



FORCEPOINT

Sidewinder

Release Notes

8.3.2P13

Revision A

Contents

- [About this release](#) on page 2
- [Resolved issues](#) on page 6
- [Installation notes](#) on page 9
- [Find product documentation](#) on page 10

About this release

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

Forcepoint Sidewinder version 8.3.2P13 resolves issues present in the previous release.

Supported firewall types

Sidewinder supports these firewall types.

- Forcepoint Sidewinder appliances
- Forcepoint Sidewinder, Virtual Appliance

Compatible products

Sidewinder is compatible with the following products.

- McAfee® Firewall Enterprise ePolicy Orchestrator® Extension
- Forcepoint Sidewinder Control Center
- McAfee® Logon Collector
- McAfee Endpoint Intelligence Agent (McAfee EIA)

For more information, see Knowledge Base article [9275](#) and the Technical Note *Using Firewall Enterprise with other McAfee products* at <https://support.forcepoint.com>.


Requirements

Before you install this version, make sure the Admin Console and Sidewinder requirements are met.

Admin Console requirements

The computer that hosts the Admin Console must meet these requirements.

Admin Console minimum requirements

Component	Requirements
Operating system	<p>One of these Microsoft operating systems:</p> <ul style="list-style-type: none"> • Windows Server 2008 • Windows 7 • Windows 8 • Windows 10 <p> Note: Windows 8 and Windows 10 are supported in traditional desktop mode. Tablet mode is not supported. Touchscreen is not supported.</p> <p>Compatible legacy Microsoft operating systems:</p> <ul style="list-style-type: none"> • Windows Vista
Web browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer, version 7 or later • Mozilla Firefox, version 1.0 or later • Google Chrome • Microsoft Edge

Component	Requirements
Hardware	<ul style="list-style-type: none"> • 2 GHz x86-compatible processor • 2 GB of memory • 300 MB of available disk space • CD drive • 1024 x 768 display • Network card (to connect to your firewall) • USB port

Sidewinder requirements

The firewall must meet these requirements.

Minimum requirements by type

Firewall type	Platform requirements
Sidewinder appliance	<p>Appliance with a valid support contract:</p> <ul style="list-style-type: none"> • 1 GB of memory • AMD64-compatible processor
Sidewinder, Virtual Appliance	<p>Virtualization server:</p> <ul style="list-style-type: none"> • Hypervisor operating system — VMware ESX/ESXi version 4.0 or later <div data-bbox="557 1077 612 1134" data-label="Image"> </div> <div data-bbox="639 1092 1435 1249" data-label="Text"> <p>Note: Sidewinder, Virtual Appliance is installed in 64-bit mode by default. Your system must support Intel VT technology (or equivalent) to run properly in a virtual environment. Before starting the virtual appliance, verify that VT is enabled in your computer BIOS.</p> </div> <ul style="list-style-type: none"> • Hardware resources: <ul style="list-style-type: none"> • 2 virtual processors • AMD64-compatible processor • 1 GB of memory • 30 GB of free disk space • 2 or more NICs of type e1000 • Internet connectivity — The firewall requires a persistent Internet connection to maintain an active license and full functionality.

McAfee EIA requirements

Systems must meet these requirements to install McAfee EIA.

McAfee EIA minimum requirements

Component	Requirements
Operating system	One of these 32-bit or 64-bit Microsoft operating systems: <ul style="list-style-type: none">• Windows 8.1• Windows 7• Windows XP Service Pack 2 and later• Windows Server 2012 R2• Windows Server 2012• Windows Server 2008 R2• Windows Server 2008• Windows Server 2003 Service Pack 1 and later• Windows Server 2003 R2 Service Pack 1 and later
Hardware	<ul style="list-style-type: none">• 2 GHz x86-compatible processor• 2 GB of memory• 300 MB of available disk space• 1024 x 768 display• Network card (to connect to your firewall)• One of the following:<ul style="list-style-type: none">• USB port• CD drive
Other products	McAfee EIA deployment requires: <ul style="list-style-type: none">• McAfee® Endpoint Intelligence Manager (McAfee EIM) version 2.2.0 and later• McAfee® ePolicy Orchestrator® (McAfee ePO™) version 4.6.5, 5.x, and later• McAfee® Agent Agent version 4.8.0 patch 2 and later

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Common Vulnerabilities and Exposures (CVEs)

BIND

- Upgrade BIND to version 9.11.37.
- Import fixes for the following CVEs:

```
CVE-2020-8616 CVE-2020-8617 CVE-2020-8619 CVE-2020-8620 CVE-2020-8621
CVE-2020-8622 CVE-2020-8623 CVE-2020-8624 CVE-2020-8625 CVE-2021-25214
CVE-2021-25215 CVE-2021-25216 CVE-2021-25220
```

(1115951 1115952 1115984 1115986 1116031 1116033 1116034 1116169 1116254 1116255 1116256 1116500)

Kernel

- Import fixes for the following CVEs:

```
CVE-2018-17154 CVE-2018-17155 CVE-2018-6925 CVE-2019-15878 CVE-2019-5607
CVE-2020-7454 CVE-2020-7455 CVE-2020-7456 CVE-2020-7457 CVE-2020-7469
CVE-2021-29629 FreeBSD SA-20:12 FreeBSD SA-20:13 FreeBSD-SA-20:04
```

(1115119 1115458 1115916 1115943 1115970 1115973 1115974 1116010 1116309 1116311)

libarchive

- Import fixes for the following CVEs:

```
CVE-2020-9308
```

(1115898)

libfetch

- Import fixes for the following CVEs:

(1116374)

```
CVE-2021-36159
```

libc regex/regcomp

- Import fixes for VU#695940.
(1040602)

NTP

- Upgrade to NTP version 4.2.8P14.
- Import fixes for FreeBSD-SA-20:09.ntp security advisory. (1115917)

- Imports fixes for the following CVEs:

CVE-2018-8956, CVE-2020-11868, and CVE-2020-13817

(1115928 1115979 1115999)

OpenSSH

- Import fixes for the following CVEs:

CVE-2020-15778 and CVE-2021-28041

(1116016 1116194)

OpenSSL

- Upgrade to OpenSSL version 1.1.1n.
- Import fixes for the following CVEs:

CVE-2020-1971 CVE-2021-23839 CVE-2021-23840 CVE-2021-23841 CVE-2022-0778

(1115295 1116013 1116036 1116186 1116187 1116191 1116124 1116508)

Quagga

- Import fixes for the following CVEs:

CVE-2016-2342

(1113962)

SNMP

- Import fixes for the following CVEs:

CVE-2018-18065 CVE-2020-15861 CVE-2020-15862

(1115131 1116042 1116052)

Tcpdump

- Import fixes for the following CVEs:

CVE-2019-1010220

(1115486)

General Maintenance Changes

ACLD

- Correct an issue in an error path that might cause an acld traceback. (1116044)

Antivirus

- Change working directory of `vscanupdate` and `vscandownload` to `/var/run/scanners`. If `vscanupdate` or `vscandownload` are core files, the files will go in that directory. Modify `cf_antivirus` to produce an error audit if `vscanupdate` fails. Allow read and delete capabilities for `vscanupdate` and `vscandownload` core files. (1116312)
- Increase `virus_scanner` memory limit in `server.conf` from 512MB to 640MB. (1116388)
- Remove `/secureos/avdata/tmp/*`. Remove `/secureos/sophos_avdata/working/*` if the McAfee engine is in use. Remove antivirus core files if found. (1116467)

Audit

- Improve memory management in `auditdbd`. (1115111)
- Fix the spelling of `sysctl net.inet.ip.maxfragsperpacket` in audit messages. (1115046)

Certificate management

- Correct an issue that caused `cmd validator` to core. (1116168)
- Update list of Trusted Internet CAs with new list from Mozilla. (1115356)

Geolocation

- Add support for MaxMind GeoIP2 geolocation database. (1115977 1116339 1116435)

Kernel

- Prevent IP Filter from sending TCP resets on UDP sessions. (1116093)
- Import a new driver, `ixl`, for the newer 10 Gbps Ethernet modules. 40 Gbps is not supported. (1116170)

Miscellaneous

- Update the End User License Agreement. (1116054)
- Update Forcepoint Copyright year to 2021. (1116140)

OpenSSL

- Upgrade to OpenSSL version 1.1.1. (1115295 1116436 1116451)
- Support for TLS 1.3 has been added, and available cipher suites have been updated.
- Added cipher suites:
 - ECDHE-ECDSA-AES128-GCM-SHA256
 - ECDHE-ECDSA-AES128-SHA
 - ECDHE-ECDSA-AES128-SHA256
 - ECDHE-ECDSA-AES256-GCM-SHA384
 - ECDHE-ECDSA-AES256-SHA
 - ECDHE-ECDSA-AES256-SHA384
 - ECDHE-RSA-AES128-GCM-SHA256
 - ECDHE-RSA-AES128-SHA
 - ECDHE-RSA-AES128-SHA256
 - ECDHE-RSA-AES256-GCM-SHA384
 - ECDHE-RSA-AES256-SHA
 - ECDHE-RSA-AES256-SHA384
 - TLS_AES_128_GCM_SHA256
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
- Removed cipher suites:
 - EDH-RSA-DES-CBC3-SHA

- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

Proxies

- Fix traffic bytes count in audit records issued by the UDP proxy. (1116084)
- Add elliptic curve support in HTTPS. (1114668 1115908)

Sendmail

- Remove DNS based GTI option on sendmail. (1114884)

Smartfilter

- Automatically remove temporary files in **/secureos/sf4/** after a successful download. (1116480)

Installation notes

To bring your firewall to the latest patch version, follow the patch installation process appropriate for your environment.

Before you begin

The firewall must have 8.3.2P03 and 8.3.2P10 installed.

- **Standalone or HA cluster** — See the *Forcepoint Sidewinder Product Guide*, version 8.3.2P03 and later.
- **Firewall or HA cluster managed by Control Center** — See the *McAfee Firewall Enterprise Control Center Release Notes*, version 5.3.2P02 and *Forcepoint Sidewinder Control Center Product Guide*, version 5.3.2.



Note: If your firewall is managed by Control Center, it must be at version 5.3.2P15 or later to manage firewalls at version 8.3.2P13 or later.

Find product documentation

On the Forcepoint support website, 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 on the Forcepoint support website at <https://support.forcepoint.com>. There, you can access product documentation, Knowledge Base articles, downloads, cases, and contact information.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

Sidewinder documentation includes:

Typical documents

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

Hardware

- *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

Contact opensource@forcepoint.com if you need access to the modified BIND or DHCP source code, per the ISC/Mozilla license agreement.

