



FORCEPOINT

Sidewinder Control Center

Release Notes

5.3.2P13

Revision A

Contents

- [About this release](#) on page 2
- [Resolved issues](#) on page 3
- [Installation instructions](#) on page 4
- [Known issues](#) on page 7
- [Find product documentation](#) on page 7

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 5.3.2P13 provides support for Forcepoint Sidewinder version 8.3.2.P10 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.


The locations of the Control Center client applications in the Windows **Start** menu have changed for all versions of Windows excluding Windows 8. The new locations are:

- **Start > All Programs > Forcepoint > Sidewinder Control Center v5 > 5.3.2 > Sidewinder Control Center**
- **Start > All Programs > Forcepoint > Sidewinder Control Center v5 > 5.3.2 > Sidewinder Control Center Initialization Tool**

The previous Control Center client applications have been removed from the Windows **Start** menu.

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	<p>Visit https://support.forcepoint.com to find:</p> <ul style="list-style-type: none"> • Product documentation • Knowledge Base articles • Product announcements • Technical support • Product installation files • Upgrades and patches <p> Note: For information about the support life cycle, see https://support.forcepoint.com/ProductSupportLifeCycle.</p>
Product updates	Visit https://support.forcepoint.com/Downloads to get patches.

Compatible products

Control Center version 5.3.2P13 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.

- Fixes audit CVE-2015-5186. (1114817)
- Fixes bash CVE-2016-0634. (1114649)
- Fixes glibc CVE-2017-1000366. (1114556)
- Updates the kernel to address the following CVEs:

CVE-2017-1000111, CVE-2017-1000112, CVE-2017-1000253, CVE-2017-1000364, CVE-2017-1000379, CVE-2017-11600, CVE-2017-14106, CVE-2017-14991, CVE-2017-2636, CVE-2017-7541, CVE-2017-7542, CVE-2017-1000370, CVE-2017-1000371, and CVE-2017-1000380.

(1114559, 1114703, 1114650, 1114428, 1114559, 1114600, and 1114712)

- Fixes kernel CVE-2017-5754 (AKA Meltdown / Spectre). (1114779). See Knowledge Base article [14992](#) for more information.
- Fixes the following ncurses CVEs: CVE-2017-10684 and CVE-2017-10685. (1114576)
- Fixes the following OpenSSL CVEs: CVE-2016-8610, CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, and CVE-2017-3738. (1114730, 1114735, 1114742, 1114763, and 1114881). See Knowledge Base article [14990](#) for more information.
- Fixes sudo CVE-2017-1000367. (1114556)
- Updates tcpdump to address the following CVEs:

CVE-2015-3138, CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-11544, CVE-2017-11545, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004, CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010, CVE-2017-13011, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016, CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022, CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028, CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034, CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040, CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046, CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052, CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689, CVE-2017-13690, and CVE-2017-13725.

(1114589, 1114605, 1114674, 1114675, 1114676, 1114677, 1114678, 1114680, and 1114695)

- Corrects an issue with sending real-time audit data to Control Center when the firewall is in FIPS mode. Control Center UTT will now always accept TLS and DH 2048. (1114581)

- Corrects an issue with running the Control Center client on Windows 10. (1114423)
- Updates audit records. (1114667)
- Fixes a traceback in the Attack Responses and System Responses screens. (1114843)
- Prevents a recursive event loop when adding URL rules. (1114844)
- Fixes a traceback associated with the Certificate Details dialog box. (1114782)
- Fixes a client traceback when viewing a certificate request. (1114870)
- Fixes a client traceback when adding an NTP server. (1114868)
- Adds an LDAPS option for Authentication. (1114728)
- Adds validation to the rules screen which warns users of possible bad redirect port values. Users can ignore the warning if it is valid. (1114666)
- Adds an option to use the same EngineID as the SNMP agent uses for SNMP traps. (1114707)

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 Control Center 5.3.2.
- 2) If the 532P02 patch is not installed, download and install the patch.



Note: 5.3.2P13 makes the previous 5.3.2P03 through 5.3.2P12 patches obsolete.

- 3) Download and install the 5.3.2P13 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	<p>One of the following 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
Hardware	<ul style="list-style-type: none"> 3.0 GHz Intel Pentium 4 processor or higher System memory <ul style="list-style-type: none"> 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 (<i>configuration USB drive</i>) <p> Note: You must provide a configuration USB drive; the USB drive that we provided cannot be used to store the configuration file.</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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	

Component	Requirements
Operating system	<p>One of the following 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
Monitor	1024 x 768 or higher
Network interface card	Access to the network hosting your Control Center, Virtual Appliance
Browser	<ul style="list-style-type: none"> Microsoft Internet Explorer, version 7 or later Mozilla Firefox, version 1.0 or later

Known issues

For known issues in this product release, see Knowledge Base article [9762](#).

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*

