FlexEdge Secure SD-WAN Manager

7.1.9

Release Notes

Revision A

Contents

About this release

This document contains important information about this release of Forcepoint FlexEdge Secure SD-WAN Manager. We strongly recommend that you read the entire document.

For detailed information about changes introduced in the SMC API since the previous version, see the automatically generated change log reports in the `api_change_log.zip` file in the `Documentation/SMC_API` folder of the SMC installation files.

Product name change

Starting from Forcepoint FlexEdge Secure SD-WAN version 7.1 release the product name has changed from Forcepoint NGFW to Forcepoint FlexEdge Secure SD-WAN. The primary changes are listed below:

Component	Old name	New name
Solution	Forcepoint NGFW	Forcepoint FlexEdge Secure SD-WAN
Management	Security Management Center (SMC)	FlexEdge Secure SD-WAN Manager / SD-WAN Manager Console (SMC)
Engine	NGFW Engine	FlexEdge Secure SD-WAN Engine

Currently, product name change is visible in SMC and in the following documentations:

- *Forcepoint FlexEdge Secure SD-WAN Manager API User Guide*
- *Forcepoint FlexEdge Secure SD-WAN Installation Guide*
- *Forcepoint FlexEdge Secure SD-WAN Product Guide*

- *Forcepoint FlexEdge Secure SD-WAN online help*
- *Forcepoint FlexEdge Secure SD-WAN Quick Start Guide*

For more information on SMC UI terminology change, refer to the **About this Help** section in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Note

1) Some documentations, knowledge base articles, and other support information are still using the old product name.

2) There is no change in the Engine local user interface.

3) The IPS role has transitioned now from L2FW mode to L3FW mode.

Deprecated Features

Web Portal User Interface

Web Portal User Interface is deprecated and is not available by default. Web Portal Server is still available to host Web Access.

System requirements

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

SMC hardware requirements

You can install the SMC on standard hardware.

Component	Requirement
CPU	Intel® Core™ family processor or higher recommended, or equivalent on a non-Intel platform
Disk space	■ Management Server: 6 GB ■ Log Server: 50 GB

Component	Requirement
Memory	■ Management Server, Log Server, Web Portal Server: 16 GB RAM ■ If all SMC servers are on the same computer: 32 GB RAM ■ If you use the SMC Web Access feature: an additional 2 GB RAM per administrator session ■ Management Client: 2 GB RAM The SMC server requirements are the *minimum* requirements. The Management Server and Log Server in particular benefit from having more than the minimum amount of RAM. On high-end appliances that have a lot of RAM, the SMC might not provision the maximum amount of RAM for use by the SMC servers. For information about how to manually modify the provisioning, see Knowledge Base article 33316.
Management Client peripherals	■ A mouse or pointing device ■ Display with 1280x768 resolution or higher

Operating systems

You can install the SMC on the following operating systems. Only 64-bit operating systems are supported.

Linux	Microsoft Windows
■ Red Hat Enterprise Linux 7, 8, and 9 ■ SUSE Linux Enterprise 12 and 15 ■ Ubuntu 20.04 LTS and 22.04 LTS ■ Amazon Linux 2 Kernel 15	Standard and Datacenter editions of the following Windows Server versions: ■ Windows Server 2022 ■ Windows Server 2019 ■ Windows Server 2016 On Windows 10, you can install the SMC in demo mode. You can also install the Management Client.

We recommend that you only use operating system versions that are currently supported by the vendor.

Other versions of the listed operating systems might be compatible, but have not been tested. Only U.S. English language versions of the listed operating systems have been tested, but other locales might also be compatible.

Build number and checksums

The build number for Secure SD-WAN 7.1.9 is 11443. This release contains Dynamic Update package 1946.

Use checksums to make sure that files downloaded correctly.

- smc_7.1.9_11443.zip

  ```
  SHA256SUM:
  ad323b4d60ec06e1df46c6b29cdd44261c69841b4fde5c71f23fa5fcb6437fb2

  SHA512SUM:
  c8995702c2f8ac348518b4e71c61288d
  1fcfbafc6da7d2e9d42552ac175aba31
  c5a54f99a51ce5afe83c00081bdafbf9
  a93450573481ac58a888e79e380c20b3
  ```

- smc_7.1.9_11443_linux.zip

  ```
  SHA256SUM:
  5208bd0194f6d1f887befba92ea0c5f54e238904a08c188feba4b377bfac38e0

  SHA512SUM:
  56df1ccead50806d15bceb173234f4a7
  95d416ed7efff73ceba0b6933db1cb07
  c4d4fac53afa87831354cdd0c7477dcd
  91694dd01e11db6bd293e65a4adc22a2
  ```

- smc_7.1.9_11443_windows.zip

  ```
  SHA256SUM:
  1ff037910f175c2af54093673632a778c8985c2522bb6787324289edaad73389

  SHA512SUM:
  6e51b18682eb4a66262099fe13b84b46
  16e91f364a489e7d20058eefdaa715d6
  ef68b9d87e4eadad5bcd610be59809f3
  8af1bdf0c16fa7e8289cf3ba6602b970
  ```

Compatibility

SMC 7.1 can manage all compatible Secure SD-WAN Engine versions up to and including version 7.1.

SMC 7.1 is compatible with Engine 6.8 or higher.

New features

This release of the product includes these new features. For more information and configuration instructions, see the *Forcepoint FlexEdge Secure SD-WAN Product Guide* and the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*.

Forward traffic to specific tunnels or routers

By configuring the Forced Next Hop (FNH) option in the access rule you can now force forward traffic to a specific tunnel or router.

The advantage of using this option is that you can forward the matched traffic to a specific application that has the server behind a tunnel.

For more information, see *Configure Forced Next Hop routing* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

SMC contact via FQDN

Support for using FQDN as the contact address to enable the engine to contact the SMC management server or log server. This can be beneficial when you run the SMC management server or log server in a cloud environment where managing long term public IP address is not feasible or is difficult.

For more information, see *Define Management Server or Log Server contact addresses*, and *Define contact address* sections in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Additional admin user authentication methods supported

The following admin user authentication methods are supported:

- OpenID Connect authentication by using an OpenID Connect provider.
- SAML authentication by using a SAML based identity provider.

For more information, see *Authenticate administrators using OpenID authentication method*, and *Authenticate administrators using SAML v2 authentication method* sections in*Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Improved SMC Domain Overview

The Domain Overview is updated to improve its scalability and usability to help users to easily navigate and find the domain information that they are looking for.

For more information, see *Log on to a Domain from the Domain Overview* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

User Interface Themes

You can switch between light and dark theme for SMC.

For more information, see *Customize the Management Client layout* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

DNS Sinkholing

You can now configure DNS sinkholing for UDP and TCP service elements. One of the scenarios where this feature can be useful is, when there is an infected machine in the internal network. It can be identified by using the DNS sinkholing.

For more information, see *Create custom service elements* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Enhancements

This release of the product includes these enhancements.

Enhancements in SMC version 7.1.4

Enhancement	Description
Radius authentication for engine log in	It is now possible to configure engines so that local administrators are authenticated via RADIUS. Also, it is possible to control if the root admin can log in only from local console or via network using SSH. RADIUS authentications of engine supports access-challenge methods. **Note** This enhancement is only supported on engine versions 7.1.3 or later.

Enhancements in SMC version 7.1.2

Enhancement	Description
Elasticsearch version update	Updated the Elasticsearch client libraries to version 8.9.2.

Enhancements in SMC version 7.1.1

Enhancement	Description
Local Sandbox - Advanced Malware Detection & Protection option	You can now configure an Advanced Malware Detection & Protection local sandbox to detect advanced threats by analyzing the behavior of files in a restricted operating system environment. **Note** You need a local Advanced Malware Detection & Protection server to use this local sandbox service. For more information, see the *Connect Secure SD-WAN to a sandbox service and the Define Sandbox Service elements* sections in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.
Easy identification of VPN site status	Support for enabled and disabled VPN site icons are added. The appropriate VPN site icon is displayed in the preview or editor view in SMC User Interface to help easily differentiate, if the VPN site is in enabled or disabled state.

Enhancement	Description
Temporarily Ban for Multiple Failed Logon Attempts (Password Policy) option	You can now configure the password policy in the global system settings to temporarily ban an IP address, when logon attempts by a SMC administrator from a single IP address reaches the maximum failed logon attempts. For more information, see the *Centralized management of global system settings* section in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.
Updated the Elasticsearch client libraries to version 8.8.2	The Elasticsearch client libraries are updated to the version 8.8.2 to improve the indexing performance. **Note** In the Elasticsearch version 8.8.2, OpenSearch is no longer supported. For more information, see the *Requirements for using Elasticsearch with Forcepoint NGFW Security Management Center (SMC)* Knowledge Base Article.

Enhancements in SMC version 7.1.0

Enhancement	Description
BGP Monitoring Protocol (BMP) Configuration	Support for BMP configuration options from the Dynamic Routing Editor. It is used to monitor BGP sessions and send the monitored data from BGP routers to the network management entities. Also, when configured the log events includes the information for the configured options, and which in turn helps to make correlation of BMP and engine logs easy for analytics. For more information, see *Create core elements for dynamic routing*, and *Enable BGP on the Engine, Engine Cluster, or Virtual Engine* sections in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.
Improved Application Health Monitoring	The Application Health Monitoring feature now comes with the following support: ■ Enhanced engine monitoring and better support for non-TCP traffic, that is there is now support for applications that use UDP for data transport. ■ Visibility into application health history and health status history of network applications. ■ Better ISP link status monitoring. ■ Application health status history. For more information, see *Application Health Monitoring Dashboard* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.

Enhancement	Description
Improved SD-WAN algorithms and link selection logic	The following updates have been done to provide for better user experience: ■ Engine logic is updated to avoid too much packet loss before the traffic is sent to the better links. ■ The QoS link value is tuned to make QoS link value selection feature to work as intended. Also, the **Default SD-WAN Link Balancing Preference** option is made available to allow you to set the preferences on how the traffic is balanced over the links for each engine. For more information, see *Create Link Usage Profile elements* section in *Forcepoint FlexEdge Secure SD-WAN Product Guide*.
Tunnel interface now supports multiple IP addresses	It is now possible to add multiple IP addresses (that can be of types IPv4 and IPv6) for tunnel interfaces.
IPFIX forwarding	When you export IPFIX information, the following new IPFIX Element IDs are now supported: ■ EID 5 ipClassOfService ■ EID 58 vlanId (source VLAN) ■ EID 59 postVlanId (destination VLAN) ■ EID 60 ipVersion ■ EID 89 forwardingStatus ■ EID 90 mplsVpnRouteDistinguisher ■ EID 131 exporterIPv6Address **Note** 1) EID 90 mplsVpnRouteDistinguisher is exported, only when BMP monitoring is configured for the engine that originates the log entries. 2) The following IPFIX element IDs are only generated by engine version 7.1.0 or later: ■ EID 5 ipClassOfService ■ EID 89 forwardingStatus ■ EID 90 mplsVpnRouteDistinguisher

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article 4751.

Security updates

For information about third-party packages and associated vulnerabilities included with SMC in this product release, see Knowledge Base article 41766 .

Installation instructions

Use these high-level steps to install the SMC and the Secure SD-WAN Engines.

For detailed information, see the *Forcepoint FlexEdge Secure SD-WAN Installation Guide*. All guides are available for download at https://support.forcepoint.com/s/article/Documentation-Featured-Article.

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 Management Client from the **Configuration** view.

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

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

6) Create and upload a policy on the Secure SD-WAN Engines in the Management Client.

Upgrade instructions

Take the following into consideration before upgrading the SMC.

Note

The SMC (Management Server, Log Server, and Web Portal Server) must be upgraded before the Secure SD-WAN Engines are upgraded to the same major version.

- The following features are removed and are no longer supported:
  - ATD Server. This feature is only supported on engine versions 5.8 to 6.3.
  - ePO Server.
  - BrightCloud situations and categories. This feature is only supported on engine version 6.4 and older.

    Before you upgrade, if any of the legacy BrightCloud URL category situations or tags are referenced in policies, filters, or reports, you must remove these references or change references to point to the current URL categories.

    Navigate to **Configuration** > **Engine** > **Other Elements** > **Network Applications** to remove or change references of the legacy BrightCloud URL category situations or tags.

    The BrightCloud situations are identified with their name that has the pre-fix "*BC_*"

    The following is the list of BrightCloud categories:
    - URL Filtering
    - Games / Gambling
    - Lifestyle
    - Drugs
    - Information / Technology
    - Society / Education / Religion
    - Mature / Violent
    - Purchasing
    - Risk / Fraud / Crime
    - Business / Services
    - BrightCloud System Situations
    - Entertainment / Culture
    - Pornography / Nudity
    - Information / Communication
    - Network Bandwidth Loss
    - Productivity Loss
    - Security Risk
    - Legal Liability
    - Business Usage

  Important

  Before you upgrade, remove these elements or change them to current supported features in your SMC configuration.

- SMC 7.1 requires an updated license.
  - If the automatic license update function is in use, the license is updated automatically.
  - If the automatic license update function is not in use, request a license upgrade on our website at https://stonesoftlicenses.forcepoint.com. Activate the new license in the Management Client before upgrading the software.
- To upgrade a lower version of the SMC to 7.1, we strongly recommend that you stop all SMC servers and create a backup before continuing with the upgrade. After creating the backup, run the appropriate setup file, depending on the operating system. The installation program detects the old version and does the upgrade automatically.

- When you upgrade the SMC, the dynamic update package that is included with the SMC installer is imported and activated. However, if a newer version of the dynamic update package has previously been imported or downloaded before the upgrade, the newest version is activated instead.
- You can upgrade from the following SMC versions; however, only the latest maintenance release and LTS versions are tested. Hence, It is recommended to upgrade to the latest LTS release of SMC, regardless of FlexEdge Secure SD-WAN Engine versions being managed.
  - 6.8.0 – 6.8.15 (LTS release versions)
  - 6.9.0 – 6.9.3
  - 6.10.0 – 6.10.18 (LTS release versions), 6.10.100
  - 6.11.0 – 6.11.2
  - 7.0.0 – 7.0.4
  - 7.1.0 – 7.1.8 (LTS release versions)

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 FlexEdge Secure SD-WAN Product Guide*
- *Forcepoint FlexEdge Secure SD-WAN 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 FlexEdge Secure SD-WAN Installation Guide*

Other available documents include:

- *Forcepoint Hardware Guide* for your model
- *Forcepoint FlexEdge Secure SD-WAN Quick Start Guide*
- *Forcepoint FlexEdge Secure SD-WAN Manager 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 13 November 2025