FORCEPOINT

Sidewinder Control Center

Release Notes

5.3.2P15
Revision A

Contents

About this release

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

Forcepoint Sidewinder Control Center version 5.3.2P15 provides support for Forcepoint Sidewinder version 8.3.2.P13 and earlier (8.x.x and 7.0.1.03). The system must be on version 5.3.2P02 to install this patch.

This release resolves issues present in the previous release.

You can find additional information by using the resources listed in the table.

Table 1: Product resources

Component	Requirements
Help	Online Help is built into Control Center. Click **Help** on the toolbar or from a specific window.
Support	Visit https://support.forcepoint.com to find: • Product documentation • Knowledge Base articles • Product announcements • Technical support • Product installation files • Upgrades and patches **Note:** For information about the support life cycle, see https://support.forcepoint.com/ProductSupportLifeCycle.
Product updates	Visit https://support.forcepoint.com/Downloads to get patches.

Compatible products

Control Center version 5.3.2P15 is compatible with the following products:

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

For the latest information about the firewall products and versions that interoperate with Control Center, see Knowledge Base article 9275.

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.

- New Network Security End User License Agreement. (1115416 1116055)

- Update copyright year to 2021. (1116419)

- Update the UI to allow deletion of Default_enterprise_cert. (1115176)

- Update the kernel to address the following CVEs:

  ```
  CVE-2017-2647,  CVE-2018-12126, CVE-2018-12126, CVE-2018-12127, CVE-2018-12127,
  CVE-2018-12130, CVE-2018-12130, CVE-2018-12207, CVE-2018-13405, CVE-2018-13405,
  CVE-2018-17972, CVE-2019-11091, CVE-2019-11091, CVE-2019-11477, CVE-2019-11477,
  CVE-2019-11478, CVE-2019-11478, CVE-2019-11479, CVE-2019-11479, CVE-2019-11487,
  CVE-2019-11810, CVE-2019-14821, CVE-2019-14835, CVE-2019-17055, CVE-2019-17133,
  CVE-2019-17666, CVE-2019-3896,  CVE-2019-3896,  CVE-2019-3900,  CVE-2019-3900,
  CVE-2019-3900,  CVE-2019-5489,  CVE-2020-10711, CVE-2021-20265, CVE-2021-27364,
  CVE-2021-27365.
  ```

  (1115134 1115135 1115207 1115258 1115332 1115337 1115342 1115345 1115351 1115365 1115366 1115367 1115368 1115409 1115410 1115411 1115422 1115548 1115549 1115573 1115655 1115708

  Note: The fix for `CVE-2019-3896` contains only the kernel portion, and no associated microcode changes.

  1115781 1115982 1116196 1116197 1116200)

- Fix OpenSSL CVEs:

  ```
  CVE-2018-0734, CVE-2018-0739, CVE-2019-1547, CVE-2019-1551, CVE-2019-1552,
  CVE-2019-1559, CVE-2019-1563, CVE-2021-23839.
  ```

  (1115154 1115249 1115279 1115506 1115537 1115541 1115789 1116189)

- Fix DHCP `CVE-2018-5732`. (1115653)

- Fix `sudo CVE-2019-14287` and `CVE-2021-3156`. (1115650 1116144)

- Fix `net-snmp` `CVE-2020-15862`. (1116051)

- Fix unzip `CVE-2014-8141`. (1115870)

- Add script `/usr/local/bin/certgen_db.sh` to regenerate postgres certificate. (1116192)

- Upgraded Sidewinder 8.3.2P13 to OpenSSL 1.1.1.

- Added support for TLS 1.3 and updated available cipher suites. (1116288 1116402)

- New cipher suites for Sidewinder 8.3.2P13 are:

  - 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

- Cipher suites removed for Sidewinder 8.3.2P13 are:

  - EDH-RSA-DES-CBC3-SHA

  - EDH-DSS-DES-CBC3-SHA

  - DES-CBC3-SHA

  - RC4-SHA

  - RC4-MD5

- A warning about new SSL Rule ciphers will be presented when applying policy to firewalls with versions prior to 8.3.2P13. A warning about deprecated SSL Rule ciphers will be presented when applying policy to 8.3.2P13 firewalls. (1116411)

Installation instructions

You can install Control Center on a physical or virtual appliance.

Patches are available from https://support.forcepoint.com/Downloads.

For more details, see the *Forcepoint Sidewinder Control Center Installation and Migration Guide*.

Steps

1) Install 5.3.2P15 rev B.
2) Download and install the 5.3.2P15 patch.

Hardware appliance requirements

Before you install Control Center 5.3.2, make sure the Control Center Client application and Management Server requirements are met.

Client application requirements

The computer that hosts the Control Center Client application must meet these requirements.

Table 2: Client application minimum requirements

Component	Requirements
Operating system	One of the following Microsoft operating systems: • Windows Server 2008 • Windows 7 • Windows 8 • Windows 10 **Note:** Windows 8 and Windows 10 are supported in traditional desktop mode. Tablet mode is not supported. Touchscreen is not supported. Compatible legacy Microsoft operating systems: • Windows Vista

Component	Requirements
Web browser	One of the following: • Microsoft Internet Explorer, version 7 or later • Mozilla Firefox, version 1.0 or later • Google Chrome • Microsoft Edge

Hardware	• 3.0 GHz Intel Pentium 4 processor or higher
	• System memory
	  • Windows Server — 3 GB (2 GB minimum)
	  • Windows Vista, Windows 7, Windows 8, or Windows 10 — 4 GB (3 GB minimum)
	• 150 MB of available disk space
	• CD drive
	• Network card (with access to network hosting the Management Server)
	• USB port (for USB drive)
	• USB drive formatted in MS-DOS (*configuration USB drive*)
	
	Note: You must provide a configuration USB drive; the USB drive that we provided cannot be used to store the configuration file.
	
	• 1280 x 1024 display (1024 x 768 minimum)
	• Keyboard and mouse
	• Network cables

Management Server requirements

Control Center versions 5.3.0 and later use the McAfee® Linux Operating System (MLOS) 2.1.0 64-bit version.

⚠ **Important:** These requirements are applicable to both physical and virtual appliances. See the *Forcepoint Sidewinder Control Center Installation and Migration Guide* for more details.

Table 3: Management Server minimum requirements

Component	Requirements
Hardware	Examples: • C1015 • C2050

Virtual appliance requirements

The Forcepoint Sidewinder Control Center, Virtual Appliance runs on the VMware ESX 5.0 or later hypervisor operating system, providing flexible security for your virtual environment.

To run Control Center, Virtual Appliance, the following requirements must be met.

Table 4: System requirements

Component	Requirements
Control Center, Virtual Appliance	
VMware server	VMware ESX version 5.0 or later **Tip:** Make sure that VT (Virtual Technology) is enabled in your computer BIOS.
Hardware	Any server-class type hardware. Examples: • Dell R910 • Dell R610
CPU	One virtual processor
Memory	1 GB minimum (Recommended 2 GB)
Drives	150 GB of available disk space **Note:** Hard drive space is thin provisioned. 150 GB is the maximum amount of disk space the virtual machine requires. A minimal installation uses approximately 5 GB of disk space and increase as needed. **Note:** For a VMDK installation, we recommend that you select thin provisioning.
Control Center Client application	
Operating system	One of the following Microsoft operating systems: • Windows Server 2008 • Windows 7 • Windows 8 • Windows 10 **Note:** Windows 8 and Windows 10 are supported in traditional desktop mode. Tablet mode is not supported. Touchscreen is not supported. Compatible legacy Microsoft operating systems: • Windows Vista
Monitor	1024 x 768 or higher
Network interface card	Access to the network hosting your Control Center, Virtual Appliance
Browser	• Microsoft Internet Explorer, version 7 or later • Mozilla Firefox, version 1.0 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

Forcepoint Sidewinder Control Center documentation set includes the following:

Typical documents

- *Forcepoint Sidewinder Control Center Release Notes*
- *Forcepoint Sidewinder Control Center Product Guide*
- *Forcepoint Sidewinder Control Center Online Help*

Hardware

- *Firewall Enterprise Control Center Installation USB Drive Product Note*
- *Forcepoint Sidewinder Control Center Hardware Guide*, C Models
- *Forcepoint Sidewinder Control Center Installation and Migration Guide*
- *Forcepoint Sidewinder Control Center Quick Start Guide*

Certification

- *Firewall Enterprise Control Center Common Criteria Evaluated Configuration Guide*
- *Firewall Enterprise Control Center FIPS 140-2 Configuration Guide*
- *Firewall Enterprise Control Center FIPS 140-2 Level 2 Kit Installation Guide*