Forcepoint Sidewinder

8.3.x Scan Engine Update MCV07

Release Notes

Revision A

Contents

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

This Forcepoint Scan Engine MCV07 update package provides virus protection for some traffic types that Forcepoint Sidewinder passes.

This release updates the Forcepoint Scan Engine to version 6300; other firewall areas are not affected. Consider the following:

- If your firewall is already configured to automatically download and install scanning engine updates, you do not need to perform the installation procedures in this document.
  If your firewall is not configured to automatically download and install scanning engine updates, we strongly recommend that you configure this feature.
- This update does not change the patch version of your firewall.
  For example, if your firewall is at version 8.3.2 when you install this update, the firewall remains at version 8.3.2.

Note

For additional information, see Knowledge Base article 9638.

Requirements

The firewall must meet these requirements to apply the update.

- Your firewall must be at version 8.3.x.
- The Support and Anti-Virus features must be licensed on your firewall.

Installation instructions

You can configure the firewall to install updates automatically or complete the update manually, depending on your security policy.

Verify license features

To download and apply the MCV07 update, Support and Anti-Virus features must be licensed on the firewall.

Steps

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

1) Select **Maintenance** > **License**.
2) Click the **Firewall** tab.
3) Verify the status of licensed features.

Next steps

If the Support or Anti-Virus protection features are not licensed, contact your sales representative.

Configure automatic installation

Perform this procedure to configure your firewall to automatically download and install new scanning engine updates. Automatic updates do not require a restart, and do not interrupt system processes.

Steps

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

1) Select **Maintenance** > **Updates**.
2) In the service list, select **A/V signatures**.
3) Select **Enable automated scanner engine updates**.
4) Select **Enable automated updates**, then select the frequency.

   The recommended setting is **Hourly**. Signature files (DAT files) are not included in this update; however, changing your settings will ensure that you have the most current files.
5) Save your changes.

Result

When an engine update is downloaded, it will be installed the next time new signature files are installed.

Install updates manually

If your security policy does not allow automatic updates, load and install the engine update and signature files manually.

Download the update

Download the update to the firewall so it is available for installation.

> **Note**
>
> If your firewalls are in a high availability configuration, perform this task for both pair members.

Steps

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

1) Select **Maintenance** > **Software Management**.

2) Click the **Manage Packages** tab.

3) To display the available updates, click **Check for Updates**.

   Packages that are available for download appear in the table with a status of **Available** and list the download site. By default, packages are downloaded from the FTP update site.

   You can configure automatic availability checks and downloads on the **Load Packages** tab. You can also change the location of the FTP site or web server on that tab.

4) In the **Manage Packages** table, select **8.3.MCV07**.

5) On the toolbar, click **Download** > **Yes** to confirm.

   A **successfully loaded** message appears and the package status changes to **Loaded**.

Install the update

Install the update that you downloaded to the firewall.

This update does not restart your firewall.

> **Note**
>
> If you have firewalls in a high availability configuration, this task must be performed only on the primary firewall. The updates are automatically synchronized.

Steps

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

1) Create a configuration backup.

2) Select **Maintenance** > **Updates**.

3) Select **Enable Automated Scanner Engine Updates**.

4) Save your changes.

5) Click **Update Database Now**.

6) Select a download and installation method:
   - **Background** — Select this option if you want the installation to run in the background. If email notification is enabled, the firewall sends a notice when the installation completes.
   - **Wait** — Select this option if you want to wait for the installation and receive an on-screen notification when the installation completes.
   - **Cancel** — Select this option to cancel the installation of the engine and signature updates.

7) After installation is complete, in the **Database info** area, verify that the engine and signature files installed.

   The Engine version should be 6300.

8) Deselect **Enable Automated Scanner Engine Updates**.

Result

The current scanning engine and the most recent signature files are now installed.

> **Note**
>
> We recommend using the **Updates** area. You can install the update from the **Software Management** area; however, installing from the **Software Management** area requires that you manually restart the scanning engine, download the new signature files, and install only the Scan Engine update.

Uninstall the update

You can uninstall the Scan Engine update package.

> **Note**
>
> If your firewalls are in a high availability configuration, perform this task for both pair members.

Steps

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

1) Select **Maintenance** > **Software Management**.

2) Click the **Manage Packages** tab.

3) In the **Manage Packages** table, select **8.3.MCV07**.

4) On the toolbar, click **Uninstall**.

5) Select **Uninstall now**.

6) Click **OK**.

7) Verify that the status for the update is now **Loaded**.

Result

The scanning engine and signatures are now uninstalled.

Known issues

For a list of known issues in this product release, see Knowledge Base article 10143.

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 Sidewinder documentation includes:
Typical documents

- *Forcepoint Sidewinder Product Guide*
- *Forcepoint Sidewinder Release Notes*
- *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*
- *Forcepoint Sidewinder Command Line Interface Reference Guide*
- Technical Note — *Using Firewall Enterprise with other McAfee products*
- Application Note — *Configuring Department of Defense Common Access Card Authentication on Firewall Enterprise*

Hardware

- *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*
- *Forcepoint Sidewinder, Virtual Appliance Installation Guide*
- *Forcepoint Sidewinder, Virtual Appliance Evaluation for Desktop Installation Guide*

- *Forcepoint Sidewinder Quick Start Guide*
- *Forcepoint Sidewinder Hardware Guide*, models S4016, 1402-C3, S5032, S6032, and S7032
- *Forcepoint Sidewinder Hardware Guide*, models S1104, S2008, and S3008

Certification

- *Firewall Enterprise Common Criteria Evaluated Configuration Guide*
- *Firewall Enterprise FIPS 140-2 Configuration Guide*
- *Firewall Enterprise FIPS 140-2 Level 2 Kit Installation Guide*, S Models

Published 27 July 2021