Sidewinder Control Center

Installation and Migration Guide

5.3.2P13
Revision A

Contents

Installing and upgrading Control Center

The *Forcepoint Sidewinder Control Center Installation and Migration Guide* describes the installation and configuration for a Control Center standard appliance and Forcepoint Sidewinder Control Center, Virtual Appliance (Control Center, Virtual Appliance). This document provides you procedures to upgrade from Control Center version 5.3.1 to 5.3.2 for hardware and virtual appliances.

Decide to install or upgrade

You can freshly install Control Center 5.3.2 on a standard appliance, virtual appliance, or upgrade from an existing 5.3.1 system to version 5.3.2.

Make your choice

You can choose to install Forcepoint Sidewinder Control Center 5.3.2 on a physical or virtual appliance. If you have a 5.3.1 system, use these high-level steps to upgrade to 5.3.2.

Installing Control Center on a hardware appliance

Follow these sections to install on a standard Control Center appliance.

1) Prepare to install Control Center on a hardware appliance

2) Install the Control Center Client application

3)   Install the Control Center Management Server

4)   Post-installation and upgrade tasks

5)   Navigate the Control Center Client application

Installing Control Center, Virtual Appliance

Follow these sections to install a Control Center, Virtual Appliance.

1)   Prepare to install a Control Center, Virtual Appliance

2)   Install the Control Center Client application

3)   Install the Control Center Management Server

4)   Post-installation and upgrade tasks

5)   Navigate the Control Center Client application

Upgrading from 5.2.x or 5.3.0 to 5.3.2

An intermediate upgrade is required if you are upgrading from 5.2.x or 5.3.x to 5.3.2.

1)   If you are using a 5.2.x system, upgrade to version 5.3.0.

2)   If you are using a 5.3.0 system, upgrade to version 5.3.1.

After that, upgrade to 5.3.2.

Upgrading from 5.3.1 to 5.3.2

If you are using a 5.3.1 system, follow these sections to upgrade to version 5.3.2.

1)   Upgrade from Control Center 5.3.1 to 5.3.2 and then install the 5.3.2P02 patch

2)   Post-installation and upgrade tasks

Documentation requirements

You need to download these documents.

Table 1: Required documents

Source	Documents
Forcepoint Sidewinder Control Center	• *Forcepoint Sidewinder Control Center Release Notes*, version 5.3.2 • *Forcepoint Sidewinder Control Center Product Guide*, version 5.3.2
Forcepoint Sidewinder	• *Forcepoint Sidewinder Product Guide*, version 8.3.2
Links	• https://support.forcepoint.com • https://support.forcepoint.com/Downloads • http://sidewinder.downloads.forcepoint.com

Prepare to install Control Center on a hardware appliance

For a new installation, prepare to install and configure the Control Center Management Server and Client application on a hardware appliance.

Hardware appliance requirements

Before you install 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
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, or Windows 8 — 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 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

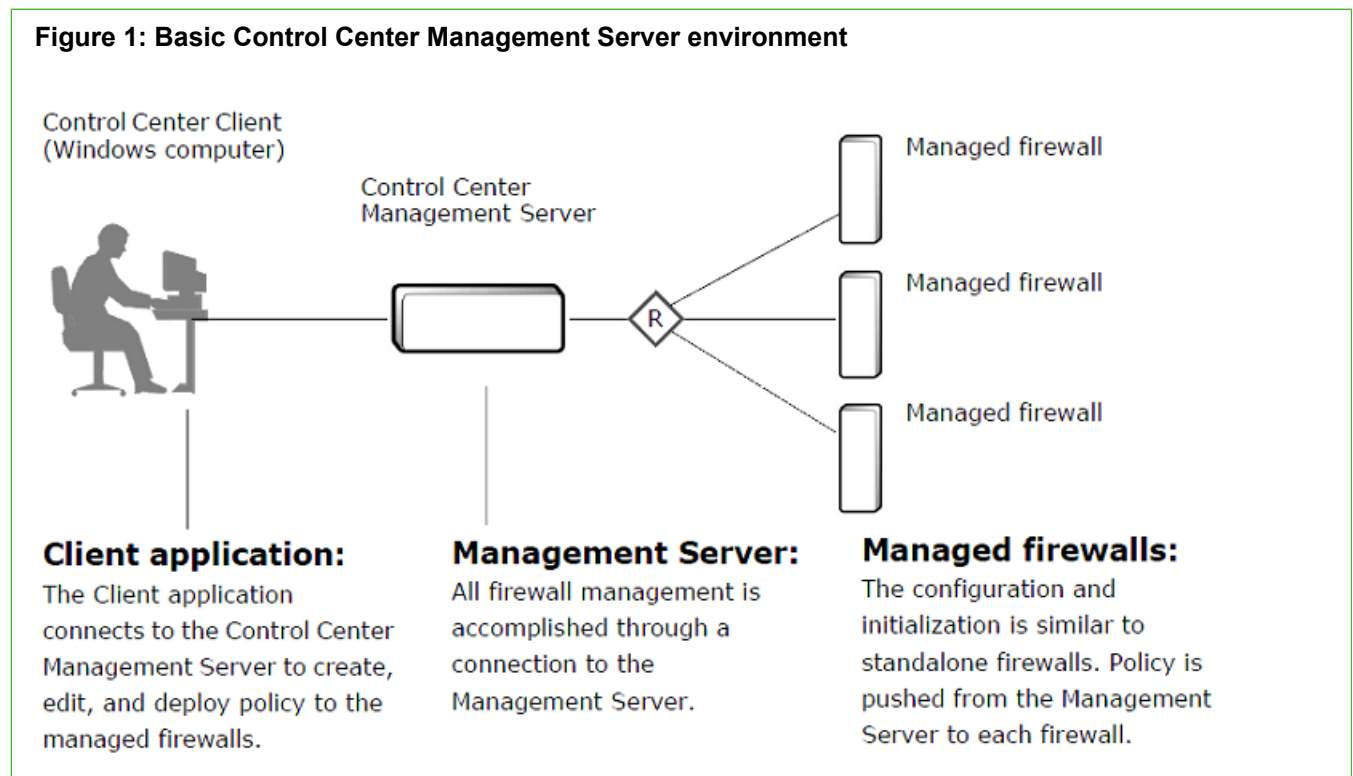| Component	Requirements

Hardware	• Examples:
	    • C1015
	    • C2050

Plan your Control Center installation

Understand options for deploying your Control Center and managed firewalls. Plan your network configuration and develop an integration schedule.

Understanding the Control Center Management Server environment

The Control Center Management Server is an enterprise-class management tool that is used to create and apply security policies across multiple firewalls.

It centrally manages policy, software updates, and reports, and monitors the firewalls in your organization. You can use the Control Center Management Server to manage hundreds of firewalls.

The Control Center uses a Windows workstation that is installed with the Control Center Client application to present a graphical user interface to enterprise administrators. The installation USB drive provides the programs to prepare the initial configuration and to manage your Management Server and its registered firewalls.

Figure 1: Basic Control Center Management Server environment

Client application:
The Client application connects to the Control Center Management Server to create, edit, and deploy policy to the managed firewalls.

Management Server:
All firewall management is accomplished through a connection to the Management Server.

Managed firewalls:
The configuration and initialization is similar to standalone firewalls. Policy is pushed from the Management Server to each firewall.

You can also implement Management Servers in a High Availability (HA) Management Server configuration, where one Management Server actively manages the registered firewalls while another Management Server acts as a standby. Use this configuration to manually switch management responsibilities to another Management Server if the active Management Server fails.

Figure 2: Control Center High Availability configuration
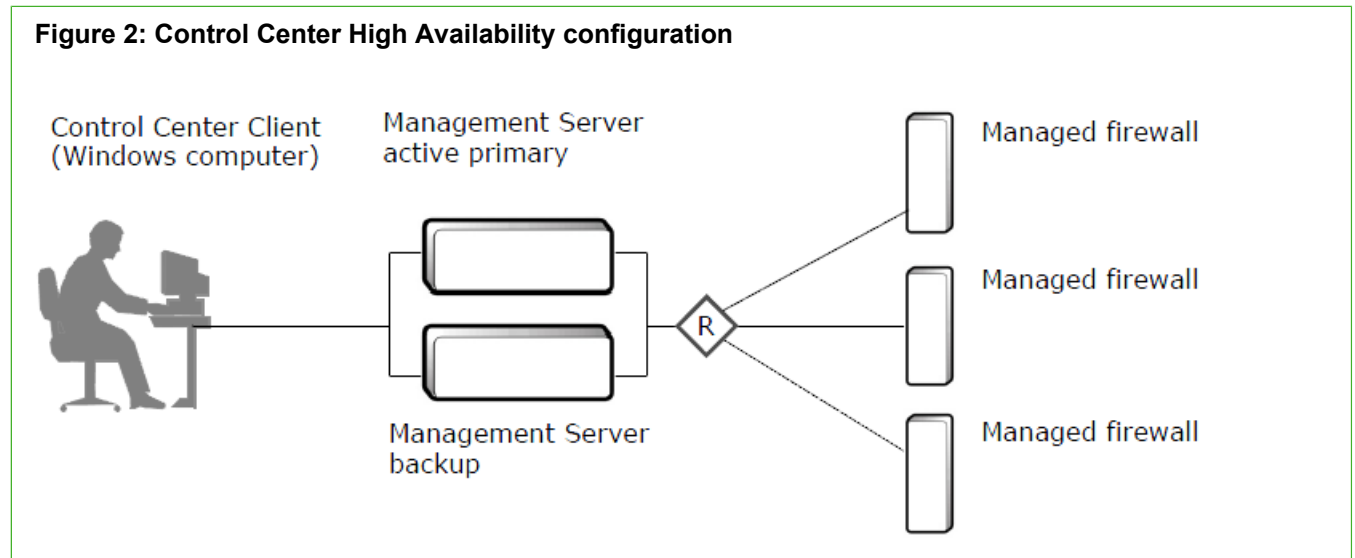
Complete the Control Center setup checklist

Use this checklist to set up your Control Center so that it is registered and fully operational. Mark off each step as you complete it.

Setup checklist
1. Plan your configuration
Read the latest Release Notes for up-to-date information. Plan your integration schedule.
2. Set up the Client application
Make sure that you have a Windows-based computer that meets the minimum requirements. Install the Client application software on the Windows-based computer by using the installation USB drive or the *Client CD*. See the *Forcepoint Sidewinder Control Center Product Guide* to set up the Control Center users and roles. Use the Sidewinder Control Center Initialization Tool to create your initial configuration file (ccinit.txt) and save it to your configuration USB drive. 📝 **Note:** Load the 5.3.1 ccinit file to the 5.3.2 Sidewinder Control Center Initialization Tool. Modify the file and create a new USB installation configuration file.
3. Set up the Management server

Setup checklist
Set up the hardware. **1)** Make sure that the Control Center Management Server is properly situated in your network. **2)** Connect the power cord and the network cable. **3)** Insert the configuration USB drive into the appropriate port. **4)** Turn on the Control Center Management Server. **5)** After the Control Center Management Server has been configured, remove the configuration USB drive that contains the ccinit.txt file. **6)** From your Client application computer, ping the IP address of the Control Center Management Server to verify connectivity. If the ping fails, perform network troubleshooting before continuing with the setup process.

4. Start managing your firewalls
Log on to your Control Center Management Server. Use the appropriate Control Center, or Admin Console, or Sidewinder Quick Start Wizard to register the firewall with the Control Center Management Server. 📝 **Note:** If you need to upgrade a firewall to a version compatible with Control Center, you must use the Control Center to register the firewall. You can do this on a firewall-by-firewall basis or you can use the multiple firewall option. Use the Control Center Client application to retrieve objects from the registered firewalls. Validate the current policy. Apply the current policy to the registered firewalls. Complete the post-setup tasks required by your environment. Example tasks include: • Update the Management Server and the managed firewalls to the latest version. • Create Control Center users. • Set up configuration domains. • Set up any alerts and reports required by your security policy.

Complete the integration schedule checklist

This sample checklist can help prepare and schedule your Control Center integration tasks. Adequate preparation greatly reduces the disruption to your production network.

Support staff and materials considerations

- **Schedule network experts** who are familiar with your existing network components to be available during installation.
- **Schedule firewall experts** who will interact with the Control Center Management Server to be available during installation.
- **Locate any manuals or documentation** that can be useful if problems are encountered.

Network services considerations

- **Develop a test plan** to verify that all key services are functioning as desired.
- **Schedule an appropriate amount of time for the installation.** Include time for preparation, the physical installation of the Management Server, and for testing critical features and services.

  > **Note:** An experienced Control Center installer requires approximately one full workday to complete the installation, configuration, and testing of a basic installation. Adjust this amount accordingly, based on your experience level and the complexity of your security policy and test plan.

- **Determine whether the managed firewalls need to be upgraded.** If the managed firewalls require a software upgrade to reach a version that is compatible with the Control Center version, your network will experience a brief disruption.

  > **Note:** Only 7.0.1.0.3 and higher firewalls can be managed by Control Center 5.3.2.

- **Tell your users and help desk** the times when the network will be unavailable. Also advise your users about any new access controls that might affect their use of the network.

Port configurations for network communication

The following ports are required for proper communication between the Control Center Management Server and Client application and also between registered firewalls and a standalone Management Server.

> **Note:** These ports must be configured before any communication is attempted between any firewall and the Control Center Management Server.

Table 4: TCP port configurations that are required for network communication

Port	Description
Control Center Management Server to firewall	
Port 9005	Firewall SSL port for the Control Center
Firewall to Control Center Management Server	
Port 7080	Control Center Management Server HTTP port
Port 9005	Control Center Management Server HTTPS/SSL port

Port	Description
Control Center Client to Control Center Management Server	
Port 9005	Control Center Management Server HTTPS/SSL port
Port 5432	Control Center Management Server database

Additionally, the following ports are optional, but must be configured for the specified features.

Table 5: Feature-specific optional TCP port configurations for network communication

Port	Description
Control Center Management Server to firewall TCP ports	
Port 22	Required for SSH communication for firewall registration by using the Add New Firewall Wizard
Firewall to Control Center Management Server	
Port 22	SCP transfers of scheduled firewall configuration backups
Port 9006	Control Center utt_server (program for receiving Secure Alerts)
Port 9009	Control Center utt_server (program for receiving real-time audit from firewalls)

Prepare to install Control Center, Virtual Appliance

Follow these sections to prepare to install on a Control Center, Virtual Appliance. Collect the required components, ESX server, and set up Control Center.

Virtual Appliance requirements

Before you set up your appliance, understand your Control Center, Virtual Appliance and make sure all requirements are met.

Sizing guidelines

Use the following table to determine the number of Control Center, Virtual Appliance packages to download and install.

📝 **Note:** These guidelines are based on average policy configuration, and might need to be adjusted for your network depending on the number of rules, rule groups, and application objects in your policy.

Table 6: Sizing guidelines

Number of managed firewalls	Number of Control Center, Virtual Appliance installations
0–60	1
61–120	2
121–180	3
181–240	4
241–300	5
301–360	6
361–420	7
421–480	8
481–540	9
541–600	10
601–660	11
661–720	12
721–780	13
781–840	14
841–900	15
901–960	16
961–1000	17

Virtual appliance requirements

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

Table 7: 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

Component	Requirements
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

Prepare the ESX server

Prepare the virtual network for Control Center.

About ESX virtual networking

Use the Add Network Wizard to configure virtual networking on these virtual machine networking objects.

- **Virtual switch (vSwitch) —** A network object in ESX that connects virtual machines to each other like a physical switch
  - If the virtual machines connected to the vSwitch need to communicate with hosts on a physical network, you can join the vSwitch to the physical network by connecting it to an appropriate physical Ethernet adapter (also known as an uplink adapter).
  - If the virtual machines connected to the vSwitch need to communicate only with each other, you do not need to connect the vSwitch to a physical Ethernet adapter.

- **Port group —** A group of ports that provides a labeled, stable anchor point for virtual machines to connect to a vSwitch

  Port groups include common parameters like VLAN tagging and bandwidth shaping. Multiple port groups can be assigned to a single vSwitch.

  > **Tip:** The Add Network Wizard always creates a new port group, but creating a new vSwitch depends on your choices.

The Control Center, Virtual Appliance has two network interfaces. Each interface must be connected to an ESX vSwitch by mapping it to a port group. Note the following networking requirements:

- Interface assignments cannot overlap; each interface must be assigned to a unique vSwitch.

- One vSwitch must be connected to a physical adapter on your ESX server that provides access to the internet.

Create a new isolated port group

Create a new port group that is not connected to a physical interface. This port group will be referenced by the unconfigured virtual firewall.

Steps

1) Connect to your ESX server using the VMware vSphere Client.

2) Click **Configuration** > **Networking**.
   The **Networking area** appears in the right pane.

3) Click **Add Networking**.
   The **Add Network Wizard Connection Type** window appears.

4) Select **Virtual Machine** > **Next**.
   The **Network Access** window appears.

5) Create a virtual switch that is not connected to any physical network adapters.

   a) Select **Create a virtual switch**.

   b) Deselect the check boxes next to the physical network adapters (vmnics).

   c) Click **Next**.

   The **Connection Settings** window appears.

6) In the **Network Label** field, type **Unconfigured**, then click **Next**.
   The **Summary** window appears.

   > **Note:** The port group must be named *Unconfigured* because it is referenced by the Control Center, Virtual Appliance during import.

7) Click **Finish**.
   The Add Network Wizard closes.
   A port group named **Unconfigured** is added.

Modify your virtual network configuration

Prepare ESX virtual networking for the deployment of Control Center, Virtual Appliance.

Steps

1) In the VMware vSphere Client, click **Configuration** > **Networking**.
The **Networking** area appears in the right pane.

2) Click **Add Networking**.
The **Add Network Wizard** window appears.

3) Select **Virtual Machine** > **Next**.
The **Network Access** window appears.

4) Select the virtual switch that will handle network traffic for this connection, then click **Next**.

- If you need to create a new vSwitch, select **Create a virtual switch**. Enable or disable physical Ethernet adapters for this vSwitch as necessary.
- To assign this connection to an existing vSwitch, select it from the list.

The **Connection Settings** window appears.

5) In the **Port Group Properties** area, configure the following items, then click **Next**.

- **Network Label** — Enter a name for this port group.
- **VLAN ID** — [Optional] To configure this port group to participate in VLAN tagging, enter a VLAN ID between 1 and 4095.

The **Summary** window appears.

6) To Examine the Preview.

- To confirm your changes, click **Finish**.
- To modify your changes, click **Back**.

The new connection configuration is complete.

> **Tip:** To modify a vSwitch after it has been created, click **Properties** next to it.

Configure the system clock

Configure your ESX server system clock.

We recommend the following:

- Synchronize your system clock with a time server using the Network Time Protocol (NTP).
- Because system clocks can drift from the ESX system clock, configure NTP on your ESX server.

To configure NTP on your ESX server:

Steps

1) In the VMware Infrastructure Client, click **Configuration** > **Time Configuration**.
The **Time Configuration** area appears in the right pane.

2) Click **Properties**.
The **Time Configuration** window appears.

3) Click **Options**.
The **NTP Daemon (ntpd) Options** window appears.

4) In the **Service Commands** area, click **Start**.
The status changes to **Running**.

5) In the left pane, click **NTP settings**.

6) Add an NTP server.

    a) Click **Add**. The **Add NTP Server** window appears.

    b) Specify the host name or IP address of an NTP server, then click **OK**.
    The **Add NTP Server** window closes and the server is added to the list of NTP servers.
    To add additional NTP servers, repeat this step.

7) Select **Restart NTP service to apply changes**, then click **OK**.
The **NTP Daemon (ntpd) Options** window closes.

8) Click **OK** to close the **Time Configuration** window.
NTP is now configured on your ESX server.

Set up Control Center, Virtual Appliance

Install and configure Control Center, Virtual Appliance and the Control Center Client application.

Download the Control Center, Virtual Appliance software

Download the Control Center, Virtual Appliance software.

Steps

1) In a web browser, navigate to https://support.forcepoint.com/Downloads.

2) Enter your logon credentials, then navigate to the appropriate product and version.

3) Download the Control Center, Virtual Appliance installation files:

- **Management Tools —** Download the Control Center, Virtual Appliance Client application executable (.exe) file.
- **Version 5.3.2 Virtual Appliance —** Download the Control Center, Virtual Appliance (.zip) file.

Install the Control Center, Virtual Appliance

Install the downloaded Control Center, Virtual Appliance on your ESX server.

> **Note:** Refer to the sizing guidelines to determine the number of Control Center, Virtual Appliance packages to download.

Steps

1) Unzip the Control Center, Virtual Appliance file onto the hard drive of your Windows-based client computer.

2) Load the Control Center, Virtual Appliance onto an ESX server.

   a) Connect to your ESX server by using the VMware vSphere Client.

   b) From the **File** menu, select **Deploy OVF Template**.
The **Deploy OVF Template** wizard appears.

   c) The **Source** window is displayed. A text message `deploy from file or URL` is displayed.

3) Click **Browse** to select the .ovf Control Center, Virtual Appliance file you extracted in Step 1, then click **Next**.
The **OVF Template Details** window appears.

4) Click **Next**. The **Name and Location** window appears.

> **Note:** If you have multiple datastores, the **Datastore** window appears post this window.

5) Specify a name for the Control Center, Virtual Appliance, then click **Next**.
The **Disk Format** window appears.

6) Select a format for the virtual machine disk, then click **Next**.
The **Network Mapping** window appears.

7) [For ESX 5.0], from the drop-down list, select **unconfigured** and click **Next**.
The **Ready to Complete** window appears.

8) Review the summary.

- If you are satisfied the summary is correct, click **Finish**.
- To make changes, click **Back**.
When you click **Finish**, the Control Center, Virtual Appliance is uploaded to your ESX server.

Configure Control Center, Virtual Appliance

Configure network mappings and administrator settings for the Control Center, Virtual Appliance.

Configure network mappings

Configure the network mappings and administrator settings for the Control Center, Virtual Appliance.

Steps

1) In the VMware vSphere Client, select the Control Center, Virtual Appliance.

2) Click **Getting Started** > **Edit virtual machine settings**.
The **Virtual Machine Properties** window appears.

3) Map one of the Control Center, Virtual Appliance network adapters to the appropriate virtual network.

    a) Refer to the following table and select the network adapter that you want to configure.

      Table 8: Network adapters

Virtual machine hardware device	Control Center, Virtual Appliance NIC
Network Adapter 1	eth0
Network Adapter 2	eth1

    b) Make sure **Connected** and **Connect at power on** are selected.

    c) From the **Network label** drop-down list, select the appropriate port group.

> 📝 **Note:** The port group you select for **Network Adapter 1** must provide Internet connectivity to allow the Control Center, Virtual Appliance to maintain a current license.

4) Click **OK**.

Perform the initial configuration

Configure basic networking and administrator settings for Control Center, Virtual Appliance.

Steps

1) In the vSphere Client, select the Control Center, Virtual Appliance.

2) On the Getting Started tab, click **Power on this virtual machine**.
The Control Center, Virtual Appliance starts.

3) Click **Console**.
After startup is complete, a *Searching for configuration* message appears.

Next steps

Follow the *Install the Control Center Management Server* section to complete the Management Server installation and configuration.

Install the Control Center Client application

Install the Client application

Install the Control Center Client application and prepare the configuration data for the Control Center Management Server to manage the firewalls in your network.

Configuration overview

Setting up Control Center includes installing software, configuring the Control Center Management Server, and registering firewalls.

The high-level steps for configuring your Control Center are:

1) Install the Control Center Client application and the Sidewinder Control Center Initialization Tool.
   Use the Client application to administer the Control Center Management Server. Use the Sidewinder Control Center Initialization Tool to create the initial configuration file.

2) Create and save an initial configuration file.
   The Management Server uses this file to obtain basic networking and administrator account information.

3) Turn on the Control Center Management Server and apply the initial configuration.

4) Connect to the Management Server from the Client application.

5) Add firewalls to the Control Center.

Install Control Center software

You can install the Control Center Client application and Sidewinder Control Center Initialization Tool on a Windows-based computer.

As of the version 5.0.0 release of the Control Center Client application, you can install multiple versions of these applications on the same computer. If you have a previous version of these applications already installed, you have the following choices when you go through the installation:

• You can upgrade the previously installed version to this version.

• You can keep your old version and install this version to another location on your computer.

Steps

1) Log on to the Windows-based computer as an administrator.

2) Insert the installation USB drive into a USB port. The **Welcome** window is displayed.

> **Tip:** Alternatively, you can use the *Client CD* instead of the installation USB drive.

> **Note:** If the installation program does not automatically start, use Windows Explorer to view the contents of the CD or USB drive, then go to the client folder and double-click the executable (.exe) file.

3) Follow the on-screen instructions.

> **Tip:** For option descriptions, press **F1**.

- If you have already installed another version of the Control Center Client application or Sidewinder Control Center Initialization Tool on this computer, make a decision about whether you want to overwrite your old versions or install the new versions at a different location. Make your selections and click **Next**.

- Accept the default settings when possible and click **Next** until the wizard is complete.

The Client application and Sidewinder Control Center Initialization Tool are now installed.

4) [Conditional] If you do not have the correct version of Microsoft™ .NET Framework installed, you must install it before you access the Client application. You have the following choices:

- If you are a new customer, this application is located on the *Client CD* in the Microsoft .NET folder.

- If you are an upgrade customer, see Knowledge Base article 10575 for instructions on obtaining this version of Microsoft .NET Framework.

Create the initial configuration file

You can create the initial configuration file with the Sidewinder Control Center Initialization Tool.

You can install and use the Sidewinder Control Center Initialization Tool to create a ccinit.txt configuration file for use during the Management Server installation. Instead you can manually configure or use a ccinit.txt from an earlier installation like 5.3.1 to install and configure the Management Server.

Steps

1) Insert your USB drive into one of the USB ports on the computer that contains the Client application.

> **Note:** Use a different USB drive than the installation USB Drive that was included with your Control Center Management Server.

2) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Control Center Initialization Tool**.

3) Use the Sidewinder Control Center Initialization Tool to specify configuration information for your Control Center Management Server.

On each window, complete the required fields. When all of the required fields on a window have been completed, click **Next** to advance to the next window.

> **Tip:** For option descriptions, press **F1**.

> **Note:** Initial configuration allows you to set up only one interface. You can add or edit the interface selection and configuration from the Client application.

4) On the **Complete** window, click **Save As** and save the file to the USB drive. Name the file *ccinit.txt*.

> **Note:** The configuration file must be in .txt format. In the **Save as type** field, select **Text File (*.txt)**.

5) Close the Sidewinder Control Center Initialization Tool.

6) Remove the USB drive.

Result

You are now ready to configure the Management Server.

Install the Control Center Management Server

Prepare to install and configure manually the Management Server or apply the initial configuration file to the Management Server. You can choose either of these options to install the Management Server.

Install the Management Server

Install the Management Server using one of these options.

Manually configure the Management Server

For a new installation perform a manual configuration for the Control Center Management Server.

Before you begin

Understand the user and roles that you will set up during the Management Server installation. All user accounts are mandatory.

> 📄 **Note:** These user roles also hold good for creating the ccinit.txt file for server installation.

For every user name and password that you create, follow these rules:

- The user name must not exceed eight characters.
- The password must be at least eight characters.
- All passwords (except Administrator Client user account) cannot contain any of the following characters: backslash (\), less-than sign (<), dollar sign ($), single quotation mark ('), double quotation mark ("), or leading dash (-).

Table 9: User accounts

Option	Definition
Root or Super user account	
root password	Specifies the super user password, who has full access to the Management Server. This is the password for the **root** account. 📄 **Note:** Make sure the password is strong and has printable ASCII characters.
Password (verify)	Re-enter the password for confirmation.
Administrative user account	
Account Name	Specifies the logon account name for the Control Center administrator. This is the same as **mgradmin** user in 5.2.x versions.

Option	Definition
Password	Specifies the password to associate with the user that you typed in the **Admin user name** field.
Password (verify)	Re-enter the password for confirmation.
Client application user account	
Account Name	Specifies the logon ID for the Management Server administrator (for example, **ccadmin**). Use this user name whenever you log on to the Management Server in the Client application logon window. By default, the administrator role is automatically assigned to this user, which provides full access, including access to all managed firewalls. You can change these settings after you finish configuring the Management Server.
Password	Specifies the password to associate with the user that you typed in the **Control Center administrator name** field.
Password (verify)	Re-enter the password for confirmation.
Firewall audit export user account	
Account Name	Specifies the user name, which denotes the Firewall audit export user account on the Management Server. This restricted logon account can be used by firewalls as the receiver for exported firewall audit logs and exported firewall backup files sent to the Control Center server via SCP. The protocol that is used to export the archives to the Management Server is SCP. This is the same as **ftp** user in 5.2.x versions.
Password	Specifies the password that is assigned to the Firewall audit export user on the Control Center Management Server.
Password (verify)	Specifies the password that you specified in the **Password** field.
Database user account	
Account Name	Specifies the administrator account that is configured in the Management Server database. This is the same as **dbuser** in 5.2.x versions. **Note:** We recommend not to name the database user as **dbadmin**.
Password	Specifies the password to associate with the database user account. This account is used to allow the Apache Tomcat server to communicate with the database.
Password (verify)	Re-enter the password for confirmation.

Perform these steps to install and configure the MLOS-based Management Server.

Steps

1) Connect to your ESX server using the VMware vSphere Client for a physical or virtual appliance.

2) From the toolbar, click **CD/DVD drive 1**. In the options, click **Connect to ISO image on local disk....** Browse to the .iso file location and double-click the Control Center Management Server .iso file.

    By default, the installation begins in 10 seconds.

3) The **Installation Finished!** screen is displayed. Remove the install media. Enter `Y` to reboot the installed system.
The **GNU GRUB** screen is displayed.

4) On the **End User License Agreement** screen, press `q` to move to the **Accept** screen to accept the agreement. Press <space> to scroll down to the next page.

5) On the **Select Configuration** screen, press `M` to manually configure the system.

6) On the **Setting Root Password** screen, enter the password for the super user account.
Confirm your root password for authentication.

7) On the **Administrative Account Creation** screen, enter the supervisor username and password . Press `Y` to create the supervisor account.

> **Tip:** Use the Tab key to move between fields and enter details.

8) On the **Client Account Creation** screen, enter the account name and password. Press `Y` to create the client account to log in.

> **Tip:** Use the Tab key to move between fields and enter details.

9) On the **Firewall Audit Export Account Creation** screen, enter the account name and password. Press `Y` to create this account for backups and audit exports to Control Center.

10) On the **Database User Account Creation** screen, enter the account name and password. Press `Y` to create this administrative account in the database of the Management Server.

11) On the **Network Selection** screen, press the `Up Arrow` and `Down Arrow` keys to select the network interface. Press `Enter`.

12) On the **Network Setup for the Main Network Interface** screen, enter network, addresses, and interface details. Press `Y` to proceed with these settings.

13) On the **Host Name Setup** screen, enter the host name. Press `Y` to create the host name.

14) On the **Domain Setup** screen, enter the domain name. Press `Y` to create the domain.

15) On the **Time Zone Setup** screen, press `Y` to select a time zone or `N` for Universal Time (UTC).
If you pressed `Y` for the time zone setup, select the time zone, continent, country, and state on the subsequent screens. Press `Y` to confirm the time zone settings.

16) (Optional) On the **NTP Setup** screen, enter the NTP server address for configuration.

17) (Optional) On the **SMTP Server Setup** screen, enter the SMTP server address.

Result

When it is finished, the **Rebooting System** screen is displayed. The Management Server automatically reboots and the logon prompt appears.

Next steps

- Register the firewall so that Firewall Audit and Backup export to Control Center is functional.

Apply the configuration file to the Management Server

You can automatically install the Management Server using the initial configuration file. Use the ccint.txt file created from the 5.3.2 Sidewinder Control Center Initialization Tool or a loaded and modified 5.3.1 ccinit.txt file to initialize the Management Server.

Refer to the prerequisites in *Manually configure the Management Server*.

Steps

1) Use a diagram of your network to determine the proper place for your Management Server. Your server must be able to reach the appropriate routers, subnets, and managed firewalls.

2) Attach the power cord to your Management Server and plug it into an electrical outlet.

> **Note:** If your Management Server has redundant power supplies, attach and plug in both power cords. If only one power supply is connected, the amber indicator blinks, indicating an error.

3) Connect the network cable.

4) Insert the configuration USB drive into a Management Server USB port.

5) Turn on the Management Server.

   The Management Server automatically loads the configuration information. When the initial configuration is complete, a logon prompt is displayed.

Result

The Management Server now has its initial configuration.

Upgrade from 5.3.1 to 5.3.2

Upgrade from your 5.3.1 system and perform post-upgrade tasks. Install the 5.3.2P02 patch on your 5.3.2 system.

> **Note:** If you are upgrading from 5.2.x or 5.3.0, refer to the *Forcepoint Sidewinder Control Center Installation and Migration Guide* 5.3.0 and 5.3.1 to upgrade to 5.3.1. After that follow these procedures to upgrade to Control Center 5.3.2 and install the 5.3.2P02 patch.

Download the Control Center 5.3.2 software

Download the Control Center 5.3.2 patch upgrade package to the system that has version 5.3.1 of the Control Center Client application installed.

Perform these steps to download the required files:

Steps

1) Open a web browser and go to http://sidewinder.downloads.forcepoint.com.

2) Navigate to the appropriate product and version.

3) Download the version 5.3.2 .zip file.

> **Tip:** Download and install the 5.3.2P02 patch file on a 5.3.2 system.

Upgrade the Management Server

Upload and apply the version 5.3.2 files for the upgrade.

Before you begin

- Save all your data and make sure that all Forcepoint Sidewinder appliances are licensed.
- Create a full configuration backup of the Management Server. For more information, see the *Forcepoint Sidewinder Control Center Product Guide*.
- If the Management Server is running with the High Availability (HA) option, use the High Availability Removal Wizard to stop HA. You must recreate and restart HA after you have upgraded.

> **Note:** After installing 701UP packages, when you select and click **Download update**, the firewall fails to point to the appropriate package. You need to manually download these packages so that they are available on the Management Server.

Load the 5.3.2 upgrade package

Upload the 5.3.2 package to the Control Center Client application.

Steps

1) Unzip the Control Center 5.3.2 .zip file onto the hard drive of your Windows-based client computer.

2) Log on to version 5.3.1 of the Client application.

    a) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

       The logon window appears.

b) Specify the information on the logon window, then click **Connect**.

The **Summary** page of the Control Center Client application appears.

3) In the navigation bar, select **Control Center** > **Control Center Updates**.

The **Control Center Update** page appears.

4) Make sure that the **Upload to Server** tab is displayed and select **Upload to Server from Client**.

5) Click **Browse** to locate the .tar file for the 5.3.2 release.

6) Click **Upload**.

A confirmation message is displayed.

7) Click **OK**.

Apply the 5.3.2 upgrade

Install the 5.3.2 upgrade on the Control Center Management Server.

> 📝 **Note:** If the Management Server was running as part of an HA pair, you must first break the HA pair, apply the upgrade, and then recreate the HA pair after upgrade.

Steps

1) Click the **Uploaded Packages** tab.

2) Select the patch and click **Apply**. A confirmation message is displayed. All of the Client applications are logged off and the Management Server restarts.

3) Click **Yes**. Wait for the Management Server to install the package and restart.

> 📝 **Note:** If this Management Server was running as part of an HA pair, you must perform this same procedure on the other Management Server of the HA pair.

Upgrade the Client application

The Control Center Client application is automatically updated to version 5.3.2 when the client connects to the Management Server.

> 📝 **Note:** You can also manually update the client by running the client Setup .exe file.

Steps

1) On your client computer, log on to version 5.3.1 of the Client application.

- Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

- Specify the information on the logon window, then click **Connect**.

> **Note:** A message appears indicating the new Client application will be uploaded to this computer from the Management Server.

2) Click **OK**. Wait for the new version of the Client application to be uploaded to your computer.

The installation program for version 5.3.2 of the Client application is displayed.

3) Follow the on-screen instructions. When the installation is complete, click **Finish**.

An informational message appears indicating the update was successfully installed.

4) Click **OK.**

The logon window for version 5.3.1 of the Client application reappears.

5) Click **Exit** to close the version 5.3.1 logon window.

6) Log on to the newly installed version 5.3.2 Client application. Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

> **Note:** Microsoft .NET Framework 3.5 Service Pack 1 is required. If you do not have this installed on your client computer, see Knowledge Base article 10575 for instructions on how to obtain that version.

Post–installation and upgrade tasks

Depending on whether you installed Control Center on a physical or virtual appliance, or performed an upgrade follow these procedure for a functional 5.3.2 system.

Connect to the Management Server

You can connect to the Management Server using the Client application.

> **Note:** This procedure assumes you are logging on to Control Center for the first time.

Steps

1) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

2) Specify the appropriate information.

> **Note:** If another version of the Control Center Client application is installed on this computer, the default information from that version is displayed in this window. Make whatever changes are necessary.

If this is the first version of the Control Center Client application that is being installed on this computer, you must complete the fields on this window.

- In the **Name** field, specify a name that quickly identifies this Management Server.
- In the **Server address** field, specify the host name or IP address of the Management Server.
- Select **Primary server**, and then complete the following fields with information appropriate for this Management Server:
  - In the **User name** field, specify a valid user name.
  - In the **Password** field, specify the password that has been assigned to this user name by the system administrator.

3) Click **OK**. A **Certificate Problem** message is displayed. The message is similar to the following example:

```
The Management Server's SSL certificate needs to be validated. The server detected the
 following error when contacting the URL "https://<IP_address>:9005/cm/certdist/ca.cer": "A
 certificate chain processed, but terminated in a root certificate which is not trusted by the
 trust provider". Do you want to ignore this error and continue?
```

This message is expected. It is displayed because the application imports a non-Certificate Authority (CA) certificate before it imports the CA certificate of the Management Server. You can safely ignore this error.

4) Click **Yes**. A **Security Warning** message is displayed. The message is similar to the following example:

```
You are about to install a certificate from certification authority (CA) claiming to represent
 CommandCenter CA
```

```
Windows cannot validate that the certificate is actually from "CommandCenter CA". You should
 confirm its origin by contacting "CommandCenter CA". The following number will assist you in
 this process: Thumbprint (sha1): <actual certificate thumbprint>
```

```
Warning:
```

```
If you install this root certificate, Windows will automatically trust any certificate issued
 by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you
 click "Yes", you acknowledge this risk. Do you want to install this certificate?
```

5) Click **Yes**.

If the Management Server and the Client application are the same version, the main logon window is displayed, and the newly created server is selected.

- **Management Server older than the Client** — If the Management Server is older than the Client application, a version warning is displayed when you attempt to log on. Click **Yes**.
  After you have finished your update, restart the Client application.

- **Client older than the Management Server** — If the Client application is older than the Management Server, a Client Software Update prompt is displayed when you attempt to log on. Click **Yes** to begin installing the Client application update.

> **Note:** The prompt is displayed only if a Client Software Update is available for download from the Management Server.

After you have finished your update, you are returned to the main logon window.

6) In the **User Name** field, type a valid Control Center user name.

7) [Optional] Click **Remember User Name** to preserve the entered user name in the field for subsequent logon attempts.

8) In the **Password** field, type the password that was assigned to this user name by the system administrator.

9) Click **Connect**. The **Certificate validation** message is displayed. The message is similar to the following example:

```
The Management Server's SSL certificate needs to be validated. When contacting the server at
 the address: nn.nn.nnn.nnn, the server presented a certificate with the following information:
 Subject Name: CN=example.example.net Issuer: CN=CommandCenter CA Expiration: (date)
 (time)Thumbprint: (thumbprint)Do you want to allow communication with this server?
```

10) Click **Yes**.

Result

You are now logged on to the Client application, which is connected to the Management Server.

Post-installation tasks

After you have completed the setup tasks, you are ready to begin creating policies, set up users, roles, and other settings.

For details, press **F1** to access Help topics for the tasks indicated in the following table.

Table 10: Post-installation tasks

Task	Location
Check for software updates	**Control Center** > **Control Center Updates**
Set up accounts for other administrators	**Control Center** > **Administrators**
Back up the current configuration	**Control Center** > **Maintenance** > **Backup System**

Task	Location
Add backup (standby) Management Servers	**Control Center** > **High Availability Setup Wizard**

See the *Forcepoint Sidewinder Control Center Product Guide* for information on post-installation tasks.

Tomcat Java settings

Set Tomcat Java heap size for better performance.

1) As a root user run the command:

```
vi /usr/local/tomcat/bin/setenv.sh
```

> **Note:** The value in `setenv.sh` must be in multiples of 128. We recommend that for large configurations, you set this value to 1024 .

2) Look for the `JAVA_OPTS` property, which will be set something like the following. The numbers in bold are variables whose values depend upon the configured RAM size.

```
JAVA_OPTS="-Xms499m -Xmx499m"
```

3) Use the following table to set JAVA_OPTS for better performance and replace it accordingly based on RAM size.

RAM Size	JAVA_OPTS Value to set
1 GB	JAVA_OPTS="-Xms512m -Xmx512m"
2 GB	JAVA_OPTS="-Xms1024m -Xmx1024m"
3 GB	JAVA_OPTS="-Xms1536m -Xmx1536m"
4 GB	JAVA_OPTS="-Xms2048m -Xmx2048m"
6 GB	JAVA_OPTS="-Xms3072m -Xmx3072m"

4) Restart the tomcat by running the following command as a root user.

```
service tomcat restart
```

> **Note:** The Java settings are automatically configured with the correct.memory.sh script during installation.

In the following complex scenarios, the settings might need further tuning and we recommend you to increase JAVA_OPTS by multiples of 128. For example, if you have a complex nested rule deployment with 3500 rules with carried over nested groups and Control Center (2GB Physical RAM and 1024m JAVA_OPTS). Control Center is throwing an Out of Memory or a GCC overhead error. So it is recommended you increase the JAVA_OPTS to 1024m+(128*2=256m)=1280m

- Continuous GCC overhead error
- Out of memory error in the CC logs or catalina logs
- Large number of rules, example beyond 2500
- Lot of nesting in the rules
- Lot of nested groups that might have come in the rules during firewall upgrade from older versions of firewall like 7x to 8x

Perform post-upgrade tasks

Perform the following tasks after the upgrade is complete.

- Re-register all the firewalls that existed prior to an upgrade. Retrieve the firewall dialog information.
- Check for updates to Control Center.
- Upgrade the signature files such as the application database.
- Create a full configuration backup of the Management Server.
- In the Client application, select **Control Center** > **Settings** > **Network** > **General and Static** tab. Copy the network information from 5.3.1 backup to the 5.3.2 system.
- If the Management Server was running in High Availability mode before the upgrade, use the High Availability Setup Wizard to implement the High Availability option mode. After an upgrade, recreate an HA pair and restart HA.
- If you want to create an HA:
  - During upgrade, if you didn't use the same host name and IP address, remove the Control Center CA certificates from 5.3.2. As a root user, run the following command:

    ```
    /usr/local/bin/clear_cacert.sh
    ```

  - Reboot the Management Server
  - Re-register all the firewalls
- Configure the Alert Processing Rule for Disk Usage to send a notification to the administrator if available disk space is low.

Add firewalls to the Control Center

Register firewalls with the Control Center Management Server. Depending on the current status of the firewall, you can register multiple firewalls at once, or each firewall individually.

Add multiple firewalls at one time

You can sign up one or more firewalls by initiating the process from the Control Center Management Server, rather than from the firewall. This process can be initiated only under specific conditions and only for specific firewalls that have been prepared to employ this option.

> **Before you begin**
>
> The firewalls must be configured for rapid deployment.

You can also import a prepared file for multiple firewalls to avoid manually specifying the details that are required to support this option. To use this feature, all the firewalls must have the same password.

Sign up multiple firewalls by using the **Sign Up Firewalls** window.

> **Note:** After you complete this task, you will still have to register each firewall separately as an additional task. To add and register a single firewall in one wizard, use the **Add New Firewall Wizard**.

To add multiple firewalls at one time:

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, right-click the **Firewalls** node and select **Sign Up Firewalls**. The **Sign Up Firewalls** window is displayed.

3) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

4) Click **OK** to start the registration process. View the progress of the firewall enrollment process on the **Deployment Status** page.

Add a single firewall

After the Control Center Management Server has been installed and the firewall-specific, Control Center-enabling configurations have been made, you can begin to add new firewall objects and their associated configuration objects to the Control Center Management Server database.

You can add and register a new firewall to the Control Center by using the **Add New Firewall Wizard**. You can also retrieve the configuration from the firewall.

To use this wizard, the Control Center must be able to have SSH access to the firewall. You must configure this SSH access on the firewall. Use the Forcepoint Sidewinder Admin Console to enable the SSH access control rule on this firewall for external sources and destinations. After you save this change, you can come back to the Control Center Client application and run the **Add New Firewall Wizard**.

Creating firewall objects is a two-part process:

1) All types of firewall objects that represent physical devices in your configuration must be identified by providing basic information.

2) All the firewall-specific configuration information must be created or retrieved for each firewall.

Both of these parts can be performed in the **Add New Firewall Wizard**. You can use the **Add New Firewall Wizard** as described in the following examples:

- You have already added several firewalls by using the **Sign Up Firewalls** window. Now you need to retrieve their configurations. Perform a retrieve for each firewall individually with this wizard.

- If a single firewall is not registered with the Control Center, you can add it, register it to Control Center, and retrieve its configuration—all in one step.

- If a single firewall has already been registered with the Control Center, you can add it and retrieve its configuration.

> **Note:** If a firewall has already been added to and registered with the Control Center Management Server, you can retrieve its configuration by using the **Firewall Retrieval Options** window.

Steps

1) In the navigation bar, select **Policy**.

2) To display the **Add New Firewall Wizard**:

- In the **Policy** tree, double-click the **Firewalls** node.
- Right-click the **Firewalls** node and select **Add Object**.

> **Tip:** For option descriptions, press **F1**.

3) To begin the process of adding the firewall to the list of firewalls in the **Policy** tree, complete the information on the **Firewall Connection Information** page and click **Next**. The **Firewall Registration Information** page is displayed.

4) Select an option to register the firewall with the Control Center Management Server.

To skip the registration process, on the **Firewall Registration Information** page, click **Next**. The **Retrieval of the firewall into Control Center** page is displayed. Skip to Step 7.

To register this firewall with the Control Center Management Server:

a) On the **Firewall Registration Information** page, select the **Register the firewall with this Management Server** checkbox.

b) Click **Next**. The **Summary** page is displayed.

5) On the **Summary** page, verify the information that you have configured. If it is correct, click **Register**; if not, correct any problems. The **Registration Status** page is displayed.

6) On the **Registration Status** page, view the progress of the firewall registration. After it successfully completes, click **Next**.

7) To retrieve items and categories from the firewall into Control Center, on the **Retrieval of the Firewall into Control Center** page, select the items and categories to be retrieved and click **Finish**. These objects are retrieved and the firewall is displayed in the list of firewalls in the **Policy** tree.

Add an HA cluster

You can register a standalone firewall or a High Availability cluster that already has a configured policy.

Steps

1) In the navigation bar, select **Policy**.

2) In the **Policy** tree, right-click the **Clusters** node and select **Add Object**. The **Add New Cluster Wizard** window is displayed.

3) Configure the fields on this window as needed.

> **Tip:** For option descriptions, press **F1**.

4) Click **OK** to start the registration process. View the progress of the firewall enrollment process on the **Deployment Status** page.

Navigate the Control Center Client application

Log in to Control Center and accomplish various tasks with the Control Center Client application.

Navigate the Control Center user interface

The Control Center Client application is designed to provide a centralized location from which you can perform all the tasks that you need to manage your security policy and firewalls in your distributed network environment.

Working with Management Servers

This section explains how to log on to, add, or delete Management Servers.

Log on to the Management Server

Launch the Client application and log on to the Control Center Management Server.

Steps

1) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

2) Specify a valid Control Center user name in the **User Name** field. After the initial installation of the Management Server, the default user name is the Control Center administrator user name specified in the ccinit.txt file.

3) [Optional] Select the **Remember User Name** checkbox to preserve the specified user name in the field or the default user value that is specified in the ccinit.txt file.

4) Specify the corresponding password in the **Password** field.

5) Select a Management Server connection from the **Server** list or select **<Add New Server>** to add a new Management Server connection.

6) Click **Connect**. A certificate validation message is displayed.

7) Click **Yes**.

Result

You are now logged on to the Management Server.

> 📝 **Note:** If you attempt to log on to a Management Server using a Client application version earlier than the Management Server version, you will be prompted to update the Client application before proceeding.

Add a backup (standby) Management Server

Configure a secondary, or backup, Control Center Management Server.

Steps

1) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

2) Specify the user name and password in their respective fields.

3) In the **Server** field, make sure that **<Add New Server>** is displayed and click **Browse**. The **Add New Server** window is displayed.

4) Configure the fields in this window, specifying whether you are adding a primary or a backup (standby) server and then specifying the related field information.

5) Click **OK**. The **Certificate Problem** message is displayed because the Management Server imports a non-Certificate Authority (CA) certificate before it imports the CA certificate. Click **Yes**. Another message is displayed. Click **Yes**. The logon window is displayed.

6) In the **Server** list, select the server to log on to. Then specify the user name and password for that server and click **Connect**.

Remove Management Servers

Use this procedure to delete a Control Center Management Server from the list of Management Servers.

Steps

1) Select **Start** > **All Programs** > **Forcepoint** > **Sidewinder Control Center v5** > **<version>** > **Sidewinder Control Center**.

2) Specify the user name and password in their respective fields.

3) In the **Server** field, select the server to be removed and click **Browse**. The **Add New Server** window is displayed.

4) Click **Remove**.

Result

The Management Server is removed from the list of available Management Servers.

User interface overview

The Control Center Client application interfaces consists of links, icons, buttons, tabs, trees, and displayed information, such as server information and the users who are logged on to this configuration domain of this Management Server. (If no configuration domains are implemented, everyone is logged on to the default domain.)

The Control Center Client application is displayed after you have successfully logged on to the Control Center Client.

The following figure shows the different areas that make up the Control Center Client application.

Figure 3: Example of the Control Center Client main window
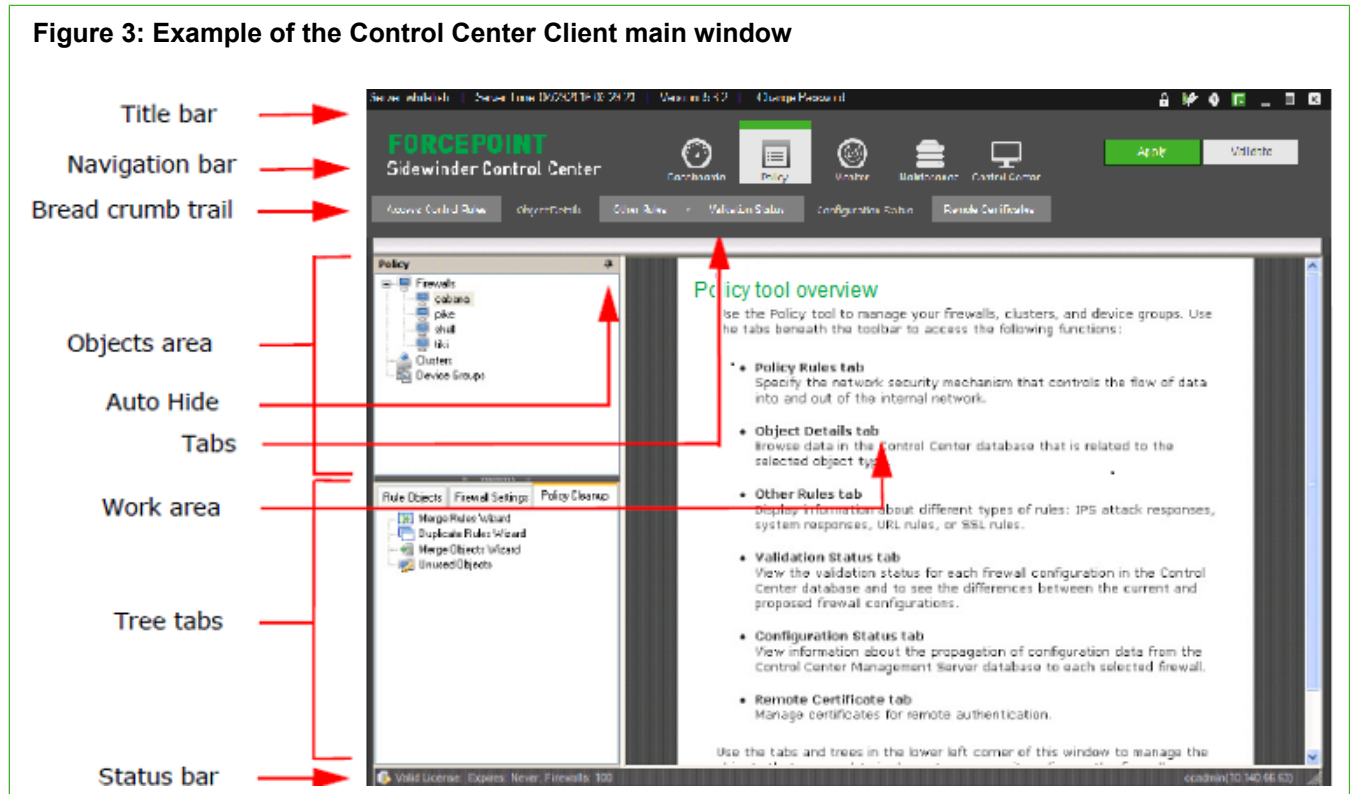
Title bar

The title bar is located across the top of the main window.

Server-related information

The information in this left portion of the title bar provides information about the Management Server and also a link for changing the password that you use to access this server.

Table 11: Server-related information

Option	Definition
Server	Displays the name of the Management Server to which you are logged on.
Server Time	Displays the current date and time of the Management Server to which you are logged on.
Version	Displays the current version of the Management Server to which you are logged on. This value is the same as the value of the Management Server Version field on the **About Forcepoint Sidewinder Control Center** window.
FIPS 140-2 processing enabled	Appears if FIPS 140-2 cryptography processing is enabled on the Control Center.

Option	Definition
Change Password	Displays the **Change User Password** window, where you can change your user password. This window is available only if your user profile has been configured to use internal authentication to access the Control Center.
	If you have administrator privileges and you want to change the password of a different user, use the **Control Center Administrator** window.

Title bar icons

There are several functions are provided by the icons located to the right in the title bar.

- **Locking objects to protect single user updates** — Protect selected objects from being simultaneously updated by multiple users by clicking **Locking Manager** on the title bar. The **Locking Manager** window is displayed, where you can select one or more objects to lock for this active session.
- **Starting and stopping a ticket to track changes** — Start a ticket to begin capturing audit data from a specific point in time. This data will be identified on the **Firewall Audit** page by the ticket number that you have assigned to this ticket. After you have started a ticket, you can stop it at any time. Perform this function by clicking (**Start ticket**) or (**Stop ticket**).
- **Accessing online Help** — Access the main Help page from anywhere in the Client by clicking **Help**. You can access window- or page-specific online Help by pressing **F1**.
- **Accessing Control Center version information** — Access information about the Control Center, such as Client, Management Server, and database versions and copyright information by clicking **About**.

Navigation bar

Several icons are located in the navigation bar area of the main window.

- Dashboards
- Policy
- Monitor
- Maintenance
- Control Center

The information that is displayed in the tab area, bread crumb area, objects area, and work area is specific to the icon that is currently selected.

Additionally, there are two buttons in the navigation bar area:

Table 12: Navigation bar area buttons

Option	Definition
Apply	Applies configuration changes to one or more firewalls. You can also apply changes for a specific firewall by right-clicking it in the **Policy** tree and selecting **Apply Configuration**.
Validate	Validates configuration changes to one or more firewalls. You can also validate changes for a specific firewall by right-clicking it in the **Policy** tree and selecting **Validate Configuration**.

Tabs

Each icon has its own set of tabs that provide access to additional functions. When selected, a tab either displays the related page in the work area or it displays a menu from which you can select additional pages.

For more information about the tabs and their menus, see the section for each icon.

In addition to these icon-specific tabs on the left part of this area, when configuration domains have been activated, the following fields and buttons are displayed, regardless of the icon that is currently selected:

Table 13: Additional fields and buttons

Option	Definition
Domain	Displays the list of configuration domains. You can change to a different domain, provided that you have access to it, by selecting it in this list. The displayed domain is the domain to which you are logged on.
Manage versions	Displays the **Manage Configuration Domain Versions** window, where you can create, modify and activate versions of a configuration domain.

Bread crumb trail

Whenever a tab is clicked or a menu option from a tab is selected, the title of the page is displayed in the bread crumb trail.

If the page that is displayed is the result of a menu selection, the entire bread crumb is displayed in the bread crumb trail. For example, on the **Monitor** icon, if you click **Reports** and then select **Policy Report**, the bread crumb trail displays **Reports** > **Policy Report**.

Object area

The object area can differ from icon to icon, depending on whether the icon has any object trees or tabs.

Trees

Some of the icons provide the ability to configure objects that are found in a tree view that is located in the object area.

The most complex icon is the **Policy** icon, with its firewall tree at the top of the object area and a set of tabs, each with its own tree at the bottom of the object area. The **Monitor** icon currently does not have an object area.

Auto Hide button

For every icon that has an objects area, there is also the **Auto Hide** button. Use this button to manage the display (or hiding) of the **Objects** area to increase the size of the work area in the main window.

To hide the objects area, click the **Auto Hide** button. To bring back the display of the objects area, click the object area name on the left to display the object area. Then click the **Auto Hide** button to lock it into its original position.

Tree tabs

Because there are many configuration objects that can be configured on the **Policy** icon, the bottom of the objects area is broken out into tabs, each with its own tree of objects to be configured.

Work area

This portion of the user interface is where the data that is associated with the pages is displayed when the associated tab for the page is selected.

Status bar

The status bar at the bottom of the main window displays information about users.

Table 14: Status bar information

Option	Definition
Users	Displays the name and the IP address of each user who is currently logged on to the current domain of the Management Server. This information is in the right corner of the status bar.

Additional navigational aids

There are additional functions that are provided in the Control Center Client to help you configure and manage the security policy for your firewalls.

- **Right-click menus** — Right-click menus are available for the objects that appear in the trees in the Objects area. You can also use the right-click menu in some of the pages that are displayed in the work area, such as the Access Control Rules page. Many of these menu options are also accessible through another way on the page, such as a tool on the toolbar for the page.

- **Edit status column** — Many tables that are displayed on windows and pages include the first column, which is an Edit column that identifies the edit status of a row in a table. The following icons can be displayed in this column:

  - **[blank]** — Indicates an existing line with associated values that is not the currently selected line.

  - **Edit** — Indicates that this row is the one that is being edited.

  - **New** — Indicates that you are creating a new row or entry.

  - **Current** — Indicates that this row is currently selected and it contains previously specified values.

Search for objects in the Control Center Client application

You can search for configurable objects within a larger list of objects by specifying certain criteria in the **Search** window.

Often, the name that is associated with an object is not enough information to identify the object that you need to find. By using the **Search** window, you can specify any character or string of characters to search through all the presented data columns to locate the item that you seek.

Steps

1) From various lists in windows and pages, click **Search**. The **Search** window is displayed.

> **Tip:** For option definitions. press **F1**.

2) Enter a search term, then click **Filter**. Items in the list that contain the search term are displayed in a drop-down list.

3) Select the item you were looking for.

Result

The item is selected (checkbox filled with a check mark) in the list.

Client application icons

Icons are provided for common tasks.

Most icons have tooltips that appear when you hover your mouse over them.

Table 15: Client application icons

Icon	Description
Common icons	
	Apply
	Delete
	Edit
	Help
	Line Selection
	Locking Manager
	Refresh
	Version Warning
	Warning
	Validate
Search icons	
	Clear Search

Icon	Description
🔍	Search
Status icons	
🔴	Status: Not Running
🟢	Status: Running
🟡	Status: Uncertain
🔮	Unknown Status
Policy Tree icons	
🖥	Firewalls
⬙	Crossbeam firewall
👤	Clusters
🗐	Device Groups
Rule Object icons	
👤	Users
👥	User Groups
🌐	External Groups
📇	McAfee® Logon Collector Users
📇	McAfee Logon Collector Groups
📇	McAfee Logon Collector Distribution Lists
Rule icons	
⊞	Add Rule
📝	Edit Rule
❌	Delete Rule
❌	Delete Rules
↪	Move to Position

Icon	Description
	Move Down
	Move Up
	Search and Replace
	Export Rule
	Rule
	Rule Group
Alerts icons	
	Alarm Sound Mapping
	Acknowledge
	Alert jump
	Alert options
	Annotate
	Clear
	Critical
	High
	Medium
	Low
	Warning
	Export to CSV
	Secure Alert Server status
	View events
	Add
	Administrators
Update icons	

Icon	Description
	Update Settings
	Schedule Firewalls
	Manual Download
Control Center Tree icons	
	Administrators
	Roles
	LDAP User Groups
	Auto-Hide
	Browse
	Clear Filter
	Clear Pending Changes
	Collapse All
	Expand All
	Manage Configuration Domain
	Move Down
	Move Left
	Move Right
	Move to Top
	Move Up
	Save Pending Changes
	Service Not Running
	Service Running
	Service Running Error

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.

Index