Sidewinder Control Center

Release Notes

5.3.2P12
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 5.3.2P12 provides support for Forcepoint Sidewinder version 8.3.2.P09 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	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 5.3.2P12 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 earlier releases, see the Release Notes for the specific release.

- Upgrades the Network Time Protocol (NTP) RPM and exposes the NTP options configuration on the 'Network Settings' client screen. Addresses the following CVEs: CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311, and CVE-2016-9312. (1114316). See Knowledge Base article 12449 for more information.
- Upgrades OpenSSH to version 7.4p1. (1114464)
- Fixes OpenSSH CVE-2016-1908. (1114473). See Knowledge Base article 12714 for more information.
- Upgrades OpenSSL to version 1.0.2k. (1114466)
- Updates the kernel to address the following CVEs:

```
CVE-2010-5328, CVE-2012-6704, CVE-2014-9914, CVE-2015-1328, CVE-2015-3288, CVE-2015-8952,
CVE-2015-8953, CVE-2015-8966, CVE-2015-8967, CVE-2015-8970, CVE-2016-6213, CVE-2016-6327,
CVE-2016-6786, CVE-2016-6787, CVE-2016-6828, CVE-2016-7039, CVE-2016-7042, CVE-2016-7097,
CVE-2016-7425, CVE-2016-8630, CVE-2016-8632, CVE-2016-8633, CVE-2016-8636, CVE-2016-8645,
CVE-2016-8646, CVE-2016-8650, CVE-2016-8655, CVE-2016-8658, CVE-2016-8660, CVE-2016-8666,
CVE-2016-9083, CVE-2016-9084, CVE-2016-9120, CVE-2016-9178, CVE-2016-9191, CVE-2016-9313,
CVE-2016-9555, CVE-2016-9576, CVE-2016-9588, CVE-2016-9644, CVE-2016-9685, CVE-2016-9754,
CVE-2016-9755, CVE-2016-9756, CVE-2016-9777, CVE-2016-9793, CVE-2016-9794, CVE-2016-9806,
CVE-2016-9919, CVE-2016-10044, CVE-2016-10088, CVE-2016-10147, CVE-2016-10150, CVE-2016-10153,
CVE-2016-10154, CVE-2016-10208, CVE-2017-2583, CVE-2017-2584, CVE-2017-2596, CVE-2017-5546,
CVE-2017-5547, CVE-2017-5548, CVE-2017-5549, CVE-2017-5550, CVE-2017-5551, CVE-2017-5576,
CVE-2017-5669, CVE-2017-5967, CVE-2017-5970, CVE-2017-5972, CVE-2017-5986, CVE-2017-6001,
CVE-2017-6074, and CVE-2017-6214
```

  (1114406, 1114405, 1114401, 1114395, 1114389, 1114364, 1114358, 1114354, 1114351, 1114350, 1114332, 1114318, and 1114291)
- Fixes SELinux CVE-2016-7545. (1114363)
- Corrects an issue where zone groups were incorrectly removed from ACL and SSL rules when retrieved to Control Center. (1114374)
- Corrects an error message which might be displayed when configuring High Availability for Control Center. (1114427)
- Corrects an issue with the license display dashboard. (1114426)
- Updates the copyright year to 2017. (1114400)
- New Network Security End User License Agreement. (1114533 and 1114566)
- Corrects an issue with registration when in FIPS mode. (1114515)
- Fixes retrieval of description of IPS Type. (1114500)
- Corrects an issue with regeneration of postgresql CSP after turning on FIPS mode. (1114463)

- • Modifications to support a new license and download server, and to support firewall patch downloads via HTTP. (1114497)

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:** 5.3.2P12 makes the previous 5.3.2P03 through 5.3.2P11 patches obsolete.

3) Download and install the 5.3.2P12 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

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

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*