



Configuring the Smart Install Network

- [Configuring the Director and DHCP Server](#)
- [Configuring the TFTP Server](#)
- [Installing and Using the GUI](#)
- [Switch Image and Configuration Upgrades](#)
- [CLI Configuration Mode in the Smart Install Server](#)

Configuring the Director and DHCP Server

- [DHCP and Smart Install](#)
- [Configuring the DHCP Server](#)
- [Using Static IP Addresses](#)
- [Configuring the Smart Install Director](#)

The director manages the switches in the network. For each group of switches, a director configuration file specifies the image list file and the Cisco Edge configuration file.

The director manages these Cisco Edge configuration files:

- Startup configuration—The configuration that a client switch uses when it starts.
- Backup configuration—An exact copy of a client switch startup configuration stored in the director.
- Seed configuration—A configuration on the director that is the basis for the client switch startup configuration. If the startup and backup configuration cannot be located, the director supplies the seed configuration to the client switch.

For information about managing and creating Cisco Edge configuration files, see the [“Managing Cisco Edge Configuration Files”](#) section on [page 2-25](#).

DHCP and Smart Install



Note

If your Smart Install network does not use DHCP, see the [“Using Static IP Addresses”](#) section on [page 2-5](#).

**Note**

This section explains some of the basic tasks for configuring the director and DHCP server in a Smart Install network. For extensive information about Smart Install and the Smart Install director, see the [Smart Install Configuration Guide, Release 12.2\(58\)SE](#).

A typical Smart Install network uses the DHCP protocol and a DHCP server. In a DHCP network, DHCP snooping is automatically enabled on the director. The director snoops DHCP offers and requests to and from the client switches and uses DHCP snooping to insert the DHCP options used in the Smart Install operation.

A DHCP server in a Smart Install network can be positioned in one of these ways:

- The Smart Install director can act as the DHCP server in the network. When the DHCP offer goes to the client switches, the director allocates the IP addresses and assigns configurations, images, and the hostname as DHCP options in the offer and the acknowledgement. DHCP snooping is enabled by default.
- The DHCP server can be another device (third-party server) in the Smart Install network. In this case, DHCP packets between the clients and the DHCP server pass through the director.

**Note**

You can configure a join-window time period so that the director can modify the DHCP offer and send the image and configuration files to the client only during the window. The join window restricts Smart Install for a specified period of time and acts as a security precaution to control when a client can receive these files. See the “Using a Join Window” section in the [Smart Install Configuration Guide, Release 12.2\(58\)SE](#).

- A third-party server and the director DHCP server can coexist in a network. In this case, the director is responsible only for the DHCP requests of the switches in the Smart Install network. The director maintains the Smart Install database and pool. The third-party server maintains the other DHCP database functions.

Configuring the DHCP Server

The DHCP server can be the director, another Cisco device running Cisco IOS, or a third-party server. You can also have the director act as the Smart Install DHCP server and have another device perform all other DHCP server functions.

Either way, use one of these procedures to set up a Cisco device as DHCP server. If you choose to configure a third-party device as DHCP server, follow the instructions in the product documentation for configuring a network address and a TFTP server.

- [Configuring the Director as the DHCP Server, page 2-3](#)
- [Configuring Another Device as the DHCP Server, page 2-4](#)

DHCP Server Configuration Guidelines

- If the director (or another device running Cisco IOS) is the DHCP server and the network reloads, the server could assign new IP addresses to the switches, which then might no longer be reachable. If the director IP address changes, it is no longer the Smart Install director. To prevent this occurrence, you should enable *DHCP remembering* by entering the **ip dhcp remember** global configuration command or the **remember** DHCP-pool configuration command on the DHCP server.

- If you use an external device as the DHCP server, you can configure the DHCP server to send option 125/suboption 16 for the director IP address to avoid the possibility of fake DHCP servers.
- A third-party DHCP servers require an IP-address-to-MAC-address binding to ensure that the same IP address is given to a switch on a reload.

Configuring the Director as the DHCP Server

You can configure the director as the DHCP server and create DHCP server pools directly from the Smart Install director.

Beginning in privileged EXEC mode, follow these steps on the director to configure it as the DHCP server:

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	vstack director <i>ip_address</i>	Configures the device as the Smart Install director by entering the IP address of an interface on the device.
Step 3	vstack basic	Enables the device as the Smart Install director.
Step 4	vstack dhcp-localserver <i>poolname</i>	Creates a name for the Smart Install DHCP server address pool, and enters vstack DHCP pool configuration mode.
Step 5	address-pool <i>network-number mask prefix-length</i>	Specifies the subnet network number and mask of the DHCP address pool. Note The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 6	default-router <i>ip_address</i>	Specifies the IP address of the DHCP default router for the pool. Note We recommend that the default router address for DHCP be on VLAN 1. Newly installed devices search VLAN 1 for DHCP and TFTP.
Step 7	file-server <i>address</i>	Specifies the IP address of the TFTP server. Note If the director is also the TFTP server, you must enable it. See the “Configuring the TFTP Server” section on page 2-7.
Step 8	exit	Returns to global configuration mode.
Step 9	ip dhcp remember	(Optional) Configures the DHCP server to remember the IP bindings of a device. If the network or device reloads, the DHCP server issues the same IP address to a client that it had before the reload.
Step 10	end	Returns to privileged EXEC mode.
Step 11	copy running-config startup config	(Optional) Saves your entries in the configuration file.
Step 12	show dhcp server	Verifies the configuration by displaying the DHCP servers recognized by the device.

This example shows how to configure the Smart Install director as the DHCP server:

```

Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# vstack dhcp-localserver pool1
Director(config-vstack-dhcp)# address-pool 1.1.1.0 255.255.255.0
Director(config-vstack-dhcp)# default-router 1.1.1.30
Director(config-vstack-dhcp)# file-server 1.1.1.40
Director(config-vstack-dhcp)# exit
Director(config)# ip dhcp remember
Director(config)# end

```

DHCP snooping is enabled by default on the director.

Configuring Another Device as the DHCP Server

If the Smart Install director is not the DHCP server, you can use the Cisco IOS DHCP commands to configure a server pool outside the Smart Install network. The director must have connectivity to the DHCP server. For procedures to configure other DHCP server options, see the “Configuring DHCP” section of the “IP Addressing Services” section of the *Cisco IOS IP Configuration Guide, Release 12.2* or the “IP Addressing Services” section of the *Cisco IOS IP Configuration Guide, Release 15.1* on Cisco.com.

Beginning in privileged EXEC mode, follow these steps:

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	ip dhcp pool <i>poolname</i>	Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.
Step 3	bootfile <i>filename</i>	Specifies the name of the configuration file to be used.
Step 4	network <i>network-number mask prefix-length</i>	Specifies the subnet network number and mask of the DHCP address pool. Note The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).
Step 5	option 150 <i>address</i>	Specifies the IP address of the TFTP server.

	Command	Purpose
Step 6	remember	(Optional) Configures the DHCP pool to remember the IP bindings of a device. If the network or device reloads, the DHCP server issues the same IP address to the device that it had before the reload.
Step 7	end	Returns to privileged EXEC mode.

This example shows how to configure another device as a DHCP server:

```
Switch # configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# network 10.10.10.0 255.255.255.0
Switch(dhcp-config)# bootfile config-boot.text
Switch(dhcp-config)# option 150 10.10.10.1
Switch(dhcp-config)# remember
Switch(config-if)# end
```

When the director is a Layer 3 switch, DHCP snooping is enabled by default. When there is a relay agent between the DHCP server and the director, you must enable DHCP snooping on the relay agent.

To enable DHCP snooping on a Cisco DHCP relay device, enter these global configuration commands:

ip dhcp snooping

ip dhcp snooping vlan 1

ip dhcp snooping vlan *vlan-id* for any other configured Smart Install VLANs

no ip dhcp snooping information option (if the DHCP server is running Cisco IOS)

You must also enter the **ip dhcp snooping trust** interface configuration command on the director interface that is connected to the server.

If the director and the DHCP server are on different VLANs, you must enable IP routing on the VLAN interface connected to the client switches, and enter this command:

ip helper *address* (IP address of the DHCP server)

Using Static IP Addresses

In a Smart Install network that uses static IP addresses, you need to configure the IP address on the client switches from the local desktop GUI.

Step 1 From the local desktop, double-click the Wired Network icon on the status bar.



Note If the Wired Network icon is not on the status bar, click the **Home** button and go to Settings > Wired Network.

Step 2 In the Wired Network window, click the **Net Configuration** button.

Step 3 In the User Authentication window, enter the root user name and password.

- Step 4** In the Network Configuration window, choose **Manual (Static)** from the Net Type drop-down list.
- Step 5** Enter the IP address (required), netmask (required), gateway (optional), DNS server, and IBD director (optional) IP address.



Note If you do not configure a gateway, enter the following Linux command to add a host route to the IBD and network file system (NFS) server:

```
# route add -net ip_address netmask subnet_mask gw gateway_ip_address
```

- Step 6** Click **OK**.

Configuring the Smart Install Director

The director in a Smart Install network must be a Layer 3 switch running Cisco IOS release 12.2(58)SE or later or a router running Cisco IOS Release 15.1(3)T or later.

To configure a device as director, enter the IP address of one of its Layer 3 interfaces in the **vstack director ip_address** global configuration command, and enable it as director by entering the **vstack basic** command.



Note If you entered the **no vstack** global configuration command to disable Smart Install on a device, the **vstack director ip_address** and **vstack basic** global configuration commands are not supported on the device. To reenable Smart Install on a device, enter the **vstack** global configuration command.

When a device is configured as director, DHCP snooping is automatically enabled by default on VLAN 1, and the director builds the director database.

The database lists the client devices in the Smart Install network and includes this information for each switch:

- Product identifier (PID)
- MAC address
- IP address
- Hostname
- Network topology including neighbors interfacing with the switch
- Serial number



Note When the director is a switch, DHCP snooping is enabled by default on VLAN 1. It is also enabled on any other Smart Install management VLANs configured by entering the **vstack vlan vlan-range** global configuration command. We recommend using the VLAN 1 interface as the director IP address because newly installed clients use VLAN 1 to broadcast DHCP requests.

In a Smart Install network that uses DHCP to assign IP addresses, you only need to configure the director. Client switches do not require any configuration.

There can be only one director for a set of clients, and you cannot configure a backup director. If the director fails:

- The director database must be rebuilt.
- Any upgrade being performed for a non-Smart Install-capable switch might fail.
- The accumulated download status is lost.
- A configuration backup might not occur before the director restarts.

The director can change status and become a client switch if:

- The director interface that has the director IP address shuts down.
- The director interface that has the director IP address is deleted.
- The director IP address is changed.

If the director becomes a client, DHCP snooping is disabled, and the director database is no longer used.

If the director IP address is provided by DHCP and you configure a different director IP address on a client switch, the client is longer part of the Smart Install network of the director.

Smart Install relies on a TFTP server to store image and configuration files. The TFTP server can be an external device, or the director can act as a TFTP server. If the director is the TFTP server, the available flash file space on the director must be able to accommodate the client Cisco IOS image and configuration files. See the [“Configuring the TFTP Server” section on page 2-7](#).

In a Smart Install network using DHCP, the DHCP server can be an external device, or the director can act as the DHCP server. See the [“DHCP Server Configuration Guidelines” section on page 2-2](#). The director snoops all DHCP packets that pass through it on VLAN 1 and on any other VLANs configured as Smart Install management VLANs. All network DHCP packets from intermediate or client switches or from an external DHCP server must pass through the director, which must be able to snoop all DHCP packets from clients.

**Note**

Smart Install options in the DCHP offer are option 125, suboption 5 (the image list file), option 125 suboption 16 (the director IP address), and option 67 (the configuration file).

The director builds a topology director database for the network by collecting information from the network Smart Install switches. The director uses the database:

- To assign a configuration file and image to a client.
- As a reference to obtain the PID, the image name, and the configuration file for an on-demand upgrade of network switches.

The director periodically updates the director database based on CDP updates from neighbor switches and from Smart Install messages sent to the director by Smart Install-capable clients. The updates contain information about the client neighbors.

Configuring the TFTP Server

Smart Install stores image and configuration files on the TFTP server.

If you use an external device as the TFTP server, the image list and configuration files are stored at these locations on the TFTP server:

Files	Location on the TFTP Server
Image list file	/opt/Tftpboot/imglist
Edge configuration file	/opt/Tftpboot/sb_conf
Group association file	/opt/Tftpboot/

If you use an external device as the TFTP server, the files that are part of the image list file are stored at these locations on the TFTP server:

Files	Location on the TFTP Server
Factory mode operating system	/opt/Tftpboot/images/FM_OS
Operating system file (includes the root file system image and bootable Linux kernel image)	/opt/Tftpboot/images/OS
Cisco application files	/opt/Tftpboot/images/CiscoApp
Third-party application files	/opt/Tftpboot/images/Partner
Fonts applications	/opt/Tftpboot/images/Fonts

The director can function as the server, eliminating the need for an external TFTP-serving device. If the director is the TFTP server, image and configuration files are stored in the director flash memory. If the director does not have available memory storage space, you can store the files on a third-party server and point to that location.

If the TFTP server is a third-party device, disable the server option to change the name of a file if another file is created with the same name. Otherwise, duplicate image list files might be created.

When you specify **flash:** as the location from which to retrieve the files, the director automatically gets the required image and configuration files and acts as the TFTP server.

Selection Guidelines

Guidelines when selecting the director to be the TFTP server:

- The total flash memory space (used and free) on the director must be large enough to contain the director image and configuration file and the image and configuration files required for client switches.
- There must be enough available flash memory on the director to hold the client Cisco IOS images and configuration files. The Cisco IOS image files vary in size, depending on the PIDs and size of the images.
- A copy of each client configuration file is stored in the root directory of the flash file system on the director. There must be enough space for each planned client.
- Most director devices have enough flash memory to hold one client Cisco IOS image and a small number of client configuration files. For example, a Catalyst 3750 switch can have a maximum flash size of 64 MB, which accommodates only four or five images, based on the image size.
- If the director is a switch and the Smart Install network includes client switches with more than one product ID, you should use an external TFTP server.

Installing and Using the GUI

- [Using the GUI](#)
- [Setting Up the GUI on the CentOS/Fedora Server](#)
- [Accessing the GUI](#)
- [Managing Switch Groups](#)
- [Managing Cisco Edge Configuration Files](#)

Using the GUI

You can configure and deploy the Cisco Edge 300 series switch in different switch groups for different audiences. For example, a primary school can offer one set of applications for first graders and another set of applications for second graders. You would use the GUI to create two switch groups, associate the switches for the first graders with one switch group and the switches for the second graders with the other switch group, and then generate and push a different switch client configuration file to each switch group.

You use the GUI to configure and manage the Cisco Edge 300 series switches in the Smart Install network. You can

- Create switch groups (see the [“Creating Switch Groups” section on page 2-17](#)).
- Add individual switches to the GUI or import lists of switches into the GUI (see the [“Managing the Edge Switch List” section on page 2-18](#)).
- Add switches to switch groups by creating a Smart Install group-device association file based on one or more of these components:
 - MAC address
 - Product identifier (PID)
 - Location

For more information, see the [“Adding Members to a Switch Group” section on page 2-20](#).

- Create a Cisco Edge configuration file (see the [“Managing Cisco Edge Configuration Files” section on page 2-25](#)).

Setting Up the GUI on the CentOS/Fedora Server

**Note**

Setting up the GUI requires familiarity with Linux distribution and Linux shell commands.

**Note**

The Internet must remain connected during the GUI installation.

Before you set up the GUI, download and install the following software:

- Internet Explorer version 9.0 or Firefox Mozilla 8.0.1 or later
- CentOS 6.2/Fedora 14, 15, and 16

- **Yum Package Manager**—This software should be part of the Fedora preinstalled software package. If you do not install a Yum package manager during the Fedora installation, you can download it from <http://yum.baseurl.org/>.



Note Make sure that the Yum repositories can be reachable. For example, if you are using Fedora 14, the default repositories of your system are deprecated.

Updating the Yum Repositories

If the default repositories of your system are deprecated, you need to update them manually.



Note If you are using CentOS, see <http://wiki.centos.org/AdditionalResources/Repositories> for the repositories information.

Before installing the GUI, use the following steps to update the Yum repositories on Fedora:

Step 1

Update `/etc/yum.repos.d/fedora.repo`

```
[fedora]
name=Fedora $releasever - $basearch
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everything/$basearch/os/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/$releasever/Everything/$basearch/os/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=fedora-$releasever&arch=$basearch
enabled=1
metadata_expire=7d
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[fedora-debuginfo]
name=Fedora $releasever - $basearch - Debug
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everything/$basearch/debug/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/$releasever/Everything/$basearch/debug/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=fedora-debug-$releasever&arch=$basearch
enabled=0
metadata_expire=7d
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[fedora-source]
name=Fedora $releasever - Source
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/releases/$releasever/Everything/source/SRPMS/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/releases/$releasever/Everything/$basearch/SRPMS/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=fedora-source-$releasever&arch=$basearch
enabled=0
metadata_expire=7d
```

```
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch
```

Step 2 Update /etc/yum.repos.d/fedora-updates.repo

```
[updates]
name=Fedora $releasever - $basearch - Updates
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/$releasever/$basearch/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/$releasever/$basearch/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-released-f$releasever&arch=$basearch
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[updates-debuginfo]
name=Fedora $releasever - $basearch - Updates - Debug
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/$releasever/$basearch/debug/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/$releasever/$basearch/debug/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-released-debug-f$releasever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[updates-source]
name=Fedora $releasever - Updates Source
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/$releasever/SRPMS/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/$releasever/SRPMS/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-released-source-f$releasever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch
```

Step 3 Update /etc/yum.repos.d/fedora-updates-testing.repo

```
[updates-testing]
name=Fedora $releasever - $basearch - Test Updates
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/testing/$releasever/$basearch/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/testing/$releasever/$basearch/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-testing-f$releasever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[updates-testing-debuginfo]
name=Fedora $releasever - $basearch - Test Updates Debug
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/testing/$releasever/$basearch/debug/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/testing/$releasever/$basearch/debug/
```

```
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-testing-debug-f$releasever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch

[updates-testing-source]
name=Fedora $releasever - Test Updates Source
failovermethod=priority
#baseurl=http://download.fedoraproject.org/pub/fedora/linux/updates/testing/$releasever/SRPMS/
baseurl=http://archives.fedoraproject.org/pub/archive/fedora/linux/updates/testing/$releasever/SRPMS/
#mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=updates-testing-source-f$releasever&arch=$basearch
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch
```

Step 4 Execute the **yum makecache** command in the terminal as root.

Installing the GUI, Associated Software Components, and Images

To install the GUI, associated software components, and images on the TFTP server, run the `installUI.sh` Linux shell script that is part of the `SMI_GUI_release_v1.3.tar.gz` release package or a later release package.

To run the Linux shell script to install the GUI, follow these steps:

-
- Step 1** Download the latest release of the Cisco Edge 300 series Operation System from the official website. The file name of the package is `edge300k9-1.3.0.tar`.
 - Step 2** Copy the package to the server that you want to set up the GUI on.
 - Step 3** Switch to the super user (root) by entering the **su** Linux command and enter your root password.
 - Step 4** Change the directory to the one that contains the release package, `edge300k9-1.3.0.tar`.
 - Step 5** Extract the package by entering **tar xvf edge300k9-1.3.0.tar** and obtain `SMI_UI_release-1.3.tar.gz`.
 - Step 6** Extract the `SMI_UI_release-1.3.tar.gz` by entering **tar zxvf SMI_UI_release-1.3.tar.gz**.
 - Step 7** Change your directory to `SMI_GUI` by entering the **cd SMI_GUI** Linux command.
 - Step 8** Make sure that the system is connected to the Internet. Run `./installUI.sh`. The GUI is installed in the `/var/www/html/smartinstall` directory on the server.
 - Step 9** When you see “Do you want to reboot the system now to finish the installation”, press **Enter** to reboot the system.
 - Step 10** Verify that you can open the GUI by opening a browser (make sure that Javascript is enabled) and then entering `https://ip-address/smartinstall`, in which *ip-address* is the IP address of the server.
-

After you run the `installUI.sh` script, the TFTP and HTTP server packages are automatically added from the Internet. You then can move the images that have a suffix of `delivery.tar.gz` in `edge300k9-1.3.0.tar` to the TFTP server by the following commands:

```
mv os-sunbird-1.3-delivery.tar.gz /opt/Tftpboot/image/OS/
mv fm-os-sunbird-1.3-delivery.tar.gz /opt/Tftpboot/image/FM_OS
```

```
mv fonts-sunbird-1.3-delivery.tar.gz /opt/Tftproot/image/Fonts
mv 3rd-app-sunbird-1.3-delivery.tar.gz /opt/Tftproot/image/Partner
```

**Note**

Director configuration files that you create with the GUI are saved in the /opt/Tftproot directory.

Accessing the GUI

You can access the GUI through Microsoft Internet Explorer or Mozilla Firefox. Make sure that JavaScript is enabled on the browser.

To access the GUI, follow these steps:

- Step 1** Open a browser, and enter the **https://ip-address/smartinstall** URL, in which *ip-address* is the IP address of the GUI server.
- Step 2** Enter your user name and password.
The default user name and password are **cisco**. For security, you should change the user name and password (see the [“Changing GUI Login Credentials”](#) section on page 2-13).
- Step 3** Click **OK**. The Home screen opens. The Home screen provides an introduction to the GUI.
- Step 4** (Optional) In the upper right of the screen, from the drop-down list, select a language.

**Note**

The GUI server must support the Chinese character set if the selected language is Simplified Chinese or traditional Chinese.

Changing GUI Login Credentials

To change your GUI login credentials, follow these steps:

- Step 1** On the menu, click **Admin Information**. The Change Admin Info screen opens.
The Original User Name field shows your existing user name.
- Step 2** In the Original Password field, enter your existing password.
- Step 3** In the New User Name field, enter a new user name.
- Step 4** In the New Password and the Confirm New Password fields, enter a new password.
The new password should follow these rules:
 - The password should contain characters from at least three of the following classes: a-z, A-Z, 0-9, and !@#\$%^&*().
 - No character in the password should be repeated more than three times consecutively.
 - The password should not be 'cisco', or any variant obtained by changing the capitalization of letters, or by substituting 1, l or ! for i, or substituting 0 for o, or substituting \$ for s.
- Step 5** Click **Submit**.

**Note**

If you forget your password, you can reset both the user name and password to *cisco* by running the `reset.sh` file in the Smart Install root directory.

Managing Image Servers (Optional)

- [Creating Image Servers](#)
- [Importing a List of Image Servers](#)
- [Cloning, Modifying, and Deleting Image Servers](#)
- [Using the Search Function to Clone, Modify, and Delete Image Servers](#)
- [Distributing Groups to Image Servers](#)

The images and configuration files for Cisco Edge switches are stored on an image server. By default, the image server is the same server that is running the GUI, but it can also be running on a separate server.

Cisco Edge images (OS, FM_OS, CiscoApp, PARTNER, and FONTS images), image list files, director configuration file, and Cisco Edge configuration files are stored on distributed image servers in each site.

To add image servers to the GUI, take one of the following actions:

- Manually add image servers to the GUI Image Server List screen.
- Import a list of image servers into the GUI Image Server List screen.
- In the GUI, clone an existing image server, and edit the image server.

Creating Image Servers

To run a separate image server, you should add this server to the GUI. To add a separate image server, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | On the menu, choose Manage > Manage Image Servers . The Manage Image Servers screen opens. |
| Step 2 | Click Add an Image Server above the table. The Add an Image Server screen opens. |
| Step 3 | In the Server Name field, enter the name of the image server that you want to add. The server name should be unique and less than 30 characters. |
| Step 4 | In the IP Address field, enter a valid IPv4 or IPv6 address of the image server. |
| Step 5 | In the Username and Password fields, enter the samba account information for the image server. |
| Step 6 | Click the Add button. The Image Server List screen opens, and the image server is added to the Image Server List table. The Image Server List table also shows a row ID for the image server and the date that the image server was created. |
-

The far-right column of the Image Server List table provides these links to manage the image server:

- **Edit**—Opens the Edit Image Server screen. This screen contains the same fields as the Add an Image Server screen. You use it to make any changes to the image server except for the server name, which is used to identify the image server. For more information, see the [“Cloning, Modifying, and Deleting Image Servers”](#) section on page 2-15.

- **Clone**—Adds an image server in fast mode if there is any existing image server added to the GUI. For more information, see the “[Cloning, Modifying, and Deleting Image Servers](#)” section on page 2-15.
- **Del**—Deletes an image server.
- **Members**—Opens a screen that you use to distribute groups to image servers. For more information, see the “[Distributing Groups to Image Servers](#)” section on page 2-16.

Importing a List of Image Servers

You can import a Microsoft Excel spreadsheet with image server information into the GUI. Follow these spreadsheet requirements:

- The spreadsheet can have any name but must be saved with a .csv extension and cannot exceed 2 MB.
- The first row of the spreadsheet must be the title row and cannot include any image server information. The image server information can start on the second row.
- The title row must consist of these titles: image server name, IP address of the server, username, and password.

To import a spreadsheet into the GUI, follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Image Servers**. The Manage Image Servers screen opens.
- Step 2** To the right of the Upload a spreadsheet field, click the icon with the black arrow.
- Step 3** Navigate to a spreadsheet file, and follow the browser instructions to place the file directory and name into the Upload a spreadsheet field.
- Step 4** Click **Upload** to upload the information into the table on the Image Server List screen.



Note

If the spreadsheet contains an IP address that is not in the required format or is a duplicate of a IP address that exists in the table on the Image Server List screen, the GUI rejects this record with an error message.

Cloning, Modifying, and Deleting Image Servers

To clone, modify, or delete image servers from the GUI, follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Image Servers**. The Manage Image Servers screen opens. The Action column of the Manage Image Servers table provides the links for editing, cloning, or deleting image servers from the GUI.
- Step 2** Take one of these actions:
- To edit an image server, click the corresponding **Edit** link in the Action column. The Edit Image Server screen opens. You can change the IP Address, Username, and Password fields. When you are done, click **Update**.
 - To clone an image server row, click the corresponding **Clone** link in the Action column. The Add an Image Server screen opens. You must modify the Server name and IP Address fields. As an option, you can modify the Username and Password fields. When you are done, click **Add**.

- To delete an image server from the GUI, click the corresponding **Del** link in the Action column. The deletion is confirmed, and the screen reloads.

Using the Search Function to Clone, Modify, and Delete Image Servers

To use the search function to clone, modify, or delete image servers from the GUI, follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Image Servers**. The Manage Image Servers screen opens.
- Step 2** Click **Search Image Servers**. The Search Image Servers screen opens.
- Step 3** Check a check box to specify the type of search condition, and then enter the condition in the corresponding field.
- For example, you can check the **Server name** check box and enter **server1** to search for all the image servers that contain server1 in the server name. You can also check the **IP Address** check box and enter the IP address in the corresponding field to search for the image server.
- Step 4** Click **Search by Above**. The search results appear in a table at the bottom of the screen. By default, all image servers are automatically selected (checked) in the table.
- Step 5** Take one of these actions:
- To edit an image server, click the corresponding **Edit** link in the Action column. The Edit Image Server screen opens. You can change the IP Address, Username, and Password fields. When you are done, click **Update**.
 - To clone an image server row, click the corresponding **Clone** link in the Action column. The Add an Image Server screen opens. You must modify the Server name and IP Address fields. As an option, you can modify the Username and Password fields. When you are done, click **Add**.
 - To delete an image server from the GUI, click the corresponding **Del** link in the Action column. The deletion is confirmed, and the screen reloads.
 - To delete all the image servers that are selected in the search results, click **Delete the selected Image Servers**. If you do not want to delete all the image servers, clear the check boxes for the image servers that you do not want to delete.
-

Distributing Groups to Image Servers

Groups can be distributed to an image server. Each group can only use one image server. You can change the members (that is, the groups) of each image server, by the following procedure:

-
- Step 1** On the menu, choose **Manage > Manage Image Servers**. The Manage Image servers screen opens.
- Step 2** For the image server to which you want to distribute groups, in the far right column (Action) of the Image Server List table, click **Member**. The Group Assignment screen opens.
- Step 3** In the Groups Without an Image Server field, choose the groups that you want to assign to the image server by pressing the **Ctrl** key on your keyboard and clicking group names.
- Step 4** Click the left angle brackets (<<) to move the groups to the Groups that use <image server name> field or the right angle brackets (>>) to move clients back to the Groups Without an Image Server field.

- Step 5** Click **Submit Changes**. The table in the lower half of the screen displays the details of the groups that you have distributed to the image server.
-

Managing Switch Groups

- [Creating Switch Groups](#)
- [Managing the Edge Switch List](#)
- [Adding Members to a Switch Group](#)
- [Using the Cisco IOS CLI to Configure Smart Install Groups](#)

You can group client switches in the Smart Install network for configuration and manageability. These groups are based on one of these switch components:

- MAC address
- Product identifier (PID)
- Location

You use the GUI to generate Smart Install group-device association files that the director uses to configure the switches in groups rather than individually. This file is stored on the TFTP server in the /opt/Tftproot/ directory with the suffix “IBDconf”. Although you can manually enter MAC addresses, PIDs, and locations, you can also import a spreadsheet with switch information into the GUI.



Note

You can use the CLI to organize client switches into groups based on MAC address or PID (see the [“Using the Cisco IOS CLI to Configure Smart Install Groups”](#) section on page 2-21). We recommend, however, that you use the GUI to organize the client switches into groups and use the CLI only if the GUI is not available.



Note

If you change any member of the group whose configuration is already downloaded to the director, an update bar will be displayed at the bottom of the page. You can click the **update** button to update the new member information to the director.

Creating Switch Groups

To create a switch group to which you can add switches, follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Groups**. The Manage Group screen opens.
- Step 2** Click **Add a Group** above the table. The Add a Group screen opens.
- Step 3** In the Group Name field, enter a name that is meaningful to you.
- Step 4** (Optional) From the Image Server drop-down list, choose an image server.
- Step 5** (Optional) In the Description field, enter a description that provides details about the group.
- Step 6** Click the **Add** button. The Group List screen opens, and the group is added to the Group List table. The Group List table also shows a row ID for the group and the date that the group was created.
-

The far right column of the Group List table provides these links to manage the group:

- **Edit**—Opens the Edit a Group screen. This screen contains the same field as the Add a Group screen. You use it to make changes to the image server and description.
- **Del**—Deletes a group.
- **Members**—Opens a screen that you use to add Smart Install switch clients to the group, or to remove them from the group. For information, see the [“Adding Members to a Switch Group” section on page 2-20](#).

Managing the Edge Switch List

The Smart Install director discovers switch clients and adds them to the director database. However, the discovered client switches do not appear on the GUI. To add client switches to the GUI:

- Import a list of client switches into the GUI Cisco Edge List screen.
- Manually add client switches to the GUI Cisco Edge List screen.
- In the GUI, clone an existing client switch, and edit the client switch.

Importing a List of Client Switches

You can import a Microsoft Excel spreadsheet or a text file with client switch information into the GUI. Follow these spreadsheet requirements:

- The spreadsheet can have any name but must be saved with a .csv or .txt extension and cannot exceed 2 MB. A text file must also have comma-separated values.
- The first row of the spreadsheet must be the title row and cannot include any switch information. The switch information can start on the second row.
- The title row must consist of these titles: MAC, PID, LOCATION. Do not include group information: groups are assigned through the GUI.
- The MAC address must consist of six groups of two hexadecimal digits, separated by colons. For example, AA:01:BB:02:CC:03.
- The PID must be alphanumeric and can consist of a maximum of 49 characters.

**Note**

A spreadsheet should not contain group information. You must use the GUI to allocate a switch to a group.

To import a spreadsheet into the GUI, follow these steps:

- Step 1** On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.
- Step 2** To the right of the Upload a spreadsheet field, click the icon with the black arrow.
- Step 3** Navigate to a spreadsheet or text file, and follow the browser instructions to place the file directory and name into the Upload a spreadsheet field.
- Step 4** Click **Upload** to upload the information into the table on the Cisco Edge List screen.

**Note**

If the spreadsheet or text file contains a MAC address that is not in the required format or is a duplicate of a MAC address that exists in the table on the Cisco Edge List screen, the GUI rejects this record with an error message.

**Note**

For more information, see [Appendix B, “Importing a Spreadsheet with Client Switch Information.”](#)

Manually Adding Client Switches

To manually add a client switch to the GUI, follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.
- Step 2** Click the **Add a Cisco Edge** tab. The Add a Cisco Edge screen opens.
- Step 3** Enter this information:
- **MAC field:** Enter the MAC address in the format of six groups of two hexadecimal digits, separated by colons. For example, AA:01:BB:02:CC:03.
-
- Note**
- If you enter a MAC address that is not in the required format or is a duplicate of a MAC address that already exists in the table on the Cisco Edge List screen, the GUI rejects your entry with an error message.
-
- **PID field:** Enter the PID, which must be alphanumerical and can consist of a maximum of 49 characters.
 - **LOCATION field:** Enter the location, which is a name that is meaningful to you. The location must be alphanumerical and can consist of a maximum of 49 characters.
 - **GROUP field:** From the drop-down list, select the group to which the switch should belong. If there is no existing group, the admin can click on the Create a group link on the right of the drop-down list to create one.
-
- Note**
- A switch can belong to only one group.
-
- Step 4** Click **Add** to save your changes and return to the Add a Cisco Edge page. You can continue to add another Cisco Edge, or click **Back** to return to the Cisco Edge List screen.
-

Cloning, Modifying, and Deleting Client Switches

To clone, modify, or delete client switches from the GUI, follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.
- The Action column of the Manage Cisco Edge table provides the links for modifying, cloning, or deleting client switches from the GUI.
- Step 2** Take one of these actions:
- To edit a switch, click the corresponding **Edit** link in the Action column. The Edit Cisco Edge screen opens. This screen contains the same fields as the Add a Cisco Edge screen. You can change the PID, and LOCATION fields, and allocate the switch to another group. When you are done, click **Update**.

- To clone a switch row, click the corresponding **Clone** link in the Action column. The Add a Cisco Edge screen opens. You must modify the MAC fields (no two switches can have the same MAC address). As an option, you can modify the PID and LOCATION fields and allocate the switch to another group. When you are done, click **Add**.
 - To delete a switch from the GUI, click the corresponding **Del** link in the Action column. The deletion is confirmed, and the screen reloads.
-

Using the Search Function to Clone, Modify, and Delete Switches

To use the search function to clone, modify, or delete client switches from the GUI, follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.
- Step 2** Click **Search Cisco Edges**. The Search Cisco Edge screen opens.
- Step 3** Check a check box to specify the type of search condition, and either enter the condition in the corresponding field, or click the condition that is shown in the field.
- For example, check the **Location** check box to search by location. You could also check the MAC check box and enter 1 in the corresponding field to search only for the switches with a MAC address that includes 1.
- Step 4** Click **Search by Above**. The search results appear in a table at the bottom of the screen. By default, all switches are automatically selected (checked) in the table.
- Step 5** Take one of these actions:
- To edit a switch, click the corresponding **Edit** link in the Action column. The Edit Cisco Edge screen opens. This screen contains the same fields as the Add a Cisco Edge screen. You can change the MAC, PID, and LOCATION fields and allocate the switch to another group. When you are done, click **Update**.
 - To clone a switch row, click the corresponding **Clone** link in the Action column. The Add a Cisco Edge screen opens. You must modify the SN and MAC fields (no two switches can have the same MAC address). As an option, you can modify the PID and LOCATION fields and allocate the switch to another group. When you are done, click **Add**.
 - To delete a switch from the GUI, click the corresponding **Del** in the Action column. The deletion is confirmed, and the screen reloads.
 - To delete all switches that are selected in the search results, click **Delete the selected Cisco Edge**. If you do not want to delete all switches, clear the check boxes for the switches that you do not want to delete.
-

Adding Members to a Switch Group

You can use the GUI to add members to a switch group or modify the members in a switch group.



Note

You can also use the CLI to add custom groups of switches based on MAC addresses or PIDs (see the [“Using the Cisco IOS CLI to Configure Smart Install Groups”](#) section on page 2-21). We recommend that you use the GUI to organize the client switches into groups and use the CLI only when the GUI is not available.

Using the Group Assignment Screen to Add Members to a Switch Group

To add clients to a switch group in the GUI (see the [“Managing Switch Groups” section on page 2-17](#)), follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Group**. The Manage Group screen opens.
 - Step 2** For the group to which you want to add clients, in the far right column (Action) of the Group List table, click **Member**. The Group Assignment screen opens.
 - Step 3** In the Available Cisco Edges field, choose the clients that you want to assign to the group by pressing the **Ctrl** key on your keyboard and clicking client names.
 - Step 4** Click the left angle brackets (<<) to move the clients to the Group field or the right angle brackets (>>) to move clients back to the Available Cisco Edges field.
 - Step 5** Click **Submit Changes**. The table in the lower half of the screen displays the details of the clients that you have added to the group.
-

Using the Search Function to Assign Members to or Change Members of a Switch Group

To use the search function to assign members to a switch group or change members from one switch group to another, follow these steps:

-
- Step 1** On the menu, choose **Manage > Manage Cisco Edges**. The Manage Cisco Edges screen opens.
 - Step 2** Click the **Group Cisco Edge** button. The Select Group Condition screen opens.
 - Step 3** Check a check box to specify the type of search condition. Either enter the condition in the corresponding field, or click the condition that is shown in the field.

For example, check the **Location** check box to search by location. You could also check the MAC check box and enter 1 in the corresponding field to search for only the switches with a MAC address that includes 1.
 - Step 4** Click **Search by Above**. The search results appear in a table at the bottom of the screen. By default, all switches are selected (checked).
 - Step 5** From the drop-down list to the right of the Group Selected Cisco Edge To button, choose a switch group for the selected switches. If you do not want to reassign some of the switches, uncheck the check boxes for those switches.
 - Step 6** Click the **Group Selected Cisco Edge To** button to complete the assignment.
-

Using the Cisco IOS CLI to Configure Smart Install Groups

You can use the CLI to organize client switches into groups based on MAC address or product ID. We recommend that you use the GUI to organize the client switches into groups, and use the CLI only when the GUI is not available.



Note

For information about using the GUI to organize the client switches into groups, see the [“Creating Switch Groups” section on page 2-17](#) and the [“Adding Members to a Switch Group” section on page 2-20](#).

**Note**

The Cisco Edge 300 series switch does not support a mixed combination of CLI-generated and GUI-generated group files. You must use *only* the GUI or *only* the CLI to generate group files.

Custom Group Based on MAC Address

You can configure a custom group based on the MAC addressees. A MAC address match takes priority over other matches. The switches that do not match the MAC addresses in the group can get the configuration and image for another group or get the default configuration.

Beginning in privileged EXEC mode, follow these steps on the director to configure a group based on MAC addresses:

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	vstack group custom <i>group_name</i> mac	Identifies a custom group based on a MAC address match, and enters Smart Install group configuration mode for the group.
Step 3	match <i>mac_address</i>	Enters the MAC address of the client switch to be added to the custom group. Repeat the command for each MAC address to be added. Note To see MAC addresses of switches in the Smart Install network, enter the show vstack neighbors all privileged EXEC command. Switches added to the group use the same image and configuration file.
Step 4	image <i>location image_name-imglist.txt</i>	Enters the location and image list file for the custom group. <ul style="list-style-type: none"> <i>location</i>—Enter flash: if the TFTP server is the director and the file is in the director flash memory, or enter tftp: and the location of the image. You can also enter flash0:, flash1:, or usb:. Note Although visible in the command-line help, these options are not supported: flash1: , ftp: , http: , https: , null: , nvr: , rcp: , scp: , system: , tmpsys: . <ul style="list-style-type: none"> <i>image_name-imglist.txt</i> is the image list file that you want to download.

	Command	Purpose
Step 5	config <i>location</i> config.text.config_filename	<p>Enters the location and configuration file for the custom group.</p> <ul style="list-style-type: none"> <i>location</i>—Enter flash: if the TFTP server is the director and the file is in the director flash memory, or enter tftp: and the location of the configuration file. You can also enter flash0:, flash1:, or usb:. <p>Note Although visible in the command-line help, these options are not supported: flash1:, ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> config.text.config_filename—Enter the filename of the configuration file for the group.
Step 6	end	Returns to privileged EXEC mode.
Step 7	copy running-config startup config	(Optional) Saves your entries in the configuration file.
Step 8	show vstack group custom detail	Verifies the configuration.

**Note**

The director automatically creates a director configuration file for the new group and saves it on the TFTP server.

This example creates a custom group named testgroup3 that includes the three switches identified by a MAC address and configures the group to use the specified image file (global-imglist.txt) and configuration file (config.text.classroom):

```
Director# configure terminal
Director(config)# vstack group custom testgroup3 mac
Director(config-vstack-group)# match mac 0023.34ca.c180
Director(config-vstack-group)# match mac 001a.a1b4.ee00
Director(config-vstack-group)# match mac 00:1B:54:44:C6:00
Director(config-vstack-group)# image tftp://101.122.33.10/global-imglist.txt
Director(config-vstack-group)# config tftp://101.122.33.10/config.text.classroom
Director(config-vstack-group)# exit
Director(config)# end
```

The director configuration file that is created for this group is testgroup3-imgelist.txt.

Custom Group Based on Product ID

You can configure a custom group based on the product IDs (PIDs). The switches that do not match the group PID can get the configuration and image for another group or get the default configuration.

Beginning in privileged EXEC mode, follow these steps on the director to configure a group based on a PID:

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	vstack group custom <i>group_name</i> product-id	Identifies a custom group based on a product-ID match, and enters Smart Install group configuration mode for the group.

	Command	Purpose
Step 3	match <i>product-id</i>	Enters the product ID of the client switches in the custom group.
Step 4	image <i>location image_name-imglist.txt</i>	<p>Enters the location and image list file for the custom group.</p> <ul style="list-style-type: none"> <i>location</i>—Enter flash: if the TFTP server is the director and the file is in the director flash memory, or enter tftp: and the location of the image. You can also enter flash0:, flash1:, or usb:. <p>Note Although visible in the command-line help, these options are not supported: flash1:, ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> <i>image_name-imglist.txt</i> is the image list file that you want to download.
Step 5	config <i>location config.text.config_filename</i>	<p>Enters the location and configuration file for the custom group.</p> <ul style="list-style-type: none"> <i>location</i>—Enter flash: if the TFTP server is the director and the file is in the director flash memory, or enter tftp: and the location of the configuration file. You can also enter flash0:, flash1:, or usb:. <p>Note Although visible in the command-line help, these options are not supported: flash1:, ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> <i>config.text.config_filename</i>—Enter the filename of the configuration file for the group.
Step 6	end	Returns to privileged EXEC mode.
Step 7	copy running-config startup config	(Optional) Saves your entries in the configuration file.
Step 8	show vstack group custom detail	Verifies the configuration.

**Note**

The director automatically creates a director configuration file for the new group and saves it on the TFTP server.

This example creates a custom group named testgroup4 that includes the switches identified by the product ID and configures the group to use the specified image file (global.imglist.txt) and configuration file (config.text.classroom).

```
Director# configure terminal
Director(config)# vstack group custom testgroup4 product-id
Director(config-vstack-group)# match EDGE_300
Director(config-vstack-group)# image tftp://101.122.33.10/global-imglist.txt
Director(config-vstack-group)# config tftp://101.122.33.10/config.text.classroom
Director(config-vstack-group)# exit
Director(config)# end
```

The director configuration file that is created for this group is testgroup4-imgelist.txt.

Managing Cisco Edge Configuration Files

- [Configuring a Group Using the GUI](#)
- [Configuring a Cisco Edge Using the GUI](#)
- [Configuring a Cisco Edge or Group Using CLI Mode](#)
- [Modifying a Group or Cisco Edge Using CLI Mode](#)
- [Using Auto-Complete to Enter Commands](#)

**Note**

On the GUI, a client switch is referred to as a Cisco Edge.

Cisco Edge Configuration File

The Cisco Edge configuration file is the client switch configuration file that is on the TFTP server and managed by the director. The Cisco Edge configuration file consists of these parts:

- A common configuration that applies to all client switches in a group and that includes GUI fields that configure the root password, set all switches to default settings, and configure interface characteristics for all switches in the group. You can also switch to CLI mode to configure the group.
- An individual configuration that applies to a single client switch and that includes GUI fields that configure the interface characteristics for only the single client switch, the Bluetooth settings, the SSID, the wireless security settings, and so on. An individual switch is identified by its MAC address. You can also switch to CLI mode to configure the Cisco Edge.

Configuring a Group Using the GUI

To configure a group using the GUI, follow these steps:

Step 1 On the menu, choose **Configure > Configure Groups**. The Configure Groups screen opens.

Step 2 Click the Configure link from the Action column for the group.

**Note**

The value of each field is set to the default value when the page is loaded for your first-time configuration. The administrator can click the **Restore default settings** button to restore the default values.

Step 3 Click the following tabs to configure the group:

Basic Settings

Group name	Display the name of the group. You can change the name of the group.
Password of root	Enter the root (admin) password for the group. This is a required field.
Password of student	Enter the default user password for the group.
Login GUI	Enable or disable access to the GUI without entering the username and password.
OS version	Choose the operating system image from the drop-down list.

Factory mode OS version	Choose the factory mode operating system image from the drop-down list.
Cisco Software version	Choose the Cisco application image from the drop-down list.
Partner Software version	Choose the partner application image from the drop-down list.
Fonts	Choose the fonts file from the drop-down list.
Resolution	Choose the video resolution from the drop-down list.
Bluetooth	Enable or disable Bluetooth.
Language	Choose the language from the drop-down list.
Time zone	Choose the time zone from the drop-down list.
NTP Server	Enter the IP address of the NTP server.
Number of Cisco Edges	Show the number of Cisco Edge switches.

WiFi	
SSID	Enter the SSID name.
Broadcast SSID	Enable or disable broadcast of the SSID name.
Radio	Enable or disable the wireless radio.
Wireless Mode	Choose a mode from the drop-down list. <ul style="list-style-type: none"> • 802.11b/g—Devices in the network support 802.11b and 802.11g. • 802.11b—All devices in the wireless network only support 802.11b. • 802.11g—All devices in the wireless network only support 802.11g. • 802.11n—All devices in the wireless network only support 802.11n. • 802.11g/n—Devices in the network support 802.11g and 802.11n. • 802.11b/g/n—Devices in the network support 802.11b, 802.11g, and 802.11n.
Channel	Choose the channel number (which sets the frequency) for the access point.
Transmit power	Choose the power at which the access point radio transmits its wireless signal.
Channel Bandwidth	Choose the channel width when the access point functions in 802.11n mode.
Encryption mode	Choose the encryption mode. Depending on the mode, you will also have to select an encryption type and enter a key.
Wifi > Advanced	
AP isolation	Configure wireless separation for clients that are connected to the same SSID.
Operating mode	Configure greenfield or mixed mode when the access point functions in 802.11n mode.
Guard interval	Configure the period between packets when the access point functions in 802.11n mode or 802.11n mixed mode.
MCS	Configure the high throughput Modulation and Coding Schemes (MCS) rate when the access point functions in 802.11n mode or 802.11n mixed mode.
RDG	Configure the Reverse Direction Grant (RDG) when the access point functions in 802.11n mode or 802.11n mixed mode.
APSD capable	Configure Wi-Fi Multimedia (WMM) power save mode for the access point.
WMM capable	Configure Wi-Fi Multimedia (WMM) for the access point.
Beacon interval	Configure the beacon interval for the access point.
Bg protection	Configure the CTS-to-self protection for the access point.
Channel allocation	Configure the channel width when the access point functions in 802.11n mode or 802.11n mixed mode.
Data beacon rate	Configure the Delivery Traffic Indication Message (DTIM) interval for the access point.

Extension channel	Configure the control side band that is used for the extension or secondary channel when the access point functions in 802.11n mode or 802.11n mixed mode.
Packet aggregation	Configure Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when the access point functions in 802.11n mode or 802.11n mixed mode.
Short slot	Configure the short-slot time when the access point functions in 802.11g mode or 802.11g mixed mode.
Transmit burst	Configure the transmit burst (Tx burst) for the access point.
Transmit preamble	Configure the preamble for the access point.
IGMP snoop	Enable or disable Internet Group Management Protocol (IGMP) snooping.
Multicast MSC	Configure the high throughput Modulation and Coding Schemes (MCS) rate on multicast frames.
Multicast phy mode	Configure PHY mode on multicast frames.
Ethernet Port	
MAC address-table aging time	Enter the number of seconds (from 15 to 3825) that a dynamic MAC address remains in the MAC address table after the address is used or updated.
Interface Gi1/Fe1/Fe2/Fe3/Fe4	Click the + icon next to the Interface to configure the interface.
Status	Enable or disable the port. Note The Gi1 port is enabled and cannot be disabled.
Output-queue-strategy	Choose the type of output traffic scheduling on an interface from the drop-down list.
Pause	Enable or disable auto-negotiation flow control on an interface. Note This option is available on the Gi1 interface.
Priority	Choose the QoS priority for incoming traffic on an interface.
Rate-limit	Choose the rate-limit and rate for broadcast and unknown unicast traffic on an interface.
Speed	Choose the speed for an interface.
Duplex Mode	Choose the duplex mode for an interface.

NFS

Note Change the status to ON to enter NFS settings.

NFS Server	Enter the IP address of the network file system (NFS) server.
NFS Server Path	Enter the path exported on the NFS server.
Cisco Edge Path	Enter the path to be mounted on the Cisco Edge 300 switch.
Status	Choose ON or OFF.

Members

Display information about the Cisco Edge switches in the group.

Note You can click the links in the Operation column to configure, power off, or reboot the Cisco Edge switch.

- Step 4** Click the **Apply changes** button. The Apply Settings window appears.
- Step 5** Enter the Smart Install Director IP address, user name, Telnet password, and Privileged EXEC mode password. If you have more than one interface on the GUI server, the GUI IP address field is displayed and you must choose an IP that is connected to the Smart Install network.
- Step 6** Click the **Apply** or the **Apply and reboot** button.



Note When you click the Apply button, the configuration file is downloaded to the director switch and all Cisco Edge switches in the group that are powered on reboot with the new configuration. Cisco Edge switches in the group that are not powered on are configured when powered on.



Note After the first-time configuration is applied, the Cisco Edge 300 switches send their IP addresses to the GUI. When the GUI has the IP addresses of Edge 300 switches, it could help to clear the /apps folder. This operation is useful as you need to clear the old application before upgrading images. The administrator can clear the /apps folder by checking the **clear /apps** checkbox in the Apply Settings window. The clear /apps operation will only be applied to those switches that are up and running, and in the group. The switches that are powered off or not in the group will not be affected.

Configuring a Cisco Edge Using the GUI



Note You must configure the Cisco Edge Group first and then configure the Cisco Edge because the Cisco Edge configuration has a higher priority than the Cisco Edge group configuration. The group-device association files are generated only when you click the **Apply** or **Apply and reboot** button in the group configuration page.

To configure a Cisco Edge using the GUI, follow these steps:

- Step 1** On the menu, choose **Configure > Configure Cisco Edge**. The Configure Cisco Edge screen opens.
- Step 2** Click the **Configure** link from the Action column for the Cisco Edge. The Cisco Edge Config screen opens.

Step 3 Click one of the following tabs to configure the group:

Basic Settings	
MAC	Display the MAC address.
PID	Display the product identifier.
Location	Display the location.
Group	Display the group to which the Cisco Edge switch belongs.
Status	Display the current status of the Cisco Edge switch (on, off).
IP	Display the IP address of the Cisco Edge switch.
Password of root	Display the root (admin) password for the group.
Password of student	Display the default user password for the group.
OS version	Display the operating system image.
Factory mode OS version	Display the factory mode operating system image version.
Cisco Software version	Display the Cisco application image version.
Partner Software version	Display the partner software version.
Fonts	Display the fonts file.
Hostname	Enter the hostname of the switch.
Login GUI	Enable or disable access to the GUI without entering the username and password.
Resolution	Choose the video resolution from the drop-down list.
Bluetooth	Enable or disable.
Language	Choose the language from the drop-down list.
Time zone	Choose the time zone from the drop-down list.
NTP Server	Enter the IP address of the NTP server.
WiFi	
SSID	Enter the SSID name.
Broadcast SSID	Enable or disable broadcast of the SSID name.
Radio	Enable or disable the wireless radio.
Wireless Mode	Choose a mode from the drop-down list. <ul style="list-style-type: none"> 802.11b/g—Devices in the network support 802.11b and 802.11g. 802.11b—All devices in the wireless network only support 802.11b. 802.11g—All devices in the wireless network only support 802.11g. 802.11n—All devices in the wireless network only support 802.11n. 802.11b/g/n—Devices in the network support 802.11b, 802.11g, and 802.11n.
Channel	Choose the channel number (which sets the frequency) for the access point.
Transmit power	Choose the power at which the access point radio transmits its wireless signal.

Channel Bandwidth	Choose the channel width when the access point functions in 802.11n mode.
Encryption mode	Choose the encryption mode. Depending on the mode, you will also have to select an encryption type and enter a key.
Wifi > Advanced	
AP isolation	Configure wireless separation for clients that are connected to the same SSID.
Operating mode	Configure greenfield or mixed mode when the access point functions in 802.11n mode.
Guard interval	Configure the period between packets when the access point functions in 802.11n mode or 802.11n mixed mode.
MCS	Configure the high throughput Modulation and Coding Schemes (MCS) rate when the access point functions in 802.11n mode or 802.11n mixed mode.
RDG	Configure the Reverse Direction Grant (RDG) when the access point functions in 802.11n mode or 802.11n mixed mode.
APSD capable	Configure Wi-Fi Multimedia (WMM) power save mode for the access point.
WMM capable	Configure Wi-Fi Multimedia (WMM) for the access point.
Beacon interval	Configure the beacon interval for the access point.
Bg protection	Configure the CTS-to-self protection for the access point.
Channel allocation	Configure the channel width when the access point functions in 802.11n mode or 802.11n mixed mode.
Data beacon rate	Configure the Delivery Traffic Indication Message (DTIM) interval for the access point.
Extension channel	Configure the control side band that is used for the extension or secondary channel when the access point functions in 802.11n mode or 802.11n mixed mode.
Packet aggregation	Configure Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when the access point functions in 802.11n mode or 802.11n mixed mode.
Short slot	Configure the short-slot time when the access point functions in 802.11g mode or 802.11g mixed mode.
Transmit burst	Configure the transmit burst (Tx burst) for the access point.
Transmit preamble	Configure the preamble for the access point.
IGMP snoop	Enable or disable Internet Group Management Protocol (IGMP) snooping.
Multicast MSC	Configure the high throughput Modulation and Coding Schemes (MCS) rate on multicast frames.
Multicast phy mode	Configure PHY mode on multicast frames.

Ethernet Port

MAC address-table aging time	Enter the number of seconds (from 15 to 3825) that a dynamic MAC address remains in the MAC address table after the address is used or updated.
Interface Gi1/Fe1/Fe2/Fe3/Fe4	Click the + icon next to the Interface to configure the interface.
Status	Enable or disable the port. The Gi1 port cannot be disabled.
Output-queue-strategy	Choose the type of output traffic scheduling on an interface from the drop-down list.
Pause	Enable or disable auto-negotiation flow control on an interface. Note This option is available on the Gi1 interface.
Priority	Choose the QoS priority for incoming traffic on an interface.
Rate-limit	Choose the rate-limit and rate for broadcast and unknown unicast traffic on an interface.
Speed	Choose the speed for an interface.
Duplex Mode	Choose the duplex mode for an interface.

NFS

Note Change the status to ON to enter NFS settings.

NFS Server	Enter the IP address of the network file system (NFS) server.
NFS Server Path	Enter the path exported on the NFS server.
Cisco Edge Path	Enter the path to be mounted on the Cisco Edge.
Status	Choose ON or OFF.

Step 4 Click the **Apply changes** button. The Apply Settings window appears.

Step 5 Click the **Apply** or **Apply and reboot** button.



Note When you click the Apply button, the configuration file is saved to the TFTP server. The configuration takes effect when the switch is rebooted.


Configuring a Cisco Edge or Group Using CLI Mode



Note Use the information in this section together with the CLI commands that are described in [Chapter 4, “Configuring Local CLI - Clish.”](#)

To use CLI mode to configure a Cisco Edge or a group, follow these steps:

Step 1 Do one of the following:

- On the menu, choose **Configure > Configure Cisco Edges**. The Configure Cisco Edges screen opens.
 - On the menu, choose **Configure > Configure Groups**. The Configure Groups screen opens.
- Step 2** Click the **Configure** link from the Action column for the Cisco Edge or group.
- Step 3** Click the **Switch to CLI Mode** link.
- Step 4** In the Image selection window, make your image selections:
- OS Images—Choose an operating system image from the drop-down list.
 - Factory mode OS version—Choose the factory mode operating system image from the drop-down list.
 - Cisco Application Images—Choose a Cisco application image from the drop-down list.
 - Partner Application Images—Choose a third-party application image from the drop-down list.
 - Fonts—Choose the fonts file from the drop-down list.
 - IP Address of Director—Enter the IP address of the director (required).
 - User Name or Director—Enter your user name to access the director name (optional).
 - Telnet Password of Director—Enter your Telnet password of the director switch (optional).
-  **Note** If you entered a director user name, enter the Telnet password for the director user name. Otherwise, enter the switch Telnet login password.
- Privileged EXEC Mode Password—Enter your password to access Privileged EXEC mode (optional).
- Step 5** In the Configuration File field, enter CLI commands or use auto-completion to enter CLI commands (see the [“Using Auto-Complete to Enter Commands”](#) section on page 2-34). For information about CLI commands, see [Chapter 4, “Configuring Local CLI - Clish.”](#)
- Step 6** Click **Parse Configuration File and Save**. The file is saved. The “Configuration file has been downloaded to the tftp server” message appears. An error message appears if the file was not saved.

Modifying a Group or Cisco Edge Using CLI Mode

To use CLI mode to modify a Cisco Edge or a group, follow these steps:

- Step 1** Do one of the following:
- On the menu, choose **Configure > Configure Cisco Edges**. The Configure Cisco Edges screen opens.
 - On the menu, choose **Configure > Configure Groups**. The Configure Groups screen opens.
- Step 2** Click the **Configure** link from the Action column for the Cisco Edge or group.
- Step 3** Click the **Switch to CLI Mode** link.
- Step 4** In the Image selection window, make these selections:
- OS Images—Choose an operating system image from the drop-down list.

- Factory mode OS version—Choose the factory mode operating system image from the drop-down list.
- Cisco Application Images—Choose a Cisco application image from the drop-down list.
- 3rd Party Application Images—Choose a third-party application image from the drop-down list.
- IP Address of Director—Enter the IP address of the director (required).
- Fonts—Choose the fonts file from the drop-down list.
- User Name or Director—Enter your user name to access the director name (optional).
- Telnet Password of Director—Enter your Telnet password of the director switch (optional).



Note If you entered a director user name, enter the Telnet password for the director user name. Otherwise, enter the switch Telnet login password.

- Privileged EXEC Mode Password—Enter your password to access Privileged EXEC mode (optional).

Step 5 In the Configuration File field, change CLI commands or enter new CLI commands. You can also use auto-complete to enter new CLI commands (see the [“Using Auto-Complete to Enter Commands”](#) section on page 2-34).

Step 6 When you are done, take one of these actions:

- Save the file under the same name:
Click **Parse Configuration File and Save** to save the file under the same name. The file is saved. The “Configuration file has been downloaded to the tftp server” message appears. An error message appears if the file was not saved.

Using Auto-Complete to Enter Commands

When you create or edit a Cisco Edge configuration file, you can use auto-complete. It can reduce command syntax errors by providing valid choices. The syntax check occurs only when you click **Parse Configuration File and Save** or **OK**.

To use auto-complete, follow these steps:

Step 1 In the smart input field (with a pound sign [#]), enter a few initial letters of a command. The available commands appear under the smart input field.

You can also place the cursor in an empty smart input field and press **Space**. Auto-complete shows the commands for the command mode that you are in under the smart input field.

Step 2 Press **Tab** to auto-complete the command.

You can also click a command that is shown under the smart input field, and it appears in the smart input field.

Step 3 Press **Enter**. The command moves to the Configuration File field.

**Note**

The prompt of the smart input field changes according to the command mode that you are in. For example, when the **configure terminal** command moves to the Configuration File field, the command mode changes: (config)#.

This is an example of how you can edit a Cisco Edge configuration file:

Step 1 In the Configuration File field, place the cursor where you want to change or add a CLI command.

Step 2 To make your edits, take one of these actions:

- Manually make an adjustment to the command without using the smart input field. You can edit the command in the Configuration File field as you would do in a regular text box.
- Enter a command in the smart input field and press **Enter** to add the command. The last location of the cursor in the Configuration File field determines where the command is inserted:
 - If you placed the cursor at the beginning of a command line, the new command is inserted above the line.
 - If you placed the cursor in a command line, the new command is inserted to the right of the cursor position.
 - If you placed the cursor at the end of a command line, the new command is inserted below the line.

Step 3 Click **Parse Configuration File and Save** to save your changes. The file is saved. The “Configuration file has been downloaded to the tftp server” message appears. An error message appears if the file was not saved.

Switch Image and Configuration Upgrades

This section describes the upgrade methods.

**Caution**

Before upgrading from software release 1.0 to release 1.1, remove the Factory Mode OS Version and Fonts selections from the GUI and apply the changes. See the [“Managing Cisco Edge Configuration Files” section on page 2-25](#).

**Note**

If there are any problems with an upgrade, see the [“Troubleshooting Software Upgrades” section on page D-2](#).

Upgrade Initiated by the User

In the room where the switch is located, a user can initiate an upgrade by one of these methods:

- Pressing the Reset button—The switch starts up in factory-default mode, connects to the director, and then downloads and installs the latest images and configuration files.

- Turning the switch off and on—The switch starts up in normal mode, connects to the director, and detects whether or not new images and configuration files are available. If new images and configuration files are available, the switch restarts in factory-default mode and automatically downloads and installs the new images and configuration files.

In either case, the switch saves a copy of the existing images and configuration files before installing the new images and files. If the installation fails, the switch restores the old configuration.

Upgrade Initiated by the Administrator

Using the GUI, you can reboot the switch to initiate an upgrade.

- Step 1** Do one of the following:
- On the menu, choose **Configure > Configure Cisco Edges**. The Configure Cisco Edges screen opens.
 - On the menu, choose **Monitor > Monitor Cisco Edges**. The Monitor Cisco Edges screen opens.
- Step 2** Click the **Reboot** link from the Operation column for the Cisco Edge.



Note If the Status of the Cisco Edge is off, the Operation links are not available.

Using the CLI, you can connect to a switch (for example, over a Telnet or secure shell (SSH) connection) and restart the switch to initiate an upgrade.



Note On-demand upgrades and scheduled downloads are not supported. You cannot upgrade switches from the director by using the **write erase** and **reload**, **vstack download-image**, **vstack download-config**, or **archive download-sw** privileged EXEC commands.

CLI Configuration Mode in the Smart Install Server

You can switch to CLI mode to create a Cisco Edge configuration file on the GUI.

The GUI can generate the configuration file. Do not edit the file directly unless you are an expert on the CLI configuration.

For information about how to enter the CLI in the GUI to create a Cisco Edge configuration file, see the [Managing Cisco Edge Configuration Files](#) section on page 2-23.

Configuration Guidelines

The CLI uses only commands that are specific to the Cisco Edge 300 series switch. Although the syntax is similar to the Cisco IOS CLI, the commands are *incompatible* with Cisco IOS commands.

Use the CLI to configure these switch settings:

- Basic switch settings—Hostname, MAC address, Bluetooth settings, password, Network Time Protocol (NTP) server, and switch language
- Ethernet interface settings—Status, speed, and quality of service (QoS)
- Wireless interface settings—Status, radio, wireless mode, channel, wireless separation, transmission power, Wi-Fi Multimedia (WMM), and advanced wireless settings
- SSID security settings—Broadcast, authentication, and encryption

Follow these configuration guidelines:

- Click the button on the web GUI to enter the CLI edit mode.
- Create one Cisco Edge configuration file for each switch group. This file is used to configure *all* switches in the group. When a switch that is part of the group is rebooted, it is configured as defined in the Cisco Edge configuration file. Any changes that were made locally to the switch are lost after the switch reboots.
- Start a Cisco Edge configuration file with the **configure terminal** global command. End the Cisco Edge configuration file with the **exit** global command.
- Within a Cisco Edge configuration file, start each individual switch configuration with the **system identifier mac_address** system configuration command. End each individual switch configuration with the **done** system configuration command.



Note We recommend that you use the **system identifier default** system configuration command to configure all the switches in the group to default settings before you configure each switch individually.

- From the system configuration mode, you can enter these configuration modes:
 - Ethernet configuration mode
Use the **interface** system configuration command to enter this mode. Use the **exit** global configuration command to return to the system configuration mode.
 - WiFi interface configuration mode
Use the **interface** system configuration command to enter this mode. We recommend that before you configure any wireless settings, that you first use the **wireless-mode** WiFi configuration command to set the 802.11 wireless mode. Use the **exit** global configuration command to return to the system configuration mode.
 - SSID configuration mode
Use the **ssid** system configuration command to enter this mode. Use the **exit** global configuration command to return to the system configuration mode.
- All commands must be entered in lowercase letters. Arguments can include uppercase letters.
- If there is a configuration conflict, the most recent configuration takes precedence. In this example, the SSID is not broadcast:

```
ssid NEWAP1
  broadcast ssid on
  broadcast ssid off
exit
```

Example of a Cisco Edge Configuration File

This is an example of a Cisco Edge configuration file with two switches: one with the hostname switch333 and MAC address 1111.1111.1211 and the other with the hostname switch344 and MAC address 1111.1111.1213.

This file is generated by the smart install server, and dispatches to different Edge switches, and every switch only executes the **system identifier default** configuration and its own **mac address system identifier** configuration.

```
configure terminal
system identifier default
done
system identifier 1111.1111.1211
    hostname switch333
    mac address-table aging-time 3825
    mac address-table static 1111.1111.1111 vlan 1 interface fe1 default
    interface gil
        speed 10
    exit
    interface fe3
        speed 10
    exit
    ssid NEWAP1
    exit
done
system identifier 1111.1111.1213
    hostname switch 344
    mac address-table aging-time 3825
    mac address-table static 1111.1111.1111 vlan 1 interface cpu critical
    interface fe3
        priority normal
        output-queue-strategy wrr
        speed 10
    exit
    ssid NEWAP2
        broadcast ssid on
        encryption mode wpa2psk type tkip pass-phrase better33safe990-than12sorry_
    exit
    interface bv11
        wireless-mode 9
        radio on
        channel number 12
        ap-isolation off
        operating-mode greenfield
        channel bandwidth 20/40
        guard-interval 800
        mcs 33
        rdg on
        extension channel upper
        bg-protection on
        beacon-interval 1000
        data-beacon-rate 255
        transmit power 99
        transmit preamble auto
        short-slot on
        packet aggregation on
    exit
done
exit
```