ECDSA public key algorithm is supported.</p> </div> |
| Key Length | <p>The length of the key in bits. Select <code>384</code>.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p> Note</p> <p>Key-size parameters of 256 bits and 521 bits are also acceptable if the configuration is not intended to be compatible with Commercial Solutions for Classified configuration.</p> </div> |
| Signature Algorithm (Not editable) | Shows the signature algorithm according to the key length. |

| Option | Definition |
|---------------------------------------|---|
| Subject Alternative Name (DNS) | The name of the Security Engine node as a fully qualified domain name (FQDN). |

Related concepts

[Configuring Single Engines](#) on page 78

[Configuring Engine Clusters](#) on page 105

[Configuring IPS engines](#) on page 127

[Configuring Layer 2 Engines](#) on page 144

[Master Security Engine and Virtual Security Engine configuration overview](#) on page 159

Related tasks

[Prepare for Security Engine Configuration Wizard configuration](#) on page 191

[Contact the Management Server on the command line](#) on page 197

Example network (Security Engines with Layer 3 Interfaces)

Contents

- [Example Engine Cluster on page 301](#)
- [Example Single Engine on page 304](#)
- [Example headquarters management network on page 305](#)

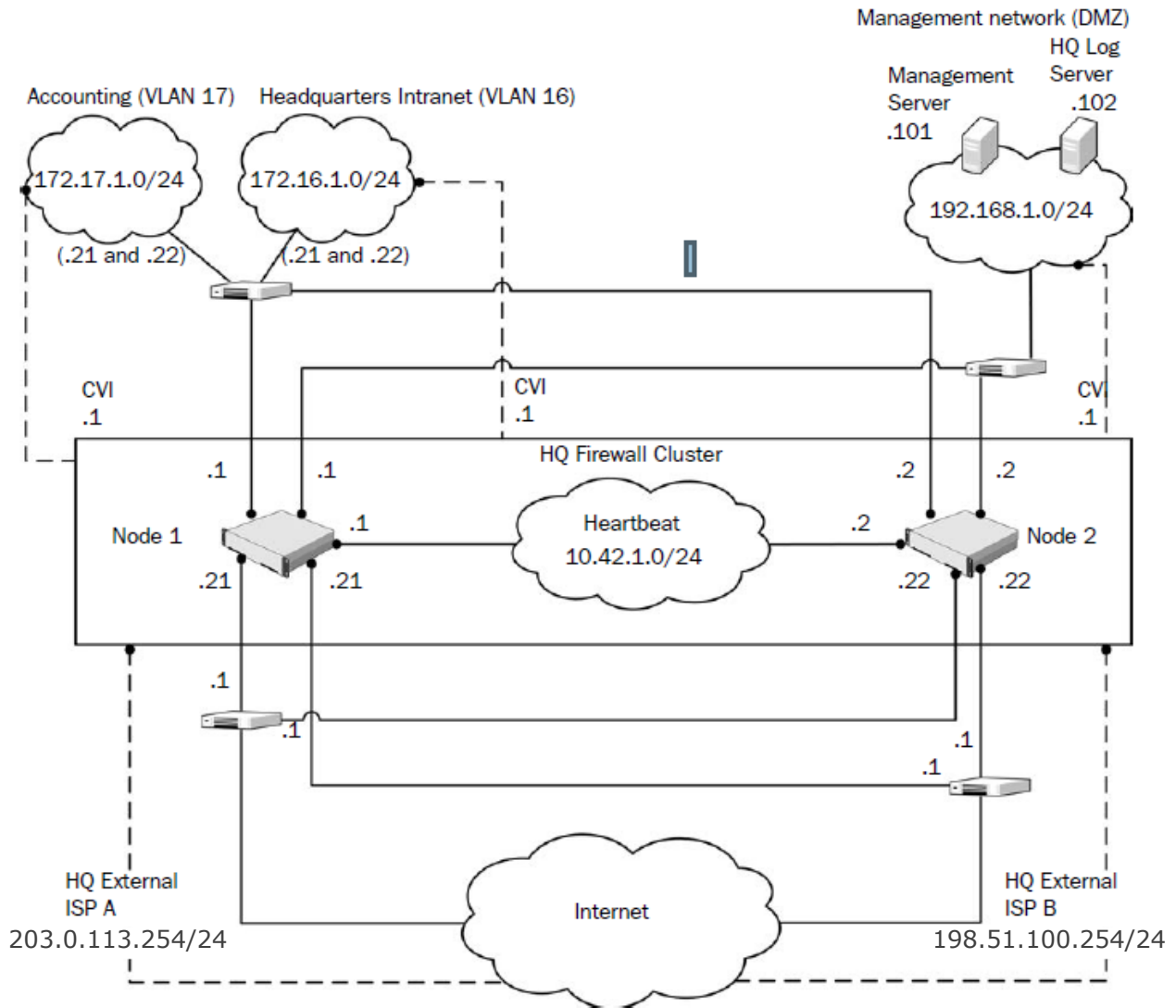
This example gives you a better understanding of how Security Engines with Layer 3 Interfaces fits into a network. The example outlines a network with two engines: a Single Engine at a branch office and a Engine Cluster at headquarters.

Example Engine Cluster

This example shows Engine Cluster interfaces in the example network.

In the example network, the HQ Engine Cluster is located in the Headquarters network. The cluster consists of two cluster nodes: Node 1 and Node 2.

Example engine scenario



| Network | Description |
|--------------------------|---|
| Heartbeat network | The heartbeat and cluster synchronization goes through the heartbeat network. CVI: no CVI defined. NDI: 10.42.1.1 (Node 1) and 10.42.1.2 (Node 2). |
| Management network (DMZ) | The management network interface is used for the control connections from the Management Server and for connecting to the HQ Log Server. CVI: 192.168.10.1. NDI: 192.168.10.21 (Node 1) and 192.168.10.22 (Node 2). |

| Network | Description |
|------------------------|--|
| ISP A external network | This connection is one of the 2 Internet connections from the Headquarters site. It is provided by ISP A. CVI: 203.0.113.254. NDI: 203.0.113.21 (Node 1) and 203.0.113.22 (Node 2). Next-hop router: 203.0.113.1. |
| ISP B external network | This connection is the other of the 2 Internet connections from the Headquarters site. It is provided by ISP B. CVI: 198.51.100.254. NDI: 198.51.100.21 (Node 1) and 198.51.100.22 (Node 2). Next-hop router: 198.51.100.1. |
| HQ intranet | This VLAN (VLAN ID 16) is connected to the same network interface on the engine with the HQ Accounting VLAN. CVI: 172.16.1.1. NDI: 172.16.1.21 (Node 1) and 172.16.1.22 (Node 2). |
| HQ Accounting network | This VLAN (VLAN ID 17) is connected to the same network interface on the engine with the HQ intranet VLAN. CVI: 172.17.1.1. NDI: 172.17.1.21 (Node 1) and 172.17.1.22 (Node 2). |

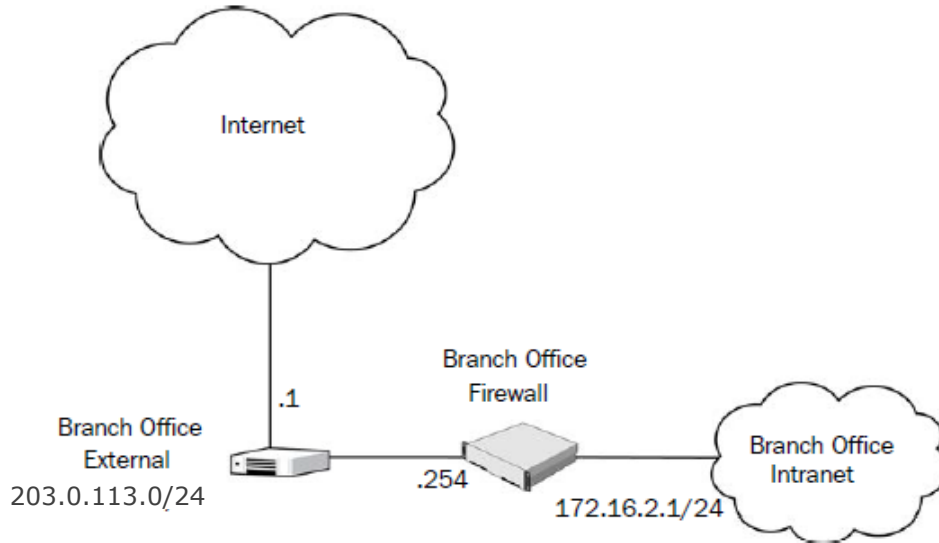
The Management Server and the HQ Log Server are at the headquarters site, in the DMZ network.

| SMC Manager component | Description |
|-----------------------|--|
| Management Server | This Management Server manages all engines and Log Servers of the example network. The Management Server in the Headquarters' Management Network (DMZ) with the IP address 192.168.1.101. |
| HQ Log Server | This Log Server receives log data from the engines. The server is located in the Headquarters' Management Network (DMZ) with the IP address 192.168.1.102. |

Example Single Engine

The Branch Office engine is a Single Engine located in the Branch Office network.

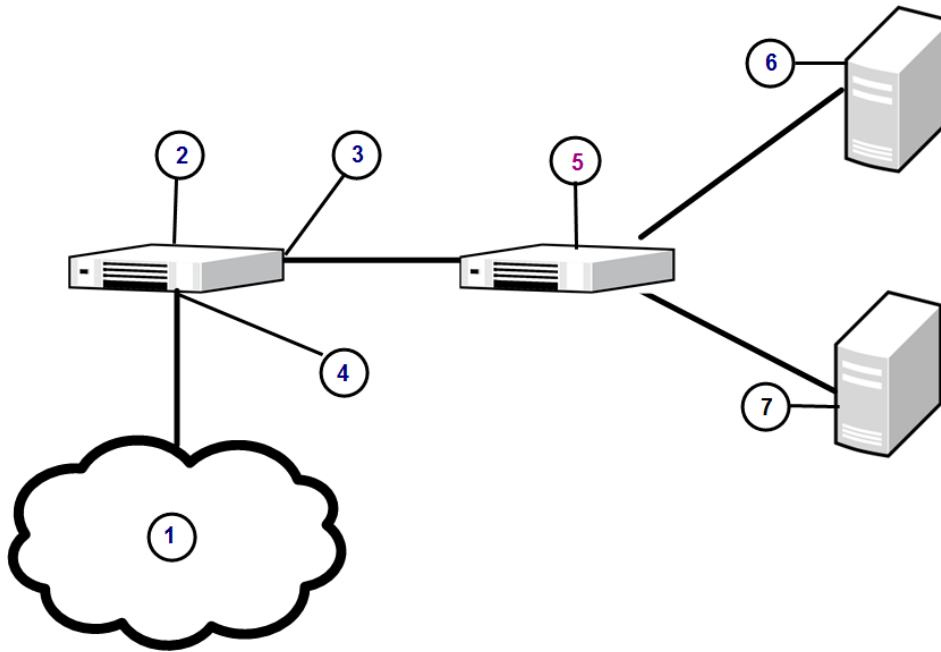
Example Single Engine



Example headquarters management network

This example shows a sample management network.

Example HQ management network



- 1 Internet
- 2 HQ Engine
- 3 192.168.10.1
- 4 203.0.113.254
- 5 Switch
- 6 Management Server 192.168.10.200
- 7 HQ Log Server 192.168.10.201

HQ Engine

The HQ Engine provides NAT for the headquarters management network.

The HQ Engine uses the following IP addresses with the headquarters management network:

- Internal: 192.168.10.1
- External: 203.0.113.254

SMC Servers

The example network includes a Management Server and a Log Server.

The following SMC Servers are included in the example network.

| SMC Server | Description |
|-------------------|---|
| Management Server | The Management Server is located in the headquarters' management network with the IP address 192.168.10.200. This Management Server manages all Engines, and Log Servers of the example network. |
| HQ Log Server | This server is located in the headquarters' management network with the IP address 192.168.10.201. This Log Server receives alerts, log data, and event data from the DMZ IPS and from the HQ IPS Cluster |

Example network (IPS)

Contents

- [Example network overview \(IPS\) on page 307](#)
- [Example headquarters intranet network on page 309](#)
- [HQ IPS Cluster on page 309](#)
- [Example headquarters DMZ network on page 310](#)

To give you a better understanding of how Security Engine in the IPS role fits into a network, this example outlines a network with IPS engines.

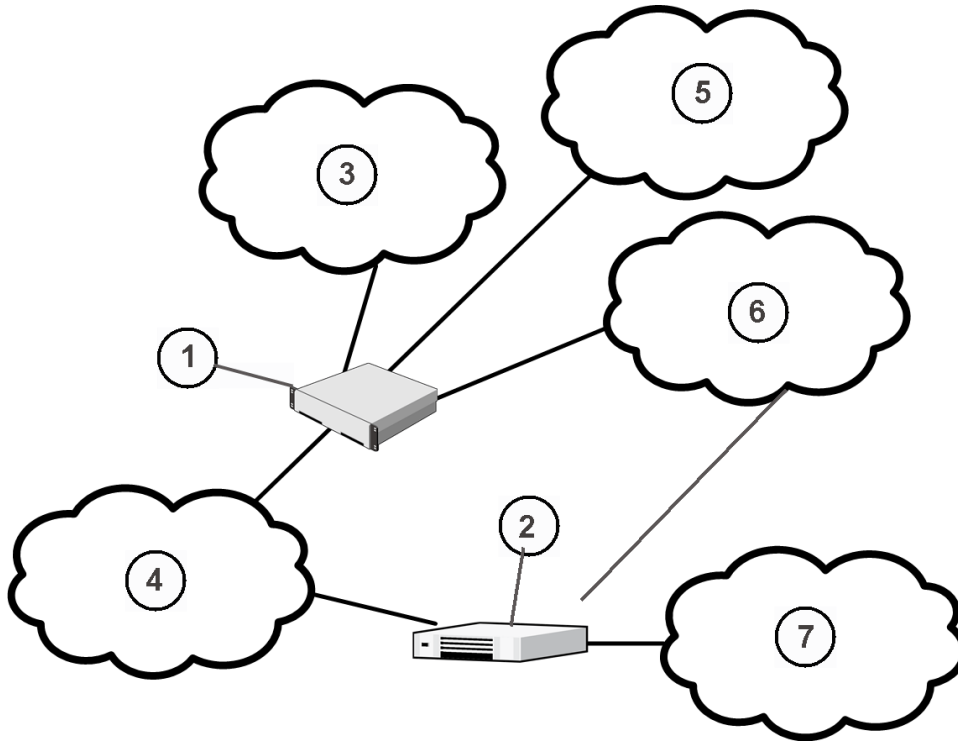
Example network overview (IPS)

This example network environment is used in all IPS examples.

There are two example IPS installations:

- An IPS Cluster in the Headquarters intranet network.
- A Single IPS in the Headquarters DMZ network.

Example network

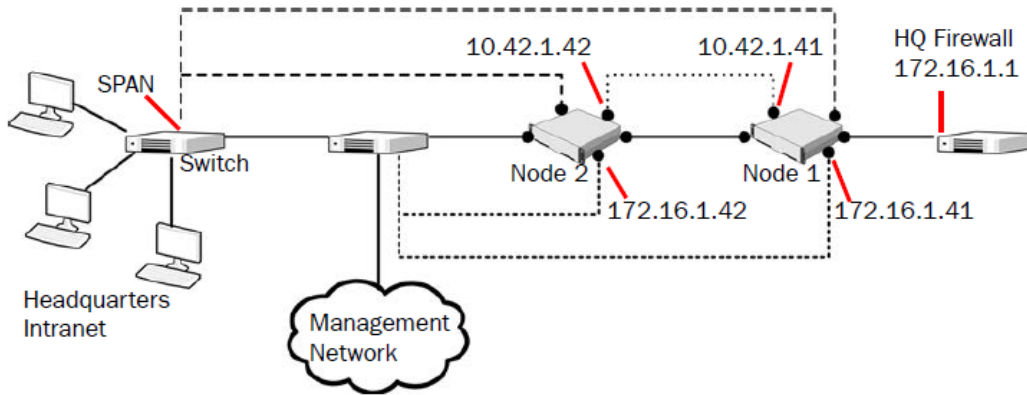


- 1 HQ Engine
- 2 Branch office Engine
- 3 HQ DMZ 192.168.1.0/24
- 4 Internet
- 5 HQ intranet 172.16.1.0/24
- 6 HQ Management 192.168.10.0/24
- 7 Branch Office intranet 172.16.1.0/24

Example headquarters intranet network

This example shows a sample headquarters intranet network.

Example headquarters intranet network.



HQ IPS Cluster

In this example, the HQ IPS Cluster is an inline serial cluster located in the Headquarters network.

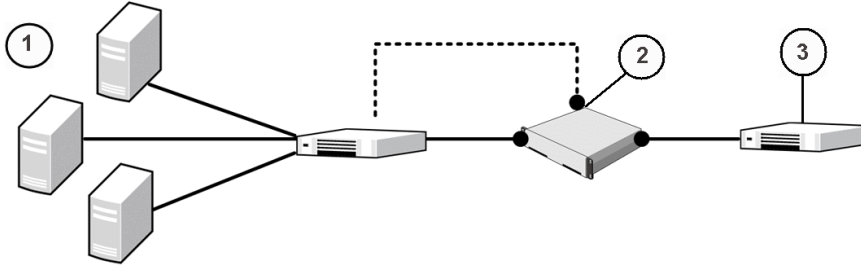
The cluster consists of two IPS engine nodes: Node 1 and Node 2.

| Network interface | Description |
|----------------------|---|
| Capture Interfaces | The HQ IPS Cluster's capture interface on each node is connected to a SPAN port in the headquarters intranet switch. All traffic in this network segment is forwarded to the SPAN ports for inspection. |
| Inline Interfaces | The cluster is deployed in the path of traffic between the engine and the headquarters intranet switch. All traffic flows through each node's Inline Interface pair. |
| Normal Interfaces | The normal interface on each node is connected to the headquarters intranet switch. Node 1's IP address is 172.16.1.41 and Node 2's address is 172.16.1.42. This normal interface is used for control connections from the Management Server, sending events to the HQ Log Server, and for sending TCP resets |
| Heartbeat Interfaces | The nodes have dedicated Heartbeat Interfaces. Node 1 uses the IP address 10.42.1.41 and Node 2 uses the IP address 10.42.1.42. |

Example headquarters DMZ network

This example shows a sample DMZ network.

Example headquarters DMZ network



- 1 DMZ servers
- 2 192.168.1.41
- 3 HQ Engine 192.168.1.1

DMZ IPS

In this example, the DMZ IPS in the headquarters DMZ network is a single inline IPS engine.

| Network interface | Description |
|-------------------|---|
| Inline Interfaces | The DMZ IPS is deployed in the path of traffic between the engine and the DMZ network switch. All traffic flows through the IPS engine's inline interface pair. |
| Normal Interfaces | The normal interface is connected to the DMZ network using the IP address 192.168.1.41. This normal interface is used for control connections from the Management Server, sending event information to the HQ Log Server, and for TCP connection termination. |

Appendix I

Cluster installation worksheet instructions

Contents

- Cluster installation worksheet on page 311

For planning the configuration of network interfaces for the engine nodes, use the worksheet.

- Interface ID** — Write the Interface ID (and the VLAN ID, if VLAN tagging is used).
- CVI** — Write the Interface ID's CVI information (if any) and on the **NDI** line, write the interfaces NDI information (if any). Use multiple lines for an Interface ID if it has multiple CVIs/NDIs defined.
- Mode** — Select all modes that apply for this Interface ID.
- IP Address and Netmask** — Define the CVI or NDI network address.
- MAC/IGMP IP Address** — Define the MAC address used. If the interface's CVI Mode is Multicast with IGMP, define the multicast IP address used for generating automatically the multicast MAC address.
- Comments** — Define, for example, a name of the connected network. Show how the NDI addresses differ between the nodes. Define a management interface's contact address if different from the interface's IP address.

Interface modes are explained in the following table. These same character codes are displayed in the engine element interface properties of the SMC Client.

Cluster installation worksheet

The following modes apply in the worksheet.

- CVI mode** — U=Unicast MAC, M=Multicast MAC, I=Multicast with IGMP, K=Packet Dispatch, A=Interface's IP address used as the identity for authentication requests
- NDI modes** — H=Primary heartbeat, h=Backup heartbeat, C=Primary control IP address, c=Backup control IP address, D=Default IP address for outgoing connection

| Interface ID | Type | Mode | IP Address | Netmask | MAC / IGMP IP Address |
|--------------|-----------------|-----------|---------------------|---------------------|--|
| | CVI | U M I K A | ____.____.____.____ | ____.____.____.____ | MAC: ____:____:____:____:____:____ or IGMP IP: ____.____.____.____ |
| | NDI | H h C c D | ____.____.____.____ | ____.____.____.____ | MAC: ____:____:____:____:____:____ |
| | Comments | | | | |
| | CVI | U M I K A | ____.____.____.____ | ____.____.____.____ | MAC: ____:____:____:____:____:____ or IGMP IP: ____.____.____.____ |

| Interface ID | Type | Mode | IP Address | Netmask | MAC / IGMP IP Address |
|--------------|-----------------|-----------|-------------------|-------------------|--|
| | NDI | H h C c D | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ |
| | Comments | | | | |
| | CVI | U M I K A | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ or IGMP IP: __ . __ . __ . __ |
| | NDI | H h C c D | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ |
| | Comments | | | | |
| | CVI | U M I K A | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ or IGMP IP: __ . __ . __ . __ |
| | NDI | H h C c D | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ |
| | Comments | | | | |
| | CVI | U M I K A | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ or IGMP IP: __ . __ . __ . __ |
| | NDI | H h C c D | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ |
| | Comments | | | | |
| | CVI | U M I K A | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ or IGMP IP: __ . __ . __ . __ |
| | NDI | H h C c D | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ |
| | Comments | | | | |
| | CVI | U M I K A | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ or IGMP IP: __ . __ . __ . __ |
| | NDI | H h C c D | __ . __ . __ . __ | __ . __ . __ . __ | MAC: __ : __ : __ : __ : __ : __ |
| | Comments | | | | |

