FlexEdge Secure SD-WAN Manager

6.10.100

Release Notes

Revision A

Contents

About this release

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

For detailed information about changes introduced in the FlexEdge Secure SD-WAN Manager 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 FlexEdge Secure SD-WAN Manager installation files.

System requirements

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

Secure SD-WAN Manager hardware requirements

You can install the Secure SD-WAN Manager 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 Secure SD-WAN Manager servers are on the same computer: 32 GB RAM - If you use the Secure SD-WAN Manager Web Access feature: an additional 2 GB RAM per administrator session - Management Client: 2 GB RAM The Secure SD-WAN Manager 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 Secure SD-WAN Manager might not provision the maximum amount of RAM for use by the Secure SD-WAN Manager servers. For information about how to manually modify the provisioning, see Knowledge Base article 33316.
Management Client peripherals	- A mouse or pointing device - SVGA (1024x768) display or higher

Note

To protect the privacy of your data, we recommend using dedicated hardware for all Secure SD-WAN Manager installations. For cloud-based virtualization platforms, use an instance type that runs on dedicated hardware. For on-premises virtualization platforms, install the Engines, Secure SD-WAN Manager components, on a hypervisor that does not host any other virtual machines. For third-party hardware, do not install any other software on the computer where you install the Engines or Secure SD-WAN Manager components.

Operating systems

You can install the Secure SD-WAN Manager on the following operating systems. Only 64-bit operating systems are supported.

Linux	Microsoft Windows
- Red Hat Enterprise Linux 7 and 8 - SUSE Linux Enterprise 12 and 15 - Ubuntu 18.04 LTS and 20.04 LTS	Standard and Datacenter editions of the following Windows Server versions: - Windows Server 2019 - Windows Server 2016 - Windows Server 2012 R2 On Windows 10, you can install the Secure SD-WAN Manager 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 Manager 6.10.100 is 11119. This release contains Dynamic Update package 1469.

Use checksums to make sure that files downloaded correctly.

- sdwan_manager_6.10.100_11119.zip

```
SHA1SUM:
69bbea63e72339f007308d2ab79ab81e0ba8f258

SHA256SUM:
9dfdbb00596cbc6ee6d0009fbbe3c61916da1b12bf1854e0e903a8b213ee6e74

SHA512SUM:
70bf7aca2c729a0b8833b4d3ca014725
8f56ae9e595b6335316c9a03ea7a8e22
a7cd0be7a0dbedccbbaf7db6d3ed4578
d932bf12e44dc6f67f9a4eec333a5e2f
```

- sdwan_manager_6.10.100_11119_linux.zip

```
SHA1SUM:
c9da8b9c38350dd87c740df51bbda9378a34820e

SHA256SUM:
38694044a04273551b6c17cb150d20691238fe83bc3aa1c546d96827f0954504

SHA512SUM:
57e5e3712d746dca350534c89eb4a6e0
1d516db8fdc98e81d10477d23dc0d742
5b9a06b5ed48123ddf94a8c5c3b566fa
c96e27005214302c06608e92b6158319
```

- sdwan_manager_6.10.100_11119_windows.zip

```
SHA1SUM:
44078baba746a726d360f2a98c0d2cbde3cba69b

SHA256SUM:
e240e75df800354d17981357be927651306a9d37bc4824d03f193f1a63c9d070

SHA512SUM:
0260fec20e7ddfae6a10540f7c6fc1e1
c1ece184038e5ad011874074c360bbc3
dba34b1036e68cdeac01c9524994c583
0ca05ff1af5ea4a84ba3c15e5d3998a0
```

Compatibility

Secure SD-WAN Manager 6.10 can manage all compatible Forcepoint Engine versions up to and including version 6.10.

Secure SD-WAN Manager 6.10 is compatible with the following component versions.

- Engine 6.3 or higher
- McAfee Enterprise Security Manager (McAfee ESM) 11.1.x or higher

Features in Secure SD-WAN Manager version 6.10.100

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*.

Features in Secure SD-WAN Manager version 6.10.100

Feature	Description
Snort inspection on Engines	The Snort network intrusion detection system and intrusion prevention system has been integrated into Engines. You can import externally created Snort configurations into Engines to use Snort rules for inspection. You can configure Snort inspection globally for all Engines, or for individual Engines. You can use both Engine deep inspection and Snort inspection for the same traffic, or you can use only Engine deep inspection or only Snort inspection.
Exact values in exported reports	You can now use exact values instead of rounded values when you export reports as tab-delimited text files. To use exact values in reports, set the value of the TXT_REPORT_RAW_VALUES parameter to true. For reports exported using the Management Client, set the parameter in the SGClientConfiguration.txt file. For reports exported on the Management Server, set the parameter in the SGConfiguration.txt file.
Improved SD-WAN monitoring	The performance of SD-WAN monitoring has been improved. New options for SD-WAN monitoring have also been introduced. ■ The performance of SD-WAN monitoring in the Home view has been improved. ■ The performance of branch connectivity monitoring has been improved. ■ Branch connectivity diagrams have been enhanced. The diagram now includes shortcuts that zoom in on specific world regions on the map. ■ The Tunnels pane of branch home pages and VPN home pages can now show the status of either individual tunnels between endpoints or an aggregate status of all tunnels between gateway pairs. Previously, the Tunnels pane only showed the status of individual tunnels between endpoints. ■ A new VPN gateways pane that summarizes the status of the Gateways in the VPN has been added to the VPN home pages. The previous VPN gateway diagram pane is still available but it is not shown by default.

Feature	Description
OWASP encoding in Secure SD-WAN Manager API responses	There is a new option in the Secure SD-WAN Manager installer to enable OWASP encoding for the Secure SD-WAN Manager API. When the option is enabled, the Secure SD-WAN Manager API uses the OWASP encoder in responses. Using the OWASP encoder reduces the risk of cross site scripting (XSS) attacks. This option is especially useful if you use the Secure SD-WAN Manager API to generate HTML pages that are shown in a browser. **Note** When you enable this option, some strings in data returned by the Secure SD-WAN Manager API, such as special characters inside JSON payloads, are also encoded. We recommend enabling this option only if you use the Secure SD-WAN Manager API in a web browser.
SHA-256 support for NTP servers	You can now configure NTP Server elements to use SHA-256 authentication keys.
Warning about timeout when importing elements	On the progress tab for importing elements, a warning message is now shown when the default timeout for resolving conflicts between elements in the import file and existing elements is about to be reached. By default, the timeout is 15 minutes. You can optionally change the timeout using the CONFLICT_RESOLVING_OPERATION_TIMEOUT_MINUTES=<number of minutes> parameter in the SGConfiguration.txt in the SGHOME/data directory on the Management Server.
Rule hit counters for sub-policies	You can run a rule counter analysis for a sub-policy regardless of which main policy refers to it or which Engine the policy is installed on.
Policy install without policy snapshot	With new Management Client, you can select options to not create policy snapshot during policy install. This is done by adding `POLICY_SNAPSHOT_CONFIGURATION=true` in the `SGClientConfiguration.txt`. The location of the file depends on the installation type of Management Client. For locally installed Management Client and standalone Management Client: - Edit the `<user_home>/.stonegate/SGClientConfiguration.txt` file on the client computer. - Edit the `<smc_installation_folder>/data/SGClientConfiguration.txt` file on the Management Server.

Known issues

For a list of known issues in this product release, see Knowledge Base article 40827

Installation instructions

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

Steps

1) Install the Management Server, the Log Servers, and optionally the Web Portal Servers.

2) Import the licenses for all components.

3) Configure the Firewall, IPS, or Layer 2 Firewall elements in the Management Client from the **Configuration** view.

4) To generate initial configurations, right-click each Engine, then select **Configuration** > **Save Initial Configuration**.

   Make a note of the one-time password.

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

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

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. See https://support.forcepoint.com/CreateAccount.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

- *Forcepoint FlexEdge Secure SD-WAN Product Guide*
- Secure SD-WAN Manager 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.

Published 06 June 2022