



# **FORCEPOINT**

## **Sidewinder**

### **Release Notes**

#### **8.3.2P09**

Revision A

# Table of contents

- 1 About this release.....3
  - Supported firewall types.....3
  - Compatible products.....3
  - Requirements.....4
- 2 Resolved issues.....7
- 3 Installation instructions.....9
- 4 Known issues.....10
- 5 Find product documentation.....11
  - Product documentation.....11

# About this release

---

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

Forcepoint™ Sidewinder® version 8.3.2P09 resolves issues present in the previous release.

## Supported firewall types

---

Sidewinder supports these firewall types.

- Forcepoint Sidewinder appliances
- Forcepoint Sidewinder, Virtual Appliance
- Forcepoint Sidewinder on Crossbeam X-Series Platforms

These features are not supported on Crossbeam X-Series Platforms for this release:

- Forcepoint Sidewinder Admin Console



**Note:** Use a Forcepoint Sidewinder Control Center Management Server to manage Sidewinder on Crossbeam X-Series Platforms.

- Multicast dynamic routing using the PIM-SM protocol
- Hybrid mode (configuring standard and transparent mode on the same firewall)
- Default route failover
- Quality of Service (QoS)
- Transparent (bridged) mode for these configurations:
  - Dual-Box High Availability (DBHA)
  - Multi-application serialization
- DBHA active-active mode



**Note:** Active-standby DBHA is supported.

- Crossbeam X-Series Operating System (XOS) features:
  - Virtual Application Processor (VAP) group hide-vlan-header parameter
  - Equal-cost multi-path routing
  - Configuration of the VRRP MAC address



**Note:** If you need functionality similar to the VRRP MAC address, Crossbeam recommends configuring a user-defined MAC address on each traffic circuit/interface pair included in the VRRP failover group. See the Crossbeam support knowledge base article 0004069.

## 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](#)
- *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.


**Table 1: Admin Console minimum requirements**

Component	Requirements
Operating system	<p>One of these Microsoft operating systems:</p> <ul style="list-style-type: none"><li>• Windows Server 2008</li><li>• Windows 7</li><li>• Windows 8</li><li>• Windows 10</li></ul> <div> <b>Note:</b> Windows 8 and Windows 10 are supported in traditional desktop mode. Tablet mode is not supported. Touchscreen is not supported.</div> <p>Compatible legacy Microsoft operating systems:</p> <ul style="list-style-type: none"><li>• Windows XP Professional</li><li>• Windows Vista</li></ul>
Web browser	<p>One of the following:</p> <ul style="list-style-type: none"><li>• Microsoft Internet Explorer, version 6 or later</li><li>• Mozilla Firefox, version 1.0 or later</li></ul>
Hardware	<ul style="list-style-type: none"><li>• 2 GHz x86-compatible processor</li><li>• 2 GB of memory</li><li>• 300 MB of available disk space</li><li>• CD drive</li><li>• 1024 x 768 display</li><li>• Network card (to connect to your firewall)</li><li>• USB port</li></ul>

# Sidewinder requirements

The firewall must meet these requirements.

**Table 2: Minimum requirements by type**

Firewall type	Platform requirements
Sidewinder appliance	Appliance with a valid support contract: <ul style="list-style-type: none"><li>1 GB of memory</li><li>AMD64-compatible processor</li></ul>
Sidewinder, Virtual Appliance	Virtualization server: <ul style="list-style-type: none"><li><b>Hypervisor operating system</b> — VMware ESX/ESXi version 4.0 or later</li></ul> <div> <b>Note:</b> 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.</div> <ul style="list-style-type: none"><li><b>Hardware resources:</b><ul style="list-style-type: none"><li>2 virtual processors</li><li>AMD64-compatible processor</li><li>1 GB of memory</li><li>30 GB of free disk space</li><li>2 or more NICs of type e1000</li></ul></li><li><b>Internet connectivity</b> — The firewall requires a persistent Internet connection to maintain an active license and full functionality.</li></ul>
Forcepoint Sidewinder on Crossbeam X-Series Platforms	Crossbeam X-Series Platform: <ul style="list-style-type: none"><li><b>Chassis</b> — X50, X60, or X80-S</li><li><b>XOS version</b> — 9.6.5 and later, 9.7.1 and later, 9.9.x, or 10.0</li><li><b>Application Processor Module</b> — APM-50 or APM-9600<ul style="list-style-type: none"><li>At least one local disk (RAID 0 and RAID 1 disk configurations are supported; two-disk, non-RAID configurations are not supported)</li><li>12 GB of memory (minimum)</li></ul></li><li><b>Network Processor Module</b> — NPM-50, NPM-86x0, or NPM-96x0</li><li><b>CBI package</b> — MFE-8.3.2-9.mr1.cbi</li></ul>

# McAfee EIA requirements

Systems must meet these requirements to install McAfee EIA.

**Table 3: 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"><li>Windows 8.1</li><li>Windows 7</li><li>Windows XP Service Pack 2 and later</li></ul>

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

# Resolved issues

---

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

## Common Vulnerabilities and Exposures (CVEs)

### BIND

- Imports a fix for CVE-2016-2776; see Knowledge Base article [8757](#) for more information. (1114207)

### Kernel

- Imports a fix for CVE-2016-1886, FreeBSD-SA-16:18.atkbd; see Knowledge Base article [10265](#) for more information. (1114052)

### NTP

- Addresses the following security vulnerabilities by upgrading NTP:  
CVE-2016-4957, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956 CVE-2016-1547, CVE-2016-1550, CVE-2016-2518, CVE-2016-2519, CVE-2015-7704, and CVE-2015-8138.
- Mitigation is incorporated for the following vulnerabilities:  
CVE-2016-1549 and CVE-2016-1548.
- Not vulnerable to CVE-2016-1551, CVE-2016-2516, or CVE-2016-2517, but a change is included for general maintenance purposes.
- See Knowledge Base article [10260](#) and Knowledge Base article [10257](#) for more information. (1114069 and 1114072)

### OpenSSH

- Addresses the following security vulnerability by upgrading OpenSSH:  
CVE-2016-6515; see Knowledge Base article [10481](#) for more information. (1114160)

### OpenSSL

Upgraded to OpenSSL 1.0.2j

- Imports fixes for CVE-2016-6304, CVE-2016-2183, CVE-2016-6303, CVE-2016-6302, CVE-2016-2182, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2181, CVE-2016-6306, and CVE-2016-7052
- Not vulnerable to CVE-2016-6305, CVE-2016-6307, CVE-2016-6308, or CVE-2016-6309 (Only affects OpenSSL 1.1.0a).
- Not vulnerable to CVE-2016-2180, but a related change is included for maintenance purposes.
- See Knowledge Base article [10448](#), Knowledge Base article [10479](#), and Knowledge Base article [10480](#) for more information. (1114095, 1114189, 1114215, 1114243, and 1114233)

## General Maintenance Changes

### Licensing and Downloads

- Changes domain names for dynamic component downloads from McAfee to Forcepoint. (1114119)

Specifically, changes:

```
downloads.securecomputing.com to sidewinder.downloads.forcepoint.com;  
used for patches and upgrades  
downloads.securecomputing.com to sidewinder.downloads.forcepoint.com;  
used for geo-location updates  
downloads.securecomputing.com to sidewinder.downloads.forcepoint.com;  
used for messages updates  
downloads.securecomputing.com to av.sidewinder.downloads.forcepoint.com;  
used for McAfee Anti-Virus updates  
downloads.securecomputing.com to sidewinder.downloads.forcepoint.com;  
used for Sophos Anti-Virus updates  
downloads.securecomputing.com to sig.sidewinder.downloads.forcepoint.com;  
used for IPS signature updates  
downloads.securecomputing.com to sig.sidewinder.downloads.forcepoint.com;  
used for AppPrism updates  
go.mcafee.com to sidewinder.activations.forcepoint.com;  
used for licensing
```

See Knowledge Base article [10504](#) for more information.

## **ACLD**

- Adds more query stats to acld; this helps when diagnosing high CPU load with acld. (1114061)

## **Admin Console**

- Upgrades the Admin Console to OpenSSL version 1.0.2. (1114095)

## **Audit**

- Fixes scp audit export to FreeBSD 10 hosts. (1114181)

## **cf**

- Fixes a disk usage calculation used when generating System Vital Statistic reports. (1113979)
- Does not allow cf pack autoload to load SOV patches unless Sophos antivirus is licensed. (1113996)

## **Certificate Authorities**

- Updates the list of Trusted Internet Certificate Authorities (CAs). (1114050)

## **Cluster Policy**

- Sidewinder firewall clusters with members running at different P-patch levels no longer synchronize policy changes between members. (1114184)

## **IKE**

- Improves support for CA groups in the isakmp daemon. (1114046)

## **MLC**

- Provides the full error message and return code when cf passport retrieve\_mlc\_cert fails. (1114002)

## **OpenSSL**

- Removes SSLv2 and minimum cipher lengths of 40 bit and 56 bit. (1114095 and 1114180)
- OpenSSL maintenance for FIPS certified firewalls.  
With 8.3.2P09, a firewall in FIPS mode no longer works with Global Threat Intelligence (GTI). (1114109)

## **RealAudio Proxy**

- Fixes a memory leak in the RealAudio proxy when acld is running slowly and the server connection encounters an unexpected error during the initial connect. (1114135)

## **SNMP Proxy**

- Increases file descriptor set size for the SNMP Proxy to prevent SNMPp from receiving invalid file descriptors. (1114057)

## **SSH Keys**

- Removes the ability to generate 1024 bit DSA keys for OpenSSH. (1114109 and 1114136)



# Installation instructions

---

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

The firewall must be at version 8.3.2P03 or later.

- **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 5.3.2P02 or later to manage firewalls at version 8.3.2P03 or later.

- **Crossbeam X-Series Platforms firewall** — See the *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*, version 8.3.x.

# Known issues

---

For a list of known issues in this product release, see Knowledge Base article [9764](#).

# 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

- *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

Copyright © 1996 - 2016 Forcepoint LLC  
Forcepoint™ is a trademark of Forcepoint LLC.  
SureView®, ThreatSeeker®, TRITON®, Sidewinder® and Stonesoft® are registered trademarks of Forcepoint LLC.  
Raytheon is a registered trademark of Raytheon Company.  
All other trademarks and registered trademarks are property of their respective owners.