Forcepoint

Network Security Platform

7.4.1

Security Engine

Release Notes

Revision A

Contents

About this release

This document contains important information about this release of the Security Engine of the Forcepoint Network Security Platform. We strongly recommend that you read the entire document.

Experimental Features

Some features are marked as *Experimental*. These are newly introduced features or enhancements that are still in the testing phase and may not yet be fully polished or stable. They are released to gather user feedback and identify potential issues before a broader rollout.

Lifecycle model

This release of Forcepoint Network Security Platform Security Management Center is a Feature Stream (FS) version.

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 (LTS) maintenance versions if you do not need any features from a Feature Stream version.

For more information about the Forcepoint Network Security Platform lifecycle policy, see https://support.forcepoint.com/ProductSupportLifeCycle.

System requirements

To use this product, your system must meet these basic hardware and software requirements.

Security Engine appliances

We strongly recommend using a pre-installed Security Engine appliance for Forcepoint Network Security Platform installations.

Note

Some features are not available for all appliance models. See Knowledge Base article 9743 for appliance-specific software compatibility information.

The majority of the following supported appliances can be used in the Security Engine with Layer 3 Interfaces, or Security Engine with Layer 2 Interfaces.

- 60 Series (60, 60L, and 61)
- 120 Series (120, 120L, 120W, 120WL, and 125L)
- 130 Series (130)
- 330 Series (330, and 335)
- 350 Series (352 and 355)
- 1100 Series (1101 and 1105)
- 1202
- 2100 Series (2101 and 2105)
- 2200 Series (2201, 2205, and 2210)
- 2300 Series (2301, 2305, and 2310)
- 3400 Series (3401, 3405, and 3410)
- 3500 Series (3505 and 3510)

Basic hardware requirements

You can install Security Engine on standard hardware with these basic requirements.

Component	Requirement
CPU	Intel® processors based on Westmere (microarchitecture) or newer.
Memory	Minimum 4 GB of RAM
Hard disk	Minimum 8 GB **Note** RAID controllers are not supported.

Component	Requirement
Peripherals	■ DVD drive / External USB storage ■ VGA-compatible display ■ Keyboard
Interfaces	■ One or more network interfaces for the Security Engine with Layer 3 Interfaces ■ Two or more network interfaces for the IPS in IDS configuration ■ Three or more network interfaces for inline Engines with Layer 2 Interfaces for IPS or Layer 2 Engine deployment For information about supported Ethernet interface types and adapters, see Knowledge Base article 9721.

Master Engine requirements

Master Engines have specific hardware requirements.

- Each Master Engine must run on a separate physical device. For more details, see the *Forcepoint Network Security Platform Installation Guide*.
- All Virtual 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 Security Engines, you must use the Master Security Engine cluster in standby mode.
- Cabling requirements for Master Security Engine clusters that host Virtual IPS engines or Layer 2 Engines:
  - Failure Mode *Bypass* (fail-open) requires IPS serial cluster cabling.
  - Failure Mode *Normal* (fail-close) requires Layer 2 Engine cluster cabling.

  For more information about cabling, see the *Forcepoint Network Security Platform Installation Guide*.

Virtual appliance node requirements

You can install Security Engine on virtual appliances with these hardware requirements. Also be aware of some limitations.

Component	Requirement
CPU	Intel® processors based on Westmere microarchitecture or newer.
Memory	Minimum 4 GB of RAM
Virtual disk space	Minimum 8 GB
Hypervisor	One of the following: ■ VMware ESXi 7.0 or 8.0 ■ KVM with Red Hat Enterprise Linux 8.5 or 9.x ■ (Engine with Layer 3 Interfaces only) Microsoft Hyper-V on Windows Server 2016 with an Intel 64-bit processor

Component	Requirement
Interfaces	■ At least one virtual network interface for the Security Engine with Layer 3 Interfaces ■ Three virtual network interfaces for Engines with Layer 2 Interfaces The following network interface card drivers are recommended: ■ VMware ESXi platform — `vmxnet3`. ■ KVM platform — `virtio_net`.

When Security Engine is run as a virtual appliance node, these limitations apply:

- Only Packet Dispatching CVI mode is supported.
- Only standby clustering mode is supported.
- Heartbeat requires a dedicated non-VLAN-tagged interface.

When Security Engine is run as a virtual appliance node in the Engines with Layer 2 Interfaces, clustering is not supported.

Supported cloud environments

You can deploy the Security Engine in Amazon Web Services (AWS), Microsoft Azure, and other public cloud environments supported by Google, IBM, and Oracle.

For more information about deploying the Security Engine:

1) In AWS, see the document *How to deploy Forcepoint Network Security Platform in the Amazon Web Services cloud* and Knowledge Base article 10156.

2) In Microsoft Azure, see the document *How to deploy Forcepoint Network Security Platform in the Azure cloud* and Knowledge Base article 14485.

3) In other cloud environments, see the Knowledge Base article 39116.

Important

a) For AWS and Microsoft Azure, Security Engine instances can be launched using 1-Click Launch and custom solution templates, respectively. Existing instances can be remotely upgraded to the latest Security Engine version.

b) For other cloud environments, the Security Engine deliverables include a qcow2 formatted virtual machine disk image, which facilitates easier deployment to cloud platforms supported by Google, IBM, and Oracle.

Build number and checksums

The build number for Security Engine 7.4.1 is 32105.

Use the checksums to make sure that the installation files downloaded correctly.

- sg_engine_7.4.1.32105_x86-64-small.iso

```
SHA256SUM:
55d213c8a917fae94cefa94fbaf0bfa9e0ceb642c7369a65b64ebda6af85a80c

SHA512SUM:
bc00140e8bf69dff8192ee754f573db4
8898f9901ba14a56fa1484debdc3ab41
d2781d3b290c9ba673655e9be81632e0
74b19289607b2559bd69871d20fdc29f
```

- sg_engine_7.4.1.32105_x86-64-small.zip

```
SHA256SUM:
91dbfb19d89c205d21a06eabe336d0debc6be5e44661f1e3ec70aa17492ea1f0

SHA512SUM:
61059c7847db0830e5d748688edfa9da
4ffe0a32fd1ba58b30c35882a1ca4587
1d4a857be81ce8dc1292f56fdb468af8
55811322d2f52523b85ef6b836dfb42a
```

- Forcepoint-NGFW-gencloud-7.4.1.32105.qcow2

```
SHA256SUM:
bee8674f0ddb98f1a37a3febd27e1c3ef958e196ee43407f32d68ee8a1d81c17

SHA512SUM:
a65cc33ad49626fb0f7745034c020090
236346d2b3a13bec5029074f52df06fc
8cce96f2674b8c91a13fbd40bd63a528
ce46253b620666ed9c38279ebf51bd57
```

Compatibility

Security Engine 7.4 is compatible with the following component versions.

- Forcepoint Security Management Center 7.4 or higher
- Dynamic Update 1957 or higher
- Forcepoint VPN Client 6.11.0 or higher for Windows
- Forcepoint VPN Client 2.0.6 or higher for MacOS
- Forcepoint VPN Client 2.0.0 or higher for Android
- Forcepoint VPN Client 2.5.0 or higher for Linux
- Server Pool Monitoring Agent 4.0.0 or higher
- Forcepoint Endpoint Context Agent (ECA) included in Forcepoint One Endpoint 24.04 or higher
- Forcepoint User ID Service 2.0.0 or higher

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint Network Security Platform Product Guide*, the *Forcepoint Network Security Platform Installation Guide*, and the *Forcepoint NGFW Manager and VPN Broker Product Guide*.

Explicit proxy support for HTTP and HTTPS protocols

The Security Engine can be configured to act as an explicit proxy for HTTP and HTTPS connections. Proxy authentication is supported.

Note

The Explicit Proxy feature requires a separate license.

HTTP/3 inspection (Experimental)

The Security Engine can now inspect the complete HTTP/3 connection by decrypting the traffic between the client and server. After inspection, the engine re-encrypts the data before forwarding it to the intended recipient. This feature's support status is experimental in this release.

SAML user authentication

Both Application Access Portal (previously SSL VPN Portal) and Browser Based User Authentication features now support user authentication via SAML.

Enhancements

This release of the product includes these enhancements.

Enhancements in Security Engine version 7.4.1

Enhancement	Description
VPN Broker Members with IPv6 endpoints when Broker Gateway uses only IPv4	The VPN Broker Gateway can provide IPv6 endpoints to other members within the same domain, even if the Gateway itself does not support IPv6 endpoints.
Automatic deployment on Oracle Cloud Infrastructure (OCI)	When deploying a single engine on Oracle Cloud Infrastructure, elements can be automatically created in SMC through the SMC API.

Enhancements in Security Engine version 7.4.0

Enhancement	Description
Application Access Portal improvements	Application Access Portal (previously SSL VPN portal) now supports TLS 1.3. Also support for WebSocket protocol has been added.

Enhancement	Description
Datagram Transport Layer Security (DTLS) tunneling protocol support	The Security Engine supports DTLS tunneling protocol for Forcepoint VPN Client versions that have the DTLS support included. This feature can now be configured normally through SMC. Using DTLS can improve remote access performance compared to TLS based tunnels when network conditions are challenging.
Local ThreatSeeker URL Categorization database	You can choose to either use the locally downloaded ThreatSeeker URL Categorization database or use the Cloud-based ThreatSeeker URL Categorization database for URL filtering.  **Note** This feature is supported on engines that have at least 16 GB of memory.
Log Server per Virtual Engine	You can now assign a dedicated log server to a virtual engine. Previously, the log data from virtual engine was sent to the same log server as the Master Engine.
Support for user authentication using email format usernames	Previously user authentication did not support usernames that contain the @-character used in email addresses or in UPN Active Directory user attribute. Forcepoint Network Security Platform can now be configured to allow the use of either an email address or a UPN as the user ID in configuration and user authentication.
URL Category sync with Forcepoint portfolio	Unified the URL category taxonomy across web security features for all Forcepoint products.  **Note** When upgrading from SMC version 7.3 or earlier to version 7.4, any URL categories that are used in policies will be automatically converted to reflect the latest changes present in the URL Categories.
User or group-based policies without directory server access	You can now include users and user groups in access policy rules for a managed engine even if SMC is not able to query an external LDAP or AD server.  **Note** The engine must be able to access the LDAP server for user authentication, even if the LDAP server is not accessible from SMC. When user authentication is SAML-based, it is also possible to operate the engine without LDAP server access.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 12232.

Security updates

For information about third-party packages and associated vulnerabilities included with the Security Engine in this product release, see Knowledge Base article 12233.

Installation instructions

Use these high-level steps to install the SMC and the Security Engines.

For detailed information, see the *Forcepoint Network Security Platform Installation Guide*. All guides are available at help.forcepoint.com.

Steps

1) Install the Management Server, the Log Servers.

2) Import the licenses for all components.
   You can generate licenses at https://stonesoftlicenses.forcepoint.com.

3) Configure the Engine elements in the SMC Client from the **Engine Configuration** navigation menu.

4) To generate initial configurations, right-click each Security Engine, then select **Configuration** > **Save Initial Configuration**.
   Make a note of the one-time password.

5) Make the initial connection from the Security Engines to the Management Server, then enter the one-time password.

6) Create and upload a policy on the Security Engines in the SMC Client.

Upgrade instructions

Take the following into consideration before upgrading licenses, Security Engines, and clusters.

Note

Upgrading to version 7.4 is only supported from version 7.1 or higher. If you have a lower version, first upgrade to version 7.1.

- Forcepoint Network Security Platform version 7.4 requires an updated license. The license upgrade can be requested at https://stonesoftlicenses.forcepoint.com. Install the new license using the SMC Client before upgrading the software. If communication between the SMC and the license server is enabled and the maintenance contract is valid, the license is updated automatically.
- To upgrade the Security Engine, use the remote upgrade feature or reboot from the installation DVD and follow the instructions. For detailed instructions, see the *Forcepoint Network Security Platform Installation Guide*.

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.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint Network Security Platform Product Guide*
- *Forcepoint Network Security Platform Online Help*

Note

By default, the Online Help is used from the Forcepoint help server. If you want to use the online Help from a local machine (for example, an intranet server or your own computer), see Knowledge Base article 10097.

- *Forcepoint Network Security Platform Installation Guide*

Other available documents include:

- *Forcepoint Hardware Guide* for your model
- *Forcepoint Network Security Platform Quick Start Guide*
- *Forcepoint Security Management Center API User Guide*
- *Forcepoint VPN Client User Guide* for Windows or Mac
- *Forcepoint VPN Client Product Guide*
- *Forcepoint NGFW Manager and VPN Broker Product Guide*

Published 08 April 2026