



Configuring Cisco Smart Install Devices

This section includes some basic scenarios and tasks that you might configure in a Smart Install network.

- [Configuration Guidelines and Recommendations, page 2-1](#)
- [Configuring the DHCP Server, page 2-5](#)
- [Configuring the TFTP Server, page 2-8](#)
- [Establishing a Remote Client Session, page 2-9](#)
- [Configuring a Network with Single or Mixed Switch Types, page 2-9](#)
- [Updating On-Demand to a New Image or Configuration, page 2-16](#)
- [Using Custom Groups to Configure Groups Based on Connectivity, MAC Address, Stack Number, or Product ID, page 2-18](#)
- [Managing Client Configuration Files, page 2-28](#)
- [Other Configuration Options, page 2-29](#)
- [Smart Install Configuration Examples, page 2-42](#)

Configuration Guidelines and Recommendations

- If the startup configuration fails to download, the client can go into an infinite loop because there is no startup configuration to update. The only way to recover from the loop is to press **Enter** when the client is coming up after a reload so that the update process stops.
- When performing a zero-touch update, you should always update both the image and the startup configuration files. To update only the image or only the configuration file, use the **vstack download-image** or **vstack download-config** privileged EXEC commands for an on-demand download instead.
- To update only the image or only the configuration file, use the **vstack download-image** or **vstack download-config** privileged EXEC commands for an on-demand download instead.
- On the Catalyst 4500 series switches, after a zero-touch upgrade goes through on a non-VLAN 1 network, the Integrated Branch Client (IBC) IP address is not updated in the director database if the seed (default) configuration does not contain the new VLAN information. In order to ensure persistent communication between the Integrated Branch Director (IBD) and IBC after an upgrade, you must update the seed configuration every time you change the start-up management VLAN.
- On the Catalyst 3750 and Catalyst 4500 series switches, beginning with Cisco Release IOS XE 3.6.(0)E, and Cisco Release IOS 15.2(1)SG, 15.0(2)SE, and 15.2.(2)E, the following combinations of zero-touch upgrade are supported

- Image and configuration zero-touch upgrade—User specifies both image and configuration on the director.
- Configuration-only zero-touch upgrade—User specifies configuration alone on the director.
- Image-only zero-touch upgrade—User specifies image alone on the director.

**Note**

We recommend you to delete the **multiple-fs** file from the flash/bootflash after **write erase** command in the case of a zero-touch upgrade.

- On the Catalyst 4500 series switch director and client functionality is supported; beginning with Cisco IOS Release IOS XE 3.6.(0)E the above mentioned combinations of zero-touch upgrade can be configured on the director or client.
- For the above features to work on the client side, the clients must be running the image with Cisco Release IOS 15.2(1)SG or higher.

**Note**

For an on-demand download, update the image and configuration on the client with the **vstack download-image** or **vstack download-config** commands.

If you trigger a zero-touch upgrade with backup enabled and Rev2 (such as, backed-up configuration) accessible on the SMI director, the Rev2 is sent for an upgrade. If you accidentally delete the Rev2 file, the zero-touch upgrade fails because the backup configuration is missing. However, the client attempts another reload and boots with the seed (default) configuration, ensuring a smoothly functioning zero-touch upgrade irrespective of the missing backup configuration.

If backup is enabled and an image-only upgrade is specified on the director, the client boots up with the backed-up configuration and the image specified when the upgrade launches on the client. However, if backup is disabled, the client boots with the image [alone] specified on the director for that client.

- Switches are updated one hop at a time. The director cannot update switches in hop 2 while it is upgrading switches in hop 1.
- Because DHCP snooping is not supported on routed ports, you should not connect routed ports directly to the client or the director. Without DHCP snooping, the director will not detect a DHCP request from the client, which prevents Smart Install from working on that client. Routed ports cannot participate in Smart Install.
- For client switches with only 16 Mb of flash memory, before upgrading the Cisco IOS image, ensure that there is enough free flash space available to download a new image and delete unnecessary files. The configuration file might not be necessary because Smart Install can provide the configuration file when the client boots up.
- In Catalyst 6500 Supervisor Engine 2T switches, flash size supports onboard and external disks to download the image and the configuration file.
- The director can act as the TFTP server, eliminating the need for an external TFTP serving device. Follow these guidelines when configuring the director as TFTP server:
 - The total flash 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 on the director to hold the client Cisco IOS images and configuration files. The Cisco IOS image files vary in size, depending on the client switch product IDs and whether or not crypto images are being installed.

- When the director is the TFTP server, a copy of the configuration file for each client switch is stored in the root directory of the flash file system on the director. There must be enough space for each planned client group.
- Most director switches have enough flash memory to hold one client Cisco IOS image and a small number of client configuration files. For example, the Catalyst 3750 switch can have a maximum flash size of 64 MB, which accommodates only 4 or 5 images, based on the image size.
- If the Smart Install network includes client switches with more than one product ID, you should use an external TFTP server.
- When the director is the TFTP server, downloading a TFTP file will be slower than the external TFTP server. If downloading the TFTP file is a priority, use an external TFTP server, especially if there are multiple clients performing TFTP downloads simultaneously.
- If the TFTP server is a third-party (non-Cisco) device, you should disable the server option to change the name of a file if another file is created with the same name. Otherwise, duplicate imagelist files might be created.
- Client switches can be on any VLANs other than the default if the director is configured to snoop on that VLAN (enter the **vstack vlan *vlan-id*** global configuration command) and if traffic from the VLAN flows through the director.
 - The director can snoop on multiple VLANs extending to clients on different Layer 2 subnets.
 - Client switches can be on different routed subnets as long as there are routes between the director and the subnet. In these cases, a relay agent between a client and director is required for Smart Install downloads.
 - Smart Install does not function if the client is connected directly to a routed port on the director.
- Stacking considerations:
 - If the director is in a switch stack and a master switchover occurs when a non-Smart Install client switch is being updated, the client switch update is not completed.
 - If the client switch is a stack and not all members are up and operational, downloading of new images to the stack members fails.
 - Upgrading a stack requires configuring a custom group matching the stack group.
 - When a stack is upgraded, you should restart all stack members at the same time.
 - When a stack is deliberately partitioned, the new stacks should have the required configuration for upgrades, that is, the stack group members must be configured correctly.
- For Catalyst 3750-X, 3750-E, 3650-X, and 3650-E client switches, install the appropriate license files before updating the image. Smart Install does not apply to image licensing.
- To disable Smart Install on a director or client, enter the **no vstack** global configuration command on the device. Enter the **show vstack status** privileged EXEC command to see if Smart Install is enabled or disabled on a device.
- Client switches with static IP addresses cannot get zero-touch downloads but can receive on-demand downloads.
- If the director temporarily loses communication with the client switches, there is no impact to the Smart Install feature unless the client is in the middle of installing Cisco IOS images or downloading the configuration. If this happens, manual intervention might be required to restart the process.
- We recommend that configuration files do not include **boot host dhcp**. If a configuration file does include this configuration, do not apply the configuration file to switches with interfaces that do not have a configured IP address.

- When a director is configured and a client joins the Smart Install network, Smart Install is automatically enabled on these devices. Beginning with Cisco IOS Release 12.2(58)SE, 15.1(1)SY, 15.0(2)SE and later, and 3.2(0)SE and later, you can disable Smart Install on a device and also shut down its Smart Install TCP ports by entering the **no vstack** global configuration command on the client or director.
 - When Smart Install is disabled on a device, any Smart Install configuration on the device remains in the running configuration but does not take effect while Smart Install is disabled.
 - When Smart Install is disabled on a device, the **vstack director ip_address** and **vstack basic** global configuration commands are not allowed.
 - If you disable Smart Install on the director and there were Smart Install DHCP IP addresses configured, you need to manually unconfigure them.
 - To re-enable Smart Install on the device, enter the **vstack** global configuration command.
- Image-only or configuration-only upgrades cannot be performed on IBCs running an image prior to Cisco IOS Release XE 3.6.0E. If an IBC is configured for an image-only or configuration-only upgrade but the IBC does not support an upgrade, the following cases apply:
 - The Director is configured to perform an image-only upgrade for the client.
Prior to Cisco IOS Release XE 3.6.0E, IBC did not receive the configuration path and the configuration-only upgrade failed, but the image upgrade proceeded and IBC reloaded.
Although the image upgrades, Cisco does not claim this process to be “Image-only” because IBC tries to download the configuration file and fails, displaying error messages.
 - The Director is configured to perform a configuration-only upgrade for the client.
Prior to Cisco IOS Release XE 3.6.0E, the configuration upgrade proceeded but IBC did not receive the image path, hence the image upgrade failed, and IBC did not reload.

Most configuration commands are visible and can be entered on the director or on a client, but only the ones configured on the director take effect. If you enter commands on a client switch, they do not take effect now, but if the client later becomes the director, the commands are then valid.

DHCP Configuration Guidelines

- Although we recommend that the director be configured to act as DHCP server for the clients, Smart Install can also use an external DHCP server. If you use an external device as DHCP server, you could configure the DHCP server to send option 125/sub-option 16 for the director IP address to avoid the possibility of fake DHCP servers.
- We recommend configuring a Cisco IOS DHCP server to **remember** IP bindings to ensure that devices in the Smart Install network retain the same IP address in the event of a network or device reload.
- In networks that do not use DHCP to assign IP addresses to the clients, you must configure the IP address of the director on each client switch.
- In a Smart Install network, we recommend not to configure DHCP snooping and DHCP relay on the same interface of the switch.

Configuring the DHCP Server

To perform zero-touch updates, the Smart Install network must be running DHCP. The DHCP server might be the director, another Cisco device running Cisco IOS, or a non-Cisco 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.

Use one of the following procedures to set up a Cisco device as DHCP server, or if you choose to configure a non-Cisco third-party device as DHCP server, follow the instructions in the product documentation for configuring a network address and a TFTP server.

**Note**

You should not configure any client switches participating in Smart Install as the DHCP server.

- [Configuring the Director as the DHCP Server, page 2-5](#)
- [Configuring Another Device as DHCP Server, page 2-7](#)

**Note**

If the DHCP server is the director or another Cisco IOS device and the network reloads, it is possible that DHCP could assign new IP addresses to the devices. This is an unlikely occurrence, but if it does happen, you might need to reassociate the director and client switches by manually entering the director IP address on the director or the client switches. To prevent this occurrence, configure the DHCP server to remember the IP bindings by entering the **ip dhcp remember** global configuration command or the **remember** DHCP pool configuration command.

Configuring the Director as the DHCP Server

You can configure the director as 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 startup-vlan <i>vlan_value</i>	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	vstack dhcp-localserver <i>poolname</i>	Creates a name for the Smart Install DHCP server address pool, and enter vstack DHCP pool configuration mode.

	Command	Purpose
Step 6	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 7	default-router <i>ip_address</i>	Specifies the IP address of the DHCP default router for the pool. Note You can use the vstack startup-vlan global configuration command to specify another VLAN that should be used for Smart Install management.
Step 8	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 2-8.
Step 9	exit	Returns to global configuration mode.
Step 10	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. This command is supported in Cisco IOS Release 12.2(53) or later on switches and in Cisco IOS Release 15.1(3)T or later on routers.
Step 11	end	Returns to privileged EXEC mode.
Step 12	copy running-config startup config	(Optional) Saves your entries in the configuration file.
Step 13	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 automatically enabled on the director. Therefore, you do not need to enable it when the director is the DHCP server.

Configuring Another Device as DHCP Server

If the Smart Install director is not the DHCP server, you can use the traditional 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* from Cisco.com. This procedure shows the minimum steps that you need to perform to configure a DHCP server.


Note

Do not configure a client switch as DHCP server. If you configure DHCP server commands on a client switch, the switch will assign IP addresses, and will not be able to use Smart Install.

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.
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 a client 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)# 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 automatically enabled on it. When there is a relay agent between the DHCP server and the director, you must enable DHCP snooping on the relay agent.

**Note**

DHCP relay is not supported on interfaces connected to vStack VLAN on which DHCP snooping is enabled.

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

- **ip dhcp snooping**
- **ip dhcp snooping vlan** *vlan-id* for 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)

Configuring the TFTP Server

Smart Install stores image, configuration files, and post install files on a TFTP server. The director can function as the TFTP server, eliminating the need for an external TFTP-serving device. If the director is the TFTP server, image, configuration files and post install 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 (non-Cisco) device, you should disable the server option to change the name of a file if another file is created with the same name. Otherwise, duplicate imagelist files might be created.

In Catalyst 6500 Supervisor Engine 2T switches, flash size supports onboard and external disks to download the image, the configuration file and post install file.

When selecting the director to be the TFTP server, follow these:

- 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, configuration files and the post install files required for client switches.
- There must be sufficient available flash memory on the director to hold the client Cisco IOS images and configuration files and post install files. The Cisco IOS image files vary in size, depending on the client product IDs and size of the images being installed.
- When the director is the TFTP server, a copy of the configuration file for each client is stored in the root directory of the flash file system on the director. There must be sufficient space for each planned client.
- Most director devices have sufficient flash memory to hold one client Cisco IOS image, a small number of client configuration files and post install files. For example, the Catalyst 3750 switch can have a maximum flash size of 64 MB, which accommodates only 4 or 5 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.

In more recent IOS releases, you do not need to configure the director as TFTP server. The director automatically gets the required image, configuration files and post install files and acts as the TFTP server when you specify **flash:** as the location from which to retrieve the files.

For example, for zero-touch updates of a default image and a configuration file, entering these commands on the director automatically configures the director as the TFTP server and enables the director DHCP server to provide these files to the clients.

```
vstack config flash:new_configuration_file
vstack image flash:image_name.tar
vstack script flash: post_install.txt
```

Establishing a Remote Client Session

You can perform configuration tasks on the client through a remote connection from the director. From the director, enter the **vstack attach** *{client - index}* | *{client IP address}* command in EXEC mode to attach to a client interface and temporarily enable it as director. Select a client by either choosing from a list that shows the active clients that are available within the Smart Install network or by entering the client IP address.

The client index list is dynamically generated in the Cisco IOS help text. If the director device is not rebooted, then the client-index is retained and it can be used in future configurations.

Configuring a Network with Single or Mixed Switch Types

- [Configuring a Network That Includes a Single Switch Type, page 2-9](#)
- [Using Built-In Groups to Configure a Mixed Network with Two Switch Types, page 2-12](#)

Configuring a Network That Includes a Single Switch Type

When all client switches in the Smart Install network are the same switch product ID and are performing the same functions, they would use the same image, the same seed (base) configuration file and same post install file. In this case, you can configure a default image, a seed configuration file, and the same post install file for all clients in the network.

Beginning in privileged EXEC mode, follow these steps on the director to set the default image and configuration file, and the post install file for all clients in the network:

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	vstack director <i>ip_address</i>	Configures the device as 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 startup-vlan <i>vlan_value</i>	Specifies the default VLAN that the director should use for Smart Install management.

	Command	Purpose
Step 5	vstack image { flash: <i>image_name.tar</i> tftp://location <i>image_name.tar</i> }	<p>Enters the location and image.</p> <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> flash:<i>image_name.tar</i>—Enter if the director is the TFTP server and the image is in the director flash memory. <p>Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the .tar extension is not available.</p> <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:.</p> <p>Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the .tar extension is not available.</p> <ul style="list-style-type: none"> tftp://location <i>image_name.tar</i> <i>image_name.tar</i>—Enter the name of the default image tar file for clients in the network.
Step 6	vstack config { flash: <i>config.txt</i> tftp://location <i>config.txt</i> }	<p>Enters the location and the default configuration file name. The configuration file is a text file that contains the configuration file to be downloaded to the client.</p> <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> For location, enter flash: if the TFTP server is the director and the configuration file is in the director flash memory. <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:.</p> <ul style="list-style-type: none"> For location, enter tftp: if the TFTP server is not the director or if the file is not in the director flash memory. In this case, enter tftp://director ip_address. <i>config.txt</i>—Enter the filename of the default seed configuration file for clients in the network.

	Command	Purpose
Step 7	vstack script { flash: <i>post_install.txt</i> tftp://location <i>post_install.txt</i> }	<p>Enters the location of the post install script file for the default group. The post install file is a text file that contains the post install CLI commands to be downloaded to the client.</p> <p>Note Although you must provide the image or the config, or the image and the config, the post install script is optional.</p> <p>this comment applies to all locations below where post-install configuration is described</p> <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, nvram:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> For location, enter flash: if the TFTP server is the director and the post install file is in the director flash memory. <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:</p> <ul style="list-style-type: none"> For location, enter tftp: if the TFTP server is not the director or if the file is not in the director flash memory. In this case enter tftp://director ip_address. <i>post_install.txt</i>—Enter the filename of the default post install file for clients in the network.
Step 8	end	Returns to privileged EXEC mode.
Step 9	copy running-config startup config	(Optional) Saves your entries in the configuration file.
Step 10	show vstack config	Verifies the configuration.

A client switch sends an error message if it is unable to download an image, a configuration file or post install file due to miscommunication, if either of the following apply:

- An image, configuration file, or post install file is unavailable.
- If a join window is configured and the DHCP acknowledgment occurs outside the configured time frame.

If a Cisco device is being used as the TFTP server, you should configure it as described in the [“Configuring the TFTP Server”](#) section on page 2-8.

This example shows how to configure a default image and configuration file for a Smart Install network if the director is the TFTP server and the default image, configuration file and post install file are in the director flash memory:

```
Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# vstack image flash:c2960-lanbase-tar.122-52SE.tar
```

```
Director(config)# vstack config flash:2960lanbase_config.txt
Director(config)# vstack script flash:2960lanbase_post_install.txt
Director(config)# end
```

This example shows how to configure a default image, configuration file, and post install file when the TFTP server is not the director:

```
Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# vstack image tftp://101.122.33.10/c2960-lanbase-tar.122-52SE.tar
Director(config)# vstack config tftp://101.122.33.10/2960LANBase_config.txt
Director(config)# vstack script tftp://101.122.33.10/2960LANBase_post_install.txt
Director(config)# end
```

Using Built-In Groups to Configure a Mixed Network with Two Switch Types

You can use built-in groups in a Smart Install network to configure a group of switches that have one product ID with an image, configuration file, and post install file, and to configure a second group of switches that have another product ID with another image, configuration file, and post install file. You could also have other clients in the network that do not belong to either of these groups and could use the default image, configuration file, and post install file if they match the default product ID.

Beginning in privileged EXEC mode, follow these steps on the director to configure the image, configuration file, and post install file for two different product IDs in the Smart Install network:



Note

If the device is already configured as an SMI director, Steps 1 thru 5 are optional. If the device is already configured as a director, skip to Step 6 for on-demand updates.

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	vstack director <i>ip_address</i>	Configures the device as 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 startup-vlan <i>vlan_value</i>	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	vstack group built-in <i>product_family1</i> <i>port_config</i>	Identifies the first built-in group product ID, and enters Smart Install group configuration mode for the group.

	Command	Purpose
Step 6	image <i>location image_name.tar</i>	<p>Enters the location and image name for group 1.</p> <ul style="list-style-type: none"> For location, enter flash: (if the TFTP server is the director and the file is stored in the director flash memory). <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:.</p> <ul style="list-style-type: none"> For location, enter tftp: and the location of the configuration file for group 1 if the file is not stored in the director flash memory. <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <p>Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the .tar extension is not available.</p> <ul style="list-style-type: none"> <i>image_name.tar</i>—Enter the name of the image tar file for clients in group 1.
Step 7	config <i>location config_filename</i>	<p>Enters the location and configuration file for group 1.</p> <ul style="list-style-type: none"> For location, enter flash: (if the TFTP server is the director and the file is stored in the director flash memory). <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:.</p> <ul style="list-style-type: none"> For location, enter tftp: and the location of the configuration file for group 1 if the file is not stored in the director flash memory. <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> <i>config_filename</i>—Enter the filename of the configuration file for group 1.

	Command	Purpose
Step 8	script <i>location post_install_filename</i>	<p>Enters the location and post install file for group 1.</p> <p>Note Although you must provide the image or the config, or the image and the config, the post install script is optional.</p> <ul style="list-style-type: none"> For location, enter flash: (if the TFTP server is the director and the file is stored in the director flash memory). <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:.</p> <ul style="list-style-type: none"> For location, enter tftp: and the location of the post install file for group 1 if the file is not stored in the director flash memory. <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> <i>post_install_filename</i>—Enter the filename of the post install file for group 1.
Step 9	exit	Returns to global configuration mode.
Step 10	vstack group built-in <i>product_family2 port_config</i>	Identifies the second built-in group product ID, and enters Smart Install group configuration mode for the group.
Step 11	image <i>location image_name.tar</i>	<p>Enters the location and image name for group 2.</p> <ul style="list-style-type: none"> For location, enter flash: (if the TFTP server is the director and the file is stored in the director flash memory). <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:.</p> <ul style="list-style-type: none"> For location, enter tftp: and the location of the configuration file for group 2 if the file is not stored in the director flash memory. <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <p>Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the .tar extension is not available.</p> <ul style="list-style-type: none"> <i>image_name.tar</i>—Enter the name of the image tar file for clients in group 2.

	Command	Purpose
Step 12	config <i>location config_filename</i>	<p>Enters the location and configuration file for group 2.</p> <ul style="list-style-type: none"> For location, enter flash: (if the TFTP server is the director and the file is stored in the director flash memory). <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:.</p> <ul style="list-style-type: none"> For location, enter tftp: and the location of the configuration file for group 2 if the file is not stored in the director flash memory. <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> <i>config_filename</i>—Enter the filename of the configuration file for group 2.
Step 13	script <i>location post_install_filename</i>	<p>Enters the location and post install file for group 2.</p> <p>Note Although you must provide the image or the config, or the image and the config, the post install script is optional.</p> <ul style="list-style-type: none"> For location, enter flash: (if the TFTP server is the director and the file is stored in the director flash memory). <p>Note Instead of flash:, you can also enter flash0:, flash1:, or usb:.</p> <ul style="list-style-type: none"> For location, enter tftp: and the location of the post install file for group 2 if the file is not stored in the director flash memory. <p>Note Although visible in the command-line help, these options are not supported: ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> <i>post_install_filename</i>—Enter the filename of the post install file for group 2.
Step 14	end	Returns to privileged EXEC mode.
Step 15	copy running-config startup config	(Optional) Saves your entries in the configuration file.
Step 16	show vstack group built-in detail	Verifies the configurations.

A client switch sends an error message if it cannot download an image, configuration file, or post install file due to misconfiguration, provided either of the two apply:

- The image, configuration file, or post install file is unavailable.
- If a join window is configured and the DHCP acknowledgment occurs outside of the configured time frame.

This example uses built-in groups to configure all 3560 24-port switches in the network with one image, configuration file, and post install file, it configures all 2960 24-port switches in the network with another image, configuration file, and post install file.

```
Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# vstack group built-in 3560 24
Director(config-vstack-group)# image tftp://101.122.33.10/c3560-ipbase1mk9-tar.122-52.SE.tar
Director(config-vstack-group)# config tftp://101.122.33.10/3560-24-ipbase_config.txt
Director(config-vstack-group)# script tftp://101.122.33.10/3560-24-ipbase_post_install.txt
Director(config)# exit
Director(config)# vstack group built-in 2960 24
Director(config-vstack-group)# image tftp://101.122.33.10/c2960-lanbasek9-tar.122-52.SE.tar
Director(config-vstack-group)# config tftp://101.122.33.10/2960-24-LANbase_config.txt
Director(config-vstack-group)# script tftp://101.122.33.10/3560-24-ipbase_post_install.txt
Director(config)# end
```

Updating On-Demand to a New Image or Configuration

When a director is established and default or group images and configuration files are defined and there is connectivity between the director and a client switch, you can perform on-demand image and configuration updates. You can use this capability on a new client switch to make it Smart Install capable or on existing clients to update the image or configuration.

The process of triggering an on-demand upgrade for Catalyst 4500 switch IBC differs from other platforms. The difference resides with the ISSU upgrade option. In a typical upgrade of a Catalyst 3500 platform, let's say, the IBC reloads after the upgrade. In contrast, to prevent the downtime for a Catalyst 4500 IBC, you can complete an On-demand upgrade by selecting the ISSU option of the **vstack download-image** CLI.

You can initiate an on-demand download if the switch has a valid IP interface. For on-demand download on a switch that is not Smart Install capable, the switch must also have an enable password configured.



Note

In Catalyst 3850 and 3650 switches, the client should be in installed mode to update the image.

Beginning with Cisco IOS Release 12.2(58)SE, 15.1(1)SY, 15.0(2)SE and later, and 3.2(0)SE and later, 3.6.(0)E, and 15.2.(2)E, you can perform on-demand updates to multiple clients simultaneously.

Beginning in privileged EXEC mode, follow these steps on the director to perform an on-demand update on a client switch.

	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 startup-vlan <i>vlan_value</i>	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	end	Returns to privileged EXEC mode.

	Command	Purpose
Step 6	<p>vstack download-image tar <i>image_URL</i> {<i>ip_address</i> index name} <i>remote_switch_password</i> [override] reload [in time]</p> <p>or</p> <p>vstack download-image built-in <i>product_family port_config</i> <i>remote_switch_password</i> [override] reload [in time]</p> <p>or</p> <p>vstack download-image {i<i>magelist_file_URL</i> {<i>ip_address</i> index name} built-in <i>product_family port_config</i>} <i>remote_switch_password</i> [override] issu [allow-reload] [in time]</p>	<p>Starts an on-demand tar image download on a Smart Install client switch:</p> <ul style="list-style-type: none"> Enter the <i>image_URL</i> and location and the IP address of the client. or Enter the <i>imagelist_file</i> and location and the IP address of the client (for releases earlier than 12.2(55)SE). <i>ip_address</i>—Enter the IP address of the client switch. index name—Enter the index name from the director database for multiple clients or a range of clients (for example, 1-3, 4). This feature was added in Cisco IOS Release 12.2(58)SE, 15.1(1)SY, 15.0(2)SE and later, or 3.2(0)SE and later. Enter built-in, and select the product family and port configuration from the command-line help. <p>Note Use this option if you have identified the image for the specified built-in group by entering the image location image_name.tar Smart Install group configuration command.</p> <ul style="list-style-type: none"> <i>remote_switch_password</i> —Enter the password for the client switch. <p>Note A password is needed only if the switch is running a Cisco IOS image earlier than 12.2(52)SE. It is not required for switches already in the Smart Install network. If you are upgrading the image for multiple clients, all clients must have the same password or must have no password (None).</p> <ul style="list-style-type: none"> (Optional) override—Overrides the existing image on the client switch. (Optional) issu attempts to upgrade using ISSU. <i>allow-reload</i> (visible only for an ISSU upgrade) allows SMI to reload the switch to complete the upgrade process if ISSU could not be performed on that particular IBC. (Optional) in time specifies the time to reload the switch using the format hh:mm. The range is from 00:00 to 23:59. If no time is specified, the reload occurs when you exit the CLI.

	Command	Purpose
Step 7	vstack download-config { <i>config_URL ip_address</i> built-in <i>product_family port_config</i> } <i>remote_switch_password startup</i> [reload] [in time]	<p>Starts an on-demand configuration download on a Smart Install client switch:</p> <ul style="list-style-type: none"> Enter the configuration filename and location and the IP address of the client Enter built-in and select the product family and port configuration from the command-line help. <p>Note Use this option if you have identified the configuration for the specified built-in group by entering the config location config_filename Smart Install group configuration command.</p> <p>The remaining keywords and arguments have these meanings:</p> <ul style="list-style-type: none"> <i>remote_switch_password</i> —Enters the password for the client switch. <p>Note A <i>password</i> is required only for switches that are not Smart Install capable. It is not required for switches already in the Smart Install network.</p> <ul style="list-style-type: none"> startup—Applies the configuration to the switch startup configuration. (Optional) reload—Reloads the switch. (Optional) in time—Specifies the <i>time</i> to reload the switch using the format hh:mm. The range is from 00:00 to 23:59. If no time is specified, the reload occurs when you exit the CLI.
Step 8	show vstack download-status	Checks status of the download.

This example shows how to configure a Smart Install director to schedule an on-demand download of an image and configuration file to the client switch with the IP address 1.1.1.30 and password of *mypassword*. The download takes place in 6 hours and 30 minutes.

```
Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# end
Director# vstack download-image tar tftp://101.122.33.10/c2960-lanbasek9-tar.122-52.SE.tar
1.1.1.30 mypassword reload in 06:30
Director# vstack download-config tftp://101.122.33.10/2960LANBase_config.txt 1.1.1.30 my
password reload in 06:30
```

This example shows the same configuration for a built-in group.

```
Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# end
Director# vstack download-image built-in 3750 24 mypassword override reload in 6:30
Director# vstack download-config built-in 3750 24 mypassword reload in 06:30
Using Custom Groups to Configure Groups Based on Connectivity, MAC Address, Stack Number,
or Product ID
```

You can configure a custom group to set up the image and configuration file for all client switches that match connectivity, MAC address, stack number, or product IDs for switches in a stack.

A client switch sends an error message if it cannot download an image or configuration file due to misconfiguration, if the image or configuration file is not available, or if a join window is configured and the DHCP acknowledgment occurs outside of the configured time frame.

Configuring Custom Group Based on Connectivity

You can configure a custom group based on the connectivity or topology of switches in a Smart Install network. For example, you would use a connectivity match to configure a group of switches that are connected to the director through a single interface or switches that are connected to the director through a specific intermediate switch. A connectivity match takes priority over product ID or stack number custom groups and over built-in groups, but not over groups based on MAC addresses. Switches that do not match the connectivity configuration would acquire the configuration file, post install file, and image in either a built-in group or through the default configuration.

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

	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 startup-vlan <i>vlan_value</i>	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	vstack group custom <i>group_name</i> connectivity	Identifies a custom group based on a connectivity match, and enters Smart Install group configuration mode for the group.
Step 6	match host <i>ip_address</i> interface <i>interface-id</i>	Identifies the client switches for the custom group: <ul style="list-style-type: none"> host <i>ip_address</i>—The IP address of the upstream neighbor of the client (this could be the director or an intermediate device). interface <i>interface-id</i>—The interface on the upstream neighbor to which the clients is connected. The interface ID must be the full identifier for the interface, such as GigabitEthernet 2/0/1.

	Command	Purpose
Step 7	image <i>location image_name.tar</i>	<p>Enters the location and image 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 stored in the director flash memory, or enter tftp: and the location of the imagefile: Instead of flash:, 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> <p>Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the .tar extension is not available.</p> <ul style="list-style-type: none"> <i>image_name.tar</i>—The image tar file that you want to download. For a switch stack, there could be multiple images for members of the stack.
Step 8	config <i>location 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 stored in the director flash memory, or enter tftp: and the location of the configuration file. Instead of flash:, 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_filename.</i>—The filename of the configuration file for the group.
Step 9	config <i>location post_install_filename</i>	<p>Enters the location and post install file for the custom group.</p> <p>Note Although you must provide the image or the config, or the image and the config, the post install script is optional.</p> <ul style="list-style-type: none"> <i>location</i>—Enter flash: if the TFTP server is the director and the file is stored in the director flash memory, or enter tftp: and the location of the post install file. Rather than flash:, you can also enter flash0:, flash1:, or usb:. <p>Note Although visible in the command-line help, these options are unsupported: flash1:, ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> <i>post_install_filename</i>—The filename of the post install file for the group.
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 vstack group custom detail	Verifies the configuration.

This example creates a custom group named *testgroup2* for all switches that are connected to the specified host and interface and configures the group to use the specified image file and configuration.

```
Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# vstack group custom testgroup2 connectivity
Director(config-vstack-group)# match host 1.1.1.10 interface GigabitEthernet 1/0/3
Director(config-vstack-group)# image tftp://101.122.33.10/c3750-ipbase-tar.122-52.SE.tar
Director(config-vstack-group)# config tftp://101.122.33.10/3750-24-ipbase_config.txt
Director(config-vstack-group)# script tftp://101.122.33.10/3750-24-ipbase_post_install.txt
Director(config-vstack-group)# exit
Director(config)# end
```

Configuring a Custom Group Based on MAC Address

You can configure a custom group based on the MAC addresses of switches in a Smart Install network. A MAC address match takes priority over any other matches. The switches that do not match the MAC addresses in the group would get the configuration, post install file, and image for another group or the default configuration.

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

	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 startup-vlan <i>vlan_value</i>	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	vstack group custom <i>group_name mac</i>	Identifies a custom group based on a MAC address match, and enters Smart Install group configuration mode for the group.
Step 6	match <i>mac_address</i>	<p>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.</p> <p>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 must be able to use the same image and configuration file.</p>

	Command	Purpose
Step 7	image <i>location image_name.tar</i>	<p>Enters the location and image 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 stored in the director flash memory, or enter tftp: and the location of the image. Instead of flash:, 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> <p>Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the .tar extension is not available.</p> <ul style="list-style-type: none"> <i>image_name.tar</i>—The image tar file that you want to download. For a switch stack, there could be multiple images for members of the stack.
Step 8	config <i>location 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 stored in the director flash memory, or enter tftp: and the location of the configuration file. Instead of flash:, 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_filename</i>—The filename of the configuration file for the group.

	Command	Purpose
Step 9	<code>script location post_install_filename</code>	<p>Enters the location and post install file for the custom group.</p> <p>Note Although you must provide the image or the config, or the image and the config, the post install script is optional.</p> <ul style="list-style-type: none"> <i>location</i>—Enter flash: if the TFTP server is the director and the file is stored in the director flash memory, or enter tftp: and the location of the post install file. Instead of flash:, you can also enter flash0:, flash1:, or usb: <p>Note Although visible in the command-line help, these options are unsupported: flash1:, ftp:, http:, https:, null:, nvr:, rcp:, scp:, system:, tmpsys:.</p> <ul style="list-style-type: none"> <i>post_install_filename</i>—The filename of the post install file for the group.
Step 10	<code>end</code>	Returns to privileged EXEC mode.
Step 11	<code>copy running-config startup config</code>	(Optional) Saves your entries in the configuration file.
Step 12	<code>show vstack group custom detail</code>	Verifies the configuration.

This example creates a custom group named *testgroup3* that includes the three switches identified by MAC address, and configures the group to use the specified image file and configuration.

```

Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
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/c3750-ipbase-tar.122-52.SE.tar
Director(config-vstack-group)# config tftp://101.122.33.10/3750-24-ipbase_config.txt
Director(config-vstack-group)# script tftp://101.122.33.10/3750-24-ipbase_post_install.txt
Director(config-vstack-group)# exit
Director(config)# end

```

Configuring a Custom Group Based on a Stack Number

You can configure a custom group based on the number of the switch in the stack. Any switch in a stack that matches the stack number and product ID gets the same configuration.



Note

A client switch in a stack can be updated only when it belongs to a custom stack group. It cannot belong to the default group.

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

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	vstack director <i>ip_address</i>	Configures the device as 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 startup-vlan <i>vlan_value</i>	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	vstack group custom <i>group_name</i> stack	Identifies a custom group based on matching the stack number and enter Smart Install group configuration mode for the group.
Step 6	match <i>switch_number</i> <i>stack</i> <i>product_family</i> <i>port_config</i>	Identifies the client switches for the custom group: <ul style="list-style-type: none"> • <i>switch_number</i>—Number of the switch in the stack. The range is from 1 to 9. • <i>product_family</i>—Select the stack product family from the command-line help. • <i>port_config</i>—Switch port configuration. To see the available port configurations, enter a? after the product family.
Step 7	image <i>location</i> <i>image_name.tar</i>	Enters the location and image 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 stored in the director flash memory or enter tftp: and the location of the imagefile. Instead of flash:, 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> <p>Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the .tar extension is not available.</p> <ul style="list-style-type: none"> • <i>image_name.tar</i> is the image tar file that you want to download.

	Command	Purpose
Step 8	<code>config location config_filename.</code>	<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 stored in the director flash memory or enter tftp: and the location of the configuration file for the group. Instead of flash:, 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_filename</i>—The filename of the configuration file for the group.
Step 9	<code>script location post_install_filename</code>	<p>Enters the location and post install file for the custom group.</p> <p>Note Although you must provide the image or the config, or the image and the config, the post install script is optional.</p> <ul style="list-style-type: none"> <i>location</i>—Enter flash: if the TFTP server is the director and the file is stored in the director flash memory or enter tftp: and the location of the post install file. Instead of flash:, 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> <p><i>post_install_filename</i>—The filename of the post install file for the group.</p>
Step 10	<code>end</code>	Returns to privileged EXEC mode.
Step 11	<code>copy running-config startup config</code>	(Optional) Saves your entries in the configuration file.
Step 12	<code>show vstack group custom detail</code>	Verifies the configuration.

This example creates a custom group named *testgroup* for all switches that are identified as switch member 2 in a Catalyst 3750 24-port stack to use the specified image, configuration file, and post install file.

```
Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# vstack group custom testgroup stack
Director(config-vstack-group)# image tftp://101.122.33.10/c3750-ipbase-tar.122-52.SE.tar
Director(config-vstack-group)# config tftp://101.122.33.10/3750stack_config.txt
Director(config-vstack-group)# script tftp://101.122.33.10/3750stack_post_install.txt
Director(config-vstack-group)# match 1 3750 24poe
```

```

Director(config-vstack-group)# match 2 3750 24poe
Director(config-vstack-group)# match 3 3750 24poe
Director(config-vstack-group)# exit
Director(config)# end

```

Custom Group Based on Product ID

You can configure a custom group based on the product ID of switches in a Smart Install network. Switches that do not match the product ID in the group can be provided the configuration file, post install file and image for another group, or the default configuration.

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

	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 startup-vlan <i>vlan_value</i>	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	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.
Step 6	match <i>product-id</i>	<p>Enters the product ID of the client switches in the custom group.</p> <p>Note The product ID can be the same as that of a built-in group. If a client matches a built-in group and a custom group, the custom group takes precedence.</p>
Step 7	image <i>location image_name.tar</i>	<p>Enters the location and image 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 stored in the director flash memory, or enter tftp: and the location of the image. Instead of flash:, 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> <p>Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the .tar extension is not available.</p> <ul style="list-style-type: none"> <i>image_name.tar</i>—The image tar file that you want to download. For a switch stack, there could be multiple images for members of the stack.

	Command	Purpose
Step 8	<code>config location config_filename.</code>	<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 stored in the director flash memory, or enter tftp: and the location of the configuration file. Instead of flash:, 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_filename</i>—The filename of the configuration file for the group.
Step 9	<code>script location post_install_filename</code>	<p>Enters the location and post install file for the custom group.</p> <p>Note Although you must provide the image or the config, or the image and the config, the post install script is optional.</p> <ul style="list-style-type: none"> <i>location</i>—Enter flash: if the TFTP server is the director and the file is stored in the director flash memory, or enter tftp: and the location of the post install file. Instead of flash:, 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>post_install_filename</i>—The filename of the post install file for the group.
Step 10	<code>end</code>	Returns to privileged EXEC mode.
Step 11	<code>copy running-config startup config</code>	(Optional) Saves your entries in the configuration file.
Step 12	<code>show vstack group custom detail</code>	Verifies the configuration.

This example creates a custom group named *testgroup4* that includes switches that match the product ID WS-C2960-48TC-L, and configures the group to use the specified image file, configuration file, and the post install file.

```

Director# configure terminal
Director(config)# vstack director 1.1.1.20
Director(config)# vstack basic
Director(config)# vstack group custom testgroup4 product-id
Director(config-vstack-group)# match WS-C2960-48TC-L
Director(config-vstack-group)# image tftp://101.122.33.10/c2960-lanbase-tar.122-52.SE.tar
Director(config-vstack-group)# config tftp://101.122.33.10/c2960-lanbase_config.txt
Director(config-vstack-group)# script tftp://101.122.33.10/c2960-lanbase_post_install.txt
Director(config-vstack-group)# exit
Director(config)# end

```

Managing Client Configuration Files

You can manage the client configuration files through the director that is set up as TFTP server, or through a third-party TFTP server. Only supported devices that are Smart Install capable can perform the role of director and save client configuration files to a repository. See [Appendix A, “Supported Devices for Smart Install”](#) to see a list of devices that can be a Smart Install network director.

The backup feature does not need to be enabled; it is on by default. However, if you have disabled it and want to save the configuration files to a repository, use the **vstack backup** global configuration command to enable the feature. After enabling the backup feature, use the **vstack backup file-server** global configuration command to specify a repository on the TFTP server to save the configurations files. The repository will define where the files are saved.

Every time the **write memory** privileged EXEC command is issued on the client, its configuration files are saved to the director-TFTP server or third-party TFTP server.

These names are assigned to the client backup files:

- *Hostname*MAC address.rev1
- *Hostname*MAC address.rev2 (most recent version)

When the client undergoes a hostname change, the configuration files are not backed up until you enter the **write memory** command. When a new mapping is created between the client with a new hostname and the two configuration files, the existing mapping is removed. On a third-party TFTP server, after a new mapping is created between the client with a new hostname and the two configuration files, the files are not removed.



Note

Do not remove the backed-up client files from the third-party TFTP server repository. Otherwise, the backup feature does not work properly.

Backing Up Files after Loss of Connection

If the client-to-director connection is lost after issuing the **write memory** command, the back-up process fails. You must reestablish the connection so that the client file is backed up on the director. If you entered the **write memory** command more than once, the files associated with the last **write memory** command event are backed up on the director. If the client reloads or fails before receiving feedback that the backup was successful, any changes made to the client startup do not take effect until you reload the client.

Extracting and Displaying Tar Files

When the client sends a tar file to the director, you can use the **vstack untar source-url [destination-url]** command in EXEC mode to extract and display the files in a specified location. However, when the client sends a tar file to a third-party TFTP server, you cannot use the director to extract and display the files.

The tar files are placed into the preconfigured directory within the repository. If the directory is not configured, the files are extracted and displayed in the director root directory flash memory.

Other Configuration Options

- [Disabling Smart Install on a Device, page 2-29](#)
- [Managing File Downloads on Clients, page 2-29](#)
- [Configuring a Client Hostname Prefix, page 2-30](#)
- [Configuring Additional Smart Install Management VLANs, page 2-30](#)
- [Configuring a Group for Standalone Catalyst 4500 Series Switch, page 2-31](#)
- [Support for Post-install Operations, page 2-38](#)

Disabling Smart Install on a Device

When a director is configured and a client joins the Smart Install network, Smart Install is automatically enabled on these devices. Beginning with Cisco IOS Release 12.2(58)SE, 15.1(1)SY, 15.0(2)SE and later, or 3.2(0)SE and later, you can disable Smart Install on a device and also shut down its Smart Install TCP ports by entering the **no vstack** global configuration command on the client or director. When Smart Install is disabled on a device, any Smart Install configuration on it remains in the running configuration but does not take effect while Smart Install is disabled.

When Smart Install is disabled on a device, the **vstack director ip_ address** and **vstack basic** global configuration commands are not allowed on the device. To reenable Smart Install on a device, enter the **vstack** global configuration command.

Managing File Downloads on Clients

You can use download management to download image and configuration files to a client. For non-Smart Install clients, an HTTP emulation process manages file downloads. For Smart Install capable clients, file downloads are performed when a request is received from the director.

Download Management for Non-Smart Install Clients

For non-Smart Install capable clients, you can initiate downloads from the director through HTTP emulation. The client initiates a new connection to the director, and the director initiates a new HTTP connection to the non-Smart Install client on port 80. The image file name and configuration file name from the group database is gathered, and a download is issued on the non-Smart Install client through HTTP emulation. After the download is complete, a **reload** is issued on the client.

**Note**

Stackable switches must have the correct configuration present because they do not have a default image and configuration.

Download Management for Smart Install Clients

For Smart Install-capable clients to receive image and configuration files, the client performs a **write erase** and **reload**. The client establishes connectivity with the director and gathers information about the image and the configuration files. When this information is gathered, the client begins the update. When the update is complete, the Smart Install-capable client **reboots**.

Configuring a Client Hostname Prefix

When configuring switches out of the box, to help identify the switches and their locations in the network, you can enter this global configuration command on the director:

```
vstack hostname-prefix prefix
```

You can then enter a prefix to the hostname for clients in the Smart Install network. The last part of the switch hostname for a switch that had a DHCP request snooped through the director contains the last 3 bytes of the switch MAC address.

This example shows how to configure the hostname *Cisco* for a client that has been DHCP-snooped. The second display shows the resulting switch hostname assignment:

```
Director(config)# vstack hostname-prefix Cisco
Director(config)# exit
```

If you then telnet to that switch from the director, the hostname is shown:

```
Director#
*Mar  1 17:21:43.281: %SYS-5-CONFIG_I: Configured from console by console
*Mar  1 17:21:52.399: %DHCP-6-ADDRESS_ASSIGN: Interface Vlan1 assigned DHCP address
172.16.0.17, mask 255.255.0.0, hostname
CISCO-bf.97c0#
```

Configuring Additional Smart Install Management VLANs

Client switches can be on any VLANs if you configure the director to snoop on the VLAN by entering the **vstack vlan** *vlan-id* global configuration command and if traffic from the VLAN flows through the director. The director can snoop on multiple VLANs extending to clients on different Layer 2 subnets.

By default, when the director is an Ethernet switch, VLAN 1 is the Smart Install management VLAN and the only VLAN that DHCP snoops on. You can, however, use the **vstack startup-vlan** global configuration command to specify another default VLAN.

You can add additional Smart Install management VLANs or a range of VLANs to participate in DHCP snooping. You can configure any number of Smart Install management VLANs.

```
vstack vlan vlan-id
```

This command is not supported when the director is a router. On a router, after you enable Smart Install with the **vstack basic** command, clients connected to any Layer 3 interface on the router will continue to communicate with Smart Install. Clients must have a default route to reach the director as specified in its DHCP pool.

Beginning in privileged EXEC mode, follow these steps on the director to configure a startup VLAN:

	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 vlan <i>vlan-id</i>	Specifies the VLAN for Smart Install management.

	Command	Purpose
Step 5	vstack startup-vlan <i>vlan_value</i>	Specifies the startup VLAN that the director should use for Smart Install management. Note Ensure that this VLAN is already present in the system as a VLAN for Smart Install management.
Step 6	no vstack startup-vlan	Removes the VLAN as the startup VLAN so that VLAN 1 now becomes the startup VLAN for Smart Install management.
Step 7	end	Returns to privileged EXEC mode.
Step 8	no vstack vlan	(Optional) Removes the earlier <i>vlan-id</i> VLAN from the Smart Install management VLAN list.
Step 9	copy running-config startup config	(Optional) Saves your entries in the configuration file.
Step 10	show vstack group custom detail	Verifies the configuration.

Configuring a Group for Standalone Catalyst 4500 Series Switch

Beginning with IOS XE 3.6.0 and IOS 15.2(2)E, the procedure to configure a built-in group for Catalyst 4500 series of switches has been updated. Because PoE and port number are capabilities of the line card and not the chassis, you must use the supervisor type to classify a switch rather than PoE or port number.

For details on the compatibility between Catalyst 4500 Switch Supervisor Engine and Chassis as well as compatibility between Catalyst 3560, 3750, 29xx and Chassis, SKU ID, and SKI, see [Supported Models for Smart Install, page B-1](#). If you want to use custom groups for the Catalyst 4500 series switch as Integrated Branch Client (IBC), you can use the following custom groups:

- Product ID based—Only the chassis ID can be used.
- MAC-based—Chassis MAC for a standalone Catalyst 4500 Series Switch and virtual MAC for VSS
- Connectivity-based

The following is a list of chassis that are supported by SMI as client:

- WS-C4503-E
- WS-C4506-E
- WS-C4507R-E
- WS-C4507R+E
- WS-C4510R-E
- WS-C4510R+E
- WS-C4900M
- WS-C4948
- WS-C4948-10GE
- WS-C4500X-32
- WS-C4500X-16

Restrictions and Guidelines

- A VSS system requires configuration in the startup-config while booting. For a zero-touch upgrade, no startup-config should exist; a zero-touch upgrade cannot be performed on VSS.
- ISSU is unsupported for a zero-touch upgrade.
- No images prior to IOS XE 3.6.0E can exist on the path between Integrated Branch Director (IBD) and 4k IBC.
- To support Catalyst 4500 IBC, the images on both IBD and IBC must be IOS XE 3.6.0E or later.
- No [explicit] limit exists for the number of Catalyst 4500 switch IBC that an IBD can support; the maximum number of supported IBCs remains unchanged, independent of the IBC platform.
- If a supervisor engine is not in IOS mode on an IBC, it is not upgraded; a supervisor engine must be in IOS mode.
- If an IBC, a line card is replaced by another line card, the IBC entry on IBD remains unchanged.
- While performing a configuration upgrade on a VSS IBC, notice that the configuration file must be compatible with that VSS IBC.
- When upgrading an image for a wireless IBC, we recommend that you use an external TFTP server, irrespective of any supported IBD. This takes lesser time.
- The **ip tftp source-interface** command should not exist in the IBC for normal SMI operations; this CLI interrupts normal TFTP operations.
- If portchannel is used on the IBD side and the IBC has zero configuration, **mac flip** messages are displayed on the IBC side.
- If you perform an image-only upgrade, the running configuration on the switch prior to reload (after the image is downloaded) is saved as the startup configuration. When the switch reboots, this startup config is loaded onto the switch.

The Procedure

Beginning in privileged EXEC mode, perform these steps to configure a group for a standalone Catalyst 4500 series switch:

	Command	Purpose
Step 1	Switch# config terminal	Enters global configuration mode.
Step 2	Switch(config)# vstack group built-in 4500 <i>supervisor type {chassis type all>}</i>	Enables group mode. <i>supervisor_type</i> is just one parameter. You must select from the list as the first example below illustrates. Use <i>chassis type</i> to configure the configuration (or image) for a particular chassis. Use <i>all</i> to configure all chassis supporting the <i>supervisor type</i> .
Step 3	Switch(config-vstack-group)# [no] config <i>path_to_config_file</i>	Configures the config file (i.e., <i>path_to_config_file</i>) for the group. Use the no keyword to unconfigure.
Step 4	Switch(config-vstack-group)# [no] image <i>path_to_image_file</i>	Configures the image file (i.e., <i>path_to_image_file</i>) for the group. Use the no keyword to unconfigure.

	Command	Purpose
Step 5	Switch(config-vstack-group)# [no] script <i>path_to_post_install_file</i>	Configures the post install file (i.e., <i>path_to_post_install_file</i>) for the group. Use the no keyword to unconfigure.
Step 6	Switch(config-vstack-group)# exit	Exits from group mode.
Step 7	Switch# show vstack group	Verifies the group changes.
Step 8	Switch# write mem	Saves the configurations.

This example shows how to configure a Catalyst 4500 group and verify with the **show vstack group** command:

```
Switch(config)# vstack group built-in ?
1783      1783 product family
1783BMS   1783BMS product family
2918      2918 product family
2960      2960 product family
2960c     2960c product family
2960cg    2960cg product family
2960g     2960g product family
2960plus  2960plus product family
2960s     2960s product family
2960s-fe  2960s-fe product family
2960x     2960x product family
2960xr    2960xr product family
2975      2975 product family
3560      3560 product family
3560c     3560c product family
3560cg    3560cg product family
3560e     3560e product family
3560g     3560g product family
3560x     3560x product family
3650      3650 product family
3750      3750 product family
3750e     3750e product family
3750g     3750g product family
3750x     3750x product family
3850      3850 product family
4500      4500 product family
4500x     4500x product family
4900      4900 product family
IE2000    IE2000 product family
IE3000    IE3000 product family
IE3010    IE3010 product family
nme-es    nme-es product family
sm-d-es2  sm-d-es2 product family
sm-d-es3  sm-d-es3 product family
sm-d-es3g sm-d-es3g product family
sm-es2    sm-es2 product family
sm-es3    sm-es3 product family
sm-es3g   sm-es3g product family
Switch(config)# vstack group built-in 4500 sup6-e 4507r-e
Switch(config-vstack-group)#

Switch(config)# vstack group built-in 4500 ?
sup6-e    sup6-e supervisor
sup6l-e   sup6l-e supervisor
sup7-e    sup7-e supervisor
sup7l-e   sup7l-e supervisor
sup8-e    sup8-e supervisor
```

```

Switch(config)# vstack group built-in 4500 sup8-e ?
  4503      4503 chassis type
  4506      4506 chassis type
  4507r+e   4507r+e chassis type
  4510r+e   4510r+e chassis type
  all       Configure all Chassis for this Sup

Switch(config)# vstack group built-in 4500 sup8-e 4506 ?
  <cr>

Switch(config)# vstack group built-in 4500 sup8-e 4506
Switch(config-vstack-group)# image bootflash:k10.tar
Switch(config-vstack-group)# config bootflash:mayagraw-4k-startup-config.txt
Switch(config-vstack-group)# exit
Switch(config)# exit
Switch# wr
Building configuration...

*Mar 19 23:16:09.869: %SYS-5-CONFIG_I: Configured from console by consoleCompressed
configuration from 8862 bytes to 3643 bytes[OK]
Switch#
Switch# show vstack group built-in detail configured
  *** Only Configured Groups will be shown ***
  -----
Group Name: sup8-e 4506
Image Name: bootflash:k10.tar
Config file name: bootflash:mayagraw-4k-startup-config.txt
No Script file specified
Switch#

```

Prior to Cisco IOS Release XE 3.6.0E the output of the **vstack group built-in** command would appear as follows:

```

Switch(config)# vstack group built-in ?
  1783      1783 product family
  1783BMS   1783BMS product family
  2918      2918 product family
  2960      2960 product family
  2960c     2960c product family
  2960cg    2960cg product family
  2960g     2960g product family
  2960plus  2960plus product family
  2960s     2960s product family
  2960s-fe  2960s-fe product family
  2960x     2960x product family
  2960xr    2960xr product family
  2975      2975 product family
  3560      3560 product family
  3560c     3560c product family
  3560cg    3560cg product family
  3560e     3560e product family
  3560g     3560g product family
  3560x     3560x product family
  3650      3650 product family
  3750      3750 product family
  3750e     3750e product family
  3750g     3750g product family
  3750x     3750x product family
  3850      3850 product family
  IE2000    IE2000 product family
  IE3000    IE3000 product family
  IE3010    IE3010 product family
  nme-es    nme-es product family

```

```

sm-d-es2    sm-d-es2 product family
sm-d-es3    sm-d-es3 product family
sm-d-es3g   sm-d-es3g product family
sm-es2      sm-es2 product family
sm-es3      sm-es3 product family
sm-es3g     sm-es3g product family

```

Starting with Cisco IOS Release XE 3.6.0E, the output of the **vstack group built-in** command would appear as follows (Notice lines in **bold** below):

```

Switch(config)# vstack group built-in ?
1783          1783 product family
1783BMS       1783BMS product family
2918          2918 product family
2960          2960 product family
2960c         2960c product family
2960cg        2960cg product family
2960g         2960g product family
2960plus      2960plus product family
2960s         2960s product family
2960s-fe      2960s-fe product family
2960x         2960x product family
2960xr        2960xr product family
2975          2975 product family
3560          3560 product family
3560c         3560c product family
3560cg        3560cg product family
3560e         3560e product family
3560g         3560g product family
3560x         3560x product family
3650          3650 product family
3750          3750 product family
3750e         3750e product family
3750g         3750g product family
3750x         3750x product family
3850          3850 product family
4500          4500 product family
4500x        4500x product family
4900          4900 product family
IE2000        IE2000 product family
IE3000        IE3000 product family
IE3010        IE3010 product family
nme-es        nme-es product family
sm-d-es2      sm-d-es2 product family
sm-d-es3      sm-d-es3 product family
sm-d-es3g     sm-d-es3g product family
sm-es2        sm-es2 product family
sm-es3        sm-es3 product family
sm-es3g       sm-es3g product family

```

This example shows how to configure a “4k” group and verify with the **show vstack group** command

```

Switch(config)# vstack group built-in 4500 sup8-e 4506
Switch(config-vstack-group)# image bootflash:k10.tar
Switch(config-vstack-group)# config bootflash:mayagraw-4k-startup-config.txt
Switch(config-vstack-group)# script bootflash:mayagraw-4k-startup-post_install.txt
Switch(config-vstack-group)# exit
Switch(config)# exit
Switch# wr
Building configuration...

```

```

*Mar 19 23:16:09.869: %SYS-5-CONFIG_I: Configured from console by consoleCompressed
configuration from 8862 bytes to 3643 bytes[OK]

```

```
Switch#
Switch# show vstack group built detail configured
*** Only Configured Groups will be shown ***
-----
Group Name: sup8-e 4506
Image Name: bootflash:k10.tar
Config file name: bootflash:mayagraw-4k-startup-config.txt
Script file name: bootflash:mayagraw-4k-startup-post_install.txt
No Script file specified
Switch#
```

On-Demand Upgrade for Catalyst 4500 Series Switch IBC

The means of triggering an on-demand upgrade for Catalyst 4500 switch IBC differs from other platforms. The difference is if user want to use the ISSU upgrade option. In a typical upgrade of a Catalyst 3500 platform, the IBC reloads after the upgrade. But for Catalyst 4500 IBC, a switch can be upgraded using ISSU to prevent the downtime.

To prevent downtime for an IBC, you can complete an On-demand upgrade with ISSU by selecting the ISSU option of the **vstack download-image** CLI.

Beginning in privileged EXEC mode, follow these steps to issue an ISSU upgrade:

	Command	Purpose
Step 1	<pre>Switch# vstack download-image {imagelist file_URL ip_address built-in ip address of the switch entry index of the switch product_family port_config} remote_switch_password [override] issu [allow-reload] [in time]</pre>	<p>Starts an on-demand image download on a Smart Install client switch:</p> <ul style="list-style-type: none"> o Enter the <i>imagelist</i> file name (and location) and the IP address of the client, which is one of the options to select the IBC that must be upgraded. <i>imagelist</i> is a text file that contains the name of the image that you want to download. <p>Note The image file must be a tar and not a bin file.</p> <ul style="list-style-type: none"> o The built-in option enables you to select the product family and port configuration from the command-line help. <p>Note A group can be used to upgrade clients with the on-demand cli, only if that particular group is already configured.</p> <ul style="list-style-type: none"> o <i>remote_switch_password</i> defines the password for the client switch. o (Optional) <i>override</i> overrides the existing image on the client switch. o issu attempts to upgrade using ISSU. o <i>allow-reload</i> (visible only for an ISSU upgrade) allows SMI to reload the switch to complete the upgrade process if ISSU could not be performed on that particular IBC. o (Optional) in time specifies the time to reload the switch using the format hh:mm. The range is from 00:00 to 23:59. If no time is specified, the reload occurs when you exit the CLI.

The following examples show how to trigger an On-demand upgrade for a Catalyst 4500 switch IBC.

The **issu** option enables the IBC to upgrade an image with ISSU, if possible from the IBC's side, whereas the **allow-reload** option enables the IBC to upgrade the switch by rebooting if triggering ISSU fails.

"12.21" indicates that an upgrade will happen whether ISSU is possible or not.

```
Switch# vstack download-image tar bootflash:cat4500e-universalk9.SSA.tar 1.1.1.3 ?
WORD password of remote switch or NONE for switches having no password
```

```
Switch# vstack download-image tar bootflash:cat4500e-universalk9.SSA.tar 1.1.1.3 NONE ?
issu Force ISSU Upgrade
override Override the existing image
reload Reload the switch
```

```
Switch# $d-image tar bootflash:cat4500e-universalk9.SSA.tar 1.1.1.3 NONE issu ?
allow-reload Allow Reloading the switch if ISSU fails
in Specify time in
<cr>
```

```

Switch# $d-image tar bootflash:cat4500e-universalk9.SSA.tar 1.1.1.3 NONE issu al
Switch# $r bootflash:cat4500e-universalk9.SSA.tar 1.1.1.3 NONE issu allow-reload ?
      in Specify time in
      <cr>

Switch# $r bootflash:cat4500e-universalk9.SSA.tar 1.1.1.3 NONE issu allow-reload in ?
      hh:mm Specify time in (hh:mm)

Switch# $h:cat4500e-universalk9.SSA.tar 1.1.1.3 NONE issu allow-reload in 12:21 ?
      <cr>

Switch# $h:: cat4500e-universalk9.SSA.tar 1.1.1.3 NONE issu allow-reload in 12:21

```

Support for Post-install Operations

Smart Install provides a single point of interaction for assigning IOS images and configurations. Prior to Cisco IOS Release XE 3.6.0E and IOS 15.2(2)E, you could not execute IOS commands like **sdm**, **system mtu**, **vtp**, on a switch via SMI; configurations required manual execution.

Prior to Cisco IOS Release XE 3.6.0E and 15.2(2)E, you need to populate a post-install text file with the list of commands you intend to execute as part of post install operation. You associate this file with each platform on the IBD analogous to how you currently associate config and image.

As part of a Zero-touch upgrade, IBD provides the config, image, and post-install file details to a valid IBC. The IBC downloads the post installation file, reads it, then reloads causing IBC to run with the new config (or image) and the post install configurations.



Note

SMI Director can operate with either Cisco IOS Release XE 3.6.0E and 15.2(2)E



Note

A post install upgrade is possible only with config upgrade or image upgrade or both. Unlike image-only and config-only upgrades, (A script-only upgrade is not possible). Scripts must be incorporated with either the image, configuration, or both.

You must create the post-install text file (for post-install operation) else the post install operation will fail.

Commas are not required. Each CLI command must be enclosed by double quote(""); a single quote(') is invalid. (The parser execute only those CLIs which are enclosed by double quote("") and all other CLIs/characters are ignored.)

Following is the required format of a post install text file. Notice that each CLI is enclosed by "double quote":.

```

"Cisco IOS CLI" "Cisco IOS CLI" ... "Cisco IOS CLI"
...
...
"Cisco IOS CLI" "Cisco IOS CLI" ... "Cisco IOS CLI"

```

Each line in a text file contains at most 20 CLI commands and all related commands must be written on one line. In the following example, all configuration commands of SDM must be on the same line in the post install text file:

```
"sdm prefer default"
```

Two distinct CLI commands must not be in same line. For example:

```
"sdm prefer default"
```

Following is an example of a well-formatted post install config file:

```
"system mtu 1600"
"sdm prefer default"
```

mtu, **sdm** and **vtp** commands are supported. An example of a valid **vtp** command is given below.

```
"vtp domain cisco"
```

Configure a Script for Default Mode

If the network consists of the same type of switches, you must configure the post install in default mode to run post install operations on all switches.

Beginning in privileged EXEC mode, perform these steps:

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	[no] vstack script <i>path_to_script_file</i>	Configures script file <i>path_to_script_file</i> for the default mode. <i>path_to_script_file</i> represents the path for the post-install file: flash:post_install.txt (similar to the config The no form of the command unconfigures the script file; the post install file is no longer configured in default configuration mode and client switches (IBCs) will not download the post install file.
Step 3	end	Exits from global configuration mode.

This example shows how to configure the post-install script file **flash:post_install.txt** for default mode:

```
Switch# config terminal
Switch(config)# vstack script flash:post_install.txt
Switch(config)# end
```

Configure a Script for the Built-in Group Mode

You can use built-in groups in a Smart Install network to configure a group of switches that have one product ID with the install file and to configure a second group of switches that have another product ID with another post install file.

Beginning in privileged EXEC mode, perform these steps:

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	[no] vstack group built-in <i>switch_family</i> <i>port_config</i>	Identifies the first built-in group product ID and enters Smart Install group configuration mode for the group. The CLI enables you to select family type and port.

	Command	Purpose
Step 3	[no] script <i>path_to_script_file</i>	Configures the script file <i>path_to_script_file</i> for the built-in group. <i>path_to_script_file</i> represents the path for the post-install file: flash:post_install.txt (similar to the config The no form of the command unconfigures the script file.
Step 4	exit	Exits from group mode.
Step 5	end	Exits from global configuration mode.

This example shows how to configure a post install file for a 2960xr 24-2sfp-il built-in group:

```
Switch(config)# vstack group built-in 2960xr 24-2sfp-il
Switch(config-vstack-group)#?
Vstack group configuration commands
config  The config file for the group
exit    Exit from group-vstack config mode
image   The image file for the group
no      Negate a command or set its defaults
script  The script file for the group
```

This example shows how to configure a post install file for any built-in group:

```
switch(config-vstack-group)# script flash:post_install.txt
switch(config-vstack-group)# end
```

Configure a Script for Custom Group Mode

You can configure the post install file for the custom group (i.e., it can be based on mac/connectivity/stack/product-id). In this instance, only member switches of that custom group download the post install file.

Beginning in privileged EXEC mode, perform the following steps:

	Command	Purpose
Step 1	config terminal	Enters global configuration mode.
Step 2	vstack group custom <i>group_name</i> {mac connectivity stack product-id}	Enables group_mode. Use <i>group_name</i> to configure image, config, or script for a particular custom group.
Step 3	[no] script <i>path_to_script_file</i>	Configure script_file <i>path_to_script_file</i> for the custom group. <i>path_to_script_file</i> represents the path for the post-install file: flash:post_install.txt (similar to the config The no form of the command unconfigures the script file.

	Command	Purpose
Step 4	exit	Exits from group mode.
Step 5	end	Exits from global configuration mode.

This example shows how to configure post install for a custom group:

```
Switch# config terminal
Switch(config)# vstack group custom 3k-stack stack
Switch(config-vstack-group)# script flash:post_install.txt
Switch(config-vstack-group)# match 1 3750x 24
Switch(config-vstack-group)# end
```

Smart Install Configuration Examples

These are examples of how to configure a client default configuration on the director. The director should have Layer 3 enabled with multiple Layer 3 interfaces. The director has an IP address on the VLAN that is used for Smart Install management, and configures an IP address on the client VLAN interface. All clients are the same model type and use the default configuration. Clients added to the network are out-of-the-box switches with no configuration, or switches that have had a **write erase** and **reload**.



Note

VLANs are not required when the director is a router.

These examples show how to configure a default configuration with the director as TFTP server and with a third-party server.

- [Director as the TFTP Server, page 2-42](#)
- [Third-Party, Non-Cisco IOS Device as the TFTP Server, page 2-44](#)

Director as the TFTP Server

In this example, the director is the TFTP server and the image and configuration file are stored in the director flash memory.

Before Configuring the Director

Define the Configuration File and Cisco IOS Image

-
- Step 1** You must transfer files to the director. TFTP is the preferred method of transferring files to and from the director. Locate a TFTP server that is IP-reachable by the director and put all files to be transferred on that server.
- Step 2** Using a text editor, create a file with the configuration commands for your default switch. In this example, the file name is *default_configuration.txt*.
- Step 3** Save the *default_configuration.txt* to the TFTP server.
- Step 4** Identify the Cisco IOS image you want loaded as the default image on the switches, for example, *c2960-lanbase-tar.122-53.SE.tar*. Put that file in the TFTP server.
- You should have two files on the TFTP server: the configuration file and the Cisco IOS image.
-



Note

After the director is enabled and configured with the default image name, it creates a tailored configuration file for boot up and an imagelist file with the default image and puts them in flash memory.

Transfer These Files to the Director

-
- Step 1** Before you start, make sure that you have room in the flash memory for the Cisco IOS image. The output of the **dir** command shows the available space near the end of the output. If you do not have enough space for the image, do one of these:

- Remove files to free up some space.
- Consider using an external TFTP server for the Smart Install. (That is a different scenario that is not described here.)

Step 2 To transfer files to the director, you must copy *from* the director, not *to* the director. The director must initiate the transfer. From the Cisco IOS console, enter these commands:

```
Director# copy tftp://tftp ip address/default_configuration.txt flash:
Director# copy tftp://tftp ip address/IOS_image_file.tar flash:
```

**Note**

This normally takes several minutes.

Configure a Director

By default, new Ethernet switches shipped from Cisco (for example, Catalyst 2960 switches) boot up without a configuration file. These switches issue a DHCP request on the default VLAN that is configured for the Smart Install director. The director recognizes the DHCP request on the VLAN and responds.

In this example, the director is both the TFTP server and the DHCP server, and it serves IP addresses on VLAN 1.

**Note**

If the director is a router, all clients connected to Layer 3 interfaces on the router will be recognized.

Step 1 Assign an IP address to the director on the VLAN 1 interface. If the director is a router, assign an IP address on any Layer 3 interface. You can also use a loopback interface on the director. In this example, the *director_ip_address* is 192.168.1.1.

```
Director(config)# interface vlan 1
Director(config)# ip address 192.168.1.1 255.255.255.0
```

Step 2 Configure the director for the default image and configuration file.

```
Director(config)# vstack config flash:default_configuration.txt
Director(config)# vstack image flash:IOS_image_file_name.tar
```

Step 3 Configure the director to serve as the DHCP server for clients.

```
Director(config)# vstack dhcp-localserver smart_install_pool
Director(config-vstack-dhcp)# address-pool network_ip_address 255.255.255.0
Director(config-vstack-dhcp)# file-server network_ip_address
Director(config-vstack-dhcp)# default-router network_ip_address
Director(config-vstack-dhcp)# exit
Director(config)# ip dhcp remember
```

Step 4 Enable Smart Install on the director.

```
Director(config)# vstack director director_ip_address
Director(config)# vstack basic
```

Any switch that boots up without a configuration file on the default Smart Install VLAN or on an Layer 3 interface on the router becomes a Smart Install client of the director. As clients are powered up and discovered by the director, they are updated and given the configuration defined in *default_configuration.txt*.

**Note**

If the configuration file is not present when the Smart Install client boots up, the client attempts to retrieve the DHCP address from VLAN 1. If VLAN 1 is not allowed in the network, then the Smart Install client attempts to identify the startup VLAN from the CDP packets that it receives from the upstream data (that is, data received either from a Smart Install client that is already part of the network, or from the director that the client is connected to).

Use these commands to see the Smart Install network:

- To see the update of new clients in progress: `Director# show vstack download`
- To see the clients and information about them: `Director# show vstack status`

Third-Party, Non-Cisco IOS Device as the TFTP Server

In this example, the customer stores all client image and configuration files on an external, third-party server reachable by the director and client switches.

Before Configuring the Director

Define the Configuration File and Cisco IOS Image

- Step 1** You must transfer files to the director and TFTP is the preferred method. Locate a TFTP server that is IP-reachable by the director, and put all files to be transferred on the TFTP server.
- Step 2** Using a text editor, create a file with the configuration commands that you want for the default switch. In this example, the file name is *default_configuration.txt*.
- Step 3** Save the *default_configuration.txt* to the TFTP server.
- Step 4** Identify the Cisco IOS image you want loaded as the default image on the switches, for example *c2960-lanbase-tar.122-53.SE.tar*. Put that file in the TFTP server.

You should have two files on the TFTP server: the configuration file and the Cisco IOS image.

**Note**

After the director is enabled and configured with the default image name, it automatically creates a tailored configuration file and an image list file for boot up and stores the files in the TFTP server.

Configure the Director

By default, new Ethernet switches shipped from Cisco (for example, Catalyst 2960 switches) boot up without a configuration file. These switches send a DHCP request on the default Smart Install VLAN. The director recognizes the DHCP request and responds.

**Note**

If the director is a router, all clients connected to Layer 3 interfaces on the router are recognized.

In this example, the director is not acting as the TFTP server. It is acting as the DHCP server, and it serves IP addresses on VLAN 1.

- Step 1** Assign an IP address to the director on the VLAN 1 interface on a switch or any Layer 3 interface on a router. In this example, the *director_ip_address* is 192.168.1.1.

```
Director(config)# interface vlan 1
Director(config)# ip address 192.168.1.1 255.255.255.0
```

- Step 2** Configure the director for the default configuration file and image.

```
Director(config)# vstack config tftp://server-ip-address/default_configuration.txt
Director(config)# vstack image tftp://server-ip-address/default_image_file.tar
```

- Step 3** Configure the director as the DHCP server for clients.

```
Director(config)# vstack dhcp-localserver smart_install_pool
Director(config-vstack-dhcp)# address-pool network_ip_address 255.255.255.0
Director(config-vstack-dhcp)# file-server network_ip_address
Director(config-vstack-dhcp)# default-router network_ip_address
Director(config-vstack-dhcp)# exit
Director(config)# ip dhcp remember
```

- Step 4** Enable Smart Install on the director.

```
Director(config)# vstack director director_ip_address
Director(config)# vstack basic
```

Any switch that boots up without a configuration file on the default Smart Install VLAN or on a Layer 3 interface on the router, becomes a Smart Install client of the director. As clients power up and are discovered by the director, they are updated and given the configuration defined in *default_configuration.txt*.

**Note**

If the configuration file is not present when the Smart Install client boots up, the client attempts to retrieve the DHCP address from VLAN 1. If VLAN 1 is not allowed in the network, then the Smart Install client attempts to identify the startup VLAN from the CDP packets that it receives from the upstream data (that is, data received either from a Smart Install client that is already part of the network, or from the director that the client is connected to).

Use these commands to see the Smart Install network.

To see the update of new clients in progress: Director# **show vstack download status**

To see the clients and information about them: Director# **show vstack status**

