Cisco Smart Install Configuration Guide

December 10, 2014

C O N T E N T S

Preface

This guide provides procedures for installing and using Smart Install and using the related commands. For information about other standard Cisco IOS Release 12.2 commands or Cisco IOS Release 15.0, see the Cisco IOS documentation set available from the Cisco.com home page at Products & Services > Cisco IOS and NX OS Software> Cisco IOS.

This guide does not describe system messages you might encounter or how to install your device. For more information, see the system message guide and the hardware installation guide for the device.

For documentation updates, and other late information, see the release notes for the specific device for this release.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in `boldface screen` font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes and cautions use these conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

⚠️

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Publications

- Catalyst 6500 Supervisor Engine 2T-10GE

  http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

- Catalyst 4500

  http://www.cisco.com/en/US/products/hw/switches/ps4324/tsd_products_support_series_home.html

- Catalyst 3850

  http://www.cisco.com/en/US/products/ps12686/tsd_products_support_series_home.html

- Catalyst 3750-X

  http://www.cisco.com/en/US/products/ps10745/tsd_products_support_series_home.html

- Catalyst 3750-E

  http://www.cisco.com/en/US/products/ps7077/tsd_products_support_series_home.html

- Catalyst 3750

  http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

- Catalyst 3650

  http://preview.cisco.com/en/US/products/ps13133/products_installation_and_configuration_guides_list.html

- Catalyst 3560

  http://www.cisco.com/en/US/products/hw/switches/ps5528/tsd_products_support_series_home.html

- Catalyst 3560-E

  http://www.cisco.com/en/US/products/ps7078/tsd_products_support_series_home.html

- Catalyst 3560-X

  http://www.cisco.com/en/US/products/ps10744/tsd_products_support_series_home.html

- Catalyst 2975

  http://www.cisco.com/en/US/products/ps10081/tsd_products_support_series_home.html

- Catalyst 2960, Catalyst 2960-S, and Catalyst 2960-SF

  http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

- Catalyst 2960-X

  http://www.cisco.com/en/US/products/ps12995/tsd_products_support_series_home.html

- Catalyst 2960-XR

  http://www.cisco.com/en/US/products/ps13078/tsd_products_support_series_home.html

- IE 2000

    http://www.cisco.com/c/en/us/support/switches/industrial-ethernet-2000-series-switches/tsd-products-support-series-home.html

- IE3000

    http://www.cisco.com/c/en/us/support/switches/industrial-ethernet-3000-series-switches/tsd-products-support-series-home.html

- IE3010

    http://www.cisco.com/c/en/us/support/switches/industrial-ethernet-3010-series-switches/tsd-products-support-series-home.html

- EtherSwitch Network Modules

    https://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_enet_switch_net_external_docbase_0900e4b18090920b_4container_external_docbase_0900e4b18096f791.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
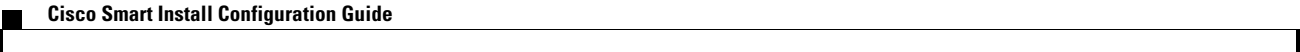
Smart Install Overview

Introduction

Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. You can ship a switch to a location, place it in the network and power it on with no configuration required on the device.

A network using Smart Install includes a group of networking devices, known as clients, that are served by a common Layer 3 switch or router that acts as a director. In a Smart Install network, you can use the Zero-Touch Installation process to install new access layer switches into the network without any assistance from the network administrator. The director provides a single management point for images and configuration of client switches. When a client switch is first installed into the network, the director automatically detects the new switch, and identifies the correct Cisco IOS image and the configuration file for downloading. It can allocate an IP address and host name to a client. If a standalone switch in the network is replaced by another switch of the same SKU (a switch with the same product ID), it automatically gets the same configuration and image as the previous one. The director can also perform on-demand configuration and software image updates of a switch or a group of switches in the network.

Zero-touch updates also take place on preconfigured switches after you have entered the **write erase** and **reload** privileged EXEC commands to clear the configuration.

⚠ **Caution**   If you touch the console keyboard during a zero-touch update and attempt to enter a command or a return on the switch, the auto install and Smart Install processes stop. To recover and restart the process, at the system prompt, enter the **write erase** and **reload** commands on the client and restart the process.

The director can act as a DHCP and TFTP server and can store the configuration and image files. These files can also be stored on a third-party TFTP server for the director to use. The client can download the image and configuration files from the director TFTP server or from a remote server.

Note Switches running releases earlier than 12.2(52)SE are not Smart Install capable, but they can be Smart Install clients if they support the **archive download-sw** privileged EXEC command. Smart Install clients can be Layer 2 or Layer 3 switches. Switches running Cisco IOS Releases 3.2(0)SE and later, and 15.0 (2)SE and later, 3.6.(0)E, and 15.2.(2)E support Smart Install.

See Appendix A, "Supported Devices for Smart Install" for a list of supported routers and switches, the roles they can play (client or director), and the required software releases.

In a typical Smart Install network, a client switch uses DHCP to get an IP address and the director snoops DHCP messages. For a client to participate in Smart Install zero-touch update, it must use DHCP, and all DHCP communication must pass through the director so that it can snoop all DHCP packets from clients. The most automatic operation is when all switches in the Smart Install network use DHCP and are Smart Install capable. However, any client switch that supports the **archive download-sw** privileged EXEC command to download a software image can be used in a zero-touch Smart Install network. Cisco IOS Release 3.2(0)SE and later, support software install.

Note A Smart Install network can have only one director.

A client switch can participate in Smart Install even if it is not directly connected to the director. The Smart Install network supports up to seven hops. Intermediate switches or clients connected to the director through an intermediate switch in a multihop environment can be, but are not necessarily Smart Install-capable, provided the management VLAN is set to default VLAN1.

If you use a VLAN other than vlan 1 for management, then the intermediate switch must be Smart Install capable switch.

Figure 1-1 shows a Smart Install network with external DHCP and TFTP servers. There can be only one director amongst TFTP servers in any Smart Install network. The director can also serve as the DHCP and TFTP server.

Figure 1-1   Typical Smart Install Network Diagram
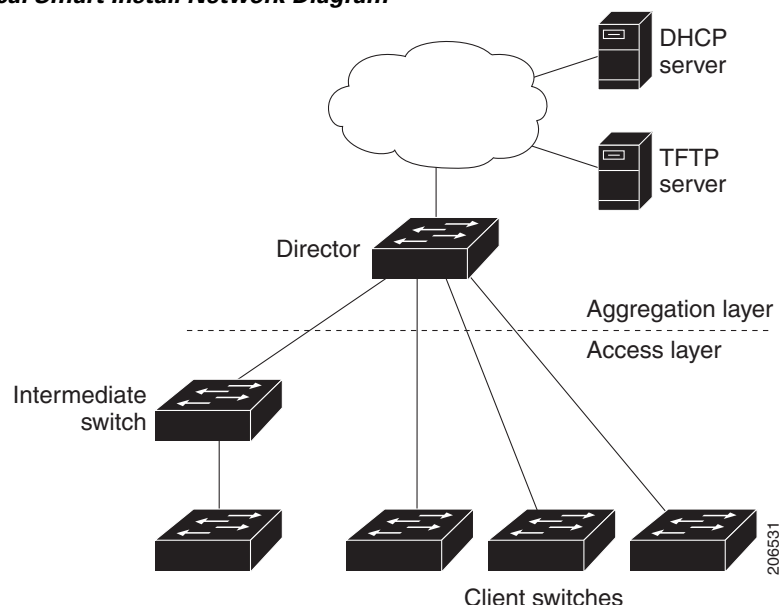
A Smart Install network can be:

- A network where all client switches are of the same product ID (PID), for example, WS-2960S-48FPS-L. In this case, you can identify a default image and a seed or basic configuration to use on all client switches.

- A network that includes switches with different PIDs. In these networks, you can configure switch groups and specify that the same images and seed configuration files are applied to all switches in the group. A group can be based on a predefined PID, or you can create groups based on product ID, MAC address, switch stack number, MAC address, or client switch connectivity to a specific upstream neighbor. When switches in a group are replaced by another switch with the same product ID, the replacement switch receives the same configuration and image.

After a switch has an image and basic configuration, you can configure specific features on individual switches and save the configuration to the startup configuration file.

Switches participating in Smart Install zero-touch updates must use DHCP to obtain their IP addresses. DHCP options are used to send:

- Image filename and location
- TFTP server IP address
- Hostname
- Configuration filename
- Director IP address to the other switches

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, XE 3.4SG, 15.1(2)SG, 15.1(1)SY, 15.0(2)SE, 3.2(0)SE and later, 3.6.(0)E, or 15.2.(2)E, 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. To reenable Smart Install on the device, enter the **vstack** global configuration command.

These sections include more detailed information on Smart Install components:

- Smart Install Director, page 1-3
- Smart Install Clients, page 1-6
- Smart Install Groups, page 1-9

Smart Install Director

The director in a Smart Install network must be a Layer 3 switch running Cisco IOS Release 12.2(52)SE or later, XE 3.4SG, 15.1(2)SG, 15.0(2)SE or later, 15.1(1)SY or later, 3.2(0)SE or later, or a router running Cisco IOS Release 15.1(3)T or later. See Appendix A, "Supported Devices for Smart Install" for a list of routers and switches that can perform the role of Smart Install director.

Note   IE2000 IE3000, and IE3010 support Director with Cisco IOS Release 15.2(2)E.

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

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

When a device is configured as director, The VLAN on which the DHCP snooping is automatically enabled becomes VLAN 1 by default. The director begins building the director database in VLAN 1. To specify another VLAN for Smart Install management, you can use the **vstack startup-vlan** global configuration command. Depending on the VLAN that is specified in the command, DHCP snooping is enabled on that VLAN so that the director can identify new switches that are connected to the network, known as non-VLAN 1 switches.

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

- Type of switch (PID) for all switches, including switches in a stack
- MAC addresses for all switches, including switches in a stack
- IP address of the switch or stack
- Hostname
- Network topology including neighbors interfacing with the switch
- Serial number (only Smart Install capable switches)

Note When the director is a switch, DHCP snooping is enabled on VLAN 1 by default. It is also enabled on other Smart Install management VLANs that are configured by entering the **vstack vlan** *vlan-range* global configuration command. You can use the **vstack startup-vlan** global configuration command to specify another VLAN that should be used for Smart Install management. Cisco IOS Releases 15.1(1)SY, 15.0(2)SE or later, 15.1(2)SG, 3.6.(0)E, 15.2.(2)E, and Cisco IOS XE 3.4SG support non-VLAN1 management and provide the ability to discover the client switches available on non-VLAN1.

In a Smart Install network that uses DHCP to assign IP addresses, you only need to configure the director. Client switches do not require any configuration. Although you can enter command-line interface commands on clients, configuration commands do not take effect unless the switch assumes the role of director.

Note You can configure the **vstack** commands in client mode. but this is effective only when the switch is converted to a director.

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

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

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

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

- The director IP address is changed.

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

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

Smart Install relies on a TFTP server to store image and configuration files. The TFTP server can be an external device, or the director can act as a TFTP server. If the director is the TFTP server, the available flash file space on the director must be adequate to accommodate the client Cisco IOS image and configuration files. See the "Configuring the TFTP Server" section on page 2-8.

In a Smart Install network using DHCP, the DHCP server can be an external device or the director can act as the DHCP server. See the "Configuring the DHCP Server" section on page 2-5. The director snoops all DHCP packets that pass through it on VLANs that are configured as Smart Install management VLANs. All network DHCP packets from intermediate or client switches or from an external DHCP server must pass through the director. The director must be able to snoop all DHCP packets from clients.

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

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

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

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

Image List File

An image list identifies the images to be loaded on the client. The image list file is the file that contains the correct image name for the client. When the director is the TFTP server, this file is stored in flash memory. Otherwise, it is stored in a remote, third-party TFTP server.

- When the file is stored in the director, the prefix for the image list is **flash://**, **usbflash0://**, **bootflash://**, **bootdisk://**, or **disk0://** based on the appropriate file systems available on the switch.
- When the file is stored in a remote TFTP server, the prefix is **tftp://***ip_address*/*image*.**tar**.

> **Note** In Catalyst Switches 3850 and 3650, the image is a bundled with **.bin** extension.

Images must be stored either on the director or on the third-party TFTP server.

For a standalone switch, the image list file contains a single image. For a stack, the image list contains images for all members of the stack, which could be the same image or different images. For a switch stack, the director creates the image list file after the user specifies the tar file for each switch in the stack.

Starting with Cisco IOS Release 12.2(55)SE or later,15.1(1)SY, 15.0(2)SE and later, 3.2(0)SE and later, XE 3.4SG, 15.1(2)SG, 3.6.(0)E, and 15.2.(2)E, when the user specifies the tar file for each switch, the director automatically creates the imagelist file.

When an external TFTP server is used, the director writes the image list file to the TFTP server. It is recommended that the TFTP server permit the director to write the image list files to the TFTP Server. If the director does not have permission to write to the file system of the TFTP server, the director logs the failure in the system log. You can create the image list files and put them on the TFTP server manually if the director fails to do so automatically; you cannot fix the issue that prevents the director from writing to the TFTP server.

Note The upgrade process is initialized even when the imagelist file is copied manually, but the director tries to copy the image list file to the TFTP server and the failure system log is displayed periodically.

Configuration Files

The director manages these configuration files:

- Startup configuration—The configuration that a client uses when it boots.
- Seed configuration—A configuration on the director that is the basis for the client startup configuration.
- Backup configuration—An exact copy of a client startup configuration stored in the director.

Smart Install Clients

Client switches have a direct or indirect connection to the director so that they can receive image and configuration downloads from it. A switch becomes a Smart Install client when either director or when the director IP address is configured on the switch manually. Client switches use the director database for image and configuration downloads and receive the image and configuration files from the Smart Install TFTP server.

A client switch can be an intermediate switch connected to another client switch. A client can be a standalone switch or a switch stack.

- Director can download images and configuration of clients that are not Smart Install. However, such clients are entered into the director database only if they are connected to a Smart Install capable switch. The director can telnet to the client switch and use the **archive download-sw** privileged EXEC command to download software to the switch. The director must know the client switch password to perform the download.
- Smart Install capable switches can communicate directly with the director to update switch information, can have images and configuration downloaded, and can be managed by the director. A Smart Install capable client with the director IP address and connectivity to the director sends switch and neighbor information to the director by using the Smart Install protocol.

Note Switches running Cisco IOS XE Releases 3.2(0)SE and later, 3.6.(0)E, and 15.2.(2)E support software install.

All switches in the network with "network" connectivity to the director can be clients, whether or not they are Smart Install capable. A client switch needs an IP address for management communication and the director must be able to communicate with that IP address. Client switch IP addresses are assigned by DHCP or statically configured.

Smart Install capable clients send switch and neighbor information to the connected director for the director database. Client switches that are not Smart Install capable or that are not connected to a Smart Install capable switch are not entered into the director database. In a multihop topology, for the director to get the complete topology overview, any client switch upstream of a group of clients must be Smart Install capable. Clients not in the director database can get an on-demand update, but they cannot get a zero-touch or group update.

Figure 1-2 shows some possible ways that clients can be interconnected in a network. Table 1-1 and Table 1-2 shows the director database knowledge of each client and the type of update that is supported.

Note The topology shown in Figure 1-2 does not represent a typical Smart Install topology but is used to demonstrate possible types of client interconnections.

Figure 1-2   Possible Interconnections of Smart Install Clients
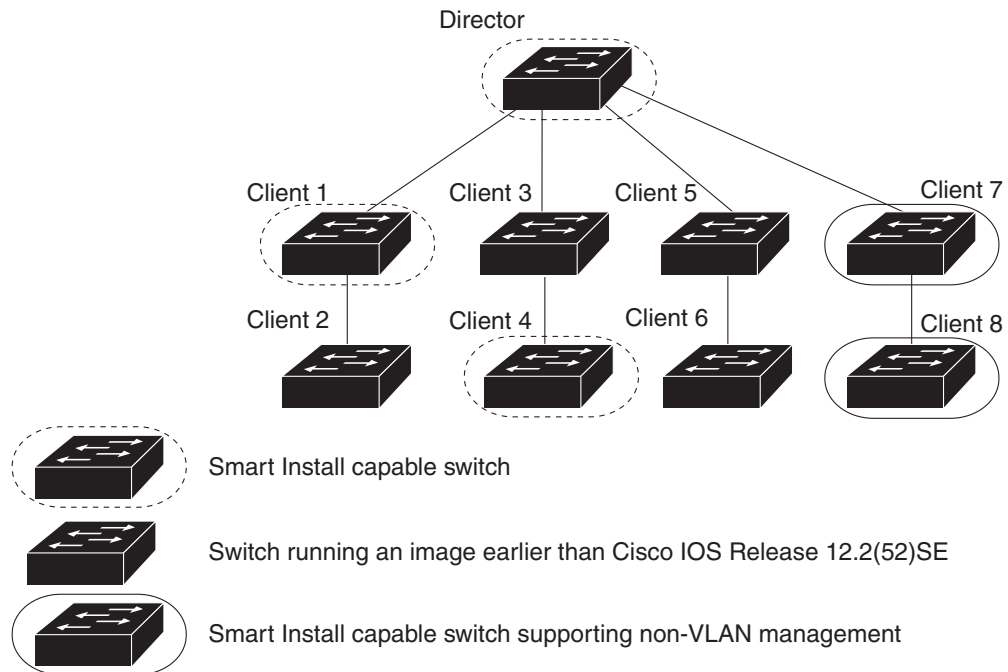
Note The Cisco IOS releases12.2(52)SE or later, XE 3.4SG, 15.1(2)SG, 15.1(1)SY and later, 15.0(2)SE and later, and 3.2(0)SE and later, support the director role. The Cisco IOS releases 15.0(2)SE, 15.1(1)SY, 15.1(2)SG, XE 3.4SG, 15.0(2)EX, 15.0(2)EX1, 3.6.(0)E, and 15.2.(2)E are Smart Install capable switches, supporting non-VLAN 1 management and providing the ability to discover the client switches available on non-VLAN 1.

Table 1-1 shows the switches that are in the director database and how the director obtained the information. When a client is a single hop from the director, the client uses CDP to send the director information about itself. When a client is a Smart Install capable switch, it sends information to the director about itself and its neighbors.

Table 1-1   Director Database Contents of Client Switches

Client Switch	In Director Database?	Source of Database Information
Client 1	Yes	Learned from CDP and from Smart Install. The client also sends information about its neighbor (Client 2).
Client 2	Yes	Information received from Client 1.
Client 3	Yes	Learned from CDP.
Client 4	No	No information available. The client is not an immediate neighbor of the director or another Smart Install switch.
Client 5	Yes	Learned from CDP.
Client 6	No	No information available. The client is not an immediate neighbor of the director or another Smart Install switch.
Client 7	Yes	Learned from CDP and from Smart Install. The client also sends information about its neighbor Client 8. Client 7 is a non-VLAN 1 switch.
Client 8	Yes	The information to Client 8 will be sent by Client 7 via non-VLAN1. Client 8 is a non-VLAN 1 switch.

Table 1-2 shows the director database knowledge of each client and the type of update that is supported in various software versions. For information about Smart Install supported switches, routers, and minimum software releases for directors and clients, see Supported Devices for Smart Install.

Table 1-2   Types of Updates Supported by Each Client

Device	Software Version	Zero-Touch Update	On-Demand Update of Client	On-Demand Update of Group
Client 1	12.2(52)SE or later	Yes	Yes	Yes
Client 2	Earlier than 12.2(52)SE	Yes	Yes	Yes
Client 3	Earlier than 12.2(52)SE	Yes	Yes	Yes
Client 4	12.2(52)SE or later	Yes	Yes	Yes
Client 5	Earlier than 12.2(52)SE	Yes	Yes	Yes
Client 6	Earlier than 12.2(52)SE	Yes	Yes	No. Switch not in director database.
Client 7	15.0(2)SE, 15.1(1)SY, 15.1(2)SG, XE 3.4SG, 15.0(2)EX, 15.0(2)EX1, 3.6.(0)E, and 15.2.(2)E	Yes	Yes	Yes
Client 8	15.0(2)SE,15.1(1)SY, 15.1(2)SG, XE 3.4SG, 15.0(2)EX, 15.0(2)EX1, 3.6.(0)E, and 15.2.(2)E	Yes	Yes	Yes

To see the types of Smart Install clients in a network, enter the **show vstack status** privileged EXEC command.

```
Director# show vstack status
SmartInstall:  ENABLED
Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress    I - done          X - failed
Config Upgrade:  c - in progress    C - done          x - failed
Director Database:
DevNo   MAC Address      Product-ID          IP_addr          Hostname     Status
=====   ==============   ================    ==============   ==========   =========
0       0018.7363.4200   WS-C3750-24TS       172.20.249.54    IBD-MXD-ST   Director
1       0016.4779.b780   WS-C3750G-24TS      172.20.249.54    IBD-MXD-ST   Director
2       d0d0.fd37.5a80   WS-C3750X-48P       172.20.249.54    IBD-MXD-ST   Director
3       0026.5285.7380   WS-C3750E-24TD      172.20.249.54    IBD-MXD-ST   Director
4       0024.13c6.b580   WS-C3750E-24TD      172.20.249.115   DEV-c6.b5c   S A a
5       0021.a1ab.9b80   WS-C2960-48TC-S     172.20.249.249   DEV-ab.9bc   S A a I C
6       0024.5111.0900   WS-C3750E-24TD      172.20.249.222   DEV-11.094   S A a I C
7       001d.45f3.f600   WS-C3750G-24TS      172.20.249.87    DEV-90.f64   S A a
8       0016.c890.f600   WS-C3750G-24TS      172.20.249.87    DEV-90.f64   S A a
9       001f.2604.8980   WS-C2960-48TC-S     172.20.249.89    DEV-04.89c   S A a I C
10      001b.d576.2500   WS-C3750E-24PD      172.20.249.91    DEV-a6.1cc   S A a I C
```

These fields were added in Cisco IOS Release 12.2(58)SE or 15.1(1)SY to provide more information about each client:

- Device type: S (Smart Install capable, running Cisco IOS Release 12.2(52)SE or later, 15.1(1)SY, 15.0(2)SE and later, 3.2(0)SE and later), 3.6.(0)E, or 15.2.(2)E, N (not a Smart Install device), or P (pending, unable to determine).

- Device health status: Active (the director is receiving periodic updates from the device) or Inactive (the device is disconnected or has not provided updates for three consecutive keepalive periods)

- Join window status: a (allowed), h (on hold), or d (denied). See the "Using a Join Window" section on page 1-15.

- Upgrade status: An image update is i (in progress), I (complete), or X (failed). A configuration upgrade is c (in progress), C (complete), or x (failed).

Smart Install Groups

When all switches in a Smart Install network have the same PID, they can run the same image and the same seed (basic) configuration file. In this case, you can assign a default image and configuration file for all clients. However, if there is more than one PID in the network or if you want a different configuration file to run on some switches, depending on their function in the network, you should configure Smart Install groups and assign an image and configuration file for each group.

- Custom groups take precedence over built-in groups and are based on:

  - Stack group—For switches in a stack, you can configure groups based on their number in the stack. Stack groups are used only for switch stack upgrades, and clients do not need to be in the director database. Starting with Cisco IOS Release 12.2(58)SE, 15.1(1)SY, 15.0(2)SE and later, 3.2(0)SE and later, 3.6.(0)E, and 15.2.(2)E if a stack is homogeneous (all one switch type), you do not need to identify each switch type.

  - MAC address—You can create a custom group of specific switches by using the MAC addresses of the switches to configure the group. You can include switches with the same or different product IDs, as long as they use the same image and configuration file. Enter the **show vstack neighbors all** privileged EXEC command to see the MAC addresses of switches in the Smart Install network.

- Connectivity—You can configure a custom group based on network topology; that is, all switches that have the same upstream neighbor. Connectivity groups take precedence over groups with matching product IDs or stack numbers. Connectivity groups include only standalone switches (not switch stacks), and clients must be in the director database.

- Product IDs (PIDs)—These product IDs are all supported models, including newer PIDs that were not shipping when the software was released and therefore are not in the CLI. PID groups include only standalone switches (not switch stacks), and clients do not need to be in the director database.

The priority of custom groups from high to low is stack group, MAC address, connectivity, and product ID.

- Built-in groups are based on PIDs that you can select from the CLI. These represent the fixed Ethernet switching products that were shipping when the software was released, for example, 3750, 3560, 2975, 2960, 3850, and 3650.

Switches that belong to a group use the image and configuration file assigned to that group. If a client switch does not belong to a group in the director database, it is assigned the default image and configuration file.

Note If there is more than one switch PID in the network, we recommend configuring built-in or custom groups. The default image and configuration is used in networks with only one product ID.

An example of the use of custom groups is a network where all client switches are the same PID, but one requires a different configuration. For example, a retail store might have checkout counters and a pharmacy, and the pharmacy switch requires a different configuration. The checkout counters would use the default configuration, but you would create a custom group for the pharmacy.

Restrictions for Smart Install

The absence of an authorization or authentication mechanism in the Smart Install protocol between the client and the director can allow a client to process crafted Smart Install messages as if these messages were from the Smart Install Director. These include the following:

- Change the TFTP server address on Smart Install clients.
- Copy the startup configuration of client switches to the previously-changed and attacker-controlled TFTP server.
- Substitute the startup configuration of clients with a configuration created by the attacker, and forcing a reload of the clients after a configured time interval.
- Upgrade the IOS image on client switches to an image supplied by the attacker.
- Execute arbitrary commands on client switches (applicable to Cisco IOS Release 15.2(2)E and later releases and Cisco IOS XE Release 3.6.0E and later releases.)

While designing a Smart Install architecture, care should be taken such that the infrastructure IP address space is not accessible to untrusted parties. Design considerations are listed in the Security Best Practices section of this document.

Security Best Practices

Security best practices around the Cisco Smart Install feature depend on how the feature is used in a specific customer environment. We differentiate the following use cases:

- Customers not using the Smart Install feature.
- Customers leveraging the Smart Install feature only for zero-touch deployment.
- Customers leveraging the Smart Install feature for more than zero-touch deployment (configuration and image-management).

The following sections describe each scenario in detail:

Customers Not Using the Smart Install Feature

Customers who do not use the Cisco Smart Install feature, and are running a release of Cisco IOS and IOS XE Software where the command is available, should disable the Smart Install feature with the **no vstack** command.

Note   The **vstack** command was introduced in Cisco IOS Release 12.2(55)SE03.

The following is sample output from the **show vstack** command on a Cisco Catalyst Switch with the Smart Install client feature disabled:

```
switch# show vstack config

Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Customers Leveraging the Smart Install Feature Only for Zero-Touch Deployment

Disable the Smart Install client functionality after the zero-touch installation is complete or use the **no vstack** command.

To propagate the **no vstack** command into the network, use one of the following methods:

- Execute the **no vstack** command on all client switches either manually or using a script.
- Add the **no vstack** command as part of the IOS configuration that is pushed into each Smart Install client as part of the zero-touch installation.
- In the releases that do not support the **vstack** command (Cisco IOS Release 12.2(55)SE02 and prior releases), apply an access control list (ACL) on client switches to block the traffic on TCP port 4786.

To enable the Smart Install client functionality later, execute the **vstack** command on all client switches either manually or by using a script.

Note   If the configuration changes in between the disabling and re-enabling of the Smart Install feature, to preserve these changes, execute the **write memory** command on client switches after re-enabling the feature. Configuring the command ensures a successful backup of the startup configuration of client switches.

Customers Leveraging the Smart Install Feature for More Than Zero-Touch Deployment

While designing a Smart Install architecture, care should be taken such that the infrastructure IP address space is not accessible to untrusted parties. In releases that do not support the **vstack** command, ensure that only the Smart Install director has TCP connectivity to all Smart Install clients on port 4786.

Administrators can use the following security best practices for Cisco Smart Install deployments on affected devices:

- Interface access control lists (ACLs)
- Control Plane Policing (CoPP). This feature is not available in all Cisco IOS Software releases.

The following example shows an interface ACL with the Smart Install director IP address as 10.10.10.1 and the Smart Install client IP address as 10.10.10.200:

```
ip access-list extended SMI_HARDENING_LIST
 permit tcp host 10.10.10.1 host 10.10.10.200 eq 4786
 deny tcp any any eq 4786
 permit ip any any
```

This ACL must be deployed on all IP interfaces on all clients. It can also be pushed via the director when switches are first deployed.

To further restrict access to all the clients within the infrastructure, administrators can use the following security best practices on other devices in the network:

- Infrastructure access control lists (iACLs)
- VLAN access control lists (VACLs)

Migration Plan

Customers who can not properly protect their Smart Install IP infrastructure address space, or need the added security of authorization and authentication between the director and clients can migrate to Cisco Plug-N-Play (PnP). For more information, see the *PnP Feature Guide*.

If your release does not support PnP, migrate to Smart Install Proxy (SMI Proxy). The SMI Proxy feature must be enabled on a network device that is configured as a PnP Agent. This device will bridge the communication between older devices running Smart Install and the PnP Server. The SMI Proxy device will contact the central PnP Server on behalf of the device running older versions, to retrieve the image and configuration information. For more information, see the *SMI Proxy* chapter.

SMI Proxy is available in Cisco IOS Release 15.2(2)E2 and later releases.

Note   The security best practices must be followed for all devices on which the SMI Proxy feature is enabled, and also for all devices on which the Smart Install feature is enabled.

DHCP and Smart Install

DHCP is recommended in Smart Install networks and is required for zero-touch updates. On-demand updates do not require DHCP. In a DHCP network, DHCP snooping is automatically enabled on the director. The director snoops DHCP offers and requests to and from the client switches and uses DHCP snooping to insert the DHCP options used in the Smart Install operation.

However, because DHCP snooping is not supported on routed ports, you should not connect routed ports directly to the client or the director.

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

- The Smart Install director can act as the DHCP server in the network. When the DHCP offer goes to the client switches, the director allocates the IP addresses and assigns configurations and images and the hostname as DHCP options in the DHCP offer and DHCP acknowledgment. DHCP snooping is automatically turned on for the director.

- The DHCP server can be another device (third-party server) in the Smart Install network. In this case, DHCP packets between the clients and DHCP server must pass through the director.

Note You can configure a join-window time period so that the director can only modify the DHCP offer and send the image and configuration files to the client during the configured window. The join window restricts Smart Install for a specified period of time and acts as a security precaution to control when a client can receive these files. See the "Using a Join Window" section on page 1-15.

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

See the "Configuring the DHCP Server" section on page 2-5 for configuration instructions.

If the Smart Install DHCP server is the director or another device running Cisco IOS and the network reloads, the server might assign new IP addresses to participating switches. If a switch IP address changes, it might no longer be reachable. If the director IP address changes, it is no longer the Smart Install director, which could break the director and client switch relationships. This is an unlikely but possible corner-case occurrence. To prevent this occurrence, you should enable *DHCP remembering* by entering the **ip dhcp remember** global configuration command or the **remember** DHCP-pool configuration command on the DHCP server,

Non-Cisco IOS third-party DHCP servers require an IP-address-to-MAC-address binding to ensure that the same IP address is given to a switch on a reload.

Note In Smart Install networks that do not use DHCP, you must manually configure the director IP address on each client switch by entering the **vstack director** *ip-address* global configuration command. Client switches require only the director IP address. Smart Install networks that do not use DHCP cannot support zero-touch updates but can support on-demand update.

Adding a Client Switch to the Network

When a switch arrives from the factory, it contains the factory default image. When it is plugged in and connected to the network and boots up, it tries to get its IP address from DHCP. When a device is added to the network, a notification is sent to the director that a new client has joined. If the switch is connected (directly or indirectly) to the Smart Install director, the director recognizes the new switch through DHCP offers and acknowledgments. The director searches its database to determine if the switch belongs to a configured group. If not, the director determines if the switch matches the Smart Install network default PID. If the director has a configuration for the type of client that was added and if the join window is open, the new client receives the image and configuration files.

Note   When clients in a Smart Install network consist of more than one PID, you should configure built-in groups or custom groups based on MAC address, connectivity, stack group, or product-ID, and define the image and configuration files for each group.

If the DHCP Server is external or internal (running on the director), the director inserts options into the DHCP response, informing the client where to download its IOS image and configuration file provided the join window is open.

Note   If a join window has been configured, the Smart Install configuration and image files are sent to the client only during the configured time period. 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 acknowledgments occurs beyond the configured time frame. See the "Using a Join Window" section on page 1-15 for more information.

After a switch has been added to the Smart Install network, you can do an on-demand download of an image or configuration file to the client at any time if the switch meets these criteria:

- A switch that is not Smart Install capable must have an enable mode password and a valid IP interface.
- A switch running the Smart Install image must have a valid IP interface.

If a client switch in the Smart-Install network is running Cisco IOS Release 12.2(55)SE or later, or 3.2(0)SE and later, 15.0(2)EX, 15.0(2)EX1, 3.6.(0)E, and 15.2.(2)E is replaced with a switch with the same product ID, the new client receives the same image and configuration as the replaced client. Se the "Replacing a Client Switch" section on page 1-15.

See Chapter 2, "Configuring Cisco Smart Install Devices" for typical configurations.

Backing Up the Client Configuration

After a client boots up, it sends a copy of its startup configuration to the director. This file is the backup configuration for that client. Any time the user, directly or through the director, saves a client configuration, a backup configuration is created. The configuration is stored on the local repository on the director or on a remote repository on a server. The backup file is used to reconfigure a client during a zero-touch replacement.

Note   Client backup is supported only when the director and client are running Cisco IOS Release 12.2(55)SE or later.

Client configuration backup is enabled by default. You can disable it by entering the **no vstack backup** global configuration command. You enable the file backup feature on the director by entering the **vstack backup** and you can configure a repository for the backup files. If you do not specify a repository, the files are stored in the director **flash:/vstack** directory.

A client configuration backup is triggered:

- When the **write memory** privileged EXEC command is entered on the client.
- When the director boots up, it requests configuration information from clients and backs up these configurations.

Replacing a Client Switch

You can use zero-touch replacement to exchange and install a like-type client in the Smart Install network. When a new switch is added to the network, a CDP database update is sent to the director, which determines if this is a new MAC address and therefore a new client. When a client needs to be replaced and is removed from the network, the CDP database lists the removed client as *inactive*. If another client MAC address with the same product-ID is detected on the same port, this client is considered a *replacement* client. The director gives it the same image and configuration that the previous client had.

The director removes the entry for the replaced client from the director database. If the replaced client is put elsewhere in the network, the director creates a new entry for it that includes the client's new information.

During a zero-touch replacement, the replacement client receives the last backed-up configuration file, which is stored in the director or a remote repository. Client configuration files are backed up by default, unless you disable this functionality on the director.

Only one Smart Install client can be replaced at a time on the same branch and only if there is one path to the director.

Note   Zero-touch replacement is supported only when the director and the replaced client are running Cisco IOS Release 12.2(55)SE or later, 15.1(1)SY, 15.0(2)SE and later, 3.2(0)SE and later, 15.0(2)EX, 15.0(2)EX1, 3.6.(0)E, or 15.2.(2)E. When a client switch running an earlier release is replaced, the new switch receives a seed replacement.

When the replacement client and existing client do not have the same product ID, port connections, or interfaces, the replacement client is considered new to the Smart Install network. For example, a replacement client must be connected to the same ports on the director and on other client switches as was the original client. When a new device is added to the network, a notification is sent to the director that a new client has joined. If the director has a configuration for the type of client that was added and if the join window is open, the new client receives the image and configuration files.

Using a Join Window

A join window is a time window during which the client can update image or configuration files. The director can provide information about the image and configuration to the client only during this window. A client attempting to join the Smart Install network outside the join window is not allowed to do so and cannot update the image and configuration files.

Use the **vstack join-window mode auto** global configuration command to automatically update clients with the latest image and configuration files when they are added during a join window. Use the **no vstack join-window mode** global configuration command to put the client in a hold state.

Use the following commands to open or close a join window:

- Enter the **vstack join-window start** [*date*] *hh:mm* [*interval*] [*end date*] [**recurring**] global configuration command to configure a time window to control downloads of configuration and image files to client switches.

- Enter the **vstack join-window close** global configuration command to manually close a join window, enter the **no vstack join-window close** global configuration command to manually open a join window.

Note   You cannot combine the **vstack join-window start** and **[no] vstack join-window** commands to close and open the join window.

If a join window *is* configured, a zero touch update is possible only during the configured window. If a switch connects to the director at any time other than during the join window, the Smart Install configuration and image files are not automatically downloaded. Instead, the new switch receives the default files from the DHCP server. This feature provides control of the files and prevents unauthorized switches from receiving the Smart Install configuration.

If a join window *is not* configured, a zero touch update can happen at any time because that is the default state.

When a join window is configured, and the DHCP acknowledgement occurs outside of the configured window, a client switch sends an error message that it cannot download an image or configuration file.

Configuring Join Window Mode

The join window mode includes a *hold* state that adds an extra level of security for the client. The hold state lets you control whether or not the client can receive a software upgrade, and how the upgrade is performed. The hold-state is either *on* or *off* when the join window is active.

You configure automatic join window mode with the **vstack join-window mode auto** global configuration command. In this mode, when a client joins the network, the director automatically upgrades it when the join window is open.

When you set the mode to manual by entering the **no vstack join-window mode** global configuration command, when a client joins the network during an open join window, the client is put on the hold list.

You can review clients on the hold list by entering the **show vstack status** user EXEC command. You can remove a client from the hold list by entering the **vstack on-hold-clients remove** global configuration command.

> **Note** When a client has been removed from the hold state to allow that client to join the network, you must restart the client to again put it in the hold state (if the mode is manual) or to automatically upgrade if the mode is auto and the join window is open.

When a new client joins the network and the mode is set to auto, the join window state is active, whether or not the join window is open or closed. When the mode is set to manual and the join window is open, the client is put on the hold list. If the join window is closed, the client cannot join the network (denied).

Table 1-3 lists the join window states and the actions that are allowed or not allowed for each state.

Table 1-3   Join Window States and Functionality

Join Window State	Zero-Touch Updates	On-Demand Updates	Configuration Backup
Active	Allowed	Allowed	Allowed
Deny	Not allowed	Allowed	Allowed
Hold	Allowed with user intervention	Allowed	Not allowed

Starting with Cisco IOS Release 12.2(58)SE,15.1(1)SY, 15.0(2)SE and later, 3.2(0)SE and later, 3.6.(0)E, and 15.2.(2)E, you can manually change the join window state for a client or multiple clients from the denied state to the active or held state by using the **vstack join-window-status index** *client-id* {**allowed** | **held**} privileged EXEC command.

Updating Client Switches

Supported types of image and configuration updates:

- Zero-touch update—For a client with no configuration. This could be for the initial installation of an image and configuration on a new client, for image and configuration installation on a client after a **write erase** and **reload**, or, in case of a replacement switch, if **vstack backup** is enabled. The Smart Install network must run DHCP to perform zero-touch updates.

  On all clients, prior to Cisco IOS Release XE 3.5.0E and Cisco IOS 15.2(1)SG, only image+config zero-touch upgrades were supported. With Cisco IOS Release XE 3.6.0E and Cisco IOS Release 15.2(1)SG, image+config zero-touch upgrade are no longer mandatory; zero-touch config alone and zero-touch image alone upgrades are now supported on all clients.

- On-demand update—For clients that are already in the network and connected to the director. On-demand updates can be performed on single client or on all clients that belong to a built-in group. DHCP is not required for on-demand updates. The director needs the IP address of a client for a single-client update if the client is not in a built-in group. For an on-demand update of a client running an image earlier than 12.2(52)SE, the client must have an enable password and an IP interface configured.

You can do zero-touch or on-demand updates to any Smart Install client switches. You can also use the **vstack download-image** and **vstack download-config** privileged EXEC commands from the director to update the image or configuration of any switch as long as the director has a connection (directly or through another switch) to the switch. You can also telnet to a client switch and use the **archive download-sw** privileged EXEC command to update switch software. When you telnet to a client switch, you must know the switch enable passwords to do any configuration.

Beginning with Cisco IOS Release 12.2(58)SE, 15.1(1)SY, 15.0(2)SE, 3.2(0)SE and later, 3.6.(0)E, you can perform a simultaneous update of multiple clients that have the same product ID and password by entering the index numbers from the director database in the **vstack download-image** privileged EXEC command.

Zero-Touch Installation

A zero-touch installation is an update initiated by the director on a client switch that has no configuration. You can perform a zero-touch installation on Smart Install capable switches and non-Smart Install switches. The zero-touch installation occurs automatically with little or no intervention. A switch with no configuration can be a new, out-of-box switch or one on which you have entered the **write erase** and **reload** privileged EXEC commands.

During a zero-touch installation, do not touch the console keyboard or attempt to enter a command or auto return on the switch. Else, the auto install and Smart Install processes stop. To recover and restart the process, you need to return to the system prompt, enter **write erase** and **reload** commands, and restart the process.

During a zero-touch installation, the VLAN specified in the seed configuration for a particular client should be the same as the startup VLAN on the director. If it is not, the configuration backup process fails.

If the TFTP server is the director, the file is saved in the director root directory. If the server is another device, it is saved in the *tftproot directory*. This is the default directory in the TFTP server where the files to be sent using TFTP are stored. The imageclist file, the new configuration file, and the image are also stored in this directory.

Connecting to a Client Switch

To connect to the client switch command-line interface, enter the **vstack attach** {*client-index* | *client_ip_address*} privileged EXEC command. The client-index number represents active clients in the Smart Install network, displayed in the command-line help by entering a question mark (?) after the **vstack attach** command. The same client number is valid until the client reboots.

```
Director# vstack attach ?
  1       c3750-2042 @ IP 10.0.0.1 : MAC 0000.0040.4080
  2       c3750-2045 @ IP 10.0.0.2 : MAC 0000.000c.0d80
  A.B.C.D  IP address of remote node to attempt attaching to
```

To attach to a client, the client switch must be configured for telnet service and have a configured enable password.

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

- 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 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 IBD 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** *ip_ address*	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** *vlan_value*	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	**vstack dhcp-localserver** *poolname*	Creates a name for the Smart Install DHCP server address pool, and enter vstack DHCP pool configuration mode.

	Command	Purpose
Step 6	**address-pool** *network-number mask prefix-length*	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** *ip_address*	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** *address*	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** *poolname*	Creates a name for the DHCP server address pool, and enters DHCP pool configuration mode.
Step 3	**bootfile** *filename*	Specifies the name of the configuration file to be used.
Step 4	**network** *network-number mask prefix-length*	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** *address*	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

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 *ip_ address*	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 *vlan_value*	Specifies the default VLAN that the director should use for Smart Install management.

	Command	Purpose
Step 5	**vstack image** {**flash:***image_name*.**tar** | **tftp://***location image_name*.**tar**}	Enters the location and image.
		Note Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• **flash:***image_name*.**tar**—Enter if the director is the TFTP server and the image is in the director flash memory.
		Note The images for the Catalyst 3850 and 3650 platforms are bundled with a .bin extension; the.tar extension is not available.
		Note Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:**
		Note The images for the Catalyst 3850 and 3650 platforms are bundled with a **.bin** extension; the **.tar** extension is not available.
		• **tftp://***location image_name*.**tar**
		• *image_name*.**tar**—Enter the name of the default image tar file for clients in the network.
Step 6	**vstack config** {**flash:** *config.txt* | **tftp://***location config.txt*}	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.
		Note Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• For location, enter **flash:** if the TFTP server is the director and the configuration file is in the director flash memory.
		Note Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:**.
		• 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*.
		• *config.txt*—Enter the filename of the default seed configuration file for clients in the network.

	Command	**Purpose**
Step 7	**vstack script** {**flash:** *post_install.txt* | **tftp://***location post_install.txt*}	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. **Note** Although you must provide the image or the config, or the image and the config, the post install script is optional. this comment applies to all locations below where post-install configuration is described **Note** Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:**. • For location, enter **flash**: if the TFTP server is the director and the post install file is in the director flash memory. **Note** Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:** • 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*. • *post_install.txt*—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** *ip_ address*	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** *vlan_value*	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	**vstack group built-in** *product_family1 port_config*	Identifies the first built-in group product ID, and enters Smart Install group configuration mode for the group.

	Command	**Purpose**
Step 6	**image** *location image_name*.**tar**	Enters the location and image name for group 1.
		• For location, enter **flash:** (if the TFTP server is the director and the file is stored in the director flash memory).
		Note Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:**.
		• 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.
		Note Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		Note The images for the Catalyst 3850 and 3650 platforms are bundled with a **.bin** extension; the **.tar** extension is not available.
		• *image_name*.**tar**—Enter the name of the image tar file for clients in group 1.
Step 7	**config** *location config_filename*	Enters the location and configuration file for group 1.
		• For location, enter **flash:** (if the TFTP server is the director and the file is stored in the director flash memory).
		Note Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:**.
		• 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.
		Note Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• *config_filename*—Enter the filename of the configuration file for group 1.

	Command	**Purpose**
Step 8	**script** *location post_install_filename*	Enters the location and post install file for group 1.
		Note Although you must provide the image or the config, or the image and the config, the post install script is optional.
		• For location, enter **flash:** (if the TFTP server is the director and the file is stored in the director flash memory).
		Note Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:**.
		• 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.
		Note Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• *post_install_filename*—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** *product_family2 port_config*	Identifies the second built-in group product ID, and enters Smart Install group configuration mode for the group.
Step 11	**image** *location image_name*.**tar**	Enters the location and image name for group 2.
		• For location, enter **flash:** (if the TFTP server is the director and the file is stored in the director flash memory).
		Note Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:**.
		• 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.
		Note Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		Note The images for the Catalyst 3850 and 3650 platforms are bundled with a **.bin** extension; the **.tar** extension is not available.
		• *image_name*.**tar**—Enter the name of the image tar file for clients in group 2.

	Command	**Purpose**
Step 12	**config** *location config_filename*	Enters the location and configuration file for group 2.
		• For location, enter **flash:** (if the TFTP server is the director and the file is stored in the director flash memory).
		Note Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:**.
		• 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.
		Note Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• *config_filename*—Enter the filename of the configuration file for group 2.
Step 13	**script** *location post_install_filename*	Enters the location and post install file for group 2.
		Note Although you must provide the image or the config, or the image and the config, the post install script is optional.
		• For location, enter **flash:** (if the TFTP server is the director and the file is stored in the director flash memory).
		Note Instead of **flash:,** you can also enter **flash0:**, **flash1:**, or **usb:**.
		• 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.
		Note Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• *post_install_filename*—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-ipbaselmk9-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** *ip_ address*	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** *vlan_value*	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	**vstack download-image tar** *image_URL* {*ip_address* | **index** *name*} *remote_switch_password* [**override**] **reload** [**in** *time*] or **vstack download-image built-in** *product_family port_config remote_switch_password* [**override**] **reload** [**in** *time*] or **vstack download-image** {*imagelist_file _URL* {*ip_address* | **index** *name*} | **built-in** *product_family port_config*} *remote_switch_password* [**override**] **issu** [**allow-reload**] [**in** *time*]	Starts an on-demand tar image download on a Smart Install client switch: • Enter the *image_URL* and location and the IP address of the client. or Enter the *imagelist_*file and location and the IP address of the client (for releases earlier than 12.2(55)SE). • *ip_address*—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. **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. • *remote_switch_password* —Enter the password for the client switch. **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). • (Optional) **override**—Overrides the existing image on the client switch. • (Optional) **issu** attempts to upgrade using ISSU. • *allow-reload* (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 {*config_URL ip_address* | **built-in** *product_family port_config*} *remote_switch_password* **startup** [**reload**] [**in** *time*]	Starts an on-demand configuration download on a Smart Install client switch: • 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. **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. The remaining keywords and arguments have these meanings: • *remote_switch_password* —Enters the password for the client switch. **Note** A *password* is required only for switches that are not Smart Install capable. It is not required for switches already in the Smart Install network. • **startup**—Applies the configuration to the switch startup configuration. • (Optional) **reload**—Reloads the switch. • (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.
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** *ip_ address*	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** *vlan_value*	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	**vstack group custom** *group_name* **connectivity**	Identifies a custom group based on a connectivity match, and enters Smart Install group configuration mode for the group.
Step 6	**match host** *ip_address* **interface** *interface-id*	Identifies the client switches for the custom group: • **host** *ip_address*—The IP address of the upstream neighbor of the client (this could be the director or an intermediate device). • **interface** *interface-id*—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** *location image_name***.tar**	Enters the location and image file for the custom group.
		• *location*—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:**.
		Note Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		Note The images for the Catalyst 3850 and 3650 platforms are bundled with a **.bin** extension; the **.tar** extension is not available.
		• *image_name***.tar**—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** *location config_filename.*	Enters the location and configuration file for the custom group.
		• *location*—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:**.
		Note Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• *config_filename*—The filename of the configuration file for the group.
Step 9	**config** *location post_install_filename*	Enters the location and post install file for the custom group.
		Note Although you must provide the image or the config, or the image and the config, the post install script is optional.
		• *location*—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:**
		Note Although visible in the command-line help, these options are unsupported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• *post_install_filename*—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 textgroup2 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 *ip_ address*	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 *vlan_value*	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	vstack group custom *group_name* mac	Identifies a custom group based on a MAC address match, and enters Smart Install group configuration mode for the group.
Step 6	match *mac_address*	Enters the MAC address of the client switch to be added to the custom group. Repeat the command for each MAC address to be added. **Note** To see MAC addresses of switches in the Smart Install network, enter the **show vstack neighbors all** privileged EXEC command. Switches added to the group must be able to use the same image and configuration file.

	Command	**Purpose**
Step 7	**image** *location image_name***.tar**	Enters the location and image file for the custom group.
		• *location*—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:.**
		Note Although visible in the command-line help, these options are not supported: **flash1:, ftp:, http:, https:, null:, nvram:, rcp:, scp:, system:, tmpsys:.**
		Note The images for the Catalyst 3850 and 3650 platforms are bundled with a **.bin** extension; the **.tar** extension is not available.
		• *image_name***.tar**—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** *location config_filename*	Enters the location and configuration file for the custom group.
		• *location*—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:.**
		Note Although visible in the command-line help, these options are not supported: **flash1:, ftp:, http:, https:, null:, nvram:, rcp:, scp:, system:, tmpsys:.**
		• *config_filename*—The filename of the configuration file for the group.

	Command	Purpose
Step 9	**script** *location post_install_filename*	Enters the location and post install file for the custom group. **Note** Although you must provide the image or the config, or the image and the config, the post install script is optional. • *location*—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:** **Note** Although visible in the command-line help, these options are unsupported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.** • *post_install_filename*—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 *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 textgroup3 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** *ip_ address*	Configures the device as Smart Install director be 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** *vlan_value*	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	**vstack group custom** *group_name* **stack**	Identifies a custom group based on matching the stack number and enter Smart Install group configuration mode for the group.
Step 6	**match** *switch_number stack product_family port_config*	Identifies the client switches for the custom group: • *switch_number*—Number of the switch in the stack. The range is from 1 to 9. • *product_family*—Select the stack product family from the command-line help. • *port_config*—Switch port configuration. To see the available port configurations, enter a **?** after the product family.
Step 7	**image** *location image_name***.tar**	Enters the location and image file for the custom group. • *location*—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:**. **Note** Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.** **Note** The images for the Catalyst 3850 and 3650 platforms are bundled with a **.bin** extension; the **.tar** extension is not available. • *image_name***.tar** is the image tar file that you want to download.

	Command	**Purpose**
Step 8	**config** *location config_filename.*	Enters the location and configuration file for the custom group.
		• *location*—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:**.
		Note Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		• *config_filename*—The filename of the configuration file for the group.
Step 9	**script** *location post_install_filename*	Enters the location and post install file for the custom group.
		Note Although you must provide the image or the config, or the image and the config, the post install script is optional.
		• *location*—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:**.
		Note Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
		post_install_filename—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 *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
```

Cisco Smart Install Configuration Guide

```
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** *ip_ address*	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** *vlan_value*	Specifies the default VLAN that the director should use for Smart Install management.
Step 5	**vstack group custom** *group_name* **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** *product-id*	Enters the product ID of the client switches in the custom group. **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.
Step 7	**image** *location image_name***.tar**	Enters the location and image file for the custom group. • *location*—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:**. **Note** Although visible in the command-line help, these options are not supported: **flash1:, ftp:, http:, https:, null:, nvram:, rcp:, scp:, system:, tmpsys:.** **Note** The images for the Catalyst 3850 and 3650 platforms are bundled with a **.bin** extension; the **.tar** extension is not available. • *image_name***.tar**—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	**config** *location config_filename.*	Enters the location and configuration file for the custom group.
		• *location*—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:**.
		Note Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:**.
		• *config_filename*—The filename of the configuration file for the group.
Step 9	**script** *location post_install_filename*	Enters the location and post install file for the custom group.
		Note Although you must provide the image or the config, or the image and the config, the post install script is optional.
		• *location*—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:**.
		Note Although visible in the command-line help, these options are not supported: **flash1:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:**.
		• *post_install_filename*—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 *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 textgroup4 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

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 DCHP 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** *ip_ address*	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** *vlan-id*	Specifies the VLAN for Smart Install management.

	Command	Purpose
Step 5	**vstack startup-vlan** *vlan_value*	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 *vlan-id* 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 SKUs 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** *supervisor type* {*chassis type* | *all>*}	Enables group mode. *supervisor_type* is just one parameter. You must select from the list as the first example below illustrates. Use *chassis type* to configure the configuration (or image) for a particular chassis. Use *all* to configure all chassis supporting the *supervisor type*.
Step 3	Switch(config-vstack-group)# [**no**] **config** *path_to_config_file*	Configures the config file (i.e., *path_to_config_file*) for the group. Use the **no** keyword to unconfigure.
Step 4	Switch(config-vstack-group)# [**no**] **image** *path_to_image_file*	Configures the image file (i.e., *path_to_image_file*) for the group. Use the **no** keyword to unconfigure.

	Command	Purpose
Step 5	`Switch(config-vstack-group)# [`**`no`**`] `**`script`** `path_to_post_install_file`	Configures the post install file (i.e., *path_to_post_install_file*) 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 appears 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 appears 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	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]**	Starts an on-demand image download on a Smart Install client switch: o Enter the *imagelist* 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. *imagelist* is a text file that contains the name of the image that you want to download. **Note** The image file must be a tar and not a bin file. o The **built-in** option enables you to select the product family and port configuration from the command-line help. **Note** A group can be used to upgrade clients with the on-demand cli, only if that particular group is already configured. o *remote_switch_password* defines the password for the client switch. o (Optional) *override* overrides the existing image on the client switch. o **issu** attempts to upgrade using ISSU. o *allow-reload* (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**, **vlan**, **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.

Comma's 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.)

Valid CLI example include:

```
"sdm prefer degault"
"vlan 12" "name TEST" "exit"  and all following examples are invalid
'sdm prefer default'
'vlan 123' , 'name VLAN' , 'exit'

>"vlan 123" "name VLAN" "exit"
```

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 VLAN 123 must be on the same line in the post install text file:

```
"vlan 123" "name VLAN" "exit"
```

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

```
"vlan 123" "system mtu 1600"
```

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

```
"system mtu 1600"
"vlan 123" "name VLAN" "exit"
"sdm prefer default"
```

mtu, **vlan**, **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** *path_to_script_file*	Configures script file *path_to_script_file* for the default mode.
		path_to_script_file 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 *switch_family port_config*	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.
Step 3	[no] script *path_to_script_file*	Configures the script file ***path_to_script_file*** for the **built-in** group.
		path_to_script_file 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 *group_name* {mac|connectivity|stack|product-id}	Enables group_mode.
		Use *group_name* to configure image, config, or script for a particular custom group.

	Command	Purpose
Step 3	[**no**] **script** *path_to_script_file*	Configure script_file *path_to_script_file* for the custom group.
		path_to_script_file 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 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**

C H A P T E R **3**

Cisco Smart Install CLI Commands

- vstack vlan, page 3-71

clear vstack

To clear the director database or the download list, use the **clear vstack** privileged EXEC command on the Smart Install director.

clear vstack {**director-db** [**entry** *index-number*] | **download-list** [**entry** *status-number*}

Syntax Description

director-db	Clears all entries in the Smart Install director database.
entry *index-number*	(Optional) Clears the specified client index from the Smart Install director database. The index number range is from 1 to 255.
download-list	Clears the Smart Install download-status list, a table of the Smart Install image and configuration download successes and failures.
entry *status-number*	(Optional) Clears an entry in the Smart Install download-status list. The entry number range is 1 to 255.

Defaults   None

Command Modes   Privileged EXEC

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(58)SE	The **entry** *index-number* keywords were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE 3.5.0E and Cisco IOS 15.2(1)SG	The **entry** *status-number* keyword was added on the Catalyst 3750 and Catalyst 4500 series switches.
15.0(2)EX	This command was integrated into Cisco IOS Release15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   You can enter this command only on a director.

Use the **entry** *index-number* keywords to remove inactive clients from the director database. However, take care not to delete valid (active) entries from the director database. If you enter the client index number of a valid client and configuration backup is enabled, a replacement switch does not get the configuration file. The switch sends a message to alert you of this.

Prior to Cisco IOS Release XE 3.5.0E and Cisco IOS Release 15.2(1)SG, the Catalyst 3750 and Catalyst 4500 series switches provided the **clear vstack download-status** command, which resulted in deleting all the entries in one-shot. With Release Cisco IOS Release XE 3.5.0E and Cisco IOS Release 15.2(1)SG, we provide the **clear vstack download-list entry** command, which enables you to delete a single entry in the download status table. This table can be viewed with the **show vstack download-status** command.

Examples   This example shows how to clear the director database:

```
Switch# clear vstack director-db
```

This example shows the message received if you try to delete a valid client from the director database:

```
Switch# clear vstack director-db entry 2
Config backup feature is ON. If IBC is replaced by another switch, that wont get backup
config file. proceed?[confirm]
```

This example shows how to delete a single entry in the download status table with an index of 1:

```
Switch# clear vstack download-list entry 1
status of upgrading client will not have correct status on clearing the download list.
proceed?[confirm]
```

This example shows how to delete a single entry in the download status table with an index 1:

```
Switch# show vstack do
SmartInstall:  ENABLED
Total no of entries : 2
No   client-IP        client-MAC      Method          Image-status  Config-status   Script-status
===  ==============   ==============  ==============  ============  =============   =============
1    10.1.1.4         0017.9570.c780  zero-touch      UPGRADED        UPGRADED        UPGRADED
2    10.1.1.6         0026.985b.bc80  zero-touch      UPGRADED        UPGRADED        UPGRADED
3    10.1.1.11        0030.7870.0c30  zero-touch      UPGRADED        UPGRADED        UPGRADED

Switch# clear vstack download-status entry 2
status of upgrading client will not have correct status on clearing the download entry.
proceed?[confirm]
Switch# show vstack download-status
SmartInstall:  ENABLED
Total no of entries : 1
No   client-IP        client-MAC      Method          Image-status  Config-status   Script-status
===  ==============   ==============  ==============  ============  =============   =============
1    10.1.1.4         0017.9570.c780  zero-touch      UPGRADED        UPGRADED        UPGRADED
2    10.1.1.11        0030.7870.0c30  zero-touch      UPGRADED        UPGRADED        UPGRADED
```

Related Commands

Command	Description
vstack basic	Enables the switch or router as the Smart Install director. This command is accepted only if the director IP address is on the switch or router.
vstack director	Configures a Smart Install director IP address.

debug vstack

To enable debugging of the Smart Install feature, use the **debug vstack** privileged EXEC command. To disable debugging, use the **no** form of this command.

> **debug vstack** {**all** | **backup** | **cli** | **director-db** | **download** | **emulation** | **fsm** | **group** | **join-window** | **protocol**

> **no debug vstack** {**all** | **backup** | **cli** | **director-db** | **download** | **emulation** | **fsm** | **group** | **join-window** | **protocol**

Syntax Description

all	Displays all Smart Install debug messages.
backup	Displays all Smart Install backup management debug messages.
cli	Displays Smart Install command-line interface (CLI) debug messages.
director-db	Displays Smart Install director database messages.
download	Displays Smart Install download debug messages.
emulation	Displays Smart Install emulation debug messages.
fsm	Displays Smart Install session-management debug messages.
group	Displays Smart Install group debug messages.
join-window	Displays all Smart Install join window debug messages.
protocol	Displays Smart Install protocol debug messages.

Command Default   Smart Install debugging is disabled.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   The **undebug vstack** command is the same as the **no debug vstack** command.

Examples   This is example output from the **debug vstack all** command on a client:

```
switch# debug vstack all
```

```
Vstack debug all debugging is on
*May 15 22:37:56.739: VSTACK_DIR_DB: smi_parse_cdp_cache_entry: Got Neighbor on the port
Gi2/5/13
*May 15 22:37:56.739: VSTACK_DIR_DB: smi_parse_cdp_cache_entry: Mac addr after masking
Neig mac 6073.5cb6.6000, Local Mac 0026.99c9.b000
*May 15 22:37:56.739: VSTACK: smi_parse_cdp_cache_entry:processing the cdp pkt for mgmt
vlan
*May 15 22:37:56.739: VSTACK:
received vlan_plus_seqno=20370001, seq no for vlan = 8247,prev_seq_no=8247
*May 15 22:37:56.739: VSTACK_DIR_DB: smi_parse_cdp_cache_entry:string in parse
WS-C3750G-24TS-1U
*May 15 22:37:56.739: VSTACK:
smi_send_mgmt_vlan_to_cdp: Seq no + Mgmt Vlan = 20370001. After conversion Mgmt vlan
withseq no = 540475393,len=9
```

Related Commands*	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.

match (Smart Install group configuration)

To configure the match type for a Smart Install custom group, use the **match** Smart Install group configuration mode command on the Smart Install director. To return to the default setting, use the **no** form of this command. The available keyword depends on the type of custom group defined.

> **match host** *ip_address* **interface** *name*
>
> **no match host** *ip_address* **interface** *name*
>
> **match mac** *mac_address*
>
> **no match mac** *mac_address*
>
> **match** *product-id*
>
> **no match** *product-id*
>
> **match** *switch_stack_number product_family port_config*
>
> **no match** *switch_stack_number product_family port_config*

Syntax Description		
	host *ip_address* **interface** *name*	This keyword is visible when the custom group is defined by connectivity. Configures a client group based on the switch topology, where host *ip_address* is the IP address of the upstream neighbor of the client. If a client matches more than one group characteristic, a connectivity match takes precedence over product ID or stack number, but not over MAC address matches.
		Identifies the interface on the upstream neighbor to which the client is connected. The interface ID must be the full identifier for the interface, such as GigabitEthernet 2/0/1.
	mac *mac_address*	This keyword is visible when the custom group is defined by the **mac** keyword. Configures a client group to include switches with the specified MAC addresses. Enter a **match** command for each MAC address to be included. If a client matches more than one group characteristic, a MAC address match takes precedence over any other match.
	product-id	This argument is visible when the custom group is defined by product-id. A client group based on the model number of the switch associated with the group, where product-id is the product ID for the group starting with WS-Cnnnn-* (for example, WS-C2960-48TC-L).
		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 when assigning image and configuration files.

switch_stack _number *product_family* *port_config*	This argument is visible when the custom group is defined by the stack keyword. Configures a client in a group based on custom stack configuration.
	• *switch_number*—Number of the switch in the stack. The range is from 1 to 9.
	• *product_family*—Stack product family. To see the available product families, enter a **?** after the switch number.
	• *port_config*—Switch port configuration. The available configurations vary, depending on the product family. To see the available port configurations, enter a **?** after the product family.
	If a client matches more than one group characteristic, a stack match takes precedence over product ID, but not over MAC address or connectivity matches.

Defaults None

Command Modes Smart Install group configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(55)SE	The *mac_address* match option was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines Although you can enter this command on a client, the configuration does not take effect. Only configuration commands entered on the director are valid. If a client becomes a director at some point, the configuration file entered on it is then valid.

To define the custom group type and enter Smart Install group configuration mode, enter the **vstack group custom** *group_name* {**connectivity** | **mac** | **product-id** | **stack**} global configuration command.

Use the **match host** *ip_address* **interface** *name* command to define connectivity groups based on the network topology; that is, based on the upstream neighbor to which the client is connected. The upstream neighbor could be the director or an intermediate device. If a client matches more than one group characteristic, a connectivity match takes precedence over product ID or a stack match, but not over a MAC address match.

Use the **match** *mac_address* command to define groups based on switch MAC addresses. You can include switches with the same or different product IDs, as long as they use the same image and configuration file. Enter the **show vstack neighbors all** privileged EXEC command to see the MAC addresses of switches in the Smart Install network.

Use the **match** *product-id* command to match any product ID, including those not defined in the **vstack group built-in** command. These could be supported devices that were not shipping when the software version was released.

Use the **match** *switch_stack _number product_family port_config* command to identify switches in a stack. For example, **match 3 3750e WS-3750E-24PD** matches switch 3 in a Catalyst 3750E stack with a port configuration of 24 PoE ports.

Examples

This example shows how to identify a custom group named *test* based on matching connectivity, to enter Smart Install group configuration mode, to specify that the group includes clients connected to the host with the IP address 2.2.2.2 through interface Gigabit Ethernet 0/1, and to identify the image and configuration files to be obtained through TFTP for the group:

```
Director(config)# vstack group custom test connectivity
Director(config-vstack-group)# match host 2.2.2.2 interface gigabitethernet0/1
Director(config-vstack-group)# image tftp://101.122.33.10/c3560-ipservices-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-post_install.txt
```

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(config)# vstack group custom textgroup3 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 0019.309d.5c80
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://101.122.33.10/3560-24-post_install.txt
```

You can verify the group settings by entering the **show vstack group custom** privileged EXEC command.

Related Commands

Command	Description
show vstack group built-in	Displays configured Smart Install built-in groups.
vstack group custom	Configures Smart Install custom groups.

show vstack

To display Smart Install information, use the **show vstack** privileged EXEC command on the Smart Install director or a client.

> **show vstack** {**config** | **host** *ip_address* | **join-window configuration** | **status** [**detail**]}

> **show vstack** {**download-status** [**detail**]

> **show vstack client** {**1** | *client_ ip_address* | **all** | **group** {**built-in** *product_family port_config chassis_config*| **custom** *group_name*} *client-password* {**running-config** | **tech-support** | **version**}

> **show vstack group** {**built-in** *product_family chassis_config* {[*port_config*] **detail}** [**configured**]} | **custom** [*group_name*] **detail**}

> **show vstack neighbors** [**1** | *client_ ip_address* | **all** | **group built-in** *product_family port_config chassis_config*

Syntax Description	config	Displays Smart Install configuration parameters.
	host	Displays information about a client within the Smart Install topology. This command is available only on the director.
	ip_address	The IP address of the director or a client.
	join-window configuration	Displays the join-window configurations.
	status	Displays the status of the CDP database. This command is available only on the director.
	detail (Optional)	Displays detailed information for the previous keyword. For example, **show vstack download-status detail** can display a detailed reason for a zero-touch update failure.
	download-status	Displays a tabulated output of the Smart Install image and configuration download successes and failures.
		Note Use this command to determine the status of updates.
		Note Beginning with IOS XE 3.6.0E (or 15.2.(2)E), the show **download-status** command displays the download upgrade of the image upgrade for a Catalyst 4500 platform. Additional fields are introduced in the output of the show **download-status** details command.
	client	Displays client information through the **remote** command
	1	Displays information about client 1 in the Smart Install network. Numbers are shown for as many clients as are in the network.
	client_ ip_address	Information about the client with the specified IP address.
	all	Displays information about all clients.
	group	Displays Smart Install group information.
	built-in	Displays information about preconfigured (built-in) groups.

product_family	The built-in product family. To see the available product families, enter **?** after **built-in**.
	If *product_family* is set to 4500 for Catalyst 4500 series switches.
port_config	The switch port configuration. The available configurations vary, depending on the product family. To see the available port configurations, enter **?** after the *product_family*.
	If *product_family* is set to 4500, *port_config* means supervisor configuration.
chassis_config	The chassis type to configure.
	If *product_family* is set to 4500, the chassis type selected here is supported by the supervisor engine assigned to *port_config*.
configured	This keyword displays only the groups that are configured rather than showing all the groups.
custom	Information about user-defined groups.
group_name	Th custom group name.
client_password	The password that is required to access the client switch to get information on **running-config	tech-support	version** of the client switch.
running-config	Displays the current operating configuration for the selected client.
tech-support	Displays system information for technical support assistance.
version	Displays system hardware and software status.
neighbors	Displays information about the specified neighbors:
	• **1**—Neighbors of client 1
	• *client_ip_address*—Neighbors of the specified client
	• **all**—All neighbors in the Smart Install network
	• **group**—Neighbors of the specified group or groups

Command Modes   Privileged EXEC

Note   The command with some, but not all, of the keywords are available at the user EXEC level.

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(55)SE	The **client**, **join-window configuration**, **neighbors**, **1**, **running-config**, **tech-support**, and **version** keywords were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release15.0(2)EX1.

3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.
15.2(2)E	The option for post install (script) was introduced for **show vstack config**, **show vstack download-status**, **show vstack download-status detail**, **show vstack status**, and **show vstack status detail** commands.
3.6.0E	The option **chassis type** for the **built-in** keyword was introduced.

Usage Guidelines   The outputs of the **show** commands are different when entered on the director or on the client. Not all keywords are available on the client.

In Cisco IOS Release 12.2(58)SE and later or Release 15.1(1)SY, the output of the **show vstack status** command shows whether or not Smart Install is enabled on the director. If enabled, it also includes this additional information about clients:

- Device status (Smart Install capable or not)
- Health status (active or inactive)
- Join-window status (allowed, hold, or denied), and
- Upgrade status for image or configuration (in progress, complete, or failed).

Beginning with Cisco IOS Release 3.6.0E (IOS 15.2(2)E), the output of the **show vstack status** command remains unchanged, but the meaning of the following fields have changed:

Note   These changes are for Catalyst 4500 Series Switch only.

- **Product-ID—***chassis-id* is used as the client's product ID and is collected from CDP. For an asymmetric chassis, the product ID may be updated dynamically.
- **MAC Address —**For a Catalyst 4500 standalone IBC, you use the chassis' MAC address whereas for VSS IBC, you use the virtual MAC selected while configuring VSS.

Note   The meaning of the fields **Hostname**, **IP** and **status** are unchanged; they are platform-independent.

If you disable Smart Install on the director by entering the **no vstack** global configuration command, the output of the **show vstack status** [**detail**] and **show vstack download-status** [**detail**] commands shows only Smart Install: DISABLED. The output of the **show vstack config** command shows the Smart Install configuration even though it is not in effect.

If the director is a Catalyst 4500 series switch, whether it is a single chassis or a VSS setup, only a single entry of the director appears in the output of the **show vstack status detail** command. The product ID shown is the chassis sku-id.

Beginning with IOS XE 3.6.0E (or 15.2.(2)E), the following apply:

- All the director entries (multiple, if the director is a stack) will be assigned the value '0,' and all the IBC stack members will have different entries (situation prior to IOS XE 3.6.0E (or 15.2.(2)E)) but they will all have the same device number.
- When you clear a DB entry and that IBC is a stack, the **clear vstack dir** command will remove all the stack entries from the database.

Examples   This is example output from the **show vstack config** command on a client:

```
Director# show vstack config
Role: Client
 Vstack Director IP address: 1.1.1.163
```

This is example output from the **show vstack config** command on a director:

```
Director# show vstack config
Role: Director
 Vstack Director IP address: 1.1.1.163
 Vstack Mode: Basic
 Vstack default management vlan: 1
 Vstack start-up management vlan:1000
 Vstack management Vlans: none
 Vstack Config file: tftp://1.1.1.100/default-config.txt
 Vstack Image file: tftp://1.1.1.100/c3750e-universalk9-tar.122-
 Vstack Script file: tftp://1.1.1.100/post-install.txt
 Join Window Details:
         Window: Open (default)
         Operation Mode: auto (default)
 Vstack Backup Details:
         Mode: On (default)
         Repository: flash:/vstack (default)
```

These are example outputs from the **show vstack download-status** command on a director:

```
Director# show vstack download-status
Total no of entries : 3
No   client-IP       client-MAC      Method          Image-status  Config-status  Script-status
===  ==============  ==============  ==============  ============  ============  ==============
1    172.20.249.3    001e.be67.3000  image-upgrade   UPGRADED      **            **
2    172.20.249.1    0022.5699.c800  zero-touch      UPGRADING     UPGRADED      UPGRADED
3    172.20.249.2    0022.0d26.6300  image-upgrade   NOT STARTED   **            **
```

This is example output from the **show vstack host** command:

```
Director# show vstack host 1.1.1.1
Host Info :
Code :
ClNum  MAC Address      Product-ID         IP_addr          DevID        status
=====  ==============  ==================  ===============  ==========  =========
1      001d.71ba.f780  WS-C2960PD-8TT-L    1.1.1.1          2960pd-47


Neighbor Info:

MAC Address      Dev ID           IP_addr          Local Int      Out Port
==============  ===============  ===============  =============  =============
0023.5e32.3780  3750e-163-smi    1.1.1.163        Fas 0/7        Gig 1/0/1
```

This is example output from the **show vstack join-window configuration** command:

```
Director# show vstack join-window configuration

Join Window Configuration Details:
         Window: Open (default)
           Mode: auto (default)
         No Join Window start/end dates and times configured
```

This is example output from the **show vstack status** command:

```
Director# show vstack status
SmartInstall:  ENABLED
Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
```

```
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress    I - done         X - failed
Config Upgrade:  c - in progress    C - done         x - failed
Director Database:
DevNo  MAC Address       Product-ID         IP_addr          Hostname    Status
=====  ==============    =================  ===============  ==========  =========
0      0018.7363.4200    WS-C3750-24TS      172.20.249.54    IBD-MXD-ST  Director
1      0016.4779.b780    WS-C3750G-24TS     172.20.249.54    IBD-MXD-ST  Director
2      d0d0.fd37.5a80    WS-C3750X-48P      172.20.249.54    IBD-MXD-ST  Director
3      0026.5285.7380    WS-C3750E-24TD     172.20.249.54    IBD-MXD-ST  Director
4      0024.13c6.b580    WS-C3750E-24TD     172.20.249.115   DEV-c6.b5c  S A a
5      0021.a1ab.9b80    WS-C2960-48TC-S    172.20.249.249   DEV-ab.9bc  S A a I C
6      0024.5111.0900    WS-C3750E-24TD     172.20.249.222   DEV-11.094  S A a I C
7      001d.45f3.f600    WS-C3750G-24TS     172.20.249.87    DEV-90.f64  S A a
8      0016.c890.f600    WS-C3750G-24TS     172.20.249.87    DEV-90.f64  S A a
9      001f.2604.8980    WS-C2960-48TC-S    172.20.249.89    DEV-04.89c  S A a I C
10     001b.d576.2500    WS-C3750E-24PD     172.20.249.91    DEV-a6.1cc  S A a I C
12     0cd9.9649.cb80    WS-C2960S-48TD-L   172.20.249.98    Switch      S A a
```

This is example output from the **show vstack status** command if you have disabled Smart Install on the director by entering the **no vstack** global configuration command:

```
Switch# show vstack status
SmartInstall:  ENABLED

Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress    I - done         X - failed
Config Upgrade:  c - in progress    C - done         x - failed
Director Database:
DevNo  MAC Address       Product-ID         IP_addr          Hostname    Status
=====  ==============    =================  ===============  ==========  =========
0      0023.04c2.95c0    WS-C4506-E         1.1.1.1          Switch      Director
4      68ef.bd08.6000    WS-C4507R-E        1.1.1.2          IBC_WOW-08  S I a C

Switch#
```

This is example output from the **show vstack status detail** command:

```
Director# show vstack status detail
SmartInstall:  ENABLED
-----------------------------------------------
Device Num    : 0
Device ID     : 3750e-163-smi
MAC Address   : 0023.5e32.3780
IP Addr       : 1.1.1.163
Hop value     : 0
Serial        : FDO1239V026
Product-ID    : WS-C3750E-24PD
Version       : 12.2(0.0.242)DEV
Image         : C3750E-UNIVERSALK9-M
Entry Role    : Entry
(N-1)HOP Entry : Already Root
Backup done   :  no
Latest backup file: none
Latest backup client name: none
File checksum   : none
Status          : Director
```

```
----------------------------------------------
Device Num      : 1
Device ID       : 3560g-10net-11
MAC Address     : 0013.c4b4.bc00
IP Addr         : 10.5.113.11
Hop value       : 1
Serial          : Not Found
Product-ID      : WS-C3560G-24PS
Version         : 12.2(50)SE3
Image           : C3560-IPSERVICESK9-M
Entry Role      : IBC Entry
(N-1)HOP Entry  : 0023.5e32.3780
Backup done     :  no
Latest backup file: none
Latest backup client name: none
File checksum    : none
Status           : NSI

----------------------------------------------
Device Num      : 2
Device ID       : 2960pd-47
MAC Address     : 001d.71ba.f780
IP Addr         : 1.1.1.1
Hop value       : 1
Serial          : FOC1138Z6P7
Product-ID      : WS-C2960PD-8TT-L
Version         : 12.2(0.0.242)DEV
Image           : C2960-LANBASEK9-M
Entry Role      : IBC Entry
(N-1)HOP Entry  : 0023.5e32.3780
Backup done     :  Yes
Latest backup file: flash:/vstack/2960pd-47-001d.71ba.f780.REV2
Latest backup client name: 2960pd-47
File checksum    : 426154BFAFE1425F527621DC8B647C38
Status           : ACT

Director# show vstack download-status detail
SmartInstall:  ENABLED
No 1:
client-ip: 172.20.249.3
client-hostname: Switch
client-mac: 001e.be67.3000
method: image-upgrade
config-fail-reason: NA
image-fail-reason: NA
script-fail-reason: NA
config downloaded at: -
image downloaded at: 02:47:39 UTC Mar 30 2011
script downloaded at: -

No 2:
client-ip: 172.20.249.1
client-hostname: Switch
client-mac: 0022.5699.c8000
method: zero-touch
config-fail-reason: NA
image-fail-reason: NA
script-fail-reason: NA
config downloaded at: 03:02:23 UTC Mar 30 2011
image downloaded at: -
script downloaded at: 02:47:39 UTC Mar 30 2011
```

```
No 3:
client-ip: 217.20.249.2
client-hostname: Switch
client-mac: 0022.0d26.6300
method: image-upgrade
config-fail-reason: NA
image-fail-reason: NA
script-fail-reason: NA
config downloaded at: -
image downloaded at: -
script downloaded at: -
```

This is example output from the **show vstack host** command:

```
Director# show vstack host 1.1.1.1
Host Info :
Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold  d - Denied
Image Upgrade:   i - in progress    I - done        X - failed
Config Upgrade:  c - in progress    C - done        x - failed
Script Upgrade:  p - in progress    P - done        F - failed
DevNo  MAC Address    Product-ID        IP_addr         Hostname    Status
=====  ==============  ================  ==============  ==========  =========
1      0023.348e.8e00  WS-C3750E-48TD    1.1.1.1         Switch.dom  S A a  C P


Neighbor Info:

MAC Address     Dev ID          IP_addr         Local Int     Out Port
==============  ==============  ==============  ============  =============
0024.5111.0880  Switch          2.2.2.1         Gig 1/0/19    Gig 1/0/9
```

This is example output from the **show vstack join-window configuration** command:

```
Director# show vstack join-window configuration

Join Window Configuration Details:
        Window: Open (default)
          Mode: auto (default)
          No Join Window start/end dates and times configured
```

This is example output from the **show vstack status** command:

```
Director# show vstack status
SmartInstall:  ENABLED
Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold  d - Denied
Image Upgrade:   i - in progress    I - done        X - failed
Config Upgrade:  c - in progress    C - done        x - failed
Script Upgrade:  p - in progress    P - done        F - failed
Director Database:
DevNo  MAC Address    Product-ID        IP_addr         Hostname    Status
=====  ==============  ================  ==============  ==========  =========
0      0018.7363.4200  WS-C3750-24TS     172.20.249.54   IBD-MXD-ST  Director
1      0016.4779.b780  WS-C3750G-24TS    172.20.249.54   IBD-MXD-ST  Director
2      d0d0.fd37.5a80  WS-C3750X-48P     172.20.249.54   IBD-MXD-ST  Director
3      0026.5285.7380  WS-C3750E-24TD    172.20.249.54   IBD-MXD-ST  Director
4      0024.13c6.b580  WS-C3750E-24TD    172.20.249.115  DEV-c6.b5c  S A a
5      0021.a1ab.9b80  WS-C2960-48TC-S   172.20.249.249  DEV-ab.9bc  S A a I C
6      0024.5111.0900  WS-C3750E-24TD    172.20.249.222  DEV-11.094  S A a I C P
7      001d.45f3.f600  WS-C3750G-24TS    172.20.249.87   DEV-90.f64  S A a
```

```
8       0016.c890.f600  WS-C3750G-24TS    172.20.249.87    DEV-90.f64  S A a
9       001f.2604.8980  WS-C2960-48TC-S   172.20.249.89    DEV-04.89c  S A a I C P
10      001b.d576.2500  WS-C3750E-24PD    172.20.249.91    DEV-a6.1cc  S A a I C
12      0cd9.9649.cb80  WS-C2960S-48TD-L  172.20.249.98    Switch      S A a
```

This is example output from the **show vstack status** command if you have disabled Smart Install on the director by entering the **no vstack** global configuration command:

```
Director # show vstack status
SmartInstall:  DISABLED
```

This is example output from the **show vstack status** command:

```
Switch# show vstack status
SmartInstall:  ENABLED

Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress    I - done         X - failed
Config Upgrade:  c - in progress    C - done         x - failed
Script Upgrade:  p - in progress    P - done         F - failed

Director Database:
DevNo  MAC Address     Product-ID        IP_addr          Hostname    Status
=====  ==============  ================  ===============  ==========  =========
0      0023.04c2.95c0  WS-C4506-E        1.1.1.1          Switch      Director
4      68ef.bd08.6000  WS-C4507R-E       1.1.1.2          IBC_WOW-08  S I a C P

Switch#
```

This is an example output from the **show vstack status detail** command:

```
Director# show vstack status detail
SmartInstall:  ENABLED
-----------------------------------------------
Device Num     : 0
Device ID      : 3750e-163-smi
MAC Address    : 0023.5e32.3780
IP Addr        : 1.1.1.163
Hop value      : 0
Serial         : FDO1239V026
Product-ID     : WS-C3750E-24PD
Version        : 12.2(0.0.242)DEV
Image          : C3750E-UNIVERSALK9-M
Entry Role     : Entry
(N-1)HOP Entry : Already Root
Backup done    :  no
Latest backup file: none
Latest backup client name: none
File checksum    : none
Status           : Director


-----------------------------------------------
Device Num     : 1
Device ID      : 3560g-10net-11
MAC Address    : 0013.c4b4.bc00
IP Addr        : 10.5.113.11
Hop value      : 1
Serial         : Not Found
Product-ID     : WS-C3560G-24PS
Version        : 12.2(50)SE3
Image          : C3560-IPSERVICESK9-M
```

```
Entry Role      : IBC Entry
(N-1)HOP Entry : 0023.5e32.3780
Backup done     :  no
Latest backup file: none
Latest backup client name: none
File checksum      : none
Status             : NSI


----------------------------------------------
Device Num      : 2
Device ID       : 2960pd-47
MAC Address     : 001d.71ba.f780
IP Addr         : 1.1.1.1
Hop value       : 1
Serial          : FOC1138Z6P7
Product-ID      : WS-C2960PD-8TT-L
Version         : 12.2(0.0.242)DEV
Image           : C2960-LANBASEK9-M
Entry Role      : IBC Entry
(N-1)HOP Entry : 0023.5e32.3780
Backup done     :  Yes
Latest backup file: flash:/vstack/2960pd-47-001d.71ba.f780.REV2
Latest backup client name: 2960pd-47
File checksum      : 426154BFAFE1425F527621DC8B647C38
Status             : ACT
```

Beginning with IOS XE 3.6.0E (or 15.2(2)E, Supervisor_ID is provided in the output of the **show vstack status detail** command, because Chassis_ID is displayed in the output of the **show vstack status** command and you require supervisor engine information to decide on the image type provided to a switch. Supervisor_ID is received through the new CDP APP TLV sent by IBC. IBD gathers this information and updates the director database. For a dual supervisor chassis or a VSS system, the supervisor type across a switch should match; hence, a single CDP APP TLV will suffice.

✎
Note   The Supervisor field will display "not applicable" for platforms that do not have the necessary supervisor engines.

```
Example:
Device ID       : IBC_WOW-08.603f
MAC Address     : 68ef.bd08.6000
IP Addr         : 1.1.1.2
Hop value       : **
Serial          : FOX1352H3FK
Product-ID      : WS-C4507R-E
Supervisor      : WS-X45-SUP7-E
Version         : 03.06.00.E
Image           : cat4500e-UNIVERSALK9-M
Entry Role      : IBC Entry
(N-1)HOP Entry : 0023.04c2.95c0
Backup done     :  Yes
Latest backup file: bootflash:/vstack/IBC_WOW-08.603f-68ef.bd08.6000.REV2
Latest backup client name:
File checksum      : 00000000000000000000000000000000
Switch replace type: Same Switch
SMI Version     : 1
Status             : S I a C
Capability      : Network derived SMI management VLAN supported

Switch#
```

The following example illustrates how to configure a built-in group for the Catalyst 4500 switch by selecting the chassis model:

```
Switch# show vst group built-in 4500 sup8-e 4503 de
---------------------------------------------
Group Name: sup8-e 4503
No Image name specified
No config file name specified
No Script file specified
Switch#
```

In the following example, we select the supervisor type rather than the chassis model. This displays all the groups for the chassis that support that particular supervisor engine.

```
Switch# show vst group built-in 4500 sup8-e de
---------------------------------------------
Group Name: sup8-e 4503
No Image name specified
No config file name specified
No Script file specified
---------------------------------------------
Group Name: sup8-e 4506
No Image name specified
No config file name specified
No Script file specified
---------------------------------------------
Group Name: sup8-e 4507r+e
No Image name specified
No config file name specified
No Script file specified
---------------------------------------------
Group Name: sup8-e 4510r+e
No Image name specified
No config file name specified
No Script file specified
Switch#
```

This is example output from the **show vstack client running-config** command for client 1:

```
Director# show vstack client 1 password running-config
----- [show running-config] for 2960pd-47 @ 1.1.1.1 -----

Building configuration...

Current configuration : 2723 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2960pd-47
!
boot-start-marker
boot-end-marker
!
enable password test
!
!
!
no aaa new-model
```

```
system mtu routing 1500
authentication mac-move permit
<output truncated>
```

This is example output from the **show vstack group built-in** command:

```
Director# show vstack group built-in
2918        2918 product family
2960        2960 product family
2960c       2960c product family
2960cg      2960cg product family
2960g       2960g product family
2960s       2960s product family
2960s-fe    2960s-fe 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
3750        3750 product family
3750e       3750e product family
3750g       3750g product family
3750x       3750x product family
3850        3850 product family
3650        3650 product family
nme-es      NME-ES product family
sm-d-es2    SM-D-ES2 product family
sm-d-es3    SM-D-ES3 product family
```

This is example output from the **show vstack group custom detail** command:

```
Director # show vstack group custom detail
---------------------------------------------
Group Name:   2960-8
Image:        tftp://1.1.1.100/c2960-lanbasek9-tar.122-0.0.221.DEV.tar
Config File:  tftp://1.1.1.100/2960-8-config.txt
Connectivity Details (IP Adress:Interface):
 1.1.1.163:FastEthernet1/0/1
---------------------------------------------
Group Name:   WS-C3560E-24TD
Image:        tftp://1.1.1.0/c3560e-ipbasek9-tar.122-0.0.221.DEV.tar
Config File:  tftp://1.1.1.100/3560e-config.txt
Product-ID:   WS-C3560E-24TD
---------------------------------------------
Group Name:   lotr-stack
Image 1:      tftp://1.1.1.100/c3750e-universalk9-tar.122-0.0.221.DEV.tar
Image 2:      tftp://1.1.1.100/c3750-ipservicesk9-tar.122-0.0.221.DEV.tar
Config File:  tftp://1.1.1.100/lotr-stack-config.txt
Stack Details (Switch_number:Product-id):
               1:3750G 24
               3:3750G 24POE
```

This is example output from the **show vstack group custom detail** command:

```
Director #show vstack group custom detail
---------------------------------------------
Group Name:   2960-8
Image:        tftp://1.1.1.100/c2960-lanbasek9-tar.122-0.0.221.DEV.tar
Config File:  tftp://1.1.1.100/2960-8-config.txt
Connectivity Details (IP Adress:Interface):
 1.1.1.163:FastEthernet1/0/1
```

```
          ----------------------------------------------
          Group Name:    WS-C3560E-24TD
          Image:         tftp://1.1.1.0/c3560e-ipbasek9-tar.122-0.0.221.DEV.tar
          Config File:   tftp://1.1.1.100/3560e-config.txt
          Product-ID:    WS-C3560E-24TD
          ----------------------------------------------
          Group Name:    lotr-stack
          Image 1:       tftp://1.1.1.100/c3750e-universalk9-tar.122-0.0.221.DEV.tar
          Image 2:       tftp://1.1.1.100/c3750-ipservicesk9-tar.122-0.0.221.DEV.tar
          Config File:   tftp://1.1.1.100/lotr-stack-config.txt
          Stack Details (Switch_number:Product-id):
                         1:3750G 24
                         3:3750G 24POE
```

This is example output from the **show vstack neighbors** command for client 1:

```
Director #show vstack neighbors 1
MAC Address     Dev ID          IP_addr         Local Int       Out Port
==============  ==============  ==============  =============   ============
001d.71ba.f780  2960pd-47       1.1.1.1         Gig 1/0/1       Fas 0/7
```

	Command	Description
Related Commands	**vstack basic**	Enables the switch or router to be the Smart Install director. This command is accepted only if the director IP address is on the switch or router.
	vstack director	Configures a Smart Install director IP address.

vstack

To enable the Smart Install feature on a director or client device, use the **vstack** global configuration command. To disable the Smart Install feature on a director or client device, use the **no** form of this command.

> **vstack**

> **no vstack**

Syntax Description   This command has no keywords.

Defaults   Smart Install is enabled.

Command Modes   Global configuration

Command History

Release	Modification
12.2(58)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Configuring Smart Install on a director or client switch opens TCP port 4786 on the director and on the client. You can use the **no vstack** global configuration command on a director or client device to disable Smart Install and shut down the TCP port.

To enable Smart Install after it has been disabled, enter the **vstack** global configuration command.

When you enter the **no vstack** command to disable Smart Install on a director or client device, if the Smart Install configuration is already present, it remains in the running configuration but does not take effect. This includes the Smart Install director IP address and other Smart Install configurations, such as group configurations.

If you disable Smart Install on a director and there were Smart Install DHCP IP addresses configured, you need to manually delete them.

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.

No warning message is generated when you disable Smart Install.

To reenable Smart Install on a device, enter the **vstack** global configuration command.

To see if Smart Install is enabled on a device, enter the **show vstack status** privileged EXEC command.

If you disable Smart Install on the director by entering the **no vstack** global configuration command, the output of the **show vstack status** [**detail**] and **show vstack download-status** [**detail**] commands shows only Smart Install: DISABLED. The output of the **show vstack config** command shows the Smart Install configuration even though it is not in effect.

Examples   This example shows how to disable Smart Install on the device:

```
Director(config)# no vstack
Director(config)#
```

Related Commands

Command	Description
show vstack status	Displays the Smart Install status.

vstack attach

To connect to a client from the director, use the **vstack attach** privileged EXEC command on the director.

> **vstack attach** {*client - index* | *client IP address*}

Syntax Description

client - index	Client index number from the list of active clients within the Smart Install network.
client IP address	Client IP address.

Command Default   None

Command Modes   Privileged EXEC mode

Command History

Release	Modification
12.2(55)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Use this command to connect to the client user interface from the director. This command is a wrapper for the **telnet** command. Select the client either by 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 same client-index numbers can be used in additional configurations.

If you are running Supervisor Engine 7-E, Supervisor Engine 7L-E, or Supervisor Engine 8-E on a Catalyst 4500 IBC, ensure that HTTP is enabled; by default, it is disabled.

Examples   This example shows how to use the client ID with the **vstack attach** command to connect to a client from the director.

```
Director# vstack attach ?
  1        c3750-2042 @ IP 10.0.0.1 : MAC 0000.0040.4080
  2        c3750-2045 @ IP 10.0.0.2 : MAC 0000.000c.0d80
  A.B.C.D  IP address of remote node to attempt attaching to
Director# vstack attach 2
```

This example shows how to use the client IP address with the **vstack attach** command:

```
Director# vstack attach 1.1.1.1
```

vstack backup

To enable the backup feature and allow client configurations to be saved in the director's repository, use the **vstack backup** global configuration command. Use the **no vstack backup** command to disable the backup feature.

vstack backup [**file-server** *url*]

no vstack backup

Syntax Description	**file-server** *url*	(Optional) Specifies the registry used for backup:

  - **flash**
  - **ftp**
  - **http**
  - **https**
  - **rcp**
  - **scp**
  - **tftp**[1]
  - **usb**

If no registry is specified, the local repository **flash**:/vstack is used.

1. **tftp** is the only supported network *url*.

Command Default Backup is enabled. The local repository **flash**:/vstack is used. It is created if it does not exist. If the directory cannot be created, the **flash**:/ directory is used.

Command Modes Global configuration mode

Command History

Release	Modification
12.2(55)SE	This command was introduced to support Smart Install devices.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines From the director, enter this command to enable the backup feature and allow clients' configurations to be saved in the director repository. You must enable this feature so that zero-touch replacement occurs when a client is replaced by another client with the same product ID.

You can enter the **file-server** keyword to specify a repository to be used for the backup. Do not include the director IP address as part of the file-server URL. If the director IP address is part of the URL, the command is not rejected, but it does not work as expected.

Note   This command works on both the director and the client. However, it is only meaningful when the device is the director.

Examples   This example shows how to enable the backup feature:

```
Director(config)# vstack backup
```

This example shows where you can specify the repository:

```
Director(config)# vstack backup file-server ?
  flash:  Repository using flash:
  ftp:    Repository using ftp:
  http:   Repository using http:
  https: Repository using https:
  rcp:    Repository using rcp:
  scp: Repository using scp:
  tftp:   Repository using tftp:
```

vstack basic

To enable a switch or router as the Smart Install director, use the **vstack basic** global configuration command. This command is accepted only if the director IP address matches one of the device IP addresses. To disable the Smart Install director function on the switch or router, use the **no** form of this command.

> **vstack basic**

> **no vstack basic**

Syntax Description   This command has no arguments or keywords.

Defaults   Smart Install director is not enabled.

Command Modes   Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   There can be only one director managing a number of clients in a Smart Install network.

The director must be running a Smart Install-capable image.

If you have disabled Smart Install on the device by entering the **no vstack** global configuration command, this command is not allowed. You can reenable Smart Install by entering the **vstack** global configuration command.

For zero-touch upgrade, all DHCP transactions in the Smart Install network between the DHCP server and the clients must run through the director.

If you enter the **vstack basic** command on a device that does not have the director IP address (either assigned by the DHCP server or configured by entering the vstack **director** *ip-address* global configuration command), the command is not accepted. If the device is a switch, it must be a client.

If you enter the **vstack basic** command before a director IP address has been assigned or configured, the command is rejected with a message that the director is not configured.

When you enable the director by entering this command, these operation occur:

- DHCP snooping is enabled on the director for VLAN 1 and any other configured Smart Install VLANs. You can, however, use the **vstack startup-vlan** global configuration command to specify another default VLAN.

- The director starts building a director database of neighboring devices.

If you enter the **no vstack basic** command to disable director functionality on the device, Smart Install configurations are not deleted but do not take effect until the device is again enabled as a director. When you enter **no vstack basic**, DHCP snooping is disabled, and the director database is no longer valid.

If the director IP address is configured on an interface, and you shut down or delete the interface or change the interface IP address, the switch becomes a client and must find another director IP address.

Examples

This example shows how to enable the switch or router as a director when the director IP address is on the device:

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

This example shows the error message that appears if you enter the command on a device when no director IP address has been configured or assigned by DHCP:

```
Director(config)# vstack basic
Command Rejected: Director IP is not configured
```

This example shows the error message that appears if you enter the command on a device configured with a director IP address that is not owned by the switch or router:

```
Director(config)# vstack basic
Command Rejected: The Director IP address does not match a switch IP address.
```

You can verify Smart Install director settings by entering the **show vstack config** privileged EXEC command.

Related Commands

Command	Description
show vstack config	Displays the Smart Install configuration.
vstack director	Configures a Smart Install director IP address.

vstack config

To identify the default configuration file for the clients, use the **vstack config** global configuration command on the Smart Install director. To remove the configuration file as the default, use the **no** form of this command.

> **vstack config** *location config_filename*

> **no vstack config**

Syntax Description		
location		Enter **flash:; flash0:,** or **flash1:** if the director is the TFTP server and the configuration file is in the director flash memory. Enter **tftp://** and the location of the default configuration file if the file is not in the director flash memory. If the director is the TFTP server, the location is the director IP address.
	Note	Although visible in the command-line help, these options are not supported: **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
config_filename		The syntax for entering the filename when not in the director flash is **tftp:**[[*//location*]/*directory*]/*config.txt*

Defaults   None

Command Modes   Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   The **vstack config** configuration command is used to identify the configuration file for application to the smart install client. It is needed for all vstack groups whose clients must have a configuration file automatically applied.

Prior to Release IOS XE 3.6.0E and IOS 15.2(2)E, the **vstack config** command was mandatory for custom and built-in vstack groups. With Release IOS XE 3.6.0E and IOS 15.2(2)E, configuring the group for configuration is optional.

Because the default group is optional, all commands to this group are also optional. If you are using the default group, however, you should always configure a default configuration, which is used when the client could not be matched to either a built-in group or custom group (i.e., when the configuration file for a client is outside of a built-in or custom group).

Although you can enter this command on any device running a Smart Install image, the configuration does not take affect if the switch is not the director. Only configuration commands entered on a director are valid. If the client switch becomes the director, the entered configuration is then valid.

A smart install client sends an error message if it cannot download the configuration file This could stem from one of the following:

- a misconfiguration on the director
- the unavailability of the configuration file
- a join window is configured and the client attempts to join the group outside the join window

Examples

This is an example of Smart Install default configuration when there is only one type of product ID (24-port Catalyst 2960) in the network, the director is the TFTP server, and the configuration file is in the director flash memory:

```
Director(config)# vstack config flash:2960-24-lanbase-config.txt
```

This is an example of Smart Install default configuration when there is only one type of product ID (24-port Catalyst 2960) in the network and the configuration file is not in the director flash memory:

```
Director(config)# vstack config tftp://1.1.1.10/2960-24-lanbase-config.txt
```

You can verify Smart Install settings by entering the **show vstack config** privileged EXEC command.

Related Commands

Command	Description
show vstack config	Displays the Smart Install configuration.
vstack image	Configures a Smart Install default image file.
vstack script	Configures a Smart Install default post install file.

vstack dhcp-localserver

To configure the Smart Install integrated director as the Smart Install DHCP server, use the **vstack dhcp-localserver** global configuration command on the director. To delete the Smart Install DHCP pool, use the **no** form of this command.

> **vstack dhcp-localserver** *poolname*

> **no vstack dhcp-localserver** *poolname*

Syntax Description		
	poolname	The name of the Smart Install DHCP server pool.

Defaults   The director is not the Smart Install DHCP server.

Command Modes   Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   When the Smart Install DHCP server is the director or another device running Cisco IOS, if the network reloads, the server could assign other IP addresses to participating devices. If the director IP address changes, it is no longer the Smart Install director, which could break the director and client relationships. You must then reassociate the clients and the director. To ensure that this does not occur, you should enter the **ip dhcp remember** global configuration command to configure the DHCP pool to remember the IP bindings. If the network or device reloads, the DHCP server issues the same IP address to a client that it had before the reload.

Enter this command only on the director. Do not enter it on a client. The command creates a Smart Install DHCP pool and enters Smart Install DHCP configuration mode.

These configuration commands are available in Smart Install DHCP configuration mode:

- **address-pool** *ip-address* {*network_mask* | */prefix-length*}—Configures the IP address and network mask or prefix-length for the DHCP pool. The prefix length is the number of bits that comprise the address prefix and is another way to specify the network mask. Enter it as a number preceded by a forward slash (*/nn*).

- **default-router** *ip-address*—Configures the DHCP default router IP address for the pool.

- **exit**—Exits Smart Install DHCP configuration mode and returns to global configuration mode.

- **file-server** *ip-address*—Configures a default TFTP server IP address. This is the same parameter configured by entering the **option 150** *ip-address* keyword in DHCP pool configuration mode.

- **no**—Negates a command or sets its default.

Examples   This example shows how to configure a Smart Install DHCP pool named *smart_install1* by entering Smart Install DHCP configuration mode and assigning a network address and default router for the pool and a TFTP server:

```
Director(config)# vstack dhcp-localserver smart_install1
Director(config-vstack-dhcp)# address-pool 1.1.1.1 /22
Director(config-vstack-dhcp)# default-router 2.2.2.2
Director(config-vstack-dhcp)# file-server 3.3.3.3
Director(config-vstack-dhcp)# exit
```

You can verify Smart Install DHCP server settings by entering the **show dhcp server** or **show ip dhcp pool** privileged EXEC command.

Related Commands

Command	Description
show dhcp server	Displays the DHCP servers.
show ip dhcp pool	Displays information about configured DHCP pools.
vstack basic	Enables the switch or router to be the Smart Install director. This command is accepted only if the director IP address is on the device.

vstack director

To manually configure the IP address of the director, use the **vstack director** global configuration command on the Smart Install director or client. To remove the director IP address configuration, use the **no** form of this command.

vstack director *ip-address*

no vstack director

Syntax Description	*ip-address*	The IP address of the switch or an interface on the switch or router intended to be the Smart Install director.
		• When entered on the director, the IP address should be one of the device interfaces.
		• When entered on a client, the IP address should be an IP address on the director.

Defaults No director IP address is configured unless it was assigned by the DHCP server.

Command Modes Global configuration

Command History	Release	Modification
	12.2(52)SE	This command was introduced.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
	3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
	15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
	15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
	15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
	3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines For a switch or router to be the director, the director IP address must be the IP address of a Layer 3 interface on the device. A Layer 2 switch cannot be the director.

If you have disabled Smart Install on the device by entering the **no vstack** global configuration command, this command is not allowed. You can re-enable Smart Install by entering the **vstack** global configuration command.

This command is not mandatory if the director IP address is configured by DHCP. For DHCP to assign the director IP address, you must configure the DHCP server with options 125 and 16.

If the director IP address is not assigned by DHCP, you must enter the **vstack director** *ip-address* command on the director and on the other Smart Install switches.

When the director IP address has been configured by entering this command or it is assigned by a DHCP server, enable the Smart Install director by entering the **vstack basic** command on the switch or router.

There can be only one director for a set of clients and there is no way to configure a backup director. If the director fails, the switch must restart before you can resume plug and play operation.

The director must be the device in the network through which all DHCP transactions between the client switches and the DHCP server pass. The director must be running a Smart Install capable image.

If you enter the **vstack director** *ip-address* command on a client with an IP address that does not match the director IP address assigned by the DHCP server, the client cannot participate in a session with the director listed by the server.

If you enter the v**stack director** *ip-address* command on a client and change the IP address from that of the director, the client attempts to contact the new director. If the new IP address is on the client, that device becomes the director.

A director changes roles and becomes a client if you shut down or delete the interface on which the director IP address is configured or if you change the interface IP address.

Examples   This example shows how to configure the director IP address on a switch or router and then enable it as the director:

```
Director(config)# vstack director 1.1.1.1
Director(config)# vstack basic
Director(config
```

You can verify Smart Install settings by entering the **show vstack config** privileged EXEC command.

Related Commands

Command	Description
show vstack config	Displays the Smart Install configuration.
vstack basic	Enables the switch or router as the Smart Install director. This command is accepted only if the director IP address is on the device.

vstack download-config

To start an on-demand configuration download for clients, use the **vstack download-config** privileged EXEC command on the Smart Install director. This command is visible only on the director.

> **vstack download-config** {*ip_address* |**index** *name*| **built-in** *product_family port_config*
> *chassis_config*} *remote_switch_password* **startup** [**reload** [**in** *time*]]

Note   A **no** form for this command does not exist.

Syntax Description	*ip_address*	The IP address of the client.
	index *name*	(Optional) Specifies the index name from the director database for multiple clients or a range of clients.
		• *name*—Enter multiple clients or a range of clients, for example 1,3-5,7,9-11.
	built-in *product_family*	Specifies the identified (built-in) product family ID. To see the available product families, enter a **?** after **built-in**.
	port_config	The switch port configuration. The available IDs depend on the product family. To see the available port configurations, enter a **?** after the product family.
		If *product_family* is set to 4500 (that is, Catalyst 4500 standalone IBC), *port_config* means supervisor configuration.
	chassis_config	The chassis type to configure.
		If *product_family* is set to 4500, the chassis type selected here is supported by the supervisor engine assigned to *port_config*.
	remote_switch_ password	The password of the client switch. Enter *none* (or any word) for switches with no password,
		Note The password is required only for switches that are not Smart Install-capable. It is not required for switches already in the Smart Install network.
	startup	Applies the configuration to the startup configuration.
	reload	(Optional) Reloads the switch.
	in *time*	(Optional) Specifies the time to reload the switch in the format hh:mm. The range is from 00:00 to 23:59. If you do not specify a time, the reload occurs when you exit the CLI.

Defaults   None.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.
3.6.0E	The **chassis** option was introduced.

Usage Guidelines   You can enter this command only on the director.

When you enter the **built-in** *product_family port_config* keywords for an on-demand configuration download, you must have first identified the configuration for the specified built-in group. Enter the **config** *location config_filename* Smart Install group configuration command.

remote_switch_password is required only for switches that are not Smart Install-capable. It is not required for switches already in the Smart Install network.

Selecting a Catalyst "4k" group is similar to configuring a Catalyst "4k" group.

Note   You must select similar parameters (product type, sup type, and chassis type) as you did while configuring the group.

Examples   This example shows how to start an on-demand image download of the configuration file for a Catalyst 2960 24-port switch on a client switch with the password *mypassword*. The download occurs when the switch starts in 10 hours:

```
Director# vstack download-config built-in 2960 24 mypassword startup reload in 10:00
```

To see the configuration files for built-in or custom groups, enter the **show vstack group** {**built-in** | **custom**} privileged EXEC command. To verify the download, enter the **show vstack download-status** privileged EXEC command.

Related Commands

Command	Description
show vstack download-status [**detail**]	Displays Smart Install download status. The **show vstack download-status detail** display includes detailed reasons for download failures.
show vstack group	Displays configures Smart Install groups.

vstack download-image

To configure an on-demand tar image download for clients, use the **vstack download-image** privileged EXEC command on the Smart Install director. This command is visible only on the director.

> **vstack download-image tar** *image_URL* {*ip_address* | **index** *name*} *remote_switch_password*
> [**override**] **reload** [**in** *time*]

> **vstack download-image built-in** *product_family port_config chassis_config*
> *remote_switch_password* [**override**] [**issu** [**allow-reload**]] [**reload**] [**in** *time*]

> **Note** For releases prior to12.2(55)SE, you must create an image list: **vstack download-image** {*imagelist_file URL ip_address* | **built-in** *product_family port_config*} *remote_switch_password* [**override**] **reload** [**in** *time*]

> **Note** A **no** form for this command does not exist.

Syntax Description

tar *image_URL*	Enter **tar** and **tftp** URL for the tar image file.
	For example, `tftp://192.168.0.50/2960.tar`
	Note Although visible in the command-line help, these options are not supported: **bs:**, **cns:**, **flash1:**, **flash:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tar:**, **tmpsys:**, **xmoden:**, **ymodem.**
ip_address	Specifies the IP address of the remote host.
index *name*	(Optional) Enter the index name from the director database for multiple clients or a range of clients.
	• *name*—Enter multiple clients or a range of clients, for example 1,3-5,7,9-11.
built-in *product_family*	Specifies the identified (built-in) product family ID. To see the available product families, enter a **?** after **built-in**.
	For the Catalyst 4500 series switch, *product_family* is set to 4500.
port_config	The port configuration. The available configurations depend on the product family. To see the available configurations, enter a **?** after the product family.
	If *product_family* is set to 4500 (i.e., Catalyst 4500 standalone IBC), *port_config* means supervisor configuration.
chassis_config	The chassis type to configure.
	If *product_family* is set to 4500, the chassis type selected here is supported by the supervisor engine assigned to *port_config*.
remote_switch_ password	The password of the client, or enter NONE if there is no password configured. The password is required only for switches that are not Smart Install-capable. It is not required for switches already in the Smart Install network.
	• When upgrading multiple clients (by entering the **index** *name* keyword), all clients must have the same password or they must all have no password.
override	(Optional) Overrides the existing image.

issu	Specifies use of ISSU for on-demand upgrade for Catalyst 4500 IBC.
allow-reload	Allows a reload if triggering ISSU fails,
	This option appears only if the ISSU keyword is selected.
reload	Allows a reload of the switch if ISSU fails to trigger.
in *time*	(Optional) Specifies the time in Specify 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.

Defaults   No download image is identified.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(52)SE	The **index** *name* keywords were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release XE 3.2(0)SE.
3.6.0E	The **built-in** *chassis_config* and **issu** keywords were added.

Usage Guidelines   You can enter this command only on the director.

The image file must be a tar and not a bin file.

When you enter the **built-in** *product_family port_config chassis_config* keywords for an on-demand image download, you must have first identified the image for the specified built-in group by entering the **image** *location image_name* Smart Install group configuration command.

The *remote_switch_password* is required only for switches that are not Smart Install-capable. It is not required for switches already in the Smart Install network.

When you use the **index** *name* keyword to upgrade multiple clients, all clients must have the same password, or must have no password configured.

When you use the **index** *name* keyword to upgrade multiple clients, if a client is not compatible with the specified image, the upgrade fails.

Examples   This example shows how to start an on-demand image download of the configured image file for a Catalyst 2960 24-port client switch with the password *mypassword*. The switch is set to reload in 10 hours:

```
Director# vstack download-image built-in 2960 24 mypassword reload in 10:00
```

This example shows how to reload the IBCs that fall under the built-in group of 4500:

```
Switch# vstack download-image built-in 4500
Switch# vstack download-image built-in 4500 sup8
Switch# vstack download-image built-in 4500 sup8-e
Switch# vstack download-image built-in 4500 sup8-e 45
Switch# vstack download-image built-in 4500 sup8-e 4507

Switch# vstack download-image built-in 4500 sup8-e 4507r+e NONE ?
  issu      Force ISSU Upgrade
  override  Override the existing image
  reload    Reload the switch

Switch# vstack download-image built-in 4500 sup8-e 4507r+e NONE issu

Switch# vstack download-image built-in 4500 sup8-e 4507r+e NONE issu ?
  allow-reload  Allow Reloading the switch if ISSU fails to trigger
  in            Specify time in
  <cr>

Switch# vstack download-image built-in 4500 sup8-e 4507r+e NONE issu alo
Switch# vstack download-image built-in 4500 sup8-e 4507r+e NONE issu all

Switch# $load-image built-in 4500 sup8-e 4507r+e NONE issu allow-reload ?
  in  Specify time in
  <cr>

Switch# $load-image built-in 4500 sup8-e 4507r+e NONE issu allow-reload
```

This command reloads the IBCs that fall under this group.

The following example shows how to start an on-demand image download of the configured image file for clients 1 through 3 and 4 in the director database and to reload in 10 hours:

```
Director# vstack download-image tar tftp://192.168.0.50/2960.tar index 1-3, 4 mypassword
reload in 10:00
```

To see the images in the director database, enter the **show vstack status detail** privileged EXEC command. To see images configured for built-in or custom groups, enter the **show vstack group** {**built-in** | **custom**} privileged EXEC command. To verify the download, enter the **show vstack download-status** privileged EXEC command.

	Command	Description
Related Commands	**show vstack download-status** [**detail**]	Displays Smart Install download status. Entering **show vstack download-status detail** includes detailed reasons for download failures.
	show vstack group	Displays configures Smart Install groups.
	show vstack status detail	Displays Smart Install images in the director database.

vstack group built-in

To identify a built-in Smart Install group and to enter Smart Install group configuration mode for the group, use the **vstack group built-in** global configuration command on the Smart Install director. To remove the configuration for the built-in group, use the **no** form of this command.

vstack group built-in *product_family port_config chassis_config*

no vstack group built-in *product_family port_config chassis_config*

Syntax Description

product_family	The identified (built-in) product family ID. To see the available product families, enter a **?** after **built-in**.
	If *product_family* is set to 4500 for Catalyst 4500 series switches.
port_config	The switch port configuration. The available choices depend on the product family. To see the available port configurations, enter a **?** after the product family.
	If *product_family* is set to 4500 (that is, Catalyst 4500 standalone IBC), *port_config* means supervisor configuration.
chassis_config	The chassis type to configure.
	If *product_family* is set to 4500, the chassis type selected here is supported by the supervisor engine assigned to *port_config*.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.
15.2(2)E	The script keyword was introduced.
3.6.0E	The *chassis config* keyword was introduced.

Usage Guidelines

Although you can enter this command on any device running a Smart Install image, the configuration does not take effect if the device is not the director. Only configuration commands entered on the director are valid. If the client becomes the director, the entered configurations are then valid.

Use this command to define the configuration file (or post install file) for a group when multiple product IDs (PIDs) exist in the network. If all switches in the network have the same PID, you would use the **vstack config** *location config_filename* (or **vstack script** *location post_install_filename)* global configuration command to configure a default configuration file for all switches.

The built-in groups are shipping products that are present in the CLI.

You can use the **vstack group built-in ?** command to display a list of the product IDs built into the configuration. You can use the **vstack group built-in** *product_family* **?** command to display a list of the port configurations for a product family.

✎

Note   To configure Catalyst 4500 "modular" series switches, set *product_family* to 4500.

If a client does not match any custom group, the switch is configured with a built-in group configuration and image. If a switch does not match any group, the default image and configuration are used.

✎

Note   Image files are specific to a product family. Configuration files are specific to a port configuration.

A client 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 the configured time frame.

These configuration commands are available in Smart Install group configuration mode for built-in groups:

- **config**—Identifies the configuration file for the group.
- **exit**—Exits Smart Install group configuration mode and returns to global configuration mode.
- **image**—Identifies the image for the group, for example, *c3560-ipservices-mz.122-52.SE.tar*. This image must be a tar and not a bin file.
- **script**—Identifies the post install file for the group.
- **no**—Negates a command or sets its default.

To identify the group post install file name (script), configuration file name (config), and the group image file name, enter **tftp**: followed by the filename.

✎

Note   Although visible in the command-line help, these keywords are not supported: **flash1:**, **flash:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:**

Examples   This example shows how to identify a group as Catalyst 3560 8-port Power over Ethernet (PoE) switches and to enter Smart Install group configuration mode. It identifies the image to be obtained through TFTP for the group as c3560-ipbase-mz.122-52.SE.tar, which contains the 3560 IP base image for Release12.2(52)SE, identifies the post install file as the 3560 IP Base image, and identifies the configuration file as the 3560 IP Base image.

```
Director(config)# vstack group built-in 3560 8poe
Director(config-vstack-group)# image tftp://1.1.1.10/c3560-ipbase-mz.122-52.SE.tar
Director(config-vstack-group)# config tftp://1.1.1.10/c3560-24-ipbase-config.txt
Director(config-vstack-group)# script tftp://1.1.1.10/c3560-24-ipbase-post_install.txt
```

You can verify group settings by entering the **show vstack group built-in** privileged EXEC command.

The following example uses the chassis type to display the configurations for a built-in group of "4k" with "sup8-e" in a 4503 chassis:

```
Switch# show vst group built-in 4500 sup8-e 4503 de
---------------------------------------------
Group Name: sup8-e 4503
No Image name specified
No config file name specified
No Script file specified
Switch#
```

In the following example, we select the supervisor type rather than the chassis type. This displays all the groups for the chassis that support that particular supervisor engine.

```
Switch# show vst group built-in 4500 sup8-e de
---------------------------------------------
Group Name: sup8-e 4503
No Image name specified
No config file name specified
No Script file specified
---------------------------------------------
Group Name: sup8-e 4506
No Image name specified
No config file name specified
No Script file specified
---------------------------------------------
Group Name: sup8-e 4507r+e
No Image name specified
No config file name specified
No Script file specified
---------------------------------------------
Group Name: sup8-e 4510r+e
No Image name specified
No config file name specified
No Script file specified
Switch#
```

Related Commands	Command	Description
	show vstack group built-in	Displays the configured Smart Install built-in groups.
	vstack group custom	Configures Smart Install custom groups.

vstack group custom

To configure a user-defined Smart Install group and to enter Smart Install group configuration mode for the group, use the **vstack group custom** global configuration command on the Smart Install director. To return to the default setting or to remove the group, use the **no** form of this command.

> **vstack group custom** *group_name* {**connectivity** | **mac** | **product-id** | **stack**}

> **no vstack group custom** *group_name*

Syntax Description

group_name	A name for the custom group.
connectivity	Matches a custom group based on connectivity or network topology. All clients that have the same upstream neighbor. If a client matches more than one group characteristic, a connectivity match takes precedence over a stack match or product-id match, but not over a MAC address match.
mac	Matches a custom group consisting of switch MAC addresses. If a client matches more than one group characteristic, a MAC address match takes precedence.
product-id	Matches a custom group based on the product ID.
stack	Matches a custom group based on switch stack membership. If a switch matches more than one group characteristic, a stack match takes precedence over product-id.

Defaults   None

Command Modes   Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.
15.2(2)E	The *script* keyword was introduced.

Usage Guidelines   Although you can enter this command on any switch or router running a Smart Install image, the configuration does not take effect if the device is not the director. Only configuration commands entered on the director are valid. If the client switch becomes the director, the entered configurations are then valid.

When you enter Smart Install group configuration mode, use the **match** command to identify the group characteristics.

All members of a custom group must be able to run the same image, post install file, and configuration file. For example, only Catalyst 3560 switches can run the image c3560-ipbase-tar.122-52.SE.tar, and each 3560 port configuration would run a different configuration and post install file.

A custom group takes precedence over a built-in group. If a switch does not match any custom group, the switch is configured with the built-in group configuration. If a switch does not match any group, the default configuration, post install file and image are used.

Among custom groups, a group matched by MAC address takes precedence over other matches. A connectivity match takes precedence over one matched by product ID or stack, and a stack match takes precedence over product ID.

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

These configuration commands are available in Smart Install group configuration mode for custom groups:

- **config**—Identifies the configuration file for the group.
- **exit**—Exits Smart Install group configuration mode and returns to global configuration mode.
- **image**—Identifies the image for the group, for example *c3750-ipservices-mz.122-52.SE.tar*. This image must be a tar and not a bin file.
- **match**—Configures the match type for the group. See the **match (Smart Install group configuration)** command for more information about defining criteria for the custom group.
- **script**—Identifies the post install file for the group.
- **no**: Negates a command or sets its default.

To identify the group configuration file name (*config*) and the group image file name, enter **tftp:** *config* followed by the filename.

Note   Although visible in the command-line help, these keywords are not supported: **flash1:**, **flash:**, **ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:**

Examples   This example shows how to identify a custom group named test based on matching connectivity and to enter Smart Install group configuration mode. It specifies that the group includes clients connected to the host with the IP address 2.2.2.2 with an interface name of finance, and identifies the image, post install file and configuration to be obtained through TFTP for the group:

```
Director(config)# vstack group custom test connectivity
Director(config-vstack-group)# match host 2.2.2.2 interface finance
Director(config-vstack-group)# image tftp://1.1.1.10/c3560-ipbase-mz.122-52.SE.tar
Director(config-vstack-group)# config tftp://1.1.1.10/3560-24-ipbaseconfig.txt
Director(config-vstack-group)# script tftp://1.1.1.10/3560-24-ipbase_post_install.txt
```

You can verify the group settings by entering the **show vstack group custom** privileged EXEC command.

Related Commands	Command	Description
	vstack hostname-prefix	Configures group parameters to match for a custom group.
	show vstack group custom	Displays the configured Smart Install custom groups.
	vstack group built-in	Configures Smart Install built-in groups.

vstack hostname-prefix

To specify a prefix for the hostname for a client, use the **vstack hostname-prefix** global configuration command on the Smart Install director. To remove the prefix name setting, use the **no** form of this command.

vstack hostname-prefix *prefix*

no vstack hostname-prefix

Syntax Description	*prefix* 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 DCHP request snooped through the director would be the last 3 bytes of the switch MAC address.

Defaults   None

Command Modes   Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Although you can enter this command on any device running a Smart Install image, the configuration does not take effect if the device is not the director. Only configuration commands entered on the director are valid. If the nondirector becomes the director, the entered configurations are then valid.

When a DHCP request is snooped through the director and this command is entered, the switch hostname includes the configured hostname followed by the last 3 bytes of the switch MAC address.

Examples   This example shows how to configure the hostname *Cisco* for a client that has been DHCP-snooped:

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

If you then telnet to that switch from the director, the display shows the resulting switch hostname assignment:

```
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#
```

You can verify the hostname prefix by entering the **show vstack config** privileged EXEC command on
the director.

Related Commands	Command	Description
	show vstack config	Displays the Smart Install configuration.

vstack image

To configure the default image filename for all clients in a Smart Install topology, use the **vstack image** global configuration command on the Smart Install director. To remove the default image, use the **no** form of this command.

vstack image *location image_name.***tar**

no vstack image

Syntax Description

location	Enter **flash:** if the director is the TFTP server and the default image is in the director flash memory. Enter **tftp://** and the location of the default image file if the image is not in the director flash memory. If the director is the TFTP server, the location is the director IP address.
	Note Although visible in the command-line help, these options are not supported: **flash1:**,**ftp:**, **http:**, **https:**, **null:**, **nvram:**, **rcp:**, **scp:**, **system:**, **tmpsys:.**
*image_name.***tar**	The image name, for example, *c2960-lanbase-tar.122-53.SE.tar.* The image must be a tar and not a bin file.

Defaults   None

Command Modes   Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   The **vstack image** configuration command is used to identify the ios image that applies to the smart install client. It is needed for all vstack groups whose clients need to have the correct ios image automatically applied.

Prior to Release IOS XE 3.6.0E and IOS 15.2(2)E, the **vstack image** command was mandatory for custom and built-in vstack groups. With Release IOS XE 3.6.0E and IOS 15.2(2)E, configuring the group for image is optional.

Because the default group is optional, all commands to this group are also optional. If you are using the default group, however, you should always configure a default image, which is used when the client could not be matched to either a built-in group or custom group (i.e., when the image for a client is outside of a built-in or custom group).

Although you can enter this command on any device running a Smart Install image, the configuration does not take effect if the device is not the director. Only configuration commands entered on the director are valid. If the client becomes the director, the entered commands are then valid.

The image name is the image that you want to download, for example, *c3750-ipservices-mz.122-52.SE.tar*. This image must be a tar and not a bin file.

Because the default group is optional, all commands to this group are also optional. If you are using the default image, however, you should always configure a default image, which is used when the client could not be matched to either a built-in group or custom group (i.e., when the configuration file for a client is outside of a built-in or custom group).

A smart install client sends an error message if it cannot download the image. This could stem from one of the following:

- a misconfiguration on the director
- the unavailability of the image
- a join window is configured and the client attempts to join the group outside the join window

Examples This is an example of Smart Install default configuration when there is only one type of product ID (24-port Catalyst 2960) in the network, the director is the TFTP server, and the image file is stored in the director flash memory:

```
Director(config)# vstack image flash:c2960-lanbase-tar.122-53.SE.tar.
```

You can verify group settings by entering the **show vstack config** privileged EXEC command.

Related Commands

Command	Description
show vstack config	Displays the Smart Install configuration.
vstack config	Configures a Smart Install default configuration file.
vstack script	Configures a Smart Install default post install file.

vstack join-window close

To completely close the join window, use the **vstack join-window close** global configuration command on the Smart Install director. To open the join window, use the **no vstack join-window close** command.

vstack join-window close

no vstack join-window close

Syntax Description   This command has not arguments or keywords.

Defaults   The join window is open.

Command Modes   Global configuration mode

Command History

Release	Modification
12.2(55)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   From the director, use the **vstack join-window close** command in global configuration mode to close the join window. The join window is a time frame during which a client that is coming up and joining the Smart Install network can be upgraded with a new image and configuration.

Note   This command works on both the director and the client. However, it is only meaningful when the device is the director.

Examples   This example shows how to close the join window.

```
Director(config)# vstack join-window close
```

Related Commands

Command	Description
vstack join-window mode auto	Configures the join window mode on the director.
vstack join-window start	Configures the time interval during which the director sends configuration and image files to clients.

vstack join-window mode auto

To configure the join window mode, use the **vstack join-window mode auto** global configuration command on the Smart Install director.

> **vstack join-window mode auto**

> **no vstack join-window mode auto**

Defaults   Clients are automatically upgraded when the join window is open.

Command Modes   Global configuration mode

Command History

Release	Modification
12.2(55)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Entering the **vstack join-window mode auto** global configuration command automatically allows clients to be upgraded to the latest image and configuration after they join the Smart Install network as long as the join window is open. This is the default.

Entering the **no vstack join-window mode** global configuration command puts clients in a hold state when they join the network. You must enter the **vstack on-hold-clients install** privileged EXEC command for the immediate upgrade of clients in the hold state.

> **Note**   You can enter this command on both the director and the client, but it is only meaningful when the device is the director.

Examples   This example shows how to configure the join-window manual mode on the director.

```
Director(config)# vstack join-window mode auto
```

Related Commands

Command	Description
vstack join-window close	Closes the join window completely.

Command	Description
vstack join-window start	Configures the time interval during which the director sends configuration and image files to clients.
vstack on-hold-clients install	Installs configuration and images files on a specified client.

vstack join-window start

To configure the time interval during which the director sends configuration and image files to clients, use the **vstack join-window start** global configuration command on the Smart Install director. To remove the join-window configuration, use the **no** form of this command.

vstack join-window start [*date*] *hh:mm* [*interval*] [**end** *date*] [**recurring**]}

no vstack join-window start

Syntax Description	*date*	(Optional) A start date for the director to send configuration and image files to the client in the format *day month year*:
		• *day* is 1 to 31.
		• *month* is the 3-letter abbreviation for the month (for example, Jun for June).
		• *year* is 1993 to 2035.
	hh:mm	The time to start sending the files in the format *hh:mm*, using a 24-hour clock, 00:00 to 23:59.
	interval (Optional)	The number of hours for which the join window remains active. The range is from 0 to 23, in the format *hh:mm*, for example, 01:30 is 1 hour and 30 minutes.
		Note The maximum duration that you can configure is 24 hours.
	end *date*	(Optional) Specifies the end date for the director to stop sending configuration and image files in the format *day month year*:
		• *day* is 1 to 31.
		• *month* is the 3-letter abbreviation for the month (for example, Jun for June).
		• *year* is 1993 to 2035.
	recurring	(Optional) Specifies that the time to send configuration and image files to the client occurs every day at the configured start time.

Defaults No director time interval is configured. When configured, if no dates or intervals are set, the start time is recurring.

Command Modes Global configuration

Command History	**Release**	**Modification**
	12.2(52)SE	This command was introduced.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
	3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
	15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.

Release	Modification
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Although you can enter this command on any device running a Smart Install image, the configuration does not take effect if the device is not the director. Only configuration commands entered on the director are valid. If the client becomes the director, the entered configurations are then valid.

Note   Before configuring a join window, you should verify that the director time is correct.

When a join window is configured and clients are detected outside the join window, the director does not send files to the client until the next configured join window. The auto-install process occurs on the client as if it were not a Smart Install client.

During the join window, clients cannot upgrade the image or configuration files except with files received from the director. Within the join window, the director passes the names and locations of the image and configuration files to the client, which then upgrades these files.

When a join window is configured, if the DHCP acknowledgment occurs outside the configured time frame, a client sends an error message that it cannot download an image or configuration file due to misconfiguration.

Examples   This example shows how to configure the director to insert DHCP options, starting at 10 a.m. and recurring every day at this time.

```
Director(config)# vstack join-window start 10:00 recurring
```

This example shows how to configure the join window to start on July 4, 2009, and remain on (no end date).

```
Director(config)# vstack join-window start 04 july 2009 09:00
```

This example shows how to configure the join window to start on July 4, 2009, and end on July 5, 2009.

```
Director(config)# vstack join-window start 04 july 2009 10:00 end 05 july 2009
```

This example shows how to configure the join window to start on July 4, 2009, at 10 a.m. and to continue for 4 hours:.

```
Director(config)# vstack join-window start 04 july 2009 10:00 04:00
```

This example shows how to configure the join window to start on July 7, 2009 at 10 a.m., operate for 4 hours, recur daily at that time until July 10, when the join window ends and remains shut.

```
Director(config)# vstack join-window start 07 july 2009 10:00 04:00 end 10 july 2009 recur
```

You can verify join-window settings by entering the **show vstack config** privileged EXEC command on the director.

Related Commands	Command	Description
	show vstack config	Displays the Smart Install configuration.

vstack join-window-status index

To move a client from the join-window deny state to the held or active state, use the **vstack join-window-status index** privileged EXEC command on the Smart Install director.

vstack join-window-status index *client-id* {**allowed** | **held**}

Syntax Description

client-id	The client ID from the director database. The client ID can be a single client, multiple clients, or a range of clients, for example 1,3-5,7,9-11.
allowed	Changes the join window state for the client or clients from deny or held to active. A client in the active state is allowed zero-touch updates, on-demand updates, or configuration backups when the join window is open.
held	Changes the join window state for the client or clients from deny to held. A client in the held state is allowed zero-touch updates and on-demand updates, but not configuration backups when the join window is open.

Defaults

The join window state for all clients is determined by the vstack join-window mode global configuration command.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(58)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines

Use this command to move a client or multiple clients out of the join-window deny state.

After you enter the command, you are asked to confirm the client state change.

You can see the current client states by entering the **show vstack status** privileged EXEC command.

Examples

This example shows how to manually change the join window state of clients 1 to 4 to active.

```
Director # vstack join-window-status index 1-4 allowed
```

Related Commands

Command	Description
show vstack status	Displays Smart Install status, including the join window state for clients.

vstack on-hold-clients install

To authorize an immediate image and configuration upgrade to an on-hold client or to all on-hold clients, use the **vstack on-hold-clients install** privileged EXEC command on the Smart Install director.

vstack on-hold-clients install {**all** | **client-id** *client index* | **ipaddr** *ip-address* | **mac** *mac address*} [**override**]

Syntax Description

all	Installs the image and configuration update on all on-hold clients.
client-id *client index*	Installs the image and configuration update on clients with the specified client ID. The client ID range is 0 to 255.
ipaddr *ip-address*	Installs the image and configuration update on the client with the specified IP address.
mac *mac address*	Installs the image and configuration update on the client with the specified MAC address.
override	(Optional) Overrides the existing image.

Command Default   None

Command Modes   Privileged EXEC mode

Command History

Release	Modification
12.2(55)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   This command is required only when you configure **no vstack join-window mode**. When the mode is **auto** (the default), clients joining the Smart Install network are automatically updated when the join window is open.

When you set the join window mode to manual by entering the **no vstack join-window mode** command, clients joining the Smart Install network are put in a *hold* state. Entering the **vstack on-hold-clients install** privileged EXEC command authorizes the director to immediately upgrade an on-hold client. Specify a client for upgrade by entering one of the keywords, or enter **all** to select all client devices for upgrade.

Examples   This example shows how to select all on-hold client devices for upgrade:

```
Director# vstack on-hold-clients install all
```

This example shows how to specify the on-hold client for upgrade by IP address:

```
Director# vstack on-hold-clients install ipaddr 10.10.10.1
```

Related Commands	Command	Description
	vstack join-window mode auto	Configures the join window mode on the director.
	vstack on-hold-clients remove	Removes a specified client from the on-hold client allowed list.

vstack on-hold-clients remove

To remove a specified client or all clients from the hold state, use the **vstack on-hold-clients remove** privileged EXEC command on the director.

vstack on-hold-clients remove {**all** | **client-id** *client index* | **ipaddr** *ip-address* | **mac** *mac address*}

Syntax Description

all	Removes on all on-hold clients from the allowed list.
client-id *client index*	Removes the client with the specified client ID. The client ID range is 0 to 255.
ipaddr *ip-address*	Removes the client with the specified IP address.
mac *mac address*	Removes the client with the specified MAC address.

Command Default   None

Command Modes   Privileged EXEC mode

Command History

Release	Modification
12.2(55)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   When you set the join window mode to manual by entering the **no vstack join-window mode** command, new clients joining the Smart Install network are put in a *hold* state. They remain in this state until you enter the **vstack on-hold clients install** privileged EXEC command to start an upgrade on the client or until you remove them from the on-hold state.

Enter the **vstack on-hold-clients remove** privileged EXEC command on the director to remove a specified client or all clients from the list of clients in the hold state. When a client has been removed from the on-hold list and you enter the **vstack on-hold clients install** privileged EXEC command for the client, the request is denied.

When you remove a client from the on-hold list, you must restart the client for an upgrade to occur.

When the mode is **auto** (the default), clients joining the Smart Install network are automatically upgraded when the join window is open.

Examples   This example shows how to remove all on-hold client devices from the hold list:

```
Director# vstack on-hold-clients remove all
```

This example shows how to specify the on-hold client for removal by IP address:

```
Director# vstack on-hold-clients remove ipaddr 10.10.10.1
```

Related Commands	Command	Description
	vstack join-window mode auto	Configures the join window mode on the director.
	vstack on-hold-clients install	Authorizes the director to grant an immediate upgrade to an on-hold client.

vstack script

To identify the default post install file for the clients, use the **vstack script** global configuration command on the Smart Install director. To remove the configuration file as the default, use the no form of this command.

Note This command is available only on switches. This command is not available when a router is the Smart Install Director.

vstack script *location post_install_filename*

no vstack script

Syntax Description		
location		Enter **flash**:; **flash0**:, or **flash1**: if the director is the TFTP server and the post install file is in the director flash memory. Enter **tftp**:// and the location of the default post install file if the file is not in the director flash memory. If the director is the TFTP server, the location is the director IP address.
	Note	Although visible in the command-line help, these options are not supported: **ftp**:, **http**:, **https**:, **null**:, **nvram**:, **rcp**:, **scp**:, **system**:, **tmpsys**:
post_install_filename		The syntax for entering the filename when not in the director flash is **tftp**:[[*//location*]/*directory*]/*post_install*.txt.

Command Default None

Command Modes Global configuration

Command History	Release	Modification
	3.6.0E	This command was introduced.
	15.2(2)E	This command was introduced.

Usage Guidelines Prior to Release IOS XE 3.6.0E and IOS 15.2(2)E, the **vstack script** command was mandatory for custom and built-in vstack groups. With Release IOS XE 3.6.0E and IOS 15.2(2)E, configuring the group for script is optional.

Because the default group is optional, all commands to this group are also optional. If you are using the default group, however, you should always configure a default script, which is used when the client could not be matched to either a built-in group or custom group (i.e., when the script for a client is outside of a built-in or custom group).You can decide not to configure post install in conjunction with image, configuration, or both.

When you configure the default configuration, that default post install file is used by the client when the client's post install file is not configured in any group (built-in or custom).

Although you can enter this command on any device running a Smart Install image, the configuration does not take affect if the switch is not the director. Only configuration commands entered on a director are valid. If the client switch becomes the director, the entered configuration becomes valid.

Use this command to define the post install script when all switches in the network have the same product ID (PID). The post install file is a text file that contains the post install command to be downloaded to the client.

A smart install client sends an error message if it cannot download the script. This could stem from one of the following:

- a misconfiguration on the director
- the unavailability of the script
- a join window is configured and the client attempts to join the group outside the join window

> **Note**   This statement is relevant only for default mode. SMI offers two types of customization: group (MAC, stack, and connectivity; and product-id based) and built-in. Post install is configurable in three modes: default, custom group, and built-in.

Examples   This is an example of Smart Install default configuration when only one type of product ID (24-port Catalyst 2960) exists in the network, the director is the TFTP server, and the post install file is in the director flash memory:

```
Director(config)# vstack script flash:2960-24-lanbase-post_install.txt
```

This is an example of Smart Install default configuration when only one type of product ID (24-port Catalyst 2960) exists in the network and the post install file is not in the director flash memory:

```
Director(config)# vstack script tftp://1.1.1.10/2960-24-lanbase-post_install.txt
```

You can verify Smart Install settings by entering the **show vstack config** privileged EXEC command.

Related Commands

Command	Description
show vstack config	Displays the Smart Install configuration.
vstack image	Configures a Smart Install default image file.
vstack config	Configures a Smart Install default configuration file.

vstack startup-vlan

To specify the default VLAN that the director should use for Smart Install management, use the **vstack startup-vlan** global configuration command.

vstack startup-vlan *vlan_value*

Syntax Description

vlan_value	The VLAN to use for Smart Install management.

Command Default   None

Command Modes   Global configuration

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Use this command to specify the default VLAN that the director should use for Smart Install operations. Depending on the VLAN that is specified in the command, DHCP snooping is enabled on that VLAN so that the director can identify new switches that are connected to the network. If this command is not entered, however, VLAN 1 is used as default.

Examples   This example shows how to specify VLAN 7 as the default VLAN for Smart Install:

```
Director# vstack startup-vlan ?
  <1-4094> Startup Management Vlan
Director# vstack startup-vlan 10
```

vstack tar

To archive files into a tar file, use the **vstack tar** privileged EXEC command on the director.

vstack tar *destination-url* [*source-url*]

Syntax Description

destination-url	The source URL alias for the local or network file system in which to archive files. The following options are supported:
	• **flash:** *tar file name*
	• **ftp:***t ar file name*
	• **http:** *tar file name*
	• **https:** *tar file name*
	• **rcp:** *tar file name*
	• **scp:** *tar file name*
	• **tftp:** *tar file name*
source-url	(Optional) The source URL.
	Note When a source URL is not specified, the entire local repository is archived. Specify the local repository with the **vstack backup file-server** command in global configuration mode.

Command Default   None

Command Modes   Privileged EXEC mode

Command History

Release	Modification
12.2(55)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Use the **vstack tar** command in privileged EXEC mode on the director to create a tar file into which to write files. Specify the destination URL for the local or network file system and the name of the tar file to be created. Specify the source URL (optional).

Note   If you do not specify a source URL, the local repository is archived. Specify the local repository with the **vstack backup file-server** global configuration command.

Examples   This example shows how to create an archive tar file (*archive.tar*) in flash memory and archive files from the repository into *mytar* directory in flash.

```
Director# vstack tar flash: archive.tar flash mytar
```

Related Commands

Command	Description
vstack untar	Extracts and archives a tar file.

vstack untar

To extract archived tar files into a directory, use the **vstack untar** privileged EXEC command on the director.

vstack untar *source-url* [*destination-url*]

Syntax Description	*source-url*	The source URL alias for the local or network file system and the name of the tar file. The following options are supported:
		• **flash**: *tar file name*
		• **ftp**: *tar file name*
		• **http**: *tar file name*
		• **https**: *tar file name*
		• **rcp**: *tar file name*
		• **scp**: *tar file name*
		• **tftp**: *tar file name*
	destination-url	(Optional) The destination URL.
		Note When you do not specify a destination URL, the local repository is used. Specify the local repository with the **vstack backup file-server** command in global configuration mode.

Command Default   None

Command Modes   Privileged EXEC mode

Command History	Release	Modification
	12.2(55)SE	This command was introduced.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
	3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
	15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
	15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
	15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
	3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Use the **vstack untar** command in privileged EXEC mode on the director to extract files from a tar file. Specify the source URL for the local or network file system and the name of the tar file. Specify the destination URL (optional).

Note   When you do not specify a destination URL, the local repository is used. Specify the local repository with the **vstack backup file-server** command in global configuration mode.

Examples   This example shows how to extract the tar file *archive.tar* from flash memory into the local repository.

```
Director# vstack untar flash: archive.tar
```

Related Commands

Command	Description
vstack tar	Creates a tar file and writes files into it.
vstack untar / table	Archives tar files in a table.

vstack untar / table

To list the contents of a tar file, use the **vstack untar/ table** privileged EXEC command on the director.

vstack untar/table *source-url*

Syntax Description

source-url	The source URL alias for the local or network file system and the name of the tar file. These options are supported:

- **flash:** *tar file name*
- **ftp:** *tar file name*
- **http**: *tar file name*
- **https:** *tar file name*
- **rcp:** *tar file name*
- **scp:** *tar file name*
- **tftp:** *tar file name*

Command Default   None

Command Modes   Privileged EXEC mode

Command History

Release	Modification
12.2(55)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Use the **vstack untar/table** command in privileged EXEC mode on the director to archive tar files. Specify the source URL for the local or network file system and the name of the tar file.

Examples   This example shows how to display the contents of the tar file *myconfig.tar* that is in flash memory.

```
Director# vstack untar/table flash:myconfig.tar
c3750-1-0000.0040.4080.REV2 (1785 bytes)
c3750-1-0000.0040.4080.REV1 (91 bytes)
c3750-0000.0040.4080.REV2 (1795 bytes)
c3750-0000.0040.4080.REV1 (1674 bytes)
c3750-ibc-0000.0040.4080.REV2 (1823 bytes)
```

Related Commands

Command	Description
vstack tar	Creates a tar file and writes files into it.
vstack untar	Extracts and archives tar files.

vstack vlan

To configure Smart Install VLANs for DHCP snooping, use the **vstack vlan** global configuration command on the Smart Install director. To remove a Smart Install management VLAN, use the **no** form of this command.

> **vstack vlan** *vlan-range*

> **no vstack vlan** *vlan-range*

Note   This command is not valid when the director is a router.

Syntax Description

vlan-range	The VLAN ID or IDs for Smart Install management VLANs. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.

Defaults   The default Smart Install management VLAN is VLAN 1.

Command Modes   Global configuration

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release 15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   Although you can enter this command on any device running a Smart Install image, the configuration does not take effect if the device is not the director. Only configuration commands entered on the director are valid. If the client becomes the director, the entered configurations are then valid.

When Smart Install is enabled on the director, DHCP snooping is automatically enabled on VLAN 1. You can, however, use the **vstack startup-vlan** global configuration command to specify another default VLAN instead of VLAN 1.

There is no limit to the number of Smart Install VLANs that you can configure.

This command does not apply to routers.

■ **vstack vlan**

Examples   This example shows how to configure VLAN 10 as a Smart Install VLAN:

```
Director(config)# vstack vlan 10
```

This example shows how to configure multiple Smart Install VLANs:

```
Director(config)# vstack vlan 10-12,100,200
```

You can verify Smart Install settings by entering the **show vstack config** privileged EXEC command.

Related Commands

Command	Description
show vstack config	Displays the Smart Install configuration.

Configuring SMI Proxy

Information about SMI Proxy

Prior to Cisco IOS XE 3.6.0E releases, Smart Install was the routine way to manage zero-touch deployments (ZTD) for Catalyst devices. Cisco's solution toward ZTD, Plug and Play (PnP) provides an agent that runs on each networking device and a server that manages your network devices with respect to configuration, image, and more.

Table 4-1   *Feature History Information for SMI Proxy*

Cisco IOS Release	Change Description
Cisco IOS XE 3.6.0E and IOS 15.2(2)E	The PnP Agent is available on Catalyst 4500 series, Catalyst 3850, Catalyst 3650, IE 2000, IE 3000, IE 3010, Catalyst 2K and Catalyst 3K switches.
	Devices running older releases (prior to Cisco IOS-XE 3.6.0E, and IOS 15.2(2)E) rely on existing ZTD solutions such as SmartInstall to enable IOS version updates. Devices running the older release cannot communicate with the central PNP Server. These devices require a migration path to reach the PNP Server.
Cisco IOS XE 3.6.3E and Cisco IOS 15.2(2)E3 and Cisco IOS XE 3.7.3E and Cisco IOS 15.2(3)E3	Beginning with the specified releases, the Catalyst 4500, Catalyst 3850, Catalyst 3750, Catalyst 3650, and Catalyst 3560 switches support SMI PnP Proxy. This feature leverages SMI functionality in an existing network device and allows for image and configuration upgrade of devices running older versions. SMI Proxy is applicable only to platforms that support SMI Director.
	The SMI Proxy feature will run on a network device that is running the required Cisco IOS release and is configured for PNP Agent and SMI Proxy. This device will bridge the communication from older devices running SmartInstall to the PNP Server. It will "proxy" as the PNP Agent for devices running older versions, enabling these devices to behave as if the SMI Proxy device is the SMI Director. The SMI Proxy device will contact the central PnP Server on behalf of the device running older versions to retrieve image and configuration information.
Cisco IOS XE 3.6.3E and Cisco IOS 15.2(3)E3	Beginning with this release, the Catalyst 4500, Catalyst 3850, Catalyst 3750, Catalyst 3650, and Catalyst 3560 support PnP discovery process via various discovery mechanisms and security methods.

This section contains:

How SMI Proxy Interacts with Smart Install Devices and the PnP Agent

After accepting different requests from various smart install clients, SMI Proxy provides all the mandatory information to the PnP Agent for each request. PnP Agent then forwards these requests to the PnP Server on behalf of the smart install client. The PnP Agent forwards the corresponding response from the PnP server to the SMI Proxy for further processing.

SMI Proxy allows a central PnP Server administrator to possess a single view of the network with respect to the image and configuration, even when some of the switches in the network are only SMI-capable.

Smartinstall Client switches
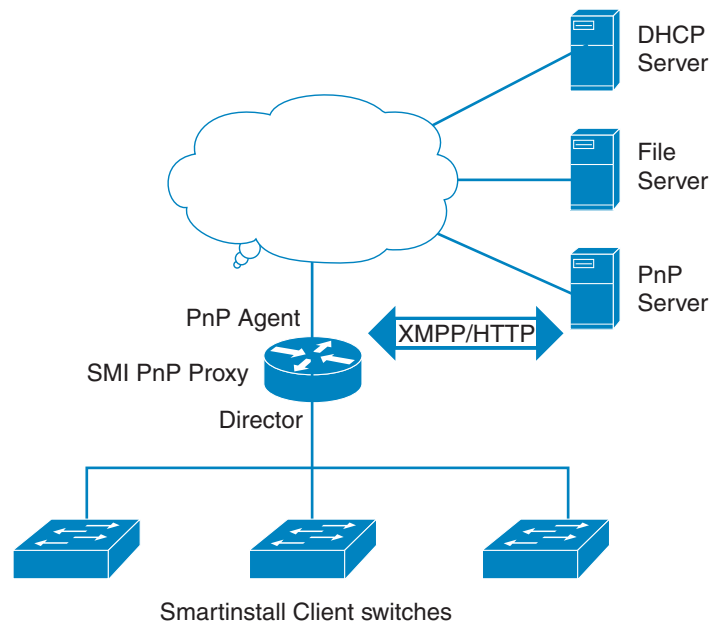
How SMI Clients and Directors Communicate

Smart Install clients can communicate with a director only within the network. SMI Proxy leverages existing client communication with the director, extracting relevant data from a networking device.

SMI Proxy mediates between Smart Install clients and the PnP Server, maintaining a database similar or equivalent to the data gleaned by the director.

How SMI Proxy and PnP Agent Communicate

SMI Proxy can trigger the PnP server to send service requests in the following ways:

- When a new SMI client device boots, it sends the "device came up notification" request to SMI Proxy, which sends the information request to the PnP Server through the PnP Agent.

- If SMI Proxy receives a backoff request for any SMI client, it starts the backoff timer. After the timer expires, SMI Proxy sends the work information request to PnP Server through PnP Agent.

- When the SMI Proxy receives the work information "bye" request from PnP Server, it immediately sends the work request to the PnP Server.

- When SMI Proxy receives the client request, PnP Agent sends that request to PnP Server and awaits a response. PnP Agent then evaluates whether the response is intended for the local device or the proxied client. If the former, the PnP Agent consumes the message; else, it is communicated to SMI Proxy.

SMI Proxy and Tailored Configuration Files

The director (IBD) controls which image or configuration is forwarded to the client switches (for example, SMI IBC). It is essential to upgrade older switches that do not run an SMI-capable image. To enable IBD to communicate with such switches and suitably upgrade them, a tailored configuration file was introduced.

In SMI proxy mode, to acquire the PID, VID, and SN of each client, SMI Proxy follows the "reverse telnet" mechanism supported by SMI on older devices.

Starting with Cisco IOS XE 3.6.3E/ Cisco IOS 15.2(2)E3 and Cisco IOS XE 3.7.3E/ Cisco IOS 15.2(3)E3 a director device supports and treats all clients as older devices. The proxy device uses the tailored configuration file to telnet [to] clients and acquire the output data for the **show version** command. When the proxy device reloads, a new tailored configuration file, client_cfg_pnp.txt, is generated.

This is an example of a newly-created tailored configuration file:

```
!
version 12.2
!
enable password cisco
!
username cisco
!
ip http authentication enable <ckadapa>:this config is required
!
do telnet 5.1.1.1 19140
!
vstack director 5.1.1.1
!
end
!
```

SMI Proxy Database

SMI functionality works off the MAC address whereas the PnP solution, the UDI. SMI Proxy creates the UDI and adds the entry in SMI Proxy database for further communications (e.g., when SMI Proxy wants to send information from the SMI Client to the PnP Server). With the client's MAC address, SMI Proxy searches the database to acquire the SMI Client's UDI. When SMI Proxy wants to send the message received from PnP server to the SMI Client, it uses UDI to acquire the MAC address of the SMI Client. SMI Proxy uses this MAC address to send that message to respective SMI Clients.

This file is created locally under "flash:/vstack" or "bootflash:/vstack" based on the platform with the name smi_pnp_proxy_db.txt. Before creating the entry, SMI Proxy searches for the entry in the database. If the entry is missing, SMI Proxy adds it to the database, which is stored in the file and contains the entries for stale devices that were in the network previously. If the entry exists, SMI Proxy takes no action. Whenever the device on which SMI Proxy is running reboots, while that device is booting, the device retrieves the database from the file. Clearing this database is disallowed. The show command alone can display the entries.

Enabling Proxy on the Device

Beginning in privileged EXEC mode, follow these steps to enable SMI Proxy:

	Command	**Purpose**
Step 1	**config terminal**	Enters global configuration mode.
Step 2	**[no] vstack proxy {ip-address** *smi-ip* **| interface** *interface name*} **[startup-vlan** *vlan_value*] **[pnp-profile** *profile-name*]	Enables SMI SMI Proxy mode. The **[no]** form of the **vstack proxy** command turns off support for SMI clients. • Enter **ip-address** and the IP address. Launches SMI and enables director functionality on a device. This is a two-step "internal" process: a. SMI Proxy calls functions related to the **vstack director** *director_IP* command. where *director_IP* must match with at least one of the switch IP. In a scenario where an external DHCP server provides the addresses and the director IP to switches, the switch with matching director and switch IP addresses is eligible for only **vstack basic** configurations. b. Executes the **vstack**, **vstack director**, **vstack basic**, and **vstack startup-vlan** commands to enable 'Director' functionality on the switch. • Enter **interface** and the interface name. Given the interface name, the SMI Proxy uses the associated IP address to enable director functionality. • Enter **startup-vlan** and the VLAN value. Defined to support a non-Vlan1 scenario. Specifies the default VLAN that the director should use for Smart Install operations. Depending on the VLAN that is specified in the command, DHCP snooping is enabled on that VLAN so that the director can identify new switches that are connected to the network. If this command is not entered, however, VLAN 1 is used as default. • (Optional) Enter **pnp-profile** and profile name. SMI Proxy is associated with the profile name. If the profile name is not specified, SMI Proxy is associated with default profile name pnp-zero-touch.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**copy running-config startup config**	(Optional) Saves your entries in the configuration file.

	Command	Purpose
Step 5	show vstack config	Verifies the configuration.
Step 6	show vstack proxy-db	Displays the SMI clients that are present in the SMI proxy database.

Once SMI Proxy is enabled, the following commands are not accessible:

- **vstack director** *ip*
- **vstack basic**
- **vstack join-window**
- **vstack backup**

When SMI Proxy is enabled the output of the configuration **vstack** command is as follows:

```
IBD(config)# vst ?
  dhcp-localserver  Configure vstack dhcp parameters
  proxy             Configure smi pnp proxy feature
  startup-vlan      Configure vstack startup management vlan
  vlan              Configure vstack management vlan
  <cr>
```

This example shows how to configure SMI Proxy on interface vlan 1:

```
Switch# configure terminal
Switch(config)# vstack proxy interface vlan 1 startup-vlan 1
Switch(config)# end
```

This example shows how to configure SMI Proxy at ip-address 4.1.1.1:

```
Switch# configure terminal
Switch(config)# vstack proxy ip-address 4.1.1.1 startup-vlan 1
Switch(config)# end


Switch# configure terminal
Switch(config)#vstack proxy ip-address 4.1.1.1 startup-vlan 1 pnp-profile pnp-zero-touch
Switch(config)# end
```

Unsupported Services

More than 20 services are supported by the PnP Solution, out of which only seven are supported by SMI Proxy:

```
"capabilities",
"config-upgrade",
"device-info",
"image-install",
"topology"
"backoff"
"bye"
```

If the PnP Server requests a service not in this list, SMI Proxy sends an error message:

Enum: PNP_ERROR_UNSUPPORTED_REQUEST

Error string: "SMI PROXY:Not supported service request"

When a configuration upgrade request is sent from a PnP service, by default, the PnP server sends a request to the SMI Proxy, to copy the configuration upgrade to the running configuration. As SMI supports only copying the configuration upgrade to the startup configuration on proxied SMI clients, the SMI Proxy sends an error message. Once the PnP server receives this error message, it sends a request to copy the configuration upgrade to the startup configuration to SMI Proxy, which is then forwarded to the SMI client.

The following enum and error strings are sent:

Enum: XSVC_ERROR_CONFIG_UPGRADE_UNSUPPORTED

Error string: "SMI PROXY: Config upgrade apply to Running Config is not supported"

SMI proxy does not support device hardware information requests and device file information requests and the PnP service sends the following enum and error strings:

For device hardware information requests:

Enum: XSVC_ERROR_DEVICE_INFO_UNSUPPORTED

Error string: "SMI PROXY:Client device hardware info not supported"

For device file information requests:

Enum: XSVC_ERROR_DEVICE_INFO_UNSUPPORTED

Error string: "SMI PROXY:Client device filesystem info not supported"

Guidelines and Restrictions

- The SMI Proxy requires SMI Director and PnP Agent on a device.
- When SMI Proxy is enabled, features like join-window and scenarios such as switch replacement are not supported. The latter is handled as a new client addition.
- Central PnP Server supports only homogeneous stack upgrades.
- After SMI Proxy is enabled, SMI Director is disabled.
- SMI Director and SMI Proxy are mutually exclusive.
- In SMI Proxy mode, once a device has completed a configuration or image upgrade successfully, you should not clear the entry of that device in the vstack download-status list. If an SMI client requires a write erase and reload, ensure that the entry is not present in the vstack download-status list.

SMI Proxy CLI Commands

vstack proxy

To enable the PnP proxy, use the **vstack proxy** privileged EXEC command. To disable the PnP proxy, use the **no** form of the command.

> **[no] vstack proxy {ip_address** *smi-ip* **| interface** *interface_name*} **[startup-vlan** *vlan_value*]
> **pnp-profile** *profile-name*]

Syntax Description		
	ip_address *smi-ip*	Launches the SmartInstall feature and enables director functionality on the device with the specified IP address.
	interface *interface_name*	Launches the SmartInstall feature and enables director functionality on the device with the IP address of the interface.
		Internally, the stack proxy command executes **vstack**, **vstack director**, **vstack basic**, and **vstack startup-vlan** commands to enable Director functionality on the switch.
	startup-vlan *vlan_value*	Specifies the default VLAN that the director should use for Smart Install operations.
	pnp-profile *profile-name*	(Optional) Specifies the profile name to associate with SMI Proxy.

Command Default   None

Command Modes   Configuration mode

Command History	Release	Modification
	3.6.3E	This command was introduced.
	15.2(2)E3	This command was introduced.
	3.7.3E	This command was introduced.
	15.2(3)E3	This command was introduced.

Usage Guidelines   You can specify either the IP address or the interface name. If you specify the interface name, SMI Proxy uses the IP address of the interface.Depending on the specified VLAN, DHCP snooping is enabled on that VLAN so that the director can identify new switches that are connected to the network.

Note   SMI Director and Proxy are mutually exclusive with respect to configuration commands. SMI Director configuration commands are not visible after a device is configured in proxy mode. However, Proxy reuses SMI Director functionality internally

Depending on the specified VLAN, DHCP snooping is enabled on that VLAN so that the director can identify new switches that are connected to the network. If this command is not entered, VLAN 1 is used as default.

After Proxy is enabled, the vstack director and vstack basic commands are inaccessible.

Optionally, SMI Proxy will be associated with the profile name entered. If no profile name is specified then SMI Proxy will be associated with default profile name pnp-zero-touch.

After SMI Proxy is enabled, the following configuration commands are not accessible:

- vstack director ip
- vstack basic
- vstack join-window
- vstack backup

Examples   This example shows how to configure SMI Proxy at ip-address 4.1.1.1:

```
Switch# configure terminal
Switch(config)# vstack proxy ip-address 4.1.1.1 startup-vlan 1
Switch(config)# end


Switch# configure terminal
Switch(config)#vstack proxy ip-address 4.1.1.1 startup-vlan 1 pnp-profile pnp-zero-touch
Switch(config)# end
```

Related Commands

Command	Description
show vstack proxy-db [detail]	Displays the status of the SMI Proxy database.

debug vstack

To enable debugging of the Smart Install feature, use the **debug vstack** privileged EXEC command. To disable debugging, use the **no** form of this command.

> **debug vstack** {**all** | **backup** | **cli** | **director-db** | **download** | **emulation** | **fsm** | **group** | **join-window** | **protocol** | **smi-proxy**}

> **no debug vstack** {**all** | **backup** | **cli** | **director-db** | **download** | **emulation** | **fsm** | **group** | **join-window** | **protocol** | **smi-proxy**}

Syntax Description

all	Displays all Smart Install debug messages.
backup	Displays all Smart Install backup management debug messages.
cli	Displays Smart Install command-line interface (CLI) debug messages.
director-db	Displays Smart Install director database messages.
download	Displays Smart Install download debug messages.
emulation	Displays Smart Install emulation debug messages.
fsm	Displays Smart Install session-management debug messages.
group	Displays Smart Install group debug messages.
join-window	Displays all Smart Install join window debug messages.
protocol	Displays Smart Install protocol debug messages.
smi-proxy	Displays Smart Install SMI PnP proxy operations.

Command Default   Smart Install debugging is disabled.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.2(52)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

Usage Guidelines   The **undebug vstack** command is the same as the **no debug vstack** command.

Examples   This is example output from the **debug vstack all** command on a client:

```
switch# debug vstack all
Vstack debug all debugging is on
*May 15 22:37:56.739: VSTACK_DIR_DB: smi_parse_cdp_cache_entry: Got Neighbor on the port
Gi2/5/13
*May 15 22:37:56.739: VSTACK_DIR_DB: smi_parse_cdp_cache_entry: Mac addr after masking
Neig mac 6073.5cb6.6000, Local Mac 0026.99c9.b000
*May 15 22:37:56.739: VSTACK: smi_parse_cdp_cache_entry:processing the cdp pkt for mgmt
vlan
*May 15 22:37:56.739: VSTACK:
received vlan_plus_seqno=20370001, seq no for vlan = 8247,prev_seq_no=8247
*May 15 22:37:56.739: VSTACK_DIR_DB: smi_parse_cdp_cache_entry:string in parse
WS-C3750G-24TS-1U
*May 15 22:37:56.739: VSTACK:
smi_send_mgmt_vlan_to_cdp: Seq no + Mgmt Vlan = 20370001. After conversion Mgmt vlan
withseq no = 540475393,len=9
```

The following example shows output of the **debug vst smi-proxy** command

```
IBD# debug vst smi-proxy
SMI PNP PROXY:EXEC cli vstack execution successful
```
Following are more example of error logs:

```
Mar 30 02:27:51.149: VSTACK_SMI_PROXY:
smi_proxy_recv_msg_from_pnp_proxy: Received the PnP service request service type:21
Mar 30 02:27:51.149: VSTACK_SMI_PROXY: smi_proxy_backoff_request_handler:Received the
backoff request from pnp agent
Mar 30 02:27:51.149: VSTACK_SMI_PROXY:
smi_proxy_backoff_request_handler: Enqueuing backoff response for the device
id:PID:WS-C3750X-24,VID:V02,SN:FDO1613R2TA
Mar 30 02:27:51.183: VSTACK_SMI_PROXY:
smi_pnp_proxy_send_work_req: Sending work request for the device
id:PID:WS-C3750X-24,VID:V02,SN:FDO1613R2TA
Mar 30 02:27:51.183: VSTACK_SMI_PROXY:
smi_pnp_proxy_malloc_proxy_data: Malloc Success
Mar 30 02:27:51.183: VSTACK_SMI_PROXY:
smi_pnp_proxy_malloc_svc_data: Malloc done
Mar 30 02:27:51.183: VSTACK_SMI_PROXY:
smi_pnp_proxy_send_work_req: Enqueuing the work request for
UDI:PID:WS-C3750X-24,VID:V02,SN:FDO1613R2TA
```

Related Commands*	Command	Description
	show debugging	Displays information about the types of debugging that are enabled.

show vstack

To display Smart Install information, use the **show vstack** privileged EXEC command on the Smart Install director or a client.

> **show vstack** {**download-status** [**detail**]

> **show vstack proxy-db**[**detail**]

Syntax Description		
	config	Displays Smart Install configuration parameters.
	host	Displays information about a client within the Smart Install topology. This command is available only on the director.
	ip_address	The IP address of the director or a client.
	join-window configuration	Displays the join-window configurations.
	status	Displays the status of the CDP database. This command is available only on the director.
	detail (Optional)	Displays detailed information for the previous keyword. For example, **show vstack download-status detail** can display a detailed reason for a zero-touch update failure.
	download-status	Displays a tabulated output of the Smart Install image and configuration download successes and failures.
		Note Use this command to determine the status of updates.
		Note Beginning with IOS XE 3.6.0E (or 15.2.(2)E), the show download-status command displays the download upgrade of the image upgrade for a Catalyst 4500 platform. Additional fields are introduced in the output of the show download-status details command.
	client	Displays client information through the remote command
	1	Displays information about client 1 in the Smart Install network. Numbers are shown for as many clients as are in the network.
	client_ ip_address	Information about the client with the specified IP address.
	all	Displays information about all clients.
	group	Displays Smart Install group information.
	built-in	Displays information about preconfigured (built-in) groups.
	product_family	The identified (built-in) product family ID. To see the available product families, enter a **?** after **built-in**.
		If *product_family* is set to 4500 for Catalyst 4500 series switches.
	port_config	The switch port configuration. The available choices depend on the product family. To see the available port configurations, enter a **?** after the product family.
		If *product_family* is set to 4500, *port_config* means supervisor configuration.

chassis_config	The chassis type to configure.
	If *product_family* is set to 4500, the chassis type selected here is supported by the supervisor engine assigned to *port_config*.
configured	This keyword displays only the groups that are configured rather than showing all the groups.
custom	Information about user-defined groups.
group_name	Th custom group name.
client_password	The password that is required to access the client switch to get information on **running-config	tech-support	version** of the client switch.
running-config	Displays the current operating configuration for the selected client.
tech-support	Displays system information for technical support assistance.
version	Displays system hardware and software status.
neighbors	Displays information about the specified neighbors: • **1**—Neighbors of client 1 • *client_ip_address*—Neighbors of the specified client • **all**—All neighbors in the Smart Install network • **group**—Neighbors of the specified group or groups
proxy-db	Displays the status of the Proxy database. **Note** This command is available only on the SMI Director. Displays all the SMI client entries that are present in the Proxy database.

Command Modes   Privileged EXEC

Note   The command with some, but not all, of the keywords are available at the user EXEC level.

Command History

Release	Modification
12.2(52)SE	This command was introduced.
12.2(55)SE	The **client**, **join-window configuration**, **neighbors**, **1**, **running-config**, **tech-support**, and **version** keywords were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
15.0(2)EX	This command was integrated into Cisco IOS Release 15.0(2)EX.
15.0(2)EX1	This command was integrated into Cisco IOS Release15.0(2)EX1.
3.2(0)SE	This command was integrated into Cisco IOS Release 3.2(0)SE.

15.2(2)E	The option for post install (script) was introduced for **show vstack config**, **show vstack download-status**, **show vstack download-status detail**, **show vstack status**, and **show vstack status detail** commands
3.6.0E	The option **chassis type** for the **built-in** keyword was introduced.
	The option **proxy-db** was introduced.

Usage Guidelines   The outputs of the **show** commands are different when entered on the director or on the client. Not all keywords are available on the client.

In Cisco IOS Release 12.2(58)SE and later or Release 15.1(1)SY, the output of the **show vstack status** command shows whether or not Smart Install is enabled on the director. If enabled, it also includes this additional information about clients:

- Device status (Smart Install capable or not)
- Health status (active or inactive)
- Join-window status (allowed, hold, or denied), and
- Upgrade status for image or configuration (in progress, complete, or failed).

Beginning with Cisco IOS Release 3.6.0E (IOS 15.2(2)E), the output of the **show vstack status** command remains unchanged, but the meaning of the following fields have changed:

> **Note** These changes are for Catalyst 4500 Series Switch only.

- **Product-ID—***chassis-id* is used as the client's product ID and is collected from CDP. For an asymmetric chassis, the product ID may be updated dynamically.
- **MAC Address —**For a Catalyst 4500 standalone IBC, you use the chassis' MAC address whereas for VSS IBC, you use the virtual MAC selected while configuring VSS.

> **Note** The meaning of the fields **Hostname**, **IP** and **status** are unchanged; they are platform-independent.

If you disable Smart Install on the director by entering the **no vstack** global configuration command, the output of the **show vstack status** [**detail**] and **show vstack download-status** [**detail**] commands shows only Smart Install: DISABLED. The output of the **show vstack config** command shows the Smart Install configuration even though it is not in effect.

If the director is a Catalyst 4500 series switch, whether it is a single chassis or a VSS setup, only a single entry of the director appears in the output of the **show vstack status detail** command. The product ID shown is the chassis sku-id.

Beginning with IOS XE 3.6.0E (or 15.2.(2)E), the following apply:

- All the director entries (multiple, if the director is a stack) will be assigned the value '0,' and all the IBC stack members will have different entries (situation prior to IOS XE 3.6.0E (or 15.2.(2)E)) but they will all have the same device number.
- When you clear a DB entry and that IBC is a stack, the **clear vstack dir** command will remove all the stack entries from the database.

show vstack proxy-db indicates whether proxy mode is enabled. Proxy database contains the SMI client information about MAC address, UDI, and entry state. This command displays all SMI client entries that are present in proxy database.

After proxy mode is enabled, only four commands are available to the user:

```
IBD# show vst ?
  config            View configuration parameters under Vstack mode
  download-status   show the status of config or image download
  proxy-db          show the proxy database
  status            show the status of CDP database
```

Proxy database will contain information about the SMI client's MAC address, IP address. switch health status, UDI, and entry state.

Examples

This is example output from the **show vstack config** command on a client:

```
Director# show vstack config
Role: Client
 Vstack Director IP address: 1.1.1.163
```

This is example output from the **show vstack config** command on a director:

```
Director# show vstack config
Role: Director
 Vstack Director IP address: 1.1.1.163
 Vstack Mode: Basic
 Vstack default management vlan: 1
 Vstack start-up management vlan:1000
 Vstack management Vlans: none
 Vstack Config file: tftp://1.1.1.100/default-config.txt
 Vstack Image file: tftp://1.1.1.100/c3750e-universalk9-tar.122-
 Vstack Script file: tftp://1.1.1.100/post-install.txt
 Join Window Details:
         Window: Open (default)
         Operation Mode: auto (default)
 Vstack Backup Details:
         Mode: On (default)
         Repository: flash:/vstack (default)
```

This is example output from the **show vstack config** command in SMI Proxy mode:
```
Switch#show vst config
 Role: Smi PnP Proxy
 Vstack Smi PnP Proxy IP address: 4.1.1.1
 Vstack default management vlan: 1
 Vstack start-up management vlan: 1
 Vstack management Vlans: 1
Switch#
```

This is example output from the **show vstack download-status** command on a director:

```
Director# show vstack download-status
Total no of entries : 3
No   client-IP       client-MAC      Method         Image-status  Config-status  Script-status
===  ==============  ==============  =============  ===========   ============   =============
1    172.20.249.3    001e.be67.3000  image-upgrade   UPGRADED      **             **
2    172.20.249.1    0022.5699.c800  zero-touch      UPGRADING     UPGRADED       UPGRADED
3    172.20.249.2    0022.0d26.6300  image-upgrade   NOT STARTED   **             **
```

This is example output from the **show vstack status** command:

```
Director# show vstack status
```

```
SmartInstall:  ENABLED
Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress    I - done         X - failed
Config Upgrade:  c - in progress    C - done         x - failed
Director Database:
DevNo  MAC Address     Product-ID        IP_addr          Hostname    Status
=====  ==============  ================  ===============  ==========  =========
0      0018.7363.4200  WS-C3750-24TS     172.20.249.54    IBD-MXD-ST  Director
1      0016.4779.b780  WS-C3750G-24TS    172.20.249.54    IBD-MXD-ST  Director
2      d0d0.fd37.5a80  WS-C3750X-48P     172.20.249.54    IBD-MXD-ST  Director
3      0026.5285.7380  WS-C3750E-24TD    172.20.249.54    IBD-MXD-ST  Director
4      0024.13c6.b580  WS-C3750E-24TD    172.20.249.115   DEV-c6.b5c  S A a
5      0021.a1ab.9b80  WS-C2960-48TC-S   172.20.249.249   DEV-ab.9bc  S A a I C
6      0024.5111.0900  WS-C3750E-24TD    172.20.249.222   DEV-11.094  S A a I C
7      001d.45f3.f600  WS-C3750G-24TS    172.20.249.87    DEV-90.f64  S A a
8      0016.c890.f600  WS-C3750G-24TS    172.20.249.87    DEV-90.f64  S A a
9      001f.2604.8980  WS-C2960-48TC-S   172.20.249.89    DEV-04.89c  S A a I C
10     001b.d576.2500  WS-C3750E-24PD    172.20.249.91    DEV-a6.1cc  S A a I C
12     0cd9.9649.cb80  WS-C2960S-48TD-L  172.20.249.98    Switch      S A a
```

This is an example output from the **show vstack status** command if you have disabled Smart Install on the director by entering the **no vstack** global configuration command:

```
Switch# show vstack status
SmartInstall:  ENABLED

Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress    I - done         X - failed
Config Upgrade:  c - in progress    C - done         x - failed
Director Database:
DevNo  MAC Address     Product-ID        IP_addr          Hostname    Status
=====  ==============  ================  ===============  ==========  =========
0      0023.04c2.95c0  WS-C4506-E        1.1.1.1          Switch      Director
4      68ef.bd08.6000  WS-C4507R-E       1.1.1.2          IBC_WOW-08  S I a C

Switch#
```

This is an example output from the **show vstack status detail** command:

```
Director# show vstack status detail
SmartInstall:  ENABLED
----------------------------------------------
Device Num    : 0
Device ID     : 3750e-163-smi
MAC Address   : 0023.5e32.3780
IP Addr       : 1.1.1.163
Hop value     : 0
Serial        : FDO1239V026
Product-ID    : WS-C3750E-24PD
Version       : 12.2(0.0.242)DEV
Image         : C3750E-UNIVERSALK9-M
Entry Role    : Entry
(N-1)HOP Entry : Already Root
Backup done   :  no
Latest backup file: none
```

```
                   Latest backup client name: none
                   File checksum     : none
                   Status            : Director


                   ------------------------------------------------
                   Device Num     : 1
                   Device ID      : 3560g-10net-11
                   MAC Address    : 0013.c4b4.bc00
                   IP Addr        : 10.5.113.11
                   Hop value      : 1
                   Serial         : Not Found
                   Product-ID     : WS-C3560G-24PS
                   Version        : 12.2(50)SE3
                   Image          : C3560-IPSERVICESK9-M
                   Entry Role     : IBC Entry
                   (N-1)HOP Entry : 0023.5e32.3780
                   Backup done    :  no
                   Latest backup file: none
                   Latest backup client name: none
                   File checksum     : none
                   Status            : NSI


                   ------------------------------------------------
                   Device Num     : 2
                   Device ID      : 2960pd-47
                   MAC Address    : 001d.71ba.f780
                   IP Addr        : 1.1.1.1
                   Hop value      : 1
                   Serial         : FOC1138Z6P7
                   Product-ID     : WS-C2960PD-8TT-L
                   Version        : 12.2(0.0.242)DEV
                   Image          : C2960-LANBASEK9-M
                   Entry Role     : IBC Entry
                   (N-1)HOP Entry : 0023.5e32.3780
                   Backup done    :  Yes
                   Latest backup file: flash:/vstack/2960pd-47-001d.71ba.f780.REV2
                   Latest backup client name: 2960pd-47
                   File checksum     : 426154BFAFE1425F527621DC8B647C38
                   Status            : ACT


                   Director# show vstack download-status detail
                   SmartInstall:  ENABLED
                   No 1:
                   client-ip: 172.20.249.3
                   client-hostname: Switch
                   client-mac: 001e.be67.3000
                   method: image-upgrade
                   config-fail-reason: NA
                   image-fail-reason: NA
                   script-fail-reason: NA
                   config downloaded at: -
                   image downloaded at: 02:47:39 UTC Mar 30 2011
                   script downloaded at: -

                   No 2:
                   client-ip: 172.20.249.1
                   client-hostname: Switch
                   client-mac: 0022.5699.c8000
                   method: zero-touch
                   config-fail-reason: NA
                   image-fail-reason: NA
                   script-fail-reason: NA
```

```
config downloaded at: 03:02:23 UTC Mar 30 2011
image downloaded at: -
script downloaded at: 02:47:39 UTC Mar 30 2011

No 3:
client-ip: 217.20.249.2
client-hostname: Switch
client-mac: 0022.0d26.6300
method: image-upgrade
config-fail-reason: NA
image-fail-reason: NA
script-fail-reason: NA
config downloaded at: -
image downloaded at: -
script downloaded at: -
```

This is example output from the **show vstack status** command:

```
Director# show vstack status
SmartInstall:  ENABLED
Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress    I - done         X - failed
Config Upgrade:  c - in progress    C - done         x - failed
Script Upgrade:  p - in progress    P - done         F - failed
Director Database:
DevNo  MAC Address      Product-ID        IP_addr          Hostname    Status
=====  ==============   ================  ==============   ==========  =========
0      0018.7363.4200   WS-C3750-24TS     172.20.249.54    IBD-MXD-ST  Director
1      0016.4779.b780   WS-C3750G-24TS    172.20.249.54    IBD-MXD-ST  Director
2      d0d0.fd37.5a80   WS-C3750X-48P     172.20.249.54    IBD-MXD-ST  Director
3      0026.5285.7380   WS-C3750E-24TD    172.20.249.54    IBD-MXD-ST  Director
4      0024.13c6.b580   WS-C3750E-24TD    172.20.249.115   DEV-c6.b5c  S A a
5      0021.a1ab.9b80   WS-C2960-48TC-S   172.20.249.249   DEV-ab.9bc  S A a I C
6      0024.5111.0900   WS-C3750E-24TD    172.20.249.222   DEV-11.094  S A a I C P
7      001d.45f3.f600   WS-C3750G-24TS    172.20.249.87    DEV-90.f64  S A a
8      0016.c890.f600   WS-C3750G-24TS    172.20.249.87    DEV-90.f64  S A a
9      001f.2604.8980   WS-C2960-48TC-S   172.20.249.89    DEV-04.89c  S A a I C P
10     001b.d576.2500   WS-C3750E-24PD    172.20.249.91    DEV-a6.1cc  S A a I C
12     0cd9.9649.cb80   WS-C2960S-48TD-L  172.20.249.98    Switch      S A a
```
This is an example output from the **show vstack status** command if you have disabled Smart Install on the director by entering the **no vstack** global configuration command:

```
Director # show vstack status
SmartInstall:  DISABLED
```

This is example output from the **show vstack status** command:

```
Switch# show vstack status
SmartInstall:  ENABLED

Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress    I - done         X - failed
Config Upgrade:  c - in progress    C - done         x - failed
Script Upgrade:  p - in progress    P - done         F - failed

Director Database:
DevNo  MAC Address      Product-ID        IP_addr          Hostname    Status
=====  ==============   ================  ==============   ==========  =========
```

```
0       0023.04c2.95c0  WS-C4506-E           1.1.1.1            Switch    Director
4       68ef.bd08.6000  WS-C4507R-E          1.1.1.2            IBC_WOW-08  S I a C P

Switch#
```

This is an example output from the **show vstack status detail** command:

```
Director# show vstack status detail
SmartInstall:  ENABLED
------------------------------------------------
Device Num     : 0
Device ID      : 3750e-163-smi
MAC Address    : 0023.5e32.3780
IP Addr        : 1.1.1.163
Hop value      : 0
Serial         : FDO1239V026
Product-ID     : WS-C3750E-24PD
Version        : 12.2(0.0.242)DEV
Image          : C3750E-UNIVERSALK9-M
Entry Role     : Entry
(N-1)HOP Entry : Already Root
Backup done    :  no
Latest backup file: none
Latest backup client name: none
File checksum     : none
Status            : Director


------------------------------------------------
Device Num     : 1
Device ID      : 3560g-10net-11
MAC Address    : 0013.c4b4.bc00
IP Addr        : 10.5.113.11
Hop value      : 1
Serial         : Not Found
Product-ID     : WS-C3560G-24PS
Version        : 12.2(50)SE3
Image          : C3560-IPSERVICESK9-M
Entry Role     : IBC Entry
(N-1)HOP Entry : 0023.5e32.3780
Backup done    :  no
Latest backup file: none
Latest backup client name: none
File checksum     : none
Status            : NSI


------------------------------------------------
Device Num     : 2
Device ID      : 2960pd-47
MAC Address    : 001d.71ba.f780
IP Addr        : 1.1.1.1
Hop value      : 1
Serial         : FOC1138Z6P7
Product-ID     : WS-C2960PD-8TT-L
Version        : 12.2(0.0.242)DEV
Image          : C2960-LANBASEK9-M
Entry Role     : IBC Entry
(N-1)HOP Entry : 0023.5e32.3780
Backup done    :  Yes
Latest backup file: flash:/vstack/2960pd-47-001d.71ba.f780.REV2
Latest backup client name: 2960pd-47
File checksum     : 426154BFAFE1425F527621DC8B647C38
Status            : ACT
```

This example shows the output of the **show vstack proxy-db** command:

```
IBD# show vstack proxy-db
Smi PnP Proxy:    ENABLED


Proxy Database:
MAC ADDR          UDI                                           State
=========         =====================================        ======
001e.f76d.af80    PID:WS-C3750E-48TD,VID:V01,SN:FDO1152V10R     NO STATE
```

After proxy mode is enabled, only three commands are available to the user:

```
Status: Health_status
Health_status: A - Active I - Inactive
Proxy Database:
MAC ADDR          IP_addr        Hostname        Status
=========         ============   ============    ======
001e.f76d.af80  5.1.1.4          Switch                  A
```

```
IBD# show vstack proxy-db detail
Smi PnP Proxy:    ENABLED


-------------------------------------------------
Device ID         : Switch
MAC Address   : 001e.f76d.af80
IP Addr           : 5.1.1.4
UDI                 : PID:WS-C3750E-48TD,VID:V01,SN:FDO1152V10R
state                 : HELLO
status               : A
After proxy mode is enabled, only the following commands are accessible:
Switch# show vstack ?
  config           View configuration parameters under Vstack mode
  download-status  show the status of config or image download
  proxy-db         show the proxy database
  status           show the status of CDP database
```

After proxy mode is enabled, only three commands are accessible:

```
IBD# show vst ?
  config    View configuration parameters under Vstack mode
  proxy-db  show the proxy database
  status    show the status of CDP database
```

Related Commands	Command	Description
	vstack basic	Enables the switch or router to be the Smart Install director. This command is accepted only if the director IP address is on the switch or router.
	vstack director	Configures a Smart Install director IP address.

Security Methods

The following security methods are supported, to secure PnP client and server communication. For detailed information, see the Security Methods for the PnP Discovery Process and Security Methods for Post-PnP Discovery Process in the *Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E* on cisco.com.

Security Methods for the PnP Discovery Process

- Self-Signed Certificate based Authentication
- Mobile Device based Secured Installation
- CA-Signed Certificate based Authentication
  - DHCP Option-based Discovery
  - DNS-based Discovery

Security Methods for Post-PnP Discovery Process

- Certificate Install Service
- SUDI-based PnP Application Level Authentication
  - SUDI-based Client Certificate Validation
  - SUDI-based Serial Number
  - SUDI-Based Device Authentication

Smart Install MIBs and System Messages

SNMP MIBs

Simple Management Network Protocol (SNMP) development and use is centered around the Management Information Base (MIB). An SNMP MIB is an abstract database, which is a conceptual specification for information that a management application may read and modify in a certain form. This does not imply that the information is kept in the managed system in that same form. The SNMP agent translates between the internal data structures and formats of the managed system and the external data structures and formats defined for the MIB.

The SNMP MIB is conceptually a tree structure with conceptual tables. Relative to this tree structure, the term MIB has two functions:

- It is actually a MIB branch, usually containing information for a single aspect of technology, such as a transmission medium or a routing protocol. A MIB used this way is more accurately called a MIB module, and is usually defined in a single document.

- A MIB is a collection of such branches. This collection might comprise, for example, all the MIB modules implemented by a given agent or the entire collection of MIB modules defined for SNMP.

A MIB is a tree where the leaves are individual items of data called objects. An object may be a counter or a protocol status. MIB objects are also sometimes called variables.

Cisco Smart Install MIB

The CISCO-SMART-INSTALL-MIB.my MIB module defines managed objects that facilitate the management of the Smart Install feature. Smart Install is a plug-and-play image and configuration management feature that enables zero-touch deployment of Cisco network devices in an enterprise branch network.

This MIB module is supported only on the director and is designed for the following:

- Checks most of the Smart Install configurations on the director.

- Supports monitoring of client devices discovered by the director.

- Provides status of the deployed client image and configuration as a result of operator-defined profiles.

- Provides notifications for these events:

  - New client joined

  - Client removed

  - Upgrade failure

  - Director functionality enabled or disabled

Note   SNMP set is not supported in this release.

Downloading and Working with MIBs

These sections provide information about how to download the CISCO-SMART-INSTALL-MIB.my. for the Smart Install feature.

- Guidelines for Working with MIBs

- Downloading MIBs

Guidelines for Working with MIBs

While working with MIBs, consider the following guidelines:

- Mismatches on datatype definitions might cause compiler errors or warning messages. Although Cisco MIB datatype definitions are not mismatched, some standard RFC MIBs do mismatch. For example:

```
MIB A defines: SomeDatatype ::= INTEGER(0..100)
MIB B defines: SomeDatatype ::= INTEGER(1..50)
```

This example is considered to be a trivial error and the MIB loads successfully with a warning message.

The next example is considered as a nontrivial error (even though the two definitions are essentially equivalent), and the MIB is not successfully parsed.

```
MIB A defines: SomeDatatype ::= DisplayString
MIB B defines: SomeDatatype ::= OCTET STRING (SIZE(0..255))
```

If your MIB compiler treats these as errors, or you want to delete the warning messages, edit one of the MIBs that define this same datatype so that the definitions match.

- Many MIBs import definitions from other MIBs. If your management application requires MIBs to be loaded, and you experience problems with undefined objects, you might want to load the following MIBs in this order:

  RFC1213-MIB.my
  IF-MIB.my
  CISCO-SMI.my
  CISCO-PRODUCTS-MIB.my
  CISCO-TC.my

- For information about how to download and compile Cisco MIBs, go to the following URL:

  http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00800b4cee.shtml

Downloading MIBs

To download the MIBs onto your system if they are not already there, follow these steps:

Step 1   Review the guidelines in the previous section ("Guidelines for Working with MIBs").

Step 2   Search for the CISCO-SMART-INSTALL-MIB.my. If the MIB you want to download is not there, try the other URL and search again.

Go to one of the following Cisco URLs:

ftp://ftp.cisco.com/pub/mibs/v2

ftp://ftp.cisco.com/pub/mibs/v1

Step 3   Click the link for a MIB to download to your system.

Step 4   Select **File > Save** or **File > Save As** to save the MIB on your system.

System Messages

How to Read System Messages

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Messages appear in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)

seq no:timestamp: %facility-severity-MNEMONIC:description

By default, a switch sends the output from system messages to a logging process. In a switch stack, stack members append their hostnames to the output from system messages and redirect the output to the logging process on the stack master.

Each system message begins with a percent sign (%) and is structured as follows:

%FACILITY-SEVERITY-MNEMONIC: Message-text

- FACILITY is two or more uppercase letters that show the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software. The facility for Smart Install messages is *SMI*.
- SEVERITY is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.

Table 5-1   Message Severity Levels

Severity Level	Description
0 – emergency	System is unusable.
1 – alert	Immediate action required.

Table 5-1   Message Severity Levels (continued)

Severity Level	Description
2 – critical	Critical condition.
3 – error	Error condition.
4 – warning	Warning condition.
5 – notification	Normal but significant condition.
6 – informational	Informational message only.
7 – debugging	Message that appears during debugging only.

- MNEMONIC is a code that uniquely identifies the message.

- Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec].

Table 5-2   Variable Fields

Representation	Type of Information
[dec]	Decimal integer
[char]	Single character
[chars]	Character string
[enet]	Ethernet address (for example, 0000.FEED.00C0)
[hex]	Hexadecimal integer
[inet]	Internet address

Error Message Traceback Reports

Some messages describe internal errors and contain traceback information. Include this information when you report a problem to your technical support representative.

This message example includes traceback information:

```
-Process= "Exec", level= 0, pid= 17
-Traceback= 1A82 1AB4 6378 A072 1054 1860
```

Some system messages ask you to copy the error messages and take further action.

Output Interpreter

The Output Interpreter provides additional information and suggested resolutions based on the output of many CLI commands, such as the **show tech-support** privileged EXEC command.

https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl

Bug Toolkit

The Bug Toolkit provides information on open and closed caveats. You can search for all known bugs in a specific Cisco IOS Release.

http://tools.cisco.com/Support/BugToolKit/

Smart Install System Messages

Error Message `SMI-3-IMAGELIST_FAILED: Default imagelist creation failed.`

Explanation The creation of the default image list file failed in flash memory. Possible reasons for this failure are that there is insufficient space in the flash memory of the Smart Install director, an error occurred while the default image list file was created, or there is no default image configured.

Recommended Action Verify that the director flash memory has sufficient space. If necessary, free some flash memory space (a default image list file would need about 100 bytes of space). If necessary, reconfigure the director.

Error Message `SMI-3-IMG_CFG_NOT_CONFIGURED: [chars] (IP Address :[inet]) : The Director does not have a image list file or a configuration file configured for this Product-ID`

Explanation The Smart Install director does not have an image list file or configuration file for the device, preventing a successful upgrade. [chars] is the Smart Install device on which the message is displayed, which can be either the client or director, and [inet] it the IP address of that device.

> **Note** When the message appears on the director, [chars] provides redundant information.

Recommended Action Make sure that the device is added to a built-in group or user-defined group. Configure an image list file or configuration file for the group by using the **vstack group built-in** global configuration command for the built-in group or **vstack group custom** global configuration command for the user-defined group.

Error Message `SMI-3-INTERNAL_ERROR: [chars] - [dec]`

Explanation An internal software error occurred on the Smart Install director switch. [chars] describes the error, and [dec] is the error return code.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SMI-3-NOMEMORY: Smart Install memory allocation failure; could not allocate [chars]`

Explanation The Smart Install client switch has failed to allocate memory. [chars] is the data table that is allocated during initialization for MIB objects.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SMI-3-SMI_CLIENT_BACKUP_FAILURE: Client Device startup configuration backup fail on repository`

Explanation The Smart Install client switch has failed to back up its startup configuration to the repository. (This message appears only on the client switch.)

Recommended Action Verify that you can ping the director switch from the client switch. Verify that the client switch can reach the repository. On the director, look at the output of the **show vstack config** privileged EXEC command to verify that the configuration parameters are correct and that the backup mode is on. Verify that the directory setting on the repository is correct, especially if the repository is an external TFTP server.

Error Message `SMI-3-SMI_DIRECTOR_BACKUP_FAILURE: Client Device ([inet]) startup configuration backup fail on repository: [chars] - reason: [chars]`

Explanation The Smart Install client switch has failed to back up its startup configuration to the repository. [inet] is the IP address of the client switch. The first [chars] is the repository path, and the seconds [chars] is the reason for the failure. (This message appears only on the director switch.)

Recommended Action Verify that you can ping the director switch from the client switch. Verify that the client switch can reach the repository. On the director, look at the output of the **show vstack config** privileged EXEC command to verify that the configuration parameters are correct and that the backup mode is on. Verify that the directory setting on the repository is correct, especially if the repository is an external TFTP server.

Error Message `SMI-3-TAILOR_FAILED: Legacy switches will not be upgraded`

Explanation The creation of a tailored Smart Install configuration file failed. Possible reasons for this failure are that there is insufficient space in the director flash memory or an error occurred while the new configuration file was created.

Recommended Action Verify that the director flash memory has sufficient space. If necessary, free some flash memory space (a tailored configuration would need about 100 bytes of space). If necessary, reconfigure the director.

Error Message `SMI-3-UPGRD_FAILED: Device (IP address: [inet]) [chars] upgrade failed`

Explanation The Smart Install client switch could not upgrade. [inet] is the IP address of the client switch. [chars] is the image or the configuration.

Recommended Action Verify that the configuration on the director switch is correct. Verify that the client switch can reach the TFTP server. Verify that the image or configuration file exists on the TFTP server and is specified correctly.

Error Message `SMI-5-DIRECTOR: Director is [chars]`

Explanation The status of the Smart Install director changed. [chars] is the status (*Enabled* or *Disabled*).

Recommended Action No action is required.

Error Message `SMI-6-AUTOINSTALL: [chars] AUTOINSTALL`

Explanation The auto install and Smart Install processes stopped or continued. [chars] is the status of the processes, which can be either *aborted* or *continued*.

Recommended Action No action is required.

Error Message `SMI-6-CLIENT_CONN_FAILED: Device (IP address: [inet]) failed to connect to Director (IP address : [inet])`

Explanation A Smart Install client did not connect to the director because it did not have the IP address of the director or could not reach the director for other reasons. The first [inet] is the IP address of the client, and the second [inet] is the IP address of the director.

Recommended Action Verify that the IP address of the director is correctly configured on the client.

Error Message `SMI-6-INCORRECT_CFG: No image and config configured for this [chars] [chars]`

Explanation The Smart Install director does not have a configuration for the device. The first [chars] is the type of device (*switch*, *switch-stack*, or *sku type*). If the type of device is *sku type*, the second [chars] is the model number.

Recommended Action Configure a group with a configuration for the device.

Error Message `SMI-6-SMI_CLIENT_BACKUP_SUCCESS: Client Device startup configuration backup successful on repository`

Explanation The Smart Install client switch has successfully backed up its startup configuration to the repository. (This message appears only on the client switch.)

Recommended Action No action is required.

Error Message `SMI-6-SMI_DHCP_ERR: Device failed to [chars] DHCP [chars]`

Explanation The Smart Install director did not configure or remove a DHCP parameter, such as a DHCP pool, subnet, or DHCP pool option. The first [chars] is the status, which can be *configure* or *remove*, and the second [chars] is the DHCP parameter.

Recommended Action Verify that the DHCP parameter is a permitted value.

Error Message `SMI-6-SMI_DIRECTOR_BACKUP_SUCCESS: Client Device ([inet]) startup configuration backup successful on repository: [chars]`

Explanation The Smart Install client switch has successfully backed up its startup configuration to the repository. [inet] is the IP address of the client switch. [chars] is the repository path. (This message appears only on the director switch.)

Recommended Action No action is required.

Error Message `SMI-6-SMI_INVALID_MESSAGE: Received invalid message from [chars] (IP Address : [inet]), SMI Version : [dec] Message Type : [dec]`

Explanation The Smart Install client or director received an invalid message type. This occurs when a newer version of the Smart Install Protocol interoperates with an older version of the protocol that does not support the new message. [chars] is the Smart Install device, which can be either the client or the director, and [inet] it the IP address of that device. The first [dec] is the Smart Install Protocol version on the device that sent the invalid message, and the second [dec] is the type of invalid message.

Recommended Action Make sure that the director switch runs the latest version of the Smart Install Protocol. A director switch that runs the latest version of the protocol can interoperate with a client switch that runs an older version, but not the other way around.

Error Message `SMI-6-SMI_JOIN_WINDOW_MESSAGE: SMI Join window [chars] on IBD(IP address: [inet]`

Explanation A Smart Install join window was opened or closed. [chars] is the status of the window, which can be either *Start* or *End*, and [inet] is the IP address of the device on which the join window was opened or closed.

Recommended Action No action is required.

Error Message `SMI-6-SWITCH_ADD: New Device detected by Director with mac address: [enet]`

Explanation The Smart Install director detected a new device and added it to the database. [enet] is the Ethernet address of the new device.

Recommended Action No action is required.

Error Message `SMI-6-SWITCH_REMOVE: Device [enet] removed from the Director Database`

Explanation A device stopped communicating and was removed from the Smart Install director database. The device might have also been removed from the Smart Install network. [enet] is the Ethernet address of the device.

Recommended Action No action is required.

Error Message `SMI-6-SWITCH_REPLACE: Device [enet] is being replaced by [enet] Device`

Explanation A device was replaced by another device in a Smart Install network. The first [enet] is the Ethernet address of the device that was replaced, and the second [enet] is the Ethernet address of the replacement device.

Recommended Action No action is required.

Error Message `SMI-6-UPGRD_STARTED: Device (IP address: [inet]) [chars] upgrade has started`

Explanation An image or configuration file upgrade started on the Smart Install client. [inet] is the IP address of the client, and [chars] is the name of the image or configuration file.

Recommended Action No action is required.

Error Message `SMI-6-UPGRD_SUCCESS: Device (IP address: [inet]) [chars] has upgraded successfully`

Explanation The Smart Install client was upgraded with a new image or configuration file. [inet] is the IP address of the client, and [chars] is the name of the new image or configuration file.

Recommended Action No action is required.

Supported Devices for Smart Install

Table A-1   Supported Switches

Switch	Can be Director?	Can be Client?
Catalyst 6500 Supervisor Engine 2T-10GE	Yes	No
Catalyst 4500 Supervisor Engine, 6E, 6LE, 7E, 7LE	Yes	No
Catalyst 3850	Yes	Yes
Catalyst 3750-X	Yes	Yes
Catalyst 3750-E	Yes	Yes
Catalyst 3750	Yes	Yes
Catalyst 3650	Yes	Yes
Catalyst 3560-X	Yes	Yes
Catalyst 3560-E	Yes	Yes
Catalyst 3560-C	No	Yes
Catalyst 3560	Yes	Yes
Catalyst 2960-S	No	Yes
Catalyst 2960-SF	No	Yes
Catalyst 2960-C	No	Yes
Catalyst 2960-P	No	Yes
Catalyst 2960	No	Yes
Catalyst 2975	No	Yes
IE 2000	Yes	Yes
IE 3000	Yes	Yes
IE 3010	Yes	Yes
SM-ES2 SKUs	No	Yes
SM-ES3 SKUs	No	Yes

Table A-1   Supported Switches

Switch	Can be Director?	Can be Client?
NME-16ES-1G-P	No	Yes
SM-X-ES3 SKUs	Yes	Yes

Table A-2   Supported Routers

Router	Can be Director?	Can be Client?
Cisco 3900 Series Integrated Services Routers G2	Yes	No
Cisco 2900 Series Integrated Services Routers G2	Yes	No
Cisco 1900 Series Integrated Services Routers G2	Yes	No
Cisco 3800 Series Integrated Services Routers	Yes	No
Cisco 2800 Series Integrated Services Routers	Yes	No
Cisco 1800 Series Integrated Services Routers	Yes	No

Table A-3   Minimum Software Releases for Directors and Clients

Directors	Minimum Software Release
Catalyst 6500 Supervisor Engine 2T-10GE	Cisco IOS Release 15.1(1)SY
Catalyst 4500 Supervisor Engine 7E and 7LE	Cisco IOS Release XE 3.4SG
Catalyst 4500 Supervisor Engine 6K and 6LE	Cisco IOS Release 15.1(2)SG
Catalyst 3850	Cisco IOS Release 3.2(0)SE
Catalyst 3650	Cisco IOS Release 3.3(0)SE
Cisco 3900, 2900, and 1900 Series Integrated Services Routers G2	Cisco IOS Release 15.1(3)T
Cisco 3800, 2800, and 1800 Series Integrated Services Routers	Cisco IOS Release 15.1(3)T
Catalyst 3750-E, 3750, 3560-E, and 3560 Switches	Cisco IOS Release 12.2(55)SE
Catalyst 3750-X and 3560-X Switches	Cisco IOS Release 12.2(55)SE
SM-X-ES3 SKUs	Cisco IOS Release 15.0(2)EJ

Table A-4   Minimum Software Releases for Clients

Smart-Install Capable Clients[1]	Minimum Software Release
Catalyst 3750-E, 3750, 3560-E, and 3560 Switches	Cisco IOS Release 12.2(52)SE
Catalyst 3750-X and 3560-X Switches	Cisco IOS Release 12.2(53)SE2
Catalyst 3560-C Compact Switches	Cisco IOS Release 12.2(55)EX
Catalyst 2960 and 2975 Switches	Cisco IOS Release 12.2(52)SE
Catalyst 2960-S Switches	Cisco IOS Release 12.2(53)SE1
Catalyst 2960-C Compact Switches	Cisco IOS Release 12.2(55)EX1

Table A-4   Minimum Software Releases for Clients

Smart-Install Capable Clients[1]	Minimum Software Release
Catalyst 2960-SF	Cisco IOS Release 15.0(2)SE
Catalyst 2960- P	Cisco IOS Release 15.2(2)SE
IE 2000	Cisco IOS Release 15.2(2)SE
IE 3000	Cisco IOS Release 15.2(2)SE
IE 3010	Cisco IOS Release 15.2(2)SE
SM-ES3 SKUs, NME-16ES-1G-P	Cisco IOS Release 12.2(52)SE
SM-ES2 SKUs	Cisco IOS Release 12.2(53)SE1
SM-X-ES3 SKUs	Cisco IOS Release 15.0(2)EJ

1. Listed switches running earlier Cisco IOS releases are not Smart Install capable, but can be clients in Smart Install networks as long as they support the **archive download-sw** privileged EXEC command.

Supported SKUs for Smart Install

Table 2-1 Compatibility between Catalyst 4500 Switch Supervisor Engine and Chassis

Supervisor Engine	Chassis Type
Supervisor Engine 6-E	
	WS-4503
	WS-4506
	WS-4507R+E
	WS-4507R-E
	WS-4510R+E
	WS-4510R-E
Supervisor Engine 6L-E	
	WS-4503
	WS-4506
	WS-4507R+E
	WS-4507R-E
Supervisor Engine 7-E	
	WS-4503
	WS-4506
	WS-4507R+E
	WS-4507R-E
	WS-4510R+E
	WS-4510R-E
Supervisor Engine 7L-E	
	WS-4503
	WS-4506
	WS-4507R+E
	WS-4507R-E

Table 2-1   Compatibility between Catalyst 4500 Switch Supervisor Engine and Chassis

Supervisor Engine	Chassis Type
Supervisor Engine 8-E	
	WS-4503
	WS-4506
	WS-4507R+E
	WS-4507R-E

Table 2-2   Compatibility between Catalyst 2k and 3k Chassis, SKU ID, and SKI

Chassis	SKU ID	SKI
3560		
	3560_48_POE	3560 48 port POE
	3560_24_POE	3560 24 port POE
	3560_48	3560 48 port non POE
	3560_24	3560 24 port non POE
	3560_12	3560 12 port non POE
	3560_8	3560 8 port POE
3560E		
	3560_48_POE	3560 48 port POE
	3560_24_POE	3560 24 port POE
	3560_48	3560 48 port non POE
	3560_24	3560 24 port non POE
	3560E_12_10gig	12 port 10 gig
3750		
	3750_48_POE	3750 48 port POE
	3750_24_POE	3750 24 port POE
	3750_48	3750 48 port non POE
	3750_24	3750 24 port non POE
3750E		
	3750E_48_POE	3750 48 port POE
	3750E_24_POE	3750 24 port POE
	3750E_48	3750 48 port non POE
	3750E_24	3750 24 port non POE
2918		
	2918_24	2918 24 port
	2918_48	2918 48 port
2960 LAN Base		

Table 2-2   Compatibility between Catalyst 2k and 3k Chassis, SKU ID, and SKI

Chassis	SKU ID	SKI
	2960_48	2 dual purpose or TT uplinks
	2960_24	2 dual purpose or TT uplinks
	2960_48_POE	48 port POE
	2960_24_POE	24 port POE
	2960_24_8_POE	24 port SKU with 8 port POE
	2960_8_POE_PD	8 port POE PD switch <**PD????**>
	2960_8	8 port + 1 dual
	2960_8_gig	7 ports + 1 dual
	2960_24_gig	4 dual purpose or TT uplinks
	2960_48_gig	4 dual purpose or TT uplinks
2960 LAN-lite		
	2960_8_LL	8 port lan lite
	2960_24_LL_nouplink	24 port with no uplinks
	2960_24_LL	24 port lan lite
	2960_48_LL	48 port lan lite
2975 2K Stackable		
	2975_48_poe	24 port 2K stackable
2960X LAN Base	2960X-24PD-L	24 ports, 2 SFP+, PoE
	2960X-24PS-L	24 ports, 4 SFP, PoE
	2960X-24PSQ-L	24 ports, 2 SFP, 8PoE
	2960X-24TD-L	24 ports, 2 SFP+
	2960X-24TS-L	24 ports, 4 SFP
	2960X-48FPD-L	48 ports, 2 SFP+, PoE
	2960X-48FPS-L	48 ports, 4 SFP, PoE
	2960X-48LPD-L	48 ports, 2 SFP+, PoE
	2960X-48LPS-L	48 ports, 4 SFP, PoE
	2960X-48TD-L	48 ports, 2 SFP+,
	2960X-48TS-L	48 ports, 2 SFP
2960X LAN Lite	2960X-24TS-LL	24 ports, 2 SFP
	2960X-48TS-LL	48 ports, 2 SFP

Table 2-2   Compatibility between Catalyst 2k and 3k Chassis, SKU ID, and SKI

Chassis	SKU ID	SKI
2960XR- IP Lite	2960XR-48FPD-I	48 ports, 2 SFP+, PoE
	2960XR-48LPD-I	48 ports, 2 SFP+, PoE
	2960XR-24PD-I	24 ports, 2 SFP+, PoE
	2960XR-48TD-I	48 ports, 2 SFP+, PoE
	2960XR-24TD-I	24 ports, 2 SFP+
	2960XR-48FPS-I	48 ports, 4 SFP, PoE
	2960XR-48LPS-I	48 ports, 4 SFP, PoE
	2960XR-24PS-I	24 ports, 4 SFP, PoE
	2960XR-48TS-I	48 ports, 4 SFP
	2960XR-24TS-I	24 ports, 4 SFP
3850	WS-C3850-24T	24 ports
	WS-C3850-48T	48 ports
	WS-C3850-24P	24 PoE+
	WS-C3850-48P	48 PoE+
	WS-C3850-48F	48 PoE+
	WS-C3850-24U	24 UPOE
	WS-C3850-48U	48 UPOE
	WS-C3850-12S	12 SFP
	WS-C3850-24S	24 SFP
3650	WS-C3650-24TS	24 ports
	WS-C3650-48TS	48 ports
	WS-C3650-24PS	24 ports, PoE+
	WS-C3650-48PS	48 ports, PoE+
	WS-C3650-48FS	48 ports, PoE+
	WS-C3650-24TD	24 ports
	WS-C3650-48TS	48 ports
	WS-C3650-24PD	24 ports, PoE+
	WS-C3650-48PD	48 ports, PoE+
	WS-C3650-48FD	48 ports, PoE+
	WS-C3650-48TQ	48 ports
	WS-C3650-48PQ	48 ports PoE+
	WS-C3650-48FQ	48 ports PoE+

Table 2-2   Compatibility between Catalyst 2k and 3k Chassis, SKU ID, and SKI

Chassis	SKU ID	SKI
IE2000 LAN Lite	IE-2000-4TS-L1	6 ports, 2FE SFP ports
	IE-2000-4T-L	6 ports, 6FE RJ45 ports
	IE-2000-4TS-G-L	6 ports, 2GE SFP ports
	IE-2000-4T-G-L	6 ports, 4 FE, 2GE RJ45 ports
	IE-2000-4S-TS-G-L	6 ports, 4 FE, 2GE SFP ports
	IE-2000-8TC-L	10 ports, 2FE SFP ports
	IE-2000-8TC-G-L	10 ports, 2GE Combo ports
	IE-2000-16TC-L	20 ports, 2FE SFP ports
	IE-2000-16TC-G-L	20 ports, 2 FE SFP ports
	IE-2000-16PTC-G-L	18 ports, 2GE Combo ports
IE2000 LAN Base	IE-2000-4TS-B	6 ports, 2FE SFP ports
	IE-2000-4T-B	6 ports, 6FE RJ45 ports
	IE-2000-4TS-G-B	6 ports, 2GE Combo ports
	IE-2000-4T-G-B	6 ports, 4FE, 2GE Combo ports
	IE-2000-4S-TS-G-B	6 ports, 4FE, 2GE Combo ports
	IE-2000-8TC-B	10 ports, 2FE SFP ports
	IE-2000-8TC-G-B	10 ports, 2FE SFP ports
	IE-2000-8TC-G-E	10 ports, 2GE Combo ports
	IE-2000-16TC-B	20 ports, 2FE SFP ports
	IE-2000-16TC-G-E	20 ports, 2FE SFP ports
	IE-2000-16TC-G-X	20 ports, 2FE SFP ports
	IE-2000-16PTC-G-E	18 ports, 2GE Combo ports
IE2000 Enhanced LAN Base	IE-2000-8TC-G-N	10 ports, 2GE Combo ports
	IE-2000-16TC-G-N	20 ports, 2FE SFP ports
	IE-2000-16PTC-G-NX	18 ports, 2GE Combo ports

Cisco Smart Install Configuration Guide

Table 2-2   Compatibility between Catalyst 2k and 3k Chassis, SKU ID, and SKI

Chassis	SKU ID	SKI
IE-3000 LAN Base	IE-3000-4TC	4 ports, 2 dual-purpose uplinks
	IE-3000-8TC	8 ports, 2 dual-purpose uplinks
IE-3010	IE-3010-16S-8PC	16 ports, 8 PoE ports
	IE-3010-24TC	24 ports, 2 SFP ports

CHAPTER C

Features by Release

The Smart Install is introduced in Cisco IOS Releases 12.2(52)SE, 15.0(2)SE and later, 15.1(2)SG, XE 3.4SG, 15.1(1)SY, 3.2(0)SE and later,15.3(3)M, 15.2.(2)E, 15.2.(3)E and later.

Minimum Cisco IOS Release for Major Features

Table C-1 lists the minimum software release (after the first release) required to support the major features. Features not listed are supported in all releases.

Table C-1   Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	New or Revised Commands for the Release
Cisco IOS Release 12.2(53)SE	
Tailored configuration file automatically created by director.	—
Image list file automatically created by the director when the default image is stored in the director flash memory.	
Support for the **flash:** keyword instead of **tftp://** when the director is the TFTP server for storing the default image and a seed configuration file.	
Cisco IOS Release 12.2(55)SE	
Support for routers as Smart Install directors. See Appendix A.	

Table C-1   Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	New or Revised Commands for the Release
You can configure the Smart Install network for clients to join only if they are on the on-hold list and it is during the configured join window.	**vstack attach**
Support for two backup files per client.	**vstack backup**
When backup is enabled, zero-touch replacement is supported for Smart Install clients (with some restrictions for stack replacement). The replacement configuration file is a seed configuration file with only the basic features.	**vstack backup file-server** **vstack join-window close** **vstack join-window mode**
All image list file generation automatically done by the director.	**vstack on-hold clients install**
Configuration synchronization and directory structure for the director.	**vstack on-hold clients remove**
Configurable file repository for images and configuration in the Smart Install network.	**vstack tar** **vstack untar**
Support for hostname changes on Smart Install clients if none is configured.	**vstack untar/table**
Ability of the director to transparently connect to any Smart Install client.	
You no longer need to specify the director port for zero-touch upgrades of non-Smart Install switches as 4787.	
No need to specify the imaglist name for on-demand downloads. You can use the image name instead, for example, **flash://image.tar**.	
In addition to **tftp/flash/flash1** for image and seed configuration file storage, the **usb** keyword is supported.	
Changes in the output of the **show vstack config** and **show vstack status** privileged EXEC commands.	
Cisco IOS Release 12.2(58)SE, **15.1(1)SY, 15.0(2)SE, 15.1(2)SG, 3.2(0)SE and later, 15.3(3)M, and 15.2(2)E**	
Change the client health state from denied to the allowed or held state for the join window	**vstack join-window-status index** *client-id* {**allowed** | **held**}
Simultaneous on-demand upgrades of multiple clients.	**vstack download-image tar** *image_URL* {*ip_address* | **index** *name*} *remote_switch_password* [**override**] **reload** [**in** *time*] (index name keywords)
Option to remove selected clients from director database.	
Better monitoring with more information in **show vstack status** command output to show client device status, health statue, and upgrade status.	**clear vstack** {**director-db** [**entry** *index-number*]
New predefined homogeneous stack group.	[**no**] **vstack** (global configuration)
Command to disable and re-enable Smart Install on client or director devices.	
Cisco IOS Release 15.0(2)SE and later, 15.1(2)SG, XE 3.4SG, 15.1(1)SY, and 15.3(3)M, and 15.2(2)E	
You can use the **vstack startup-vlan** global configuration command to specify another VLAN that should be used for Smart Install management. Supports non-VLAN1 management and provides the ability to discover the client switches available on non-VLAN1.	**vstack startup-vlan**
Cisco IOS Release 3.6.(0)E and 15.2.(2)E	
vstack script command to identify the default post install file for the clients.	**vstack script**

Table C-1   Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	New or Revised Commands for the Release
Option for post install (script) for **show vstack config**, **show vstack download-status**, **show vstack download-status detail**, **show vstack status**, and **show vstack status detail** commands. **chassis type** option for the **built-in** keyword.	**show vstack**
Added **chassis type** to configure a chassis.	**vstack download-config**
Added the built-in *chassis_config* and *issu* keywords.	**vstack download-image**
Added the *chassis config* keyword.	**vstack group built-in**