

Release Notes for Catalyst 3850 Series Switch, Cisco IOS XE Denali 16.3.x

First Published: August 03, 2016
Last Updated: February 28, 2020

This release note gives an overview of the features for the Cisco IOS XE Denali 16.3.x software on the Cisco Catalyst 3850 Series Switches.

Unless otherwise noted, the terms *switch* and *device* refer to a standalone switch and to a switch stack.

Note - For information about unsupported features, see Important Notes, page 18.
- For information about software and hardware restrictions and limitations, see Limitations and Restrictions, page 69.
- For information about open issues with the software and past opens that are resolved now, see Caveats, page 71.

Introduction

Cisco Catalyst 3850 Series Switches are the next generation of enterprise class stackable access layer switches that provide full convergence between wired and wireless networks on a single platform. This convergence is built on the resilience of new and improved 480-Gbps StackWise-480 and Cisco StackPower. Wired and wireless security and wireless application visibility and control are natively built into the switch.

Cisco Catalyst 3850 Series Switches also support full IEEE 802.3at Power over Ethernet Plus (PoE+), modular and field replaceable network modules, redundant fans, and power supplies. Cisco Catalyst 3850 Series Switches enhance productivity by enabling applications such as IP telephony, wireless, and video for a true borderless network experience.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco IOS XE Denali 16.x.x and Cisco IOS XE represent the continuing evolution of the preeminent Cisco IOS operating system. The Cisco IOS XE architecture and well-defined set of APIs extend the Cisco IOS software to improve portability across platforms and extensibility outside the Cisco IOS environment. The Cisco IOS XE software retains the same look and feel of the Cisco IOS software, while providing enhanced future-proofing and improved functionality.

Whats New in Cisco IOS XE Denali 16.3.11

There are no new software or hardware features and no resolved caveats in Cisco IOS XE Denali 16.3.11.

Whats New in Cisco IOS XE Denali 16.3.10

There are no new software or hardware features and no resolved caveats in Cisco IOS XE Denali 16.3.10.

Whats New in Cisco IOS XE Denali 16.3.9

There are no new software or hardware features in Cisco IOS XE Denali 16.3.9.

For a list of the caveats that have been resolved in this release, see Resolved Caveats in Cisco IOS XE Denali 16.3.9, page 72

Whats New in Cisco IOS XE Denali 16.3.8

There are no new software or hardware features in Cisco IOS XE Denali 16.3.8.

For a list of the caveats that have been resolved in this release, see Resolved Caveats in Cisco IOS XE Denali 16.3.8, page 73

Whats New in Cisco IOS XE Denali 16.3.7

There are no new software or hardware features in Cisco IOS XE Denali 16.3.7.

For a list of the caveats that have been resolved in this release, see Resolved Caveats in Cisco IOS XE Denali 16.3.7, page 73

Whats New in Cisco IOS XE Denali 16.3.6

Software Features in Cisco IOS XE Denali 16.3.6

Feature Name	Description and License Level Information
New in Wired Switching	
Digital Optical Monitoring (DOM)	Enables you to monitor optical input and output power, temperature, and voltage. The feature is supported on all transceivers that support DOM and is disabled by default. See Interface and Hardware Components (LAN Base, IP Base, and IP Services)

For a list of the caveats that have been resolved in this release, see Resolved Caveats in Cisco IOS XE Denali 16.3.6, page 74

Whats New in Cisco IOS XE Denali 16.3.5b

There are no new software or hardware features in Cisco IOS XE Denali 16.3.5b

For a list of the caveats that have been resolved in this release, see Resolved Caveats in Cisco IOS XE Denali 16.3.5b, page 76

Whats New in Cisco IOS XE Denali 16.3.5

Software Features in Cisco IOS XE Denali 16.3.5

Feature Name	Description and License Level Information
New in Wired Switching	
RADIUS over Datagram Transport Layer Security protocol (DTLS)	DTLS provides encryption services over RADIUS, which is transported over a secure tunnel. RADIUS over DTLS is implemented in both client and server. Client side controls radius authentication, authorization, and accounting (AAA) and server side controls Change of Authorization (CoA) (LAN Base, IP Base and IP Services)
New in Wireless Switching	
Application Visibility and Control (AVC) Downstream Quality of Service (QoS)	AP downstream QoS is the process of marking traffic from the controller to the AP. This is achieved by using the flow information from AP on the downstream traffic. (IP Base and IP Services)

Feature Name	Description and License Level Information
XOR Radio Resource Management (RRM)	In Cisco Aironet 2800/3800 series access points, slot 0 is an XOR (Dual-Band) radio that offers the ability to serve either 2.4- or 5-GHz band, or passively monitor both bands on the same radio. (IP Services)
Support is added for these access points	Cisco Aironet 1562 Series Access Points Cisco Aironet 1815 Series Access Points

Whats New in Cisco IOS XE Denali 16.3.3

Hardware Features in Cisco IOS XE Denali 16.3.3

Feature Name	Description
40-Gigabit Ethernet Transceiver Modules (QSFP-40G-ER4=). 40GBASE-ER4, 1310 nm, SMF with OTU3 data-rate support, LC connector	The Cisco Catalyst 3850 Series Switches now support the QSFP-40G-ER4= transceiver module on these switch models: WS-C3850-24XU-L,WS-C3850-24XU-S, WS-C3850-24XU-E, WS-C3850-12X48U-L, WS-C3850-12X48U-S, WS-C3850-12X48U-E WS-C3850-12XS-S, WS-C3850-12XS-E WS-C3850-24XS-S, WS-C3850-24XS-E WS-C3850-48XS-S, WS-C3850-48XS-E, WS-C3850-48XS-F-S, WS-C3850-48XS-F-E
100-Megabit Ethernet SFP Modules (GLC-GE-100FX) 100BASE-FX SFP module for Gigabit Ethernet ports, 1310 nm wavelength, 2 km over MMF	The Cisco Catalyst 3850 Series Switches now support the GLC-GE-100FX SFP transceiver module. The module is supported on downlink ports and 8 X10 Gigabit Ethernet fixed uplink ports, on these switch models: WS-C3850-12XS-S, WS-C3850-12XS-E WS-C3850-16XS-S, WS-C3850-16XS-E WS-C3850-24XS-S, WS-C3850-24XS-E WS-C3850-32XS-S, WS-C3850-32XS-E WS-C3850-48XS-S, WS-C3850-48XS-E WS-C3850-48XS-F-S, WS-C3850-48XS-F-E The module is supported only on uplink ports, on these switch models: WS-C3850-24XU-L,WS-C3850-24XU-S, WS-C3850-24XU-E, WS-C3850-12X48U-L, WS-C3850-12X48U-S, WS-C3850-12X48U-E

Software Features in Cisco IOS XE Denali 16.3.3

Feature Name	Description and License Level Information
New in Wired Switching	
Cisco StackWise Virtual	A network system virtualization technology that pairs two Cisco Catalyst 3850 Series Switches into one virtual switch to simplify operational efficiency with a single control and management plane. **Note** The feature is available only on the WS-C3850-48XS-S, WS-C3850-48XS-E, WS-C3850-48XS-F-S, and WS-C3850-48XS-F-E models of the series. See Configuring Cisco StackWise Virtual and Cisco StackWise Virtual Video. (IP Base and IP Services)
New in Documentation	
Network as an Enforcer (NaaE) feature guide[1].	Describes the role that security group-based access control lists (SGACLs) play in a Cisco TrustSec solution, to enforce role-based access control, identity-aware networking, and data confidentiality—thus securing the network and its resources. See Network as an Enforcer Feature Guide (Catalyst 3850 Switches, Catalyst 3650 Switches).

1. Such end-to-end feature guides complement existing configuration information.

Whats New in Cisco IOS XE Denali 16.3.2

Software Features in Cisco IOS XE Denali 16.3.2

Feature Name	Description and License Level Information
New in Wired Switching	
Audio Video Bridging (AVB): IEEE 802.1BA • Hierarchical QoS • Multi-Gigabit Ethernet (mGig) for AVB	Enhanced to support hierarchical QoS, which provides a two level parent-child policy. With hierarchical QoS, you can specify QoS behavior at multiple policy levels, which provides a high degree of granularity in traffic management. AVB is supported on mGig interfaces on the following switch models: • WS-3850-12X48U • WS-C3850-24XU See Audio Video Bridging. (IP Base and IP Services)

Feature Name	Description and License Level Information
Boot Integrity Visibility	Creates a checksum record for each stage of the boot loading activity. You can retrieve and compare the checksum record with a Cisco-certified record, to verify if your software image is genuine. See Boot Integrity Visibility. (LAN Base, IP Base, and IP Services)
Federal Information Processing Standard Publication 140-2 (FIPS 140-2) and applicable Common Criteria compliance	Cisco IOS XE Denali 16.3.2 on the Cisco Catalyst 3850 Series Switches is being submitted for certification under FIPS 140-2 and Common Criteria compliance with the US Government, Security Requirements for Network Devices. (For Base Configuration—LAN Base, IP Base, and IP Services) (For IP Security—IP Services)
Media Access Control Security (MACSec): 256-bit AES MACsec (IEEE 802.1AE) host link encryption) with MACsec Key Agreement (MKA) 256-bit AES MACsec (IEEE 802.1AE) inter-network device encryption with MKA Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) method support for MKA	MACsec features are now available with IP Base and IP Services license levels. See MACSec Encryption. (IP Base and IP Services)
mGig Visibility Enhancement: Downshift	Available with mGig interfaces. When downshift is enabled, the system automatically downshifts to a lower port speed if the link quality is poor or if the link is continuously down. See Configuring Interface Characteristics. (LAN Base, IP Base, and IP Services)
Multiprotocol Label Switching (MPLS) Multicast VPN (MVPN)	MVPN provides the ability to support multicast over a Layer 3 VPN. As enterprises extend the reach of their multicast applications, service providers can accommodate them over their MPLS core network. IP multicast is used to stream video, voice, and data over an MPLS VPN network core. See Configuring Multicast Virtual Private Network. (IP Services)
Network Automation with Plug and Play (PnP)	Individual device credential support, allowing the controller to manage devices that require individual TACACS or RADIUS credentials for access. The credentials are passed to the device securely and the password is not logged. This feature requires Cisco IOS XE Denali 16.3.2 or a later software release on the device. See Release Notes for Cisco Network Plug and Play, Release 1.3x and Configuring Cisco Network Plug and Play.

Feature Name	Description and License Level Information
Programmability: • Network Bootloader • Embedded Event Manager Launching	Network boot loader—Supports booting from a device based or network-based source. With network boot loaders, you can: • Boot an image located on an HTTP or FTP server. • Support IPv4 networks. • Provide off-box event logging to a syslog server. See Programmability: Network Bootloader. (LAN Base, IP Base, and IP Services)
Wired Application Visibility and Control (Wired AVC) Flexible NetFlow (FNF)	Support for FNF is now enabled for wired AVC. The feature uses a flow record with an application name as the key, to provide statistics per interface, client, server, and application. The record is similar to the Easy Performance Monitor (EzPM) **application-client-server-stats** traffic monitor, which is available in **application-statistics** and **application-performance** profiles. See Configuring Application Visibility and Control. (IP Base and IP Services)

Whats New in Cisco IOS XE Denali 16.3.1

Software Features in Cisco IOS XE Denali 16.3.1

Feature Name	Description and License Level Information
Auto-Upgrade for Operating System (OS) Mismatch	Enables a switch joining an existing stack to be automatically upgraded to the same version as the existing stack, so that the switch can successfully join the existing stack. Previously, Cisco IOS XE Denali 16.x.x releases supported this feature only on switches running an IOS XE Denali 16.x.x image joining an existing stack with a different Cisco IOS XE Denali 16.x.x image version. Starting with this release, the active switch can resolve a mismatch across Cisco IOS XE Release 3.xE and Cisco IOS XE Denali 16.3.x releases. For this activity to happen automatically, you must have enabled the **software auto-upgrade enable** global configuration command, on the active switch. If not, you can start the process manually by entering the **request platform software package install auto upgrade** privileged EXEC command, on the active switch. See Managing Switch Stacks.
In-Place Package Expansion for Software Images	The software image installation process is now optimized: • The space required for installation is reduced—after you have copied the.bin file to flash, only 20MB of additional space is required to complete the installation. • The.bin file is automatically deleted after completion of installation. The installation procedure you have to follow remains the same. See Upgrading the Switch Software, page 34
New in Wired Switching	

Feature Name	Description and License Level Information
Audio Video Bridging (AVB): IEEE 802.1BA	Refers to standard IEEE 802.1 BA - AVB. This feature defines a mechanism whereby endpoints and the network function as a whole to enable high-quality streaming of professional audio and video (AV) over an Ethernet infrastructure. Instead of one-to-one, the network transport enables many-to-many seamless plug-n-play connections for multiple AV endpoints including talkers and listeners. AVB is composed of the following: Generalized Precision Time Protocol (gPTP)—IEEE 802.1AS. Provides a mechanism to synchronize clocks of the bridges and end point devices in an AVB network. Quality of Service (QoS)—IEEE 802.1Qav. Guarantees bandwidth and minimum bounded latency for the time-sensitive audio and video streams. Multiple Stream Reservation Protocol (MSRP)—IEEE 802.1Qat. Provides a mechanism for end stations to reserve network resources that will guarantee the transmission and reception of data streams across a network with the requested bandwidth. Multiple VLAN Registration Protocol (MVRP)—Provides a mechanism for dynamic maintenance of the contents of Dynamic VLAN Registration Entries for each VLAN IDs, and for propagating the information they contain to other Bridges. See Audio Video Bridging. (IP Base and IP Services)
Autonomic Networking Infrastructure	Makes network devices intelligent by introducing self-management concepts that simplify network management. See Configuring Autonomic Networking. (IP Base and IP Services)
Bidirectional Forwarding Detection (BFD)	Provides fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. It also provides a consistent failure detection method for network administrators. See Configuring Bidirectional Forwarding Detection. (IP Services)
Campus Fabric	A virtual topology that can be used to logically connect devices that are a part your physical network, facilitating simple segmentation constructs to build secure boundaries. Fabric Overlay uses alternative forwarding attributes to provide services such as host mobility and enhanced security, which are additional to normal switching and routing capabilities. See Campus Fabric. (IP Base and IP Services)

Feature Name	Description and License Level Information
Cisco TrustSec: Security Group ACL (SGACL) Monitor Mode	Supports the following commands to ensure that SGACL enforcement does not cause any network disruptions in Cisco TrustSec deployments: • **cts role-based monitor** • **cts role-based permissions** • **show cts role-based permissions** See Security Commands. (IP Base and IP Services)
Cisco TrustSec: SGACL Logging	Supports the following commands to troubleshoot Cisco TrustSec deployments: • **cts role-based enforcement** See Security Commands. (IP Base and IP Services)
Cisco TrustSec: Virtual Routing and Forwarding Aware (VRF-Aware) Security Group Tag (SGT)	Enables a device to communicate with RADIUS servers through VRF interfaces. This feature allows protected access credential (PAC) and Environment-Data to be requested from the authentication device, Cisco Identity Services Engine (Cisco ISE), when Cisco ISE is in a VRF network. See VRF-Aware SGT. (IP Services)
Display of free memory on the CLI	Starting with this release, the amount of free memory is computed more accurately. The output of the following commands (privileged EXEC mode) displays this information: • **show memory platform** • **show platform resources** • **show processes memory platform** • **show platform software status control-processor** • **show platform software process list switch active R0 summary** See Interface and Hardware Commands.
Encapsulated Remote Switched Port Analyzer (ERSPAN)	Enables you to monitor traffic on ports or VLANs and to send monitored traffic to destination ports. See Configuring ERSPAN. (IP Base and IP Services)
Federal Information Processing Standard Publication 140-2 (FIPS 140-2) and the Common Criteria for Information Technology Security Evaluation standard (Common Criteria or CC)	Cisco IOS XE Denali 16.3.1on the Cisco Catalyst 3850 Series Switches is being submitted for certification under FIPS 140-2 and Common Criteria compliance with the US Government, Security Requirements for Network Devices..

Feature Name	Description and License Level Information
IPv4 Multicast over Point-to-Point Generic Routing Encapsulation (GRE) Tunnels	Supports IPv4 multicasting over a GRE tunnel. See Configuring Multicast Routing over GRE Tunnels. (IP Base and IP Services)
IPv6 Support for VLAN ACLs (VACLs)	Supports filtering of IPv6 traffic by creating IPv6 VACLs and applying them to interfaces. VACLs access control network traffic by filtering all packets that are bridged within a VLAN in the switch or the switch stack. See Configuring IPv6 ACLs. (IP Base and IP Services)
IPv6 ACL Support for HTTP Servers	Supports the attachment of IPv6 ACLs to configure a secure HTTP server. **Note** The existing CLIs that specify (only IPv4) ACLs are supported, but are going to be deprecated. Use the new CLIs that support both IPv4 and IPv6 ACLs instead. See Configuring Secure Socket Layer HTTP (IP Services)

Feature Name	Description and License Level Information
Media Access Control Security (MACsec): 256-bit AES MACsec (IEEE 802.1AE) host link encryption) with MACsec Key Agreement (MKA) 256-bit AES MACsec (IEEE 802.1AE) inter-network device encryption with MKA Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) method support for MKA	Supports the IEEE 802.1x standard-based Layer 2 encryption with MKA on both uplink (switch-to-switch) and downlink (switch-to-host device) ports for 256-bit level encryption using EAP-TLS and Preshared Key (PSK). Supported on the Cisco Catalyst 3850 Series MultiGigabit Switches and Cisco Catalyst 3850 Series 10G SFP+ Switches. The model numbers are listed below: Cisco Catalyst 3850 Series MultiGigabit Switches – WS-C3850-24XU-L – WS-C3850-24XU-S – WS-C3850-24XU-E – WS-C3850-12X48U-L – WS-C3850-12X48U-S – WS-C3850-12X48U-E Cisco Catalyst 3850 Series 10G SFP+ Switches – WS-C3850-12XS-S – WS-C3850-12XS-E – WS-C3850-16XS-S – WS-C3850-16XS-E – WS-C3850-24XS-S – WS-C3850-24XS-E – WS-C3850-32XS-S – WS-C3850-32XS-E – WS-C3850-48XS-S – WS-C3850-48XS-E – WS-C3850-48XS-F-S – WS-C3850-48XS-F-E See MACSec Encryption. (IP Services)
Multiprotocol Label Switching (MPLS)	Combines the performance and capabilities of Layer 2 (data link layer) switching with the proven scalability of Layer 3 (network layer) routing. MPLS enables service providers to meet the challenges of explosive growth in network utilization while providing the opportunity to differentiate services without sacrificing the existing network infrastructure. See Multiprotocol Label Switching (MPLS) and the end-to-end feature guide to complement configuration information, at Multiprotocol Label Switching Feature Guide. (IP Services)

Feature Name	Description and License Level Information
Network Edge Authentication Topology (NEAT)	Enables extended secure access in areas outside the wiring closet. It allows you to configure a switch to act as a supplicant to another switch. NEAT utilizes the Client Information Signalling Protocol (CISP) to propagate client MAC addresses and VLAN information between supplicant and authenticator switches. See Configuring IEEE 802.1x Port-Based Authentication. (LAN Base, IP Base, and IP Services)
Network-Powered Lighting: Constrained Application Protocol (CoAP)	Enables network-powered lighting capability on a switch. It includes the following components: Two Event Classification for PoE – A physical layer mechanism to rapidly negotiate and grant PoE power to capable end-devices in less than 1sec without traditional Link Layer Discovery Protocol (LLDP) power negotiation. Perpetual-PoE – A mechanism to deliver power to PoE end-devices without interruption during warm reboot (image upgrades, switch reload etc.) Fast PoE – A mechanism to restore power to end-devices within 30s of resumption of power after an outage without waiting for complete control plane boot-up. CoAP Proxy Server – CoAP is a lightweight IoT optimized standard protocol specified in RFC 7252. An On-Switch standards based COAP Proxy Server provides secure messaging, discovery mechanism, local resource directory and RESTful API access for applications. Resources can be organized in a hierarchical manner across the network in a parent/child fashion and accessed by querying the CoAP proxy server. Autosmart Ports - Enhanced to include lighting endpoint specific macros, to be triggered on detecting a lighting endpoint. See Network Powered Lighting. (LAN Base, IP Base, and IP Services)

Feature Name	Description and License Level Information
Next Hop Resolution Protocol (NHRP)	An Address Resolution Protocol (ARP)-like protocol that dynamically maps a nonbroadcast multiaccess (NBMA) network. With NHRP, systems attached to an NBMA network can dynamically learn the NBMA (physical) address of the other systems that are part of that network,allowing these systems to directly communicate. NHRP is a client and server protocol where the hub is the Next Hop Server (NHS) and the spokes are the Next Hop Clients (NHCs). The hub maintains an NHRP database of the public interface addresses of each spoke. Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes to build direct tunnels. See Configuring NHRP. (IP Base and IP Services)
Wired Application Visibility and Control (AVC)	Support for AVC has been enabled on wired ports - for standalone switches, as well as a switch stack. See Configuring Application Visibility and Control. For important limitations related to this feature, see Limitations and Restrictions, page 69. (IP Base and IP Services)
Yet Another Next Generation (YANG) data-modeling language	Support for the YANG data-modeling language, which replaces the process of manual configuration with a programmatic and standards-based way of writing configurations to any network device. It supports the automation of configuration for multiple switches across the network using data models. See Configuring YANG Datamodel. For important limitations related to this feature, see Limitations and Restrictions, page 69. (LAN Base, IP Base, and IP Services)

Feature Name	Description and License Level Information
New in Wireless Switching	
–B Domain Support	The FCC (USA) rule making on 5 GHz released on April 1, 2014 (FCC 14-30 Report and Order) goes into effect for products that are sold or shipped on or after June 2, 2016. Cisco APs and Cisco WLCs will comply with the new rules by supporting the new regulatory domain, –B, for the US and will create new AP SKUs that are certified under the new rules. Examples of new rules include new 5-GHz band channels permitted for indoor and outdoor use, and transmission (Tx) power level increased for indoor, outdoor, and point-to-point transmissions. Cisco APs and Cisco WLCs that are in the –A domain category can continue to operate and even coexist with –B domain devices without any issues. We recommend that you upgrade Cisco APs and Cisco WLCs to the appropriate software release that supports –B domain. –B Domain Compliant Cisco APs starting with Cisco IOS XE Denali 16.2.2 are: 702i, 702w,1532, 1572, 1600, 1700,1810W, 1830, 1850, 2600, 2800, 3600, 3700, 3800.
AP2800 802.11 ac Wave 2 and AP3800 802.11 ac Wave 2: Cisco Multi-Gig (mGig) Enabled Ethernet Ports	Enables the current network to carry a higher bandwidth using mGig enabled Ethernet Ports. Speeds that cap at 1Gbps can now go upto 2.5Gpbs and 5Gbps speeds. These speeds can be achieved on the existing CAT5e and above type of LAN cables. **Note** Flexible Radio Assignment and 160 MH Channel width is not supported. (IP Base and IP Services)
AVC Support on 802.11 ac Wave2 APs	Support for Application Visibility and Control (AVC) on the following Access Points (APs): Cisco Aironet 1810w Series APs Cisco Aironet 1830 Series APs Cisco Aironet 1850 Series APs Cisco Aironet 2800 Series APs Cisco Aironet 3800 Series APs You can now also capture AVC statistics for the last 48 hours. Use the **show platform software fed switch active avc statistics byte-count-window hours 48 raw** privilege EXEC command. (IP Base and IP Services)

Feature Name	Description and License Level Information
Cisco Hyperlocation Module with Integrated Bluetooth Low Energy (BLE) Radio	Enables transmission of BLE broadcast messages by using up to 5 BLE transmitters. The Cisco Wireless Controller (Cisco WLC) is used to configure the transmission parameters such as interval for the beacons, UUID, and transmission power, per beacon globally for all the access points. Also, the Cisco WLC can configure major, minor, and transmission power value of each access point, thus providing more beacon granularity. This feature works in conjunction with Cisco Hyperlocation Radio Module and the Cisco Hyperlocation feature. See Cisco Hyperlocation. (IP Base and IP Services)
Fast Locate with Local Mode	Provides reporting of location performance via data packets RSSI through Local Mode radios through CPU cycle stealing when Cisco Hyperlocation radio module is not installed on an AP. This is available on the following APs: Cisco Aironet 700 Series APs Cisco Aironet 1700 Series APs Cisco Aironet 2600 Series APs Cisco Aironet 2700 Series APs Cisco Aironet 3600 Series APs Cisco Aironet 3700 Series APs You can now configure Cisco Hyperlocation for an AP group. Previously, Cisco Hyperlocation configuration was applicable to all APs globally See Cisco Hyperlocation. (IP Base and IP Services)
Radio Frequency (RF) Profiles on Converged Access	Provide control over the data rates and power (TPC) values. These RF profiles allows you to optimize the RF settings for AP groups which operate in different environments or coverage zones. These profiles can be created for both radio bands - 2.4-GHz and 5-GHz. See Configuring RF Profiles on CA. For information about important limitations related to this feature, see Limitations and Restrictions, page 69. (IP Base and IP Services)

Feature Name	Description and License Level Information
Wall Plate 802.11 ac Wave 2 AP: Remote LAN	Support for Remote-LAN. This feature is similar to Wireless LAN (WLAN). While WLAN is used for wireless connection, Remote-LAN is used for wired ports. Configuring a Remote-LAN profile on the local Gigabit Ethernet ports enables the traffic from wired devices to connect to the WLAN controller. Cisco 1810W T series APs come with three local Gigabit Ethernet ports, one uplink Gigabit Ethernet port and one passive pass-through RJ-45 port. See Configuring Remote-LAN. (IP Base and IP Services)
New on the Web User Interface (Web UI)	
Web UI support for BLE Beacons and RF Profiles, Cisco Hyperlocation FastLocate	Features introduced and updated on the Web UI in this release: • BLE Beacons (IP Base and IP Services) • RF Profiles (IP Base and IP Services) • Cisco Hyperlocation Fast Locate (IP Base and IP Services) • Cisco Application Visibility for Wired Devices • Wired Alerts (LAN Base, IP Base, and IP Services) • Support for access points that have Ethernet ports to which the device can securely connect. (IP Base and IP Services)

Important Notes

- Starting with Cisco IOS XE Denali 16.1.x, a DHCP client that includes option 61 (used by DHCP clients to specify their unique client identifier) in their DHCP discover/offer packet must accept the response message with option 61 from the DHCP server/relay. A client that fails to accept the response message with option 61, is not in compliance with RFC 6842 and requires a firmware upgrade.
- In a Smart Install network when vstack is enabled, system log messages are generated every hour. The running configuration displays whether vstack is enabled or disabled. When running the command **show vstack config**, there are a few output differences compared to the older releases.
- Starting with Cisco IOS XE Denali 16.3.x, Secure Shell (SSH) Version 1 is deprecated. Use SSH Version 2 instead.
- Although visible in the CLI, the following commands are not supported:
  - **collect flow username**
  - **authorize-lsc-ap** (CSCui93659)
- The Cisco Plug-In for OpenFlow (OpenFlow 1.0 and 1.3) feature is available in Cisco IOS XE Release 3.7.3E, and is not supported in Cisco IOS XE Denali 16.3.x:
- The Cisco Discovery Protocol (CDP) Bypass feature is available in Cisco IOS XE Release 3.6.3, but is not supported in Cisco IOS XE Denali 16.3.x:
- The following features are not supported in Cisco IOS XE Denali 16.3.x:
  - 802.1x Configurable username and password for MAB
  - AAA: TACACS over IPv6 Transport
  - Auto QoS for Video endpoints
  - Cisco Group Management Protocol (CGMP)
  - Cisco TrustSec 802.1x
  - Cisco TrustSec Critical Auth
  - Cisco TrustSec for IPv6
  - CNS Config Agent
  - Command Switch Redundancy
  - Device classifier for ASP
  - DHCP snooping ASCII circuit ID
  - DHCPv6 Relay Source Configuration
  - DVMRP Tunneling
  - Dynamic Access Ports
  - EX SFP Support (GLC-EX-SMD)
  - Fallback bridging for non-IP traffic
  - Fast SSID support for guest access WLANs
  - IEEE 802.1X-2010 with 802.1AE support
  - Improvements in QoS policing rates
  - Ingress Strict Priority Queuing (Expedite)

- Ingress/egress Shared Queues
- IP-in-IP (IPIP) Tunneling
- IPsec with FIPS
- IPSLA Media Operation
- IPv6 IKEv2 / IPSecv3
- IPv6 Ready Logo phase II - Host
- IPv6 Static Route support on LAN Base images
- IPv6 Strict Host Mode Support
- Layer 2 Tunneling Protocol Enhancements
- Link-State Tracking
- Mesh, FlexConnect, and OfficeExtend access point deployment
- Medianet
- MSE 8.x is not supported with Cisco IOS XE Denali 16.x.x.
- Packet Based Storm Control
- Passive Monitoring
- Per VLAN Policy & Per Port Policer
- Performance Monitor (Phase 1)
- Port Security on EtherChannel
- Pragmatic General Multicast (PGM)
- Protocol Storm Protection
- RFC 4292 IP-FORWARD-MIB (IPv6 only)
- RFC 4293 IP-MIB (IPv6 only)
- RFC4292/RFC4293 MIBs for IPv6 traffic
- RFC5460 DHCPv6 Bulk Leasequery
- Trust Boundary Configuration
- UniDirectional Link Routing (UDLR)
- VACL Logging of access denied
- Weighted Random Early Detect (WRED)
- Wireless Guest Anchor Controller (Cisco Catalyst 3850 Series Switches can be configured as a foreign controller.)
- WIPs is not supported with Cisco IOS XE Denali 16.x.x since the CMX WIPs solution is not available

Supported Hardware

Catalyst 3850 Switch Models

Table 1 Catalyst 3850 Switch Models

Switch Model	Cisco IOS Image	Description
WS-C3850-24T-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48T-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-24P-L	LAN Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48P-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-48F-L	LAN Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, LAN Base feature set (StackPower cables must be purchased separately)
WS-C3850-24U-L	LAN Base	Stackable 24 10/100/1000 Cisco UPOE3 ports, 1 network module slot, 1100 W power supply
WS-C3850-48U-L	LAN Base	Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-12X48U-L	LAN Base	Stackable 12 100M/1G/2.5G/5G/10G and 36 1G UPoE ports, 1 network module slot, 1100 W power supply
WS-C3850-24XU-L	LAN Base	Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100 W AC power supply 1RU
WS-C3850-24T-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set
WS-C3850-48T-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Base feature set
WS-C3850-24P-S	IP Base	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set

Table 1 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-48P-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Base feature set
WS-C3850-48F-S	IP Base	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply, 1 RU.
WS-C3850-24U-S	IP Base	Stackable 24 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-48U-S	IP Base	Stackable 48 10/100/1000 Cisco UPOE ports, 1 network module slot, 1100 W power supply
WS-C3850-48W-S	IP Base	Cisco Catalyst 3850 48-port PoE IP Base with 5-access point license
WS-C3850-24PW-S	IP Base	Cisco Catalyst 3850 24-port PoE IP Base with 5-access point license
WS-C3850-48PW-S	IP Base	Cisco Catalyst 3850 48-port PoE IP Base with 5-access point license
WS-C3850-24UW-S	IP Base	Cisco Catalyst 3850 24-port UPOE IP Base with 5-access point license
WS-C3850-48UW-S	IP Base	Cisco Catalyst 3850 48-port UPOE IP Base with 5-access point license
WS-C3850-12S-S	IP Base	12 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-S	IP Base	24 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-12XS-S	IP Base	Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply
WS-C3850-16XS-S	IP Base	Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply. 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-S switch.
WS-C3850-24XS-S	IP Base	Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply.
WS-C3850-32XS-S	IP Base	Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply. 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-S switch.

Table 1 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-48XS-S	IP Base	Standalone Cisco Catalyst 3850 Switch, that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750WAC front-to-back power supply. 1 RU.
WS-C3850-48XS-F-S	IP Base	Standalone Cisco Catalyst 3850 Switch that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750WAC back-to-front power supply. 1 RU.
WS-C3850-12X48U-S	IP Base	Stackable 12 100M/1G/2.5G/5G/10G and 36 1 G UPoE ports, 1 network module slot, 1100 W power supply
WS-C3850-12X48UW-S	IP Base	Stackable 12 100M/1G/2.5G/5G/10G and 36 1 G UPoE ports, 1 network module slot, 1100 W power supply
WS-C3850-24XU-S	IP Base	Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100 W AC power supply 1RU
WS-C3850-24XUW-S	IP Base	Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100-W power supply
WS-C3850-24T-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set
WS-C3850-48T-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet ports, with 350-WAC power supply 1 RU, IP Services feature set
WS-C3850-24P-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set
WS-C3850-48P-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 715-WAC power supply 1 RU, IP Services feature set
WS-C3850-48F-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Ethernet PoE+ ports, with 1100-WAC power supply 1 RU, IP Services feature set
WS-C3850-24U-E	IP Services	Cisco Catalyst 3850 Stackable 24 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply
WS-C3850-48U-E	IP Services	Cisco Catalyst 3850 Stackable 48 10/100/1000 Cisco UPOE ports,1 network module slot, 1100-W power supply
WS-C3850-12S-E	IP Services	12 SFP module slots, 1 network module slot, 350-W power supply
WS-C3850-24S-E	IP Services	24 SFP module slots, 1 network module slot, 350-W power supply

Table 1 Catalyst 3850 Switch Models (continued)

Switch Model	Cisco IOS Image	Description
WS-C3850-12XS-E	IP Services	Catalyst 3850 12-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 -W power supply
WS-C3850-16XS-E	IP Services	Catalyst 3850 16-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 350 W power supply 16 ports are available when the C3850-NM-4-10G network module is plugged into the WS-C3850-12XS-E switch.
WS-C3850-24XS-E	IP Services	Catalyst 3850 24-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply
WS-C3850-32XS-E	IP Services	Catalyst 3850 32-port SFP+ transceiver, 1 network module slot, support for up to 10 G SFP+, 715 W power supply 32 ports are available when the C3850-NM-8-10G network module is plugged into the WS-C3850-24XS-E switch
WS-C3850-12X48U-E	IP Services	Stackable 12 100M/1G/2.5G/5G/10G and 36 1 G UPoE ports, 1 network module slot, 1100 W power supply
WS-C3850-24XU-E	IP Services	Stackable 24 100M/1G/2.5G/5G/10G UPoE ports, 1 network module slot, 1100 W AC power supply 1RU
WS-C3850-48XS-E	IP Services	Standalone Cisco Catalyst 3850 Switch that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750 WAC front-to-back power supply. 1 RU.
WS-C3850-48XS-F-E	IP Services	Standalone Cisco Catalyst 3850 Switch that supports SFP+ transceivers, 48 ports that support up to 10G, and 4 QSFP ports that support up to 40G, and 750WAC back-to-front power supply. 1 RU.

Network Modules

Table 2 lists the three optional uplink network modules with 1-Gigabit and 10-Gigabit slots. You should only operate the switch with either a network module or a blank module installed.

Table 2 Supported Network Modules

Network Module	Description
C3850-NM-4-1G	This module has four 1 G SFP module slots. Any combination of standard SFP modules are supported. SFP+ modules are not supported. If you insert an SFP+ module in the 1G network module, the SFP+ module does not operate, and the switch logs an error message. **Note** This is supported on the following switch models: – WS-C3850-24T/P/U – WS-C3850-48T/F/P/U – WS-C3850-12X48U – WS-C3850-24XU – WS-C3850-12S – WS-C3850-24S
C3850-NM-2-10G	This module has four slots: Two slots (left side) support only 1 G SFP modules and two slots (right side) support either 1 G SFP or 10 G SFP modules. **Note** This is supported on the following switch models: – WS-C3850-24T/P/U – WS-C3850-48T/F/P/U – WS-C3850-12X48U – WS-C3850-24XU – WS-C3850-12S – WS-C3850-24S
C3850-NM-4-10G	This module has four 10 G slots or four 1 G slots. **Note** This is supported on the following switch models: – WS-C3850-48T/F/P/U – WS-C3850-12X48U – WS-C3850-24XU – WS-C3850-12XS – WS-C3850-24XS

Table 2 Supported Network Modules (continued)

Network Module	Description
C3850-NM-8-10G	This module has eight 10 G slots with an SFP+ port in each slot. Each port supports a 1 G or 10 G connection **Note** This is supported on the following switch models: – WS-C3850-12X48U – WS-C3850-24XU – WS-C3850-24XS
C3850-NM-2-40G	This module has two 40 G slots with a QSFP+ connector in each slot. **Note** This is supported on the following switch models: – WS-C3850-12X48U – WS-C3850-24XU – WS-C3850-24XS

Optics Modules

Catalyst switches support a wide range of optics. Because the list of supported optics is updated on a regular basis, consult the tables at this URL for the latest (SFP) compatibility information:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Access Points and Connected Mobile Experiences (CMX)

Table 3 lists the supported products of the Catalyst 3850 Switch.

Note Telnet is not supported on Cisco 1800 Series APs

Table 3 Catalyst 3850 Switch Supported Products

Product	Platform Supported
Access Point	Cisco Aironet 700, 700W, 1040, 1140, 1260, 1562,1530, 1570, 1600, 1700, 1810W, 1815i, 1830, 1850, 2600, 2700, 2800, 3500, 3600, 3700, 3800
Mobility Services Engine	3365, Virtual Appliance

Table 4 lists the specific supported Cisco access points.

Table 4 Supported Access Points

Access Points	
Cisco Aironet 700 Series	AIR-CAP702I-x-K9
Cisco Aironet 700W Series	AIR-CAP702Wx-K9
Cisco Aironet 1140 Series	AIR-AP1141N
	AIR-AP1142N
	AIR-LAP1141N
	AIR-LAP1142N
Cisco Aironet 1260 Series	AIR-LAP1261N
	AIR-LAP1262N
	AIR-AP1261N
	AIR-AP1262N
Cisco Aironet 1530 Series	AIR-CAP1532I-x-K9
	AIR-CAP1532E-x-K9
Cisco Aironet 1562 Series	AIR-AP1562E-x-K9
Cisco Aironet 1570 Series	AIR-AP1572EAC-A-K9
	AIR-AP1572ECx-A-K9
	AIR-AP1572ICx-A-K9
Cisco Aironet 1600 Series	AIR-CAP1602E
	AIR-CAP1602I
Cisco Aironet 1700 Series	AIR-CAP1702I-x-K9
Cisco Aironet 1810W Series	AIR-AP1810w-x-K9
Cisco Aironet 1815i Series	AIR-AP1815i-x-K9
	AIR-AP1815i-x-K9C
Cisco Aironet 1830 Series	AIR-AP1832I-UXK9
	AIR-AP1832I-UXK9C
	AIR-AP1832I-x-K9
	AIR-AP1832I-x-K9C
Cisco Aironet 1850 Series	AIR-AP1852I-UXK9
	AIR-AP1852I-UXK9C
	AIR-AP1852E-UXK9
	AIR-AP1852E-UXK9C
	AIR-AP1852E-x-K9
	AIR-AP1852E-x-K9C
	AIR-AP1852I-x-K9
	AIR-AP1852I-x-K9C
Cisco Aironet 2600 Series	AIR-CAP2602E
	AIR-CAP2602I

Table 4 Supported Access Points (continued)

Access Points	
Cisco Aironet 2700 Series	AIR-CAP2702I-x-K9
	AIR-CAP2702E-x-K9
Cisco Aironet 2800 Series	AIR-AP2802I-x-K9
	AIR-AP2802E-x-K9
Cisco Aironet 3500 Series	AIR-CAP3501E
	AIR-CAP3501I
	AIR-CAP3501P
	AIR-CAP3502E
	AIR-CAP3502I
	AIR-CAP3502P
Cisco Aironet 3600 Series Modules Supported: • AIR-RM3000AC-x-K9= • AIR-RM3000M= • AIR-RM3010L-x-K9= with AIR-ANT-LOC-01=	AIR-CAP3602E
	AIR-CAP3602I
Cisco Aironet 3700 Series Modules supported: • AIR-RM3000M= • AIR-RM3010L-x-K9= with AIR-ANT-LOC-01=	AIR-CAP3702I
	AIR-CAP3702E
	AIR-CAP3702P
Cisco Aironet 3800 Series	AIR-AP3802I-x-K9
	AIR-AP3802E-x-K9

Compatibility Matrix

Table 5 Software Compatibility Matrix

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 WLC or WiSM2 with Guest Anchor Controller support	Cisco 5508 WLC or WiSM2 with Mobility Controller support	MSE/CMX	ISE	ACS	Cisco PI
Denali 16.3.8	03.07.04E 03.06.09E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.2 Patch 2 (wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack. See Prime Infrastructure 3.1 on cisco.com PI update PI 3.1 + PI 3.1 latest maintenance release 3.1.7[1] +PI 3.1 latest device pack 16[1] (Wireless). See Prime Infrastructure 3.1 on cisco.com
Denali 16.3.8	03.07.04E 03.06.09E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.2 Patch 2 (wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1 latest maintenance release + PI 3.1 latest device pack. See Prime Infrastructure 3.1 on cisco.com PI update PI 3.1 + PI 3.1 latest maintenance release 3.1.7[1] +PI 3.1 latest device pack 16[1] (Wireless). See Prime Infrastructure 3.1 on cisco.com

Table 5 Software Compatibility Matrix

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 WLC or WiSM2 with Guest Anchor Controller support	Cisco 5508 WLC or WiSM2 with Mobility Controller support	MSE/CMX	ISE	ACS	Cisco PI
Denali 16.3.7	03.07.04E 03.06.05E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.2 Patch 2 (wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1 latest maintenance release 3.1.7[1] +PI 3.1 latest device pack 16[1] (Wired). See Prime Infrastructure 3.1 on cisco.com PI update PI 3.1 + PI 3.1 latest maintenance release 3.1.7[1] +PI 3.1 latest device pack 16[1] (Wireless). See Prime Infrastructure 3.1 on cisco.com
Denali 16.3.6	03.07.04E 03.06.05E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.2 Patch 2 (wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1 latest maintenance release 3.1.7[1] + PI 3.1 latest device pack 16[1] (Wired). See Prime Infrastructure 3.1 on cisco.com PI update PI 3.1 + PI 3.1 latest maintenance release 3.1.7[1] + PI 3.1 latest device pack 14[1] (Wireless). See Prime Infrastructure 3.1 on cisco.com
Denali 16.3.5b	03.07.04E 03.06.05E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.2 Patch 2 (wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1.5[2] + PI 3.1.5 update 1[1]+ PI 3.1 latest device pack[1] (Wired) See Prime Infrastructure 3.1 on cisco.com PI 3.1 + PI 3.1 maintenance release 7[1]+ PI 3.1 latest device pack[1] (Wireless) See Prime Infrastructure 3.1 on cisco.com

Table 5 Software Compatibility Matrix

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 WLC or WiSM2 with Guest Anchor Controller support	Cisco 5508 WLC or WiSM2 with Mobility Controller support	MSE/CMX	ISE	ACS	Cisco PI
Denali 16.3.5	03.07.04E 03.06.05E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.2 Patch 2 (wired and wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1.5[2] + PI 3.1.5 update 1 + PI 3.1 latest device pack[1] (Wired) See Prime Infrastructure 3.1 on cisco.com PI 3.1 + PI 3.1 maintenance release 7+ PI 3.1 latest device pack[1] (Wireless) See Prime Infrastructure 3.1 on cisco.com
Denali 16.3.3	03.07.04E 03.06.05E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.1 Patch 1 (Wired and Wireless)	5.4 5.5	PI update PI 3.1 + PI 3.1.5[2] + PI 3.1.5 update 1 + PI 3.1 latest device pack[1] (Wired) See Prime Infrastructure 3.1 on cisco.com PI 3.1 + PI 3.1 latest maintenance release[1] + PI 3.1 latest device pack[1] (Wireless) See Prime Infrastructure 3.1 on cisco.com
Denali 16.3.2	03.07.04E 03.06.05E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.1 Patch 1 (Wired and Wireless)	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release[1] + PI 3.1 latest device pack[1] (Wired and Wireless). See Prime Infrastructure 3.1 on cisco.com.
Denali 16.3.1	03.07.04E 03.06.05E	8.2.0, 8.3.0	Not Supported	CMX 10.2.2	2.0 Patch 3 1.4 Patch 7 1.3 Patch 6 (Wired and Wireless)	5.4 5.5	PI 3.1 + PI 3.1 latest maintenance release[1] + PI 3.1 latest device pack[1] (Wired and Wireless). See Prime Infrastructure 3.1 on cisco.com.

Table 5 Software Compatibility Matrix

Catalyst 3850	Cisco 5700 WLC	Cisco 5508 WLC or WiSM2 with Guest Anchor Controller support	Cisco 5508 WLC or WiSM2 with Mobility Controller support	MSE/CMX	ISE	ACS	Cisco PI
Denali 16.2.2	03.07.03E 03.06.03E[3]	8.1.0, 8.2.0	Not Supported	CMX 10.2.2	1.3 Patch 5 (Wired and Wireless)	5.3 5.4	3.1.0 + Device Pack 1 (Wired and Wireless)
Denali 16.2.1	03.07.03E 03.06.03E[3]	8.1.0, 8.2.0	Not Supported	CMX 10.2.2	1.3 Patch 5 (Wired and Wireless)	5.3 5.4	3.1.0 (Wired) 3.1.0, 3.0.2[4] + Device Pack 4 + PI 3.0 Technology Pack (Wireless)
Denali 16.1.3	03.07.02E 03.06.03E[3]	8.1.0	Not Supported	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + Device Pack 5+ PI 3.0 Technology Pack
Denali 16.1.2	03.07.02E 03.06.03E[3]	8.1.0	Not Supported	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + Device Pack 4 + PI 3.0 Technology Pack
Denali 16.1.1	03.07.02E 03.06.03E[3]	8.1.0	Not Supported	CMX 10.2.0	1.3 Patch 3 (Wired) 1.4 (Wireless)	5.3 5.4	3.0.2 + PI 3.0 Device Pack 2 + PI 3.0 Technology Pack
03.07.03E 03.07.02E 03.07.01E 03.07.00E	03.07.03E 03.07.02E 03.07.01E 03.07.00E	8.0 8.0 8.0 7.6		8.0 8.0[5]	1.3 1.3	5.2 5.2 5.3	2.2
03.06.04E 03.06.03E 03.06.02aE 03.06.01E 03.06.00E	03.06.04E 03.06.02aE 03.06.01E 03.06.00E	8.0 8.0 7.6		8.0 8.0	1.3 1.2	5.2 5.2 5.3	2.2 2.2, 2.1.2, or 2.1.1 if MSE is also deployed[6] 2.1.0 if MSE is not deployed
03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	03.03.03SE 03.03.02SE 03.03.01SE 03.03.00SE	7.6[7] 7.5[8]		7.6 7.5	1.2	5.2 5.3	2.0

1. For maintenance release patches, go to Prime Infrastructure Software. For the latest device pack, go to Prime Infrastructure Device Pack.
2. For patches, go to Prime Infrastructure Patches.
3. Cisco 5700 (with Cisco IOS XE Release 03.06.03E/Cisco IOS XE Release 03.07.02E) inter-operates as a Peer MC with Catalyst 3850 running Cisco IOS XE Denali 16.1.1.
4. The Cisco IOS XE Denali 16.2.1 features are not available with 3.0.2, but 3.0.2 is compatible with Cisco IOS XE Denali 16.2.1.
5. Because of SHA-2 certificate implementation, MSE 7.6 is not compatible with Cisco IOS XE Release 3.6E and later. Therefore, we recommend that you upgrade to MSE 8.0.

6. If MSE is deployed on your network, we recommend that you upgrade to Cisco Prime Infrastructure 2.1.2.
7. Cisco WLC Release 7.6 is not compatible with Cisco Prime Infrastructure 2.0.
8. Prime Infrastructure 2.0 enables you to manage Cisco WLC 7.5.102.0 with the features of Cisco WLC 7.4.110.0 and earlier releases. Prime Infrastructure 2.0 does not support any features of Cisco WLC 7.5.102.0 including the new AP platforms.

For more information on the compatibility of wireless software components across releases, see the *Cisco Wireless Solutions*

Web UI System Requirements

Hardware Requirements

Table 6 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software Requirements

- Operating Systems
  - Windows 10
  - Mac OS X 10.9.5
- Browsers
  - Google Chrome—Version 38 and later (On Windows)
  - Microsoft Internet Explorer—Versions 10 and later (On Windows)
  - Mozilla Firefox—Version 33 and later (On Windows and Mac)
  - Safari—Version 10 and later (On Mac)

Finding the Software Version and Feature Set

Table 7 shows the mapping of the Cisco IOS XE version number and the Cisco IOS version number.

Table 7 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
Denali 16.3.9	Not applicable	Denali 16.3.9	15.3(3)JPC11
Denali 16.3.8	Not applicable	Denali 16.3.8	15.3(3)JPC10
Denali 16.3.7	Not applicable	Denali 16.3.7	15.3(3)JPC9
Denali 16.3.6	Not applicable	Denali 16.3.6	15.3(3)JPC7

Table 7 Cisco IOS XE to Cisco IOS Version Number Mapping

Cisco IOS XE Version	Cisco IOSd Version	Cisco Wireless Control Module Version	Access Point Version
Denali 16.3.5b	Not applicable	Denali 16.3.5b	15.3(3)JPC6
Denal 16.3.5	Not applicable	Denali 16.3.5	15.3(3)JPC5
Denali 16.3.3	Not applicable	Denali 16.3.3	15.3(3)JPC3
Denali 16.3.2	Not applicable	Denali 16.3.2	15.3(3)JPC2
Denali 16.3.1	Not applicable	Denali 16.3.1	15.3(3)JPC
Denali 16.2.2	Not applicable	Denali 16.2.2	15.3(3)JPB1
Denali 16.2.1	Not applicable	Denali 16.2.1	15.3(3)JPB
Denali 16.1.3	Not applicable	Denali 16.1.3	15.3(3)JNP2
Denali 16.1.2	Not applicable	Denali 16.1.2	15.3(3)JNP1
Denali 16.1.1	Not applicable	Denali 16.1.1	15.3(3)JNP
03.07.03E	15.2(3)E3	10.3.130.0	15.3(3)JNB3
03.07.02E	15.2(3)E2	10.3.100.0	15.3(3)JNB1
03.07.01E	15.2(3)E1	10.3.100.0	15.3(3)JNB1
03.07.00E	15.2(3)E	10.3.100.0	15.3(3)JNB
03.06.04E	15.2(2)E4	10.2.140.0	15.3(3)JN8
03.06.03E	15.2(2)E3	10.2.131.0	15.3(3)JN7
03.06.02aE	15.2(2)E2	10.2.120.0	15.3(3)JN4
03.06.01E	15.2(2)E1	10.2.111.0	15.3(3)JN3
03.06.00E	15.2(2)E	10.2.102.0	15.3(3)JN
03.03.05SE	15.0(1)EZ5	10.1.150.0	15.2(4)JB7
03.03.04SE	15.0(1)EZ4	10.1.140.0	15.2(4)JB6
03.03.03SE	15.0(1)EZ3	10.1.130.0	15.2(4)JB5h
03.03.02SE	15.0(1)EZ2	10.1.121.0	15.2(4)JB5
03.03.01SE	15.0(1)EZ1	10.1.110.0	15.2(4)JB2
03.03.00SE	15.0(1)EZ	10.1.100.0	15.2(4)JN

The package files for the Cisco IOS XE software are stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.



Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Upgrading the Switch Software

This section covers the following scenarios:

- Automatic Boot Loader Upgrade
- Automatic Microcode Upgrade
- Upgrading from Cisco IOS XE 3.xE to Cisco IOS XE Denali 16.1.x, 16.2.x, or 16.3.x in Install Mode
- Upgrading from Cisco IOS XE 3.xE to Cisco IOS XE Denali 16.1.x, 16.2.x, or 16.3.x in Bundle Mode
- Upgrading from Cisco IOS XE Denali 16.1.1 to 16.1.x, 16.2.x, or 16.3.x in Install Mode
- Upgrading from Cisco IOS XE Denali 16.3.x to Cisco IOS XE 16.x in Install Mode
- Downgrade from Cisco IOS XE 16.x to Cisco IOS XE 3.xE in Install Mode
- Downgrade from Cisco IOS XE 16.x to Cisco IOS XE 3.xE in Bundle Mode
- WCM Sub Package Software Image Upgrade

Note You cannot use the Web UI to install, upgrade to, or downgrade from Cisco IOS XE Denali 16.1.x, 16.2.x or 16.3.x.

Table 8 Software Images

Release	Image	File Name
Cisco IOS XE Denali 16.3.9	Universal	cat3k_caa-universalk9.16.03.09.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.09.SPA.bin
Cisco IOS XE Denali 16.3.8	Universal	cat3k_caa-universalk9.16.03.08.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.08.SPA.bin
Cisco IOS XE Denali 16.3.7	Universal	cat3k_caa-universalk9.16.03.07.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.07.SPA.bin
Cisco IOS XE Denali 16.3.6	Universal	cat3k_caa-universalk9.16.03.06.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.06.SPA.bin
Cisco IOS XE Denali 16.3.5b	Universal	cat3k_caa-universalk9.16.03.05b.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.05b.SPA.bin
Cisco IOS XE Denali 16.3.5	Universal	cat3k_caa-universalk9.16.03.05.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.05.SPA.bin
Cisco IOS XE Denali 16.3.3	Universal	cat3k_caa-universalk9.16.03.03.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.03.SPA.bin
Cisco IOS XE Denali 16.3.2	Universal	cat3k_caa-universalk9.16.03.02.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.02.SPA.bin
Cisco IOS XE Denali 16.3.1a	Universal	cat3k_caa-universalk9.16.03.01a.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.01a.SPA.bin

Release	Image	File Name
Cisco IOS XE Denali 16.3.1	Universal	cat3k_caa-universalk9.16.03.01.SPA.bin
	Universal without DTLS	cat3k_caa-universalk9ldpe.16.03.01.SPA.bin

Table 9 Changes in Software Installation CLI Commands

Cisco IOS XE 3.xE	
`Switch#software ?`	
`auto-upgrade`	Initiate auto upgrade for switches running incompatible software
`clean`	Clean unused package files from local media
`commit`	Commit the provisioned software and cancel the automatic rollback timer
`expand`	Expand a software bundle to local storage, default location is where the bundle currently resides
`install`	Install software
`rollback`	Rollback the committed software
Cisco IOS XE Denali 16.x Commands	
`Switch#request platform software package ?`	
`clean`	Clean unnecessary package files from media
`copy`	Copy package to media
`describe`	Describe package content
`expand`	Expand all-in-one package to media
`install`	Package installation
`uninstall`	Package uninstall
`verify`	Verify ISSU software package compatibility

Automatic Boot Loader Upgrade

When you upgrade from any prior IOS 3.xE release to an IOS XE 16.x.x release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload. If you go back to an IOS 3.xE release, your boot loader will not be downgraded. The updated boot loader supports all previous IOS 3.xE releases.

For subsequent IOS XE 16.x.x releases, if there is a new bootloader in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.

Caution Do not power cycle your switch during the upgrade.

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Denali 16.3.5 or Cisco IOS XE Denali 16.3.5b or Cisco IOS XE Denali 16.3.6 or Cisco IOS XE Denali 16.3.7 or Cisco IOS XE Denali 16.3.7 or Cisco IOS XE Denali 16.3.8 or Cisco IOS XE Denali 16.3.9 for the first time	The boot loader may be upgraded to version 4.68. For example:
	`BOOTLDR:CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.68, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Denali 16.3.5, you will see the following on the console:
	`%IOSXEBOOT-Wed-###: (rp/0): Sep 27 20:53:16 Universal 2017 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

If you boot Cisco IOS XE Denali 16.3.3 the first time	The boot loader may be upgraded to version 4.38. For example:
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.38, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Denali 16.3.3, you will see the following on the console:
	`%IOSXEBOOT-Wed-###: (rp/0): Nov 2 20:46:19 Universal 2016 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

If you boot Cisco IOS XE Denali 16.3.2 the first time	The boot loader may be upgraded to version 4.28. For example:
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.28, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Denali 16.3.2, you will see the following on the console:
	`%IOSXEBOOT-Wed-###: (rp/0): Nov 2 20:46:19 Universal 2016 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

If you boot Cisco IOS XE Denali 16.3.1 the first time	The boot loader may be upgraded to version 3.78. For example:
	`CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 3.78, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Denali 16.3.1, you will see the following on the console:
	`%IOSXEBOOT-Mon-###: (rp/0): Jul 25 16:22:25 Universal 2016 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

Scenario	Automatic Boot Loader Response

If you boot Cisco IOS XE Denali 16.2.x the first time	The boot loader may be upgraded to version 3.58. For example:
	`switch: ver`
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 3.58, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade, while booting Cisco IOS XE Denali 16.2.1, you will see the following on the console:
	`%IOSXEBOOT-Thu-###: (rp/0): Mar 24 18:18:10 Universal 2016 PLEASE DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-loader-boot: (rp/0): upgrade successful`

If you boot Cisco IOS XE Denali 16.1.x the first time	The boot loader may be upgraded to version 3.2. For example:
	`BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 3.2, RELEASE SOFTWARE (P)`
	During the automatic boot loader upgrade while booting Cisco IOS XE Denali 16.1.x, you will see the following on the console:
	`%IOSXEBOOT-PLEASE-###: (rp/0): DO NOT POWER CYCLE ### BOOT LOADER UPGRADING`
	`%IOSXEBOOT-Nov-Tue: (rp/0): 24 11:04:42 Universal 2015 boot loader upgrade successful`

Automatic Microcode Upgrade

During an IOS image upgrade or downgrade on a PoE or UPoE switch, the microcode is updated to reflect applicable feature enhancements and bug fixes. Do not restart the switch during the upgrade or downgrade process. With the Cisco IOS XE Denali 16.x.x release, it takes approximately an additional 4 minutes to complete the microcode upgrade in addition to the normal reload time. The microcode update occurs only during an image upgrade or downgrade on PoE or UPoE switches. It does not occur during switch reloads or on non-PoE switches.

The following console messages are displayed during microcode upgrade:

```
Front-end Microcode IMG MGR: found 4 microcode images for 1 device.
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_0
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_1
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_2
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_3

Front-end Microcode IMG MGR: Preparing to program device microcode...
Front-end Microcode IMG MGR: Preparing to program device[0]...594412 bytes....
Skipped[0].
Front-end Microcode IMG MGR: Preparing to program device[0]...381758 bytes.
Front-end Microcode IMG MGR: Programming device
0...rwRrrrrrrw..0%.....................................................................
.
..10%.....................................................................20%........
.
.....................................................................30%.....................
.................................................40%.................................
.....................................50%.............................................
.........................60%.......................................................
............70%.
.....................................................................80%...........
```

```
.............................................................90%.....................
.............................................100%
Front-end Microcode IMG MGR: Preparing to program device[0]...25166 bytes.
Front-end Microcode IMG MGR: Programming device
0...rrrrrrw..0%....10%....20%......30%...40%......50%....60%......70%...80%......90%..
..100%
Front-end Microcode IMG MGR: Microcode programming complete for device 0.
Front-end Microcode IMG MGR: Preparing to program device[0]...86370 bytes....
Skipped[3].
Front-end Microcode IMG MGR: Microcode programming complete in 237 seconds
```

Upgrading from Cisco IOS XE 3.xE to Cisco IOS XE Denali 16.1.x, 16.2.x, or 16.3.x in Install Mode

Follow these instructions to upgrade from Cisco IOS XE 3.xE to Cisco IOS XE Denali 16.1.x, 16.2.x, or 16.3.x in Install Mode:

Copy New Image to Stack

When you expand the image, if you point to the source image on your TFTP server, you can skip this section and go to Software Install Image to Flash, page 39.

Step 1 Make sure your tftp server is reachable from IOS via GigabitEthernet0/0.

```
Switch# show run | i tftp
ip tftp source-interface GigabitEthernet0/0
ip tftp blocksize 8192
Switch#
Switch# show run | i ip route vrf
ip route vrf Mgmt-vrf 5.0.0.0 255.0.0.0 5.30.0.1
Switch#
Switch# show run int GigabitEthernet0/0
Building configuration...

Current configuration : 115 bytes
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 ip address 5.30.12.121 255.255.0.0
 negotiation auto
end
Switch#
Switch# ping vrf Mgmt-vrf ip 5.28.11.250
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.28.11.250, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Step 2 Copy the image from your tftp server to flash.

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.16.03.05.SPA.bin flash:
Destination filename [cat3k_caa-universalk9.16.03.05.SPA.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.16.03.05.SPA.bin...
Loading cat3k_caa-universalk9.16.03.05.SPA.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!
!!!!!!!!!!!!!!!
[OK - 489159804 bytes]
```

```
489159804 bytes copied in 143.802 secs (3401620 bytes/sec)
Switch#
```

Step 3 Use the **dir flash** command to confirm that the image has been successfully copied to flash.

```
Switch#dir flash:*.bin
Directory of flash:/*.bin

   14  -rw-   489159804  Aug 1 2016 20:50:59 +00:00
cat3k_caa-universalk9.16.03.05.SPA.bin

1621966848 bytes total (827838464 bytes free)
Switch#
```

Software Install Image to Flash

Step 4 Use the **software install** command with the 'new' and 'force' options to expand the target image to flash. You can point to the source image on your TFTP server or in flash if you have it copied to flash.

Note When you upgrade to Cisco IOS XE Denali 16.3.5 the SSH access is lost, because it cannot use the CISCO_IDEVID_SUDI_LEGACY RSA server key. Before upgrade, generate the server key using the **crypto key generate rsa** command in global configuration mode.
To verify whether the RSA server key is available on your device, run the **show crypto key** command.

```
Switch# software install file flash:cat3k_caa-universalk9.16.03.05.SPA.bin new force
Preparing install operation ...
[1]: Copying software from active switch 1 to switches 2,3,4
[1]: Finished copying software to switches 2,3,4
[1 2 3 4]: Starting install operation
[1 2 3 4]: Expanding bundle flash:cat3k_caa-universalk9.16.03.05.SPA.bin
[1 2 3 4]: Copying package files
[1 2 3 4]: Package files copied
[1 2 3 4]: Finished expanding bundle flash:cat3k_caa-universalk9.16.03.05.SPA.bin
[1 2 3 4]: Verifying and copying expanded package files to flash:
[1 2 3 4]: Verified and copied expanded package files to flash:
[1 2 3 4]: Starting compatibility checks
[1 2 3 4]: Bypassing peer package compatibility checks due to 'force' command option
[1 2 3 4]: Finished compatibility checks
[1 2 3 4]: Starting application pre-installation processing
[1 2 3 4]: Finished application pre-installation processing
[1]: Old files list:
    Removed cat3k_caa-base.SPA.03.07.03E.pkg
    Removed cat3k_caa-drivers.SPA.03.07.03E.pkg
    Removed cat3k_caa-infra.SPA.03.07.03E.pkg
    Removed cat3k_caa-iosd-universalk9.SPA.152-3.E3.pkg
    Removed cat3k_caa-platform.SPA.03.07.03E.pkg
    Removed cat3k_caa-wcm.SPA.10.3.130.0.pkg
[2]: Old files list:
    Removed cat3k_caa-base.SPA.03.07.03E.pkg
    Removed cat3k_caa-drivers.SPA.03.07.03E.pkg
    Removed cat3k_caa-infra.SPA.03.07.03E.pkg
    Removed cat3k_caa-iosd-universalk9.SPA.152-3.E3.pkg
    Removed cat3k_caa-platform.SPA.03.07.03E.pkg
    Removed cat3k_caa-wcm.SPA.10.3.130.0.pkg
[3]: Old files list:
    Removed cat3k_caa-base.SPA.03.07.03E.pkg
    Removed cat3k_caa-drivers.SPA.03.07.03E.pkg
    Removed cat3k_caa-infra.SPA.03.07.03E.pkg
```

```
    Removed cat3k_caa-iosd-universalk9.SPA.152-3.E3.pkg
    Removed cat3k_caa-platform.SPA.03.07.03E.pkg
    Removed cat3k_caa-wcm.SPA.10.3.130.0.pkg
[4]: Old files list:
    Removed cat3k_caa-base.SPA.03.07.03E.pkg
    Removed cat3k_caa-drivers.SPA.03.07.03E.pkg
    Removed cat3k_caa-infra.SPA.03.07.03E.pkg
    Removed cat3k_caa-iosd-universalk9.SPA.152-3.E3.pkg
    Removed cat3k_caa-platform.SPA.03.07.03E.pkg
    Removed cat3k_caa-wcm.SPA.10.3.130.0.pkg
[1]: New files list:
    Added cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-rpbase.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-rpcore.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-srdriver.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-wcm.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-webui.16.03.05.prd1.SPA.pkg
[2]: New files list:
    Added cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-rpbase.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-rpcore.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-srdriver.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-wcm.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-webui.16.03.05.prd1.SPA.pkg
[3]: New files list:
    Added cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-rpbase.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-rpcore.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-srdriver.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-wcm.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-webui.16.03.05.prd1.SPA.pkg
[4]: New files list:
    Added cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-rpbase.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-rpcore.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-srdriver.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-wcm.16.03.05.prd1.SPA.pkg
    Added cat3k_caa-webui.16.03.05.prd1.SPA.pkg

[1 2 3 4]: Creating pending provisioning file
[1 2 3 4]: Finished installing software.  New software will load on reboot.
[1 2 3 4]: Committing provisioning file

[1 2 3 4]: Do you want to proceed with reload? [yes/no]: yes
[1 2 3 4]: Reloading

Switch#
```

Note Old files listed in the logs should be removed using the **request platform software package clean switch all** command, after reload

Reload

Step 5 If you said 'Yes' to the prompt in software install and your switches are configured with auto boot, the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
switch: boot flash:packages.conf
```

Note When you boot the new image, it will automatically update the boot loader.

Step 6 When the new image boots up, you can verify the version of the new image, by checking **show version**

```
Switch# show version
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 16.3.5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Tue 19-Sep-17 18:36 by mcpre
```

Step 7 After you have successfully installed the image, you no longer need the .bin image and the file can be deleted from flash of each switch if it was copied to flash.

```
Switch#delete flash:cat3k_caa-universalk9.16.03.05.SPA.bin
Delete filename [cat3k_caa-universalk9.16.03.05.SPA.bin]?
Delete flash:/cat3k_caa-universalk9.16.03.05.SPA.bin? [confirm]
Switch#
```

Upgrading from Cisco IOS XE 3.xE to Cisco IOS XE Denali 16.1.x, 16.2.x, or 16.3.x in Bundle Mode

Warning **You cannot boot Cisco IOS XE Denali 16.1.1 via TFTP for the first time with a Cisco IOS XE 3.xE boot loader. The Cisco IOS XE 3.xE boot loaders have a limitation that they cannot boot an image larger than 400MB via the TFTP server. Since Cisco IOS XE Denali 16.1.x is larger than 400MB, you must boot the image via flash drive. Refer to the upgrade sections in install mode.**

Warning **Starting from 16.3.5 release, you will not be able to boot Cisco IOS XE Denali 16.3.5 in bundle mode via flash drive for the first time with a Cisco IOS XE 3.xE boot loader. The Cisco IOS XE 3.xE boot loaders have a limitation that they cannot boot an image larger than 512MB via flash. Refer to the upgrade sections in install mode.**

Upgrading from Cisco IOS XE Denali 16.1.1 to 16.1.x, 16.2.x, or 16.3.x in Install Mode

Follow these instructions to upgrade from Cisco IOS XE Denali 16.1.1 to Cisco IOS XE Denali 16.1.x, 16.2.x, or 16.3.x in install mode. In order to do a software image upgrade, you must be booted into IOS using the **boot flash:packages.conf**.

Clean Up

Step 1 Ensure you have enough space in flash to expand a new image by cleaning up old installation files.

Note Use the **switch all** option to clean up all switches in your stack.

```
Switch#request platform software package clean switch all file flash:
Running command on switch 1
Cleaning up unnecessary package files
```

```
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat3k_caa-rpbase.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.01.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 2
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat3k_caa-rpbase.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.01.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 3
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat3k_caa-rpbase.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.01.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 4
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    packages.conf
      File is in use, will not delete.
    cat3k_caa-rpbase.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.01.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.01.01.SPA.pkg
      File is in use, will not delete.
  done.
```

```
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
```

Copy New Image to Stack

Step 2 Copy the new image to flash: (or skip this step if you want to use the new image from your TFTP server).

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.16.03.05.SPA.bin
flash:cat3k_caa-universalk9.16.03.05.SPA.bin
Destination filename [cat3k_caa-universalk9.16.03.05.SPA.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.16.03.05.SPA.bin...
Loading cat3k_caa-universalk9.16.03.05.SPA.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!
[OK - 489159804 bytes]

489159804 bytes copied in 143.802 secs (3401620 bytes/sec)
Switch#
```

Step 3 Use the **dir flash** command to confirm that the image has been successfully copied to flash.

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

 7759  -rw-   489159804  Aug 1 2016 04:35:43 +00:00
cat3k_caa-universalk9.16.03.05.SPA.bin
1621966848 bytes total (598597632 bytes free)
Switch#
```

Software Install Image to Flash

Step 4 Use the **request platform software package install switch all file flash: new auto-copy** command to install the target image to flash. We recommend copying the image to a TFTP server or the flash drive of the active switch.

If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3:

```
request platform software package install switch all file
flash-3:cat3k_caa-universalk9.16.03.05.SPA.bin new auto-copy
      <output truncated>
Expanding image file: flash-3: cat3k_caa-universalk9.16.03.05.SPA.bin
[3]: Copying flash-3: cat3k_caa-universalk9.16.03.05.SPA.bin from switch 3 to switch 1
2 4
<output truncated>
```

Note Use the **switch all** option to upgrade all switches in your stack
Use the **new** option to upgrade from Cisco IOS XE Denali 16.1.1 to Cisco IOS XE Denali 16.1.x, 16.2.x, or 16.3.x. (There are packaging changes in Cisco IOS XE Denali 16.1.2 and later releases.)
Use the **auto-copy** option to copy the .bin image from flash: to all other switches in your stack

Note When you execute the command, the following message is displayed:
`Unknown package type 21`
This is expected and does not affect the upgrade. See CSCux82059

```
Switch# request platform software package install switch all file
flash:cat3k_caa-universalk9.16.03.05.SPA.bin new auto-copy
Expanding image file: flash:cat3k_caa-universalk9.16.03.05.SPA.bin
[1]: Copying flash:cat3k_caa-universalk9.16.03.05.SPA.bin from switch 1 to switch 2 3
4
[2 3 4]: Finished copying to switch 2 3 4
[1 2 3 4]: Expanding file
[1 2 3 4]: Finished expanding all-in-one software package in switch 1 2 3 4
SUCCESS: Finished expanding all-in-one software package.
[1 2 3 4]: Performing install

Unknown package type 21

Unknown package type 21

Unknown package type 21

Unknown package type 21
  SUCCESS: install Finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-rpbase.16.01.01E.SPA.pkg
  Removed cat3k_caa-srdriver.16.01.01E.SPA.pkg
  Removed cat3k_caa-wcm.16.01.01E.SPA.pkg
  Removed cat3k_caa-webui.16.01.01E.SPA.pkg
New files list:
  Added cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-rpbase.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-rpcore.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-srdriver.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-wcm.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-webui.16.03.05.prd1.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[1]: Finished install successful on switch 1
[2]: install package(s) on switch 2
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-rpbase.16.01.01E.SPA.pkg
  Removed cat3k_caa-srdriver.16.01.01E.SPA.pkg
  Removed cat3k_caa-wcm.16.01.01E.SPA.pkg
  Removed cat3k_caa-webui.16.01.01E.SPA.pkg
New files list:
  Added cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-rpbase.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-rpcore.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-srdriver.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-wcm.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-webui.16.03.05.prd1.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[2]: Finished install successful on switch 2
[3]: install package(s) on switch 3
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-rpbase.16.01.01E.SPA.pkg
```

```
  Removed cat3k_caa-srdriver.16.01.01E.SPA.pkg
  Removed cat3k_caa-wcm.16.01.01E.SPA.pkg
  Removed cat3k_caa-webui.16.01.01E.SPA.pkg
New files list:
  Added cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-rpbase.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-rpcore.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-srdriver.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-wcm.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-webui.16.03.05.prd1.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[3]: Finished install successful on switch 3
[4]: install package(s) on switch 4
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-rpbase.16.01.01E.SPA.pkg
  Removed cat3k_caa-srdriver.16.01.01E.SPA.pkg
  Removed cat3k_caa-wcm.16.01.01E.SPA.pkg
  Removed cat3k_caa-webui.16.01.01E.SPA.pkg
New files list:
  Added cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-rpbase.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-rpcore.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-srdriver.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-wcm.16.03.05.prd1.SPA.pkg
  Added cat3k_caa-webui.16.03.05.prd1.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[4]: Finished install successful on switch 4
Checking status of install on [1 2 3 4]
[1 2 3 4]: Finished install in switch 1 2 3 4
SUCCESS: Finished install: Success on [1 2 3 4]
Switch#
```

Note Old files listed in the logs will not be removed from flash.

Step 5 After you have successfully installed the software, verify that the flash partition has six new.pkg files and one updated packages.conf file. See sample output below:

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg


Directory of flash:/

46495  -rw-    22310603  Sep 20 2017 17:55:04 +00:00
cat3k_caa-rpbase.16.01.01.SPA.pkg
46488  -rw-     9089664  Sep 20 2017 17:55:02 +00:00
cat3k_caa-srdriver.16.01.01.SPA.pkg
46489  -rw-   212785780  Sep 20 2017 17:55:03 +00:00
cat3k_caa-wcm.16.01.01.SPA.pkg
46487  -rw-    13423228  Sep 20 2017 17:55:02 +00:00
cat3k_caa-webui.16.01.01.SPA.pkg
46490  -rw-    19169920  Sep 18 2017 22:14:25 +00:00
cat3k_caa-guestshell.16.03.05.SSA.pkg
46494  -rw-    27904300  Sep 18 2017 22:14:28 +00:00
cat3k_caa-rpbase.16.03.05.pkg
46491  -rw-   331283064  Sep 18 2017 22:14:27 +00:00
cat3k_caa-rpcore.16.03.05.pkg
46493  -rw-    15319680  Sep 18 2017 22:14:27 +00:00
```

```
cat3k_caa-srdriver.16.03.05.pkg
46486  -rw-   266064504  Sep 20 2017 17:55:01 +00:00
cat3k_caa-wcm.16.03.05.SPA.pkg
46492  -rw-    16171644  Sep 18 2017 22:14:27 +00:00
cat3k_caa-webui.16.03.05.pkg
1621966848 bytes total (581828608 bytes free)

Switch#

Switch# dir flash:*.conf
Directory of flash:/*.conf

Directory of flash:/

30994  -rw-             4676   Aug 1 2016 04:42:26 -07:00  packages.conf
30995  -rw-             4667   Aug 1 2016 04:41:40 -07:00
cat3k_caa-universalk9.16.03.05.SPA.conf
1621966848 bytes total (132620288 bytes free)
Switch#
```

Step 6 After you have successfully installed the image, you no longer need the.bin image. If you copied the file to flash, you can delete it from the flash of each switch.

```
Switch# delete flash:cat3k_caa-universalk9.16.03.05.SPA.bin
Delete filename [cat3k_caa-universalk9.16.03.05.SPA.bin]?
Delete flash:/ cat3k_caa-universalk9.16.03.05.SPA.bin? [confirm]
Switch#
```

Reload

Step 7 Reload the switch.

```
Switch# reload
```

Step 8 If the switch is configured with auto boot, then the stack automatically boots up with the new image. If not, you can manually boot flash:packages.conf

```
switch:boot flash:packages.conf
```

Step 9 When the new image boots up, you can verify the version of the new image, by using the **show version** command:

```
Switch# show version
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 16.3.5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Tue 19-Sep-17 18:36 by mcpre
```

Upgrading from Cisco IOS XE Denali 16.3.x to Cisco IOS XE 16.x in Install Mode

Follow these instructions to upgrade from Cisco IOS XE Denali 16.3.x to a future IOS XE 16.x release in Install mode. In order to do a software image upgrade, you must be booted into IOS via “boot flash:packages.conf.”

Clean Up

Step 1 Ensure you have enough space in flash to expand a new image by cleaning up old installation files.

Note Use the **switch all** option to clean up all switches in your stack.

```
Switch# request platform software package clean switch all file flash:
Running command on switch 1
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    packages.conf
      File is in use, will not delete.
    cat3k_caa-rpbase.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.03.01.SPA.pkg
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 2
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    packages.conf
      File is in use, will not delete.
    cat3k_caa-rpbase.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.03.01.SPA.pkg
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 3
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    packages.conf
      File is in use, will not delete.
    cat3k_caa-rpbase.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.03.01.SPA.pkg
```

```
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Running command on switch 4
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    packages.conf
      File is in use, will not delete.
    cat3k_caa-rpbase.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.03.01.SPA.pkg
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
Switch#
```

Copy New Image to Stack

Step 2 Copy the new image to flash: (or skip this step if you want to use the new image from your TFTP server)

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.16.05.01aSPA.bin
flash:cat3k_caa-universalk9.16.05.01a.SPA.bin
Destination filename [cat3k_caa-universalk9.16.05.01a.SPA.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.16.05.01a.SPA.bin...
Loading cat3k_caa-universalk9.16.05.01a.SPA.binfrom 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!
[OK - 465466221 bytes]

465466221 bytes copied in 118.175 secs (3938788 bytes/sec)
Switch#
```

Step 3 Use the **`dir flash`** command to confirm that the image has been successfully copied to flash.

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

 7759  -rw-   465466221  Aug 1 2016 04:35:43 +00:00
cat3k_caa-universalk9.16.05.01a.SPA.bin
1621966848 bytes total (598597632 bytes free)
Switch#
```

Software Install Image to Flash

Step 4 Use the **`request platform software package install switch all file flash: auto-copy`** command to install the target image to flash. We recommend copying the image to a TFTP server or the flash drive of the active switch.

If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive. For example, if the image is on the flash drive of member switch 3:

```
request platform software package install switch all file
flash-3:cat3k_caa-universalk9.16.03.05.SPA.bin new auto-copy
      <output truncated>
Expanding image file: flash-3: cat3k_caa-universalk9.16.03.05.SPA.bin
[3]: Copying flash-3: cat3k_caa-universalk9.16.03.05.SPA.bin from switch 3 to switch 1
2 4
<output truncated>
```



Note Use the **switch all** option to upgrade all switches in your stack
Use the **auto-copy** option to copy the .bin image from flash: to all other switches in your stack

```
Switch# request platform software package install switch all file
flash:cat3k_caa-universalk9.16.05.01a.SPA.bin auto-copy
Expanding image file: flash:cat3k_caa-universalk9.16.05.01a.SPA.bin
[1]: Copying flash:cat3k_caa-universalk9.16.05.01a.SPA.bin from switch 1 to switch 2 3
4
[2 3 4]: Finished copying to switch 2 3 4
[1 2 3 4]: Expanding file
[1 2 3 4]: Finished expanding all-in-one software package in switch 1 2 3 4
SUCCESS: Finished expanding all-in-one software package.
[1 2 3 4]: Performing install
  SUCCESS: install Finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
  Removed cat3k_caa-rpbase.16.03.05.SPA.pkg
  Removed cat3k_caa-rpcore.16.03.05.SPA.pkg
  Removed cat3k_caa-srdriver.16.03.05.SPA.pkg
  Removed cat3k_caa-wcm.16.03.05.SPA.pkg
  Removed cat3k_caa-webui.16.03.05.SPA.pkg
New files list:
  Added cat3k_caa-rpbase.16.05.01a.SPA.pkg
  Added cat3k_caa-rpcore.16.05.01a.SPA.pkg
  Added cat3k_caa-srdriver.16.05.01a.SPA.pkg
  Added cat3k_caa-guestshell.16.05.01a.SPA.pkg
  Added cat3k_caa-webui.16.05.01a.SPA.pkg
SUCCESS: Software provisioned.  New software will load on reboot.
[1]: Finished install successful on switch 1
[2]: install package(s) on switch 2
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
  Removed cat3k_caa-rpbase.16.03.05.SPA.pkg
  Removed cat3k_caa-rpcore.16.03.05.SPA.pkg
  Removed cat3k_caa-srdriver.16.03.05.SPA.pkg
  Removed cat3k_caa-wcm.16.03.05.SPA.pkg
  Removed cat3k_caa-webui.16.03.05.SPA.pkg
New files list:
  Added cat3k_caa-rpbase.16.05.01a.SPA.pkg
  Added cat3k_caa-rpcore.16.05.01a.SPA.pkg
  Added cat3k_caa-srdriver.16.05.01a.SPA.pkg
  Added cat3k_caa-guestshell.16.05.01a.SPA.pkg
  Added cat3k_caa-webui.16.05.01a.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[2]: Finished install successful on switch 2
[3]: install package(s) on switch 3
--- Starting list of software package changes ---
```

```
Old files list:
  Removed cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
  Removed cat3k_caa-rpbase.16.03.05.SPA.pkg
  Removed cat3k_caa-rpcore.16.03.05.SPA.pkg
  Removed cat3k_caa-srdriver.16.03.05.SPA.pkg
  Removed cat3k_caa-wcm.16.03.05.SPA.pkg
  Removed cat3k_caa-webui.16.03.05.SPA.pkg
New files list:
  Added cat3k_caa-rpbase.16.05.01a.SPA.pkg
  Added cat3k_caa-rpcore.16.05.01a.SPA.pkg
  Added cat3k_caa-srdriver.16.05.01a.SPA.pkg
  Added cat3k_caa-guestshell.16.05.01a.SPA.pkg
  Added cat3k_caa-webui.16.05.01a.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[3]: Finished install successful on switch 3
[4]: install package(s) on switch 4
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-guestshell.16.03.05.prd1.SPA.pkg
  Removed cat3k_caa-rpbase.16.03.05.SPA.pkg
  Removed cat3k_caa-rpcore.16.03.05.SPA.pkg
  Removed cat3k_caa-srdriver.16.03.05.SPA.pkg
  Removed cat3k_caa-wcm.16.03.05.SPA.pkg
  Removed cat3k_caa-webui.16.03.05.SPA.pkg
New files list:
  Added cat3k_caa-rpbase.16.05.01a.SPA.pkg
  Added cat3k_caa-rpcore.16.05.01a.SPA.pkg
  Added cat3k_caa-srdriver.16.05.01a.SPA.pkg
  Added cat3k_caa-guestshell.16.05.01a.SPA.pkg
  Added cat3k_caa-webui.16.05.01a.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[4]: Finished install successful on switch 4
Checking status of install on [1 2 3 4]
[1 2 3 4]: Finished install in switch 1 2 3 4
SUCCESS: Finished install: Success on [1 2 3 4]
Switch#
```

Note Old files listed in the logs will not be removed from flash.

Step 5 After the software has been successfully installed, verify that the flash partition has five new.pkg files and 1 updated packages.conf file. See sample output below.

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg

Directory of flash:/

46490  -rw-    19169920  Sep 18 2017 22:14:25 +00:00
cat3k_caa-guestshell.16.03.05.SPA.pkg
46495  -rw-    22310603  Sep 20 2017 17:55:04 +00:00
cat3k_caa-rpbase.16.03.05.SPA.pkg
46486  -rw-   266064504  Sep 20 2017 17:55:01 +00:00
cat3k_caa-rpcore.16.03.05.SPA.pkg
46488  -rw-     9089664  Sep 20 2017 17:55:02 +00:00
cat3k_caa-srdriver.16.03.05.SPA.pkg
46489  -rw-   212785780  Sep 20 2017 17:55:03 +00:00
cat3k_caa-wcm.16.03.05.SPA.pkg
46487  -rw-    13423228  Sep 20 2017 17:55:02 +00:00
cat3k_caa-webui.16.03.05.SPA.pkg
```

```
46494  -rw-    27904300  Sep 18 2017 22:14:28 +00:00
cat3k_caa-rpbase.16.05.01a.SPA.pkg
46491  -rw-   331283064  Sep 18 2017 22:14:27 +00:00
cat3k_caa-rpcore.16.05.01a.SPA.pkg
46493  -rw-    15319680  Sep 18 2017 22:14:27 +00:00
cat3k_caa-srdriver.16.05.01a.SPA.pkg
46484  -rw-    15958656  Sep 20 2017 17:55:00 +00:00
cat3k_caa-guestshell.16.05.01a.SPA.pkg
46492  -rw-    16171644  Sep 18 2017 22:14:27 +00:00
cat3k_caa-webui.16.05.01a.SPA.pkg
1621966848 bytes total (581828608 bytes free)
Switch#

Switch# dir flash:*.conf
Directory of flash:/*.conf

Directory of flash:/

 7766  -rw-        5137  Aug 1 2016 06:10:39 +00:00
cat3k_caa-universalk9.16.05.01a.SPA.conf
 7769  -rw-        5125  Aug 1 2016 06:11:19 +00:00  packages.conf
1621966848 bytes total (137928704 bytes free)
Switch#
```

Step 6 After you have successfully installed the image, you do not need the .bin image and the file can be deleted from the flash of EACH switch if you had it copied to flash.

```
Switch# delete flash:cat3k_caa-universalk9.16.05.01a.SPA.bin
Delete filename [cat3k_caa-universalk9.16.05.01a.SPA.bin]?
Delete flash:/ cat3k_caa-universalk9.16.05.01a.SPA.bin? [confirm]
Switch#
```

Reload

Step 7 Reload the switch

```
Switch# reload
```

Step 8 If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
switch: boot flash:packages.conf
```

Note When you boot the new image, it will automatically update the boot loader.

Step 9 When the new image boots up, you can verify the version of the new image, using the **show version** command:

```
Switch# show version
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 16.5.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Tue 19-Sep-17 18:36 by mcpre
```

Downgrade from Cisco IOS XE 16.x to Cisco IOS XE 3.xE in Install Mode

Follow these instructions to downgrade from Cisco IOS XE 16.x to older Cisco IOS XE 3.xE releases in Install Mode.

Clean Up

Step 1 Ensure you have enough space in flash to expand a new image by cleaning up old installation files.

Note Use the **`switch all`** option to clean up all switches in your stack.

```
Switch# request platform software package clean switch all file flash:
Running command on switch 1
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat3k_caa-rpbase.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.03.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

Running command on switch 2
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat3k_caa-rpbase.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.03.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

Running command on switch 3
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat3k_caa-rpbase.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.03.01.SPA.pkg
      File is in use, will not delete.
```

```
    cat3k_caa-wcm.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.03.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

Running command on switch 4
Cleaning up unnecessary package files
  Scanning boot directory for packages ... done.
Preparing packages list to delete ...
    cat3k_caa-rpbase.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-wcm.16.03.01.SPA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.16.03.01.SPA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

The following files will be deleted:
[1]:
/flash/cat3k_caa-rpbase.16.02.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.02.01.SPA.pkg
/flash/cat3k_caa-universalk9.16.01.01.SPA.bin
/flash/cat3k_caa-universalk9.16.01.01.SPA.conf
/flash/cat3k_caa-wcm.16.02.01.SPA.pkg
/flash/cat3k_caa-webui.16.02.01.SPA.pkg
/flash/packages.conf.00-
[2]:
/flash/cat3k_caa-rpbase.16.02.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.02.01.SPA.pkg
/flash/cat3k_caa-universalk9.16.01.01.SPA.bin
/flash/cat3k_caa-universalk9.16.01.01.SPA.conf
/flash/cat3k_caa-wcm.16.02.01.SPA.pkg
/flash/cat3k_caa-webui.16.02.01.SPA.pkg
/flash/packages.conf.00-
[3]:
/flash/cat3k_caa-rpbase.16.02.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.02.01.SPA.pkg
/flash/cat3k_caa-universalk9.16.01.01.SPA.bin
/flash/cat3k_caa-universalk9.16.01.01.SPA.conf
/flash/cat3k_caa-wcm.16.02.01.SPA.pkg
/flash/cat3k_caa-webui.16.02.01.SPA.pkg
/flash/packages.conf.00-
[4]:
/flash/cat3k_caa-rpbase.16.02.01.SPA.pkg
/flash/cat3k_caa-srdriver.16.02.01.SPA.pkg
/flash/cat3k_caa-universalk9.16.01.01.SPA.bin
/flash/cat3k_caa-universalk9.16.01.01.SPA.conf
/flash/cat3k_caa-wcm.16.02.01.SPA.pkg
/flash/cat3k_caa-webui.16.02.01.SPA.pkg
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat3k_caa-rpbase.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.02.01.SPA.pkg ... done.
```

```
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.conf ... done.
Deleting file flash:cat3k_caa-wcm.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.02.01.SPA.pkg ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[2]:
Deleting file flash:cat3k_caa-rpbase.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.conf ... done.
Deleting file flash:cat3k_caa-wcm.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.02.01.SPA.pkg ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[3]:
Deleting file flash:cat3k_caa-rpbase.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.conf ... done.
Deleting file flash:cat3k_caa-wcm.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.02.01.SPA.pkg ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[4]:
Deleting file flash:cat3k_caa-rpbase.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-srdriver.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.bin ... done.
Deleting file flash:cat3k_caa-universalk9.16.01.01.SPA.conf ... done.
Deleting file flash:cat3k_caa-wcm.16.02.01.SPA.pkg ... done.
Deleting file flash:cat3k_caa-webui.16.02.01.SPA.pkg ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
Switch#
```

Copy New Image to Stack

Step 2 Copy the target Cisco IOS XE 3.xE image to flash: (you can skip this step if you want to use the image from your TFTP server).

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
flash:
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Destination filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin...
Loading cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!
!!!!!!!!!!!!!!!
[OK - 311154824 bytes]

311154824 bytes copied in 68.781 secs (4523849 bytes/sec)
Switch#
```

Step 3 Use the **dir flash** command to confirm that the image has been successfully copied to flash.

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

47718  -rw-   311154824  Nov 25 2015 18:17:21 +00:00
```

```
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin

3458338816 bytes total (2468995072 bytes free)
Switch#
```

Downgrade Software Image

Step 4 Use the **request platform software package install** command with the **new** option to downgrade your stack. You can point to the source image on your tftp server or in flash if you have it copied to flash.

Note Use the **switch all** option is needed to upgrade all switches in your stack.
Use the **auto-copy** option to copy the .bin image from flash: to all other switches in your stack.

```
Switch# request platform software package install switch all file flash:cat3k_caa-
universalk9.SPA.03.07.02.E.152-3.E2.bin new auto-copy
Expanding image file: flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
[4]: Copying flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin from switch 4 to
switch 1 2 3
[1 2 3]: Finished copying to switch 1 2 3
[1 2 3 4]: Expanding file
[1 2 3 4]: Finished expanding all-in-one software package in switch 1 2 3 4
SUCCESS: Finished expanding all-in-one software package.
[1 2 3 4]: Performing install
  SUCCESS: install Finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-rpbase.16.03.01.SPA.pkg
  Removed cat3k_caa-rpcore.16.03.01.SPA.pkg
  Removed cat3k_caa-srdriver.16.03.01.SPA.pkg
  Removed cat3k_caa-wcm.16.03.01.SPA.pkg
  Removed cat3k_caa-webui.16.03.01.SPA.pkg
New files list:
  Added cat3k_caa-base.SPA.03.07.02E.pkg
  Added cat3k_caa-drivers.SPA.03.07.02E.pkg
  Added cat3k_caa-infra.SPA.03.07.02E.pkg
  Added cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
  Added cat3k_caa-platform.SPA.03.07.02E.pkg
  Added cat3k_caa-wcm.SPA.10.3.120.0.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[1]: Finished install successful on switch 1
[2]: install package(s) on switch 2
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-rpbase.16.03.01.SPA.pkg
  Removed cat3k_caa-rpcore.16.03.01.SPA.pkg
  Removed cat3k_caa-srdriver.16.03.01.SPA.pkg
  Removed cat3k_caa-wcm.16.03.01.SPA.pkg
  Removed cat3k_caa-webui.16.03.01.SPA.pkg
New files list:
  Added cat3k_caa-base.SPA.03.07.02E.pkg
  Added cat3k_caa-drivers.SPA.03.07.02E.pkg
  Added cat3k_caa-infra.SPA.03.07.02E.pkg
  Added cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
  Added cat3k_caa-platform.SPA.03.07.02E.pkg
  Added cat3k_caa-wcm.SPA.10.3.120.0.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
```

```
[2]: Finished install successful on switch 2
[3]: install package(s) on switch 3
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-rpbase.16.03.01.SPA.pkg
  Removed cat3k_caa-rpcore.16.03.01.SPA.pkg
  Removed cat3k_caa-srdriver.16.03.01.SPA.pkg
  Removed cat3k_caa-wcm.16.03.01.SPA.pkg
  Removed cat3k_caa-webui.16.03.01.SPA.pkg
New files list:
  Added cat3k_caa-base.SPA.03.07.02E.pkg
  Added cat3k_caa-drivers.SPA.03.07.02E.pkg
  Added cat3k_caa-infra.SPA.03.07.02E.pkg
  Added cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
  Added cat3k_caa-platform.SPA.03.07.02E.pkg
  Added cat3k_caa-wcm.SPA.10.3.120.0.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[3]: Finished install successful on switch 3
[4]: install package(s) on switch 4
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-rpbase.16.03.01.SPA.pkg
  Removed cat3k_caa-rpcore.16.03.01.SPA.pkg
  Removed cat3k_caa-srdriver.16.03.01.SPA.pkg
  Removed cat3k_caa-wcm.16.03.01.SPA.pkg
  Removed cat3k_caa-webui.16.03.01.SPA.pkg
New files list:
  Added cat3k_caa-base.SPA.03.07.02E.pkg
  Added cat3k_caa-drivers.SPA.03.07.02E.pkg
  Added cat3k_caa-infra.SPA.03.07.02E.pkg
  Added cat3k_caa-iosd-universalk9.SPA.152-3.E2.pkg
  Added cat3k_caa-platform.SPA.03.07.02E.pkg
  Added cat3k_caa-wcm.SPA.10.3.120.0.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[4]: Finished install successful on switch 4
Checking status of install on [1 2 3 4]
[1 2 3 4]: Finished install in switch 1 2 3 4
SUCCESS: Finished install: Success on [1 2 3 4]
```

Note The old files listed in the logs should be removed using the **`software clean`** command, after reload

Step 5 After you have successfully installed the image, you no longer need the .bin image and the file can be deleted from flash of each switch if you copied it to flash.

```
Switch# delete flash: cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Delete filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Delete flash:/ cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin? [confirm]
Switch#
```

Reload

Step 6 Reload the switch

```
Switch# reload
```

Step 7 If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

Note When you downgrade to a Cisco IOS XE 3.xE image, your boot loader will not automatically downgrade. It will remain updated. The new boot loader can support booting both Cisco IOS XE 3.xE releases as well as Cisco IOS XE Denali16.x releases.

Downgrade from Cisco IOS XE 16.x to Cisco IOS XE 3.xE in Bundle Mode

Follow these instructions to downgrade from Cisco IOS XE 16.x in Bundle mode to an older Cisco IOS XE 3.xE release in Bundle mode.

Copy New Image to Stack

Step 1 Make sure your TFTP server is reachable from IOS via GigabitEthernet0/0.

```
Switch# show run | i tftp
ip tftp source-interface GigabitEthernet0/0
ip tftp blocksize 8192
Switch#
Switch# show run | i ip route vrf
ip route vrf Mgmt-vrf 5.0.0.0 255.0.0.0 5.30.0.1
Switch#
Switch# show run int GigabitEthernet0/0
Building configuration...

Current configuration : 115 bytes
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 ip address 5.30.12.121 255.255.0.0
 negotiation auto
end
Switch#
Switch# ping vrf Mgmt-vrf ip 5.28.11.250
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 5.28.11.250, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Step 2 Copy the image from your TFTP server to flash.

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
flash:
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Destination filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin...
Loading cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!
!
!!!!!!!!!!!!!!
[OK - 311154824 bytes]

311154824 bytes copied in 68.781 secs (4523849 bytes/sec)
Switch#
```

Note If you have a stack, you must copy the image to the flash of each switch in your stack.

Step 3 Use the **dir flash** command to confirm that the image has been successfully copied to flash.

```
Switch# dir flash:*.bin
Directory of flash:/*.bin

Directory of flash:/

47718  -rw-   311154824  Nov 25 2015 18:17:21 +00:00
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin

3458338816 bytes total (2468995072 bytes free)
Switch#
```

Edit the Boot variable

Step 4 Clear the boot variable

```
Switch(config)# no boot system
```

Step 5 Edit the boot variable to point to the new image.

```
Switch(config)# boot system flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
```

Step 6 Use the **write memory** command to save the configuration change.

```
Switch# write memory
```

Step 7 Use the **show boot** command to confirm that your boot variable is pointing to the new image

```
Switch# show boot
----------------------------
Switch 1
----------------------------
Current Boot Variables:
BOOT variable = flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin;

Boot Variables on next reload:
BOOT variable = flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin;
Allow Dev Key = yes
Manual Boot = yes
Enable Break = yes
Switch#
```

Reload

Step 8 Reload the switch

```
Switch# reload
```

Step 9 If your switches are configured with auto boot, the stack will automatically boot up with the new image. If not, you can manually boot flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin

```
switch:boot flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
```

Note When you downgrade to a Cisco IOS XE 3.xE image, your boot loader will remain updated, and will automatically be downgraded. The new boot loader can support booting both Cisco IOS XE 3.x releases as well as Cisco IOS XE Denali 16.x releases.

Step 10 When the new image boots up, you can verify the version of the new image, by checking **show version**

```
Switch# show version
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software
(CAT3K_CAA-UNIVERSALK9-M), Version 03.07.02E RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Tue 21-Jul-15 12:51 by prod_rel_team
```

Move from Cisco IOS XE 3.xE Bundle Mode to Install Mode

Step 11 Ensure you have enough space in flash to expand a new image by cleaning up old installation files. This command will erase your Cisco IOS XE 3.xE bin image file, so ensure that you copy it to your Active again.

```
Switch# software clean file flash:
Preparing clean operation ...
[1 2 3 4]: Cleaning up unnecessary package files
[1 2 3 4]: Preparing packages list to delete ...
[1]: Files that will be deleted:
    cat3k_caa-rpbase.16.03.01.SPA.pkg
    cat3k_caa-rpcore.16.03.01.SPA.pkg
    cat3k_caa-srdriver.16.03.01.SPA.pkg
    cat3k_caa-universalk9.16.03.01.SPA.bin
    cat3k_caa-wcm.16.03.01.SPA.pkg
    cat3k_caa-webui.16.03.01.SPA.pkg
    packages.conf
[2]: Files that will be deleted:
    cat3k_caa-rpbase.16.03.01.SPA.pkg
    cat3k_caa-rpcore.16.03.01.SPA.pkg
    cat3k_caa-srdriver.16.03.01.SPA.pkg
    cat3k_caa-universalk9.16.03.01.SPA.bin
    cat3k_caa-wcm.16.03.01.SPA.pkg
    cat3k_caa-webui.16.03.01.SPA.pkg
    packages.conf
[3]: Files that will be deleted:
    cat3k_caa-rpbase.16.03.01.SPA.pkg
    cat3k_caa-rpcore.16.03.01.SPA.pkg
    cat3k_caa-srdriver.16.03.01.SPA.pkg
    cat3k_caa-universalk9.16.03.01.SPA.bin
    cat3k_caa-wcm.16.03.01.SPA.pkg
    cat3k_caa-webui.16.03.01.SPA.pkg
    packages.conf
[4]: Files that will be deleted:
    cat3k_caa-rpbase.16.03.01.SPA.pkg
    cat3k_caa-rpcore.16.03.01.SPA.pkg
    cat3k_caa-srdriver.16.03.01.SPA.pkg
    cat3k_caa-universalk9.16.03.01.SPA.bin
    cat3k_caa-wcm.16.03.01.SPA.pkg
    cat3k_caa-webui.16.03.01.SPA.pkg
    packages.conf

[1 2 3 4]: Do you want to proceed with the deletion? [yes/no]: yes
[1 2 3 4]: Clean up completed
Switch#
```

Step 12 Copy the image from your TFTP server to flash

```
Switch# copy tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
flash:
cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Destination filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Accessing tftp://5.28.11.250/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin...
Loading cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin from 5.28.11.250 (via
GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!
!
!!!!!!!!!!!!!!
[OK - 311154824 bytes]

311154824 bytes copied in 68.781 secs (4523849 bytes/sec)
Switch#
```

Step 13 Use the **software expand** command to expand the target image to flash and move from bundle mode to install mode. You can point to the source image on your TFTP server or in flash if you have it copied to flash.

```
Switch# software expand file flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Preparing expand operation ...
[1]: Copying software from active switch 1 to switches 2,3,4
[1]: Finished copying software to switches 2,3,4
[1 2 3 4]: Expanding bundle flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
[1 2 3 4]: Copying package files
[1 2 3 4]: Package files copied
[1 2 3 4]: Finished expanding bundle
flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Switch#
```

Edit the Boot variable

Step 14 Clear the boot variable

```
Switch(config)# no boot system
```

Step 15 Edit the boot variable to point to the new image.

```
Switch(config)# boot system flash:packages.conf
```

Step 16 Use the **write memory** command to save the configuration change.

```
Switch#write memory
```

Step 17 Use the **show boot** command to confirm that your boot variable is pointing to the new image

```
Switch# show boot
----------------------------
Switch 1
----------------------------
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = yes
Enable Break = yes
Switch#
```

Reload

Step 18 Reload the switch

```
Switch# reload
```

Step 19 If your switches are configured with auto boot, the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
switch:boot flash:packages.conf
```

Step 20 When the new image boots up, you can verify the version of the new image, by checking **show version**

```
Switch# show version
Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software
(CAT3K_CAA-UNIVERSALK9-M), Version 03.07.02E RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Tue 21-Jul-15 12:51 by prod_rel_team
```

Step 21 After you have successfully installed the image, you no longer need the .bin image and the file can be deleted from the flash of each switch if you had copied to flash.

```
Switch#delete flash:cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin
Delete filename [cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin]?
Delete flash:/cat3k_caa-universalk9.SPA.03.07.02.E.152-3.E2.bin? [confirm]
Switch#
```

WCM Sub Package Software Image Upgrade

The sub-package upgrade steps are similar to the bundle package upgrade, except that you only install one sub-package and not all packages. In order to perform a sub-package software image upgrade, you must be booted into IOS using **boot flash:packages.conf**.

Step 1 Copy new sub-package image to flash. For example, **cat3k_caa-wcm.16.02.01.SPA.pkg for WCM module** for the WCM module.

Step 2 Use the **request platform software package install switch <switch id> file flash:<image>** command to upgrade your switch.

```
switch# request platform software package install switch 1 file flash:
    cat3k_caa-wcm.16.02.01.SPA.pkg
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
  Removed cat3k_caa-wcm.16.01.01.SPA.pkg
New files list:
  Added cat3k_caa-wcm.16.02.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned.  New software will load on reboot.
[1]: Finished install successful on switch 1
```

Step 3 When you upgrade the WCM sub-package, and you have AP(s) connected and joined to the controller, you can pre-download the newly upgraded AP images to APs before restarting the APs. The pre-download steps are as follows:

Step	Command	Purpose
1.	**# show ap join stats summary**	Shows all APs connected to the controller, includes joined and not joined APs.
2.	**# show ap image**	Only joined AP(s) can perform the image pre-downloading process.
3.	**# ap image predownload**	While pre-downloading the AP image(s), use **#show ap image** to monitor the pre-downloading status. Go to the next step after image pre-downloading is completed.
4.	**# ap image swap**	Swaps the backup AP image with the bootup AP image on AP device.
5.	**# ap image reset**	Restarts all the APs that have connected to the controller.
6.	**# reload**	Restart the controller.

Upgrading RTU Licenses

In Cisco IOS XE Denali 16.1.1, right-to-use (RTU) licensing has been modified to allow stack members to join a stack without having the same license level as the rest of the existing stack. The mismatched switch will not be put into Lic-Mismatch state. Even though the switch with the mismatched license is allowed to join the stack, the following syslog message is displayed periodically reminding you to fix the RTU license level:

```
%STACK_RTU_LICENSE-6-IOSD_LIC_MISMATCH:Switch 5 R0/0: stack_mgr: Switch #5:
Current IOSd runs on lanbase license while RTU active license is ipservices.
Please configure RTU license to current IOSd license.
```

For more information, see CSCux27336.

The EXEC mode **Right to Use License** command allows you to activate or deactivate feature set licenses or Adder AP Count Licenses. This command provides options to activate or deactivate any license supported on the platform.

```
license right-to-use  [activate|deactivate]  [ lanbase | ipbase | ipservices |
ap-count]  {evaluation  | <count> } [ all | slot  <switch id>] {acceptEULA}
```

Ugrading an IP Base SKU to IP Services License

Step	Command	Purpose
1	license right-to-use activate ipservices slot <switch id>	Activate IP Services license. Pass the switch id. EULA will be prompted, accept the EULA by typing ‘yes’.
2	show license right-to-use summary	Check the reboot license level is ipservices.
3	reload	Reboot the switch to boot with ipservices.

Evaluating IP Services License on IP Base SKU

Step	Command	Purpose
1	license right-to-use activate ipservices evaluation slot <switch id>	Activate IP Services evaluation license. Pass the switch id. EULA will be prompted, accept the EULA by typing ‘yes’.
2	show license right-to-use summary	Check the reboot license level is ipservices eval.
3	reload	Reboot the switch to boot with ipservices eval.

Upgrading an LAN Base SKU to IP Services License Without Prompting EULA

Step	Command	Purpose
1	license right-to-use activate ipservices slot <switch id> acceptEULA	Activate IP Services license. Pass the switch id. EULA will be accepted automatically without being prompted.
2	Show license right-to-use summary	Check the reboot license level is ipservices.
3	Reload	Reboot the switch to boot with ipservices.

Deactivating Evaluation IP Services License on IP Base SKU

Step	Command	Purpose
1	license right-to-use deactivate ipservices evaluation slot <switch id>	Deactivates IP Services evaluation license.
2	Show license right-to-use summary	Check the reboot license level is ipbase.
3	Reload	Reboot the switch to boot with ipbase.

Upgrading LAN Base Stack to IP Base Stack

Step	Command	Purpose
1	license right-to-use activate ipbase all	Activate IP Base license on all the switches in the stack. EULA will be prompted, accept the EULA by typing ‘yes’.
2	Show license right-to-use	Check the reboot license level is ipbase for all the switches.
3	Reload	Reboot the switch to boot with ipbase.

Changing the License Level of License Mismatch Switch from Active’s Console

If the license mismatch switch has a lower license level than other switches in the stack, and the stack is running at IP Services and the mismatch switch is booted with IP Base license.

Step	Command	Purpose
1	show switch	Get the switch number in license mismatch state.
2	show license right-to-use mismatch	Check the license level of the license mismatch switch.
3	license right-to-use activate ipservices slot <switch-id>	Activate IP Services license on all the mismatch switches in the stack. EULA will be prompted, accept the EULA by typing ‘yes’.
4	Reload slot <switch-id>	Reboot the license mismatch switch to boot with ipservices and join the stack.

If the license mismatch switch has a higher license level than other switches in the stack, and the stack is running at IP Base and the mismatch switch is booted with IP Services license.

Step	Command	Purpose
1	show switch	Get the switch number in license mismatch state.
2	show license right-to-use mismatch	Check the license level of the license mismatch switch.
3	license right-to-use activate ipbase slot <switch-id>	Activate IP Base license on the license mismatch switch. EULA will be prompted, accept the EULA by typing ‘yes’.

Adding Adder AP Count Licenses

Step	Command	Purpose
1	license right-to-use activate apcount <count> slot <switch id>	Pass the number of AP count licenses to add as count. Pass the switch-id on which the Adder AP count licenses are to be added. EULA is prompted, accept it by typing 'yes'.
2	Show license right-to-use slot <switch-id>	Check the adder AP count licenses are incremented on the given switch.
3	Show license right-to-use summary	Check the total Adder AP count licenses are incremented and the Total available AP count are incremented.

Decrementing Adder AP Count licenses

Step	Command	Purpose
1	license right-to-use deactivate apcount <count> slot <switch id>	Pass the number of AP count licenses to be removed as count. Pass the switch-id on which the Adder AP count licenses are to be removed.
2	Show license right-to-use slot <switch-id>	Check the adder AP count licenses are decremented on the given switch.
3	Show license right-to-use summary	Check the total Adder AP count licenses are reduced by count and the Total available AP Count are reduced.

Activating Evaluation AP Count License on the Stack

Step	Command	Purpose
1	license right-to-use activate apcount evaluation	Activated evaluation AP Count licenses on the stack. EULA will be prompted, accept it.
2	Show license right-to-use summary	Check the license type evaluation with maximum supported AP Count is displayed. Base and adder AP Count licenses are not seen.
3	Show license right-to-use	To check the base and adder apcount licenses, if any.

Deactivating Evaluation AP Count License

Step	Command	Purpose
1	license right-to-use deactivate apcount evaluation	Deactivates evaluation AP Count licenses on the stack.
2	Show license right-to-use summary	Base and Adder AP Count licenses are displayed. Total available AP Count is sum of Base and Adder AP Count.

Feature Sets

The Catalyst 3850 switch supports three different feature sets:

- LAN Base feature set—Provides basic Layer 2+ features, including access control lists (ACLs) and quality of service (QoS), and up to 255 VLANs.
- IP Base feature set—Provides Layer 2+ and basic Layer 3 features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), static routing, EIGRP stub routing, IP multicast routing, Routing Information Protocol (RIP), basic IPv6 management, the Open Shortest Path First (OSPF) Protocol (for routed access only), and support for wireless controller functionality. The license supports up to 4094 VLANs.
- IP Services feature set—Provides a richer set of enterprise-class intelligent services and full IPv6 support. It includes IP Base features plus Layer 3 routing (IP unicast routing and IP multicast routing). The IP Services feature set includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP), the Open Shortest Path First (OSPF) Protocol, and support for wireless controller functionality. The license supports up to 4094 VLANs.

Note A separate access point count license is required to use the switch as a wireless controller.

For more information about the features, see the product data sheet at this URL:

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

Interoperability with Other Client Devices

This section describes the interoperability of this version of the switch software release with other client devices.

Table 10 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	16.3.1
Controller	Cisco 3850 Controller
Access points	3802, 3502, 3602, 2602, 1702, 2702, 3702, 702W, 1852
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5

Table 10 Test Bed Configuration for Interoperability

Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 5.3, ISE 1.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 11 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, and phones.

Table 11 Client Types

Client Type and Name	Version
Laptop	
Intel 5100/5300	v14.3.2.1
Intel 6200	15.15.0.1
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 1000/1030	v14.3.0.6
Intel 7260	18.33.0.2
Intel 7265	18.40.0.9
Intel 3160	18.33.0.2
Broadcom 4360	6.30.163.2005
Linksys AE6000 (USB)	5.1.2.0
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
D-Link DWA-182 (USB)	6.30.145.30
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Asus AC56(USB)	1027.7.515.2015
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
Cisco CB21	1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358

Table 11 Client Types

MacBook Pro	OSX 10.11.5
MacBook Air old	OSX 10.11.5
MacBook Air new	OSX 10.11.5
Macbook Pro with Retina Display	OSX 10.11.5
Macbook New 2015	OSX 10.11.5
Tablets	
Apple iPad2	iOS 9.3.1(13E238)
Apple iPad3	iOS 9.3.1(13E238)
Apple iPad mini with Retina display	iOS 9.3.1(13E238)
Apple iPad Air	iOS 9.3.1(13E238)
Apple iPad Air 2	iOS 9.3.1(13E238)
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 – SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3073.151
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Google Nexus 9	Android 6.0
Google Nexus 7 2nd Gen	Android 5.0
Phones	
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Apple iPhone 4S	iOS 9.2(13C75)
Apple iPhone 5	iOS 9.3.1(13E238)
Apple iPhone 5s	iOS 9.3.1(13E238)
Apple iPhone 5c	iOS 9.3.1(13E238)
Apple iPhone 6	iOS 9.3.1(13E238)
Apple iPhone 6 Plus	iOS 9.3.1(13E238)
Apple iPhone SE	iOS 9.3.1(13E238)
HTC One	Android 5.0
OnePlusOne	Android 4.3
Samsung Galaxy S4 – GT-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.1
Google Nexus 5	Android 5.1

Table 11 Client Types

Nexus 6	Android 5.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Huawei Ascend P7	Android 4.4.2
Samsung Galaxy S III	Android 4.4.2
Google Nexus 9	Android 6.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy S6	Android 6.0.1
Samsung Galaxy S5	Android 5.0.1
Xiaomi Mi 4i	Android 5.1.1
Samsung Galaxy S7	Android 6.0.1

Scaling Guidelines

Table 12 Scaling Guidelines

System Feature	Maximum Limit
Number of HTTP session redirections system-wide	Up to 100 clients per second (wired/wireless)
Number of HTTPS session redirections system-wide	Up to 5 clients per second (wireless) Up to 20 clients per second (wired)

Limitations and Restrictions

- Limitations for YANG data modeling—A maximum of 20 simultaneous NETCONF sessions are supported.
- Limitations for RF Profiles—Configuration with Cisco Prime Infrastructure is not supported. You must use the CLI to configure the feature.
- Limitations for Wired AVC:
  - NBAR2 (QOS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
  - NBAR2 based match criteria ‘match protocol’ is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
  - ‘Match Protocol’: up to 256 concurrent different protocols in all policies.
  - NBAR2 attributes based QOS is not supported (‘match protocol attribute’).
  - NBAR2 and Netflow cannot be configured together at the same time on the same interface.
  - Only IPv4 unicast (TCP/UDP) is supported.
  - AVC is not supported on management port (Gig 0/0)

  - NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.
  - Performance—Each switch member is able to handle 500 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
  - Scale—Able to handle up to 5000 bi-directional flows per 24 access ports.
- Restrictions for QoS:
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
  - QoS marking is not supported on COS-AP (Wave-2 APs) in any Cisco IOS XE Denali 16.x.x release. In these releases, QoS marking is based on table-maps and table-maps are not supported on COS-APs.
- Starting with Cisco IOS XE Denali 16.3.1, Centralized Management Mode (CMM) is no longer supported.
- You cannot configure NetFlow export using the Ethernet Management port (g0/0).
- The maximum committed information rate (CIR) for voice traffic on a wireless port is 132 Mb/sec.
- Flex Links are not supported. We recommend that you use spanning tree protocol (STP) as the alternative.
- Outdoor access points are supported only when they are in Local mode.
- Restrictions for Cisco TrustSec:
  - Dynamic SGACL download is limited to 6KB per destination group tag (DGT).
  - Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
  - Cisco TrustSec cannot be configured on a pure bridging domain with IPSG feature enabled. You must either enable IP routing or disable the IPSG feature in the bridging domain.
- Restriction for VLAN: It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may crash. As a workaround, disable the logging discriminator on the device.
- For the WS-C3850-12X48U-L, WS-C3850-12X48U-S and WS-C3850-12X48U-E switch models, a maximum of 28 ports are available for UPoE connections.

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

- Cisco Bug Search Tool, page 71
- Open Caveats in Cisco IOS XE Denali 16.3.x, page 71
- Resolved Caveats in Cisco IOS XE Denali 16.3.11, page 72
- Resolved Caveats in Cisco IOS XE Denali 16.3.10, page 72
- Resolved Caveats in Cisco IOS XE Denali 16.3.6, page 74
- Resolved Caveats in Cisco IOS XE Denali 16.3.5b, page 76
- Resolved Caveats in Cisco IOS XE Denali 16.3.5, page 76
- Resolved Caveats in Cisco IOS XE Denali 16.3.3, page 79
- Resolved Caveats in Cisco IOS XE Denali 16.3.2, page 79
- Resolved Caveats in Cisco IOS XE Denali 16.3.1a, page 82
- Resolved Caveats in Cisco IOS XE Denali 16.3.1, page 83

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats in Cisco IOS XE Denali 16.3.x

The following are the open caveats in Cisco IOS XE Denali 16.3.x. Click on the identifier to view the details of a caveat in the BST.

Identifier	Description
CSCva85191	Input drops on G0/0
CSCvb86896	Traceback found PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT in arp_send
CSCve47576	IPSec traffic may be classified as 'unknown' by NBAR
CSCvg44450	Cisco 2800,3800,1560 AP cannot forward packets downstream; 'Failed to get ARP entry for WLC'
CSCvg44907	Unexpected Reboot With MACsec During CTS Configuration
CSCvi38244	IPv6 VRRP Master is using vlan BIA MAC while sending Neighbor advertisements (NA)

Identifier	Description
CSCvk30813	MAB fails to start negotiation after device moves to another layer 2 adjacent switch
CSCvm57125	Periodic accounting update is not being sent
CSCvv38627	SPAN on uplink switchport not capturing some sourced traffic from its own WCM

Resolved Caveats in Cisco IOS XE Denali 16.3.11

There are no resolved caveats in Cisco IOS XE Denali 16.3.11.

Resolved Caveats in Cisco IOS XE Denali 16.3.10

There are no resolved caveats in Cisco IOS XE Denali 16.3.10.

Resolved Caveats in Cisco IOS XE Denali 16.3.9

Caveat ID Number	Description
CSCus83638	5-GHz radio on Cisco AP beaconing but not accepting client associations
CSCuw51380	object-group ACL CLI should not be supported at Catalyst 3850 switch.
CSCvk00889	APs with -S domain rejected to join the switch due to Invalid regulatory domain.
CSCvm68624	Cisco Wave 1 AP console display logs 'DTX DUMP'
CSCvn30230	Catalyst 3000 Series/Catalyst 9000 Series switches: Slow memory leak in linux_iosd-imag
CSCvn57892	High Memory utilization due to Wireless Manager IOSD process
CSCvn79221	MAC address learning failure on port configured with port-security
CSCvo02493	Inconsistent stack state after losing active member during "HA sync in progress"
CSCvo32811	GRE forwarding/programming issues on Catalyst 3850 switch if the tunnel destination route flaps too often
CSCvo34804	Catalyst 3850 stack SFP cannot be recognized on some port and the port link also do not up
CSCvo46822	Packet loops are noticed when WCCP redirect out is enabled on VLAN interface of Catalyst 3850 switch.
CSCvo65974	QinQ tunnels causing L2 loop in specific topology of Catalyst 3850 switch.
CSCvo71264	Catalyst 3000 Series/Catalyst 9000 Series switches Gateway routes DHCP offer incorrectly after DHCP snooping.
CSCvo85183	Catalyst 3650 Uplinkfast take time when recovery from link failure.
CSCvp30239	Catalyst 3850 no response.
CSCvp40615	Fed process crash due to memory corruption.
CSCvp70393	16.3.9- Catalyst 3850 switch remains up/up to opposite device even though Catalyst 3850 is down.

Caveat ID Number	Description
CSCvp88369	Catalyst 3000 series switches crash while accessing OBFL.
CSCvq25360	Powered Devices not getting PoE on multiple interfaces in Catalyst 3850 stack.

Resolved Caveats in Cisco IOS XE Denali 16.3.8

Caveat ID Number	Description
CSCvi48988	SNMP timeout when querying entSensorValueEntry
CSCvj76601	WCM crash due to apfRogueTask
CSCvk01056	WLC in 16.3.X not sending vlan override info in guest anchor scenario
CSCvk22455	3650 configured with AE and PK country codes crashes when 3800 AP plugged in
CSCvk28593	Standby 3850 running 16.3.6 APF-RG-Q full causing logging messages and high CPU
CSCvk50081	Interface on standby switch in stack is not coming up after soft reload
CSCvk56606	Wireless clients associating to controller with wrong downloadable acl
CSCvk58143	500~600 secs Increase in boot time when "ip domain lookup" is configured.
CSCvk60100	“switchport block multicast” blocks IPv6 RA (CSCvh81931)
CSCvk63600	Host limit of 32 for session monitoring sessions for 16.3
CSCvk76401	Post 3650 Mobility Agent Reload the Mobility Tunnel down due to "DTLS handshake error"
CSCuz72531	PC mac deleted from port-security table even with sticky config
CSCvm36748	FED crash at expired "FED MAC AGING TIMER" or "unknown" timer.
CSCvn08136	Removing FNF config using the command "no vlan config 1-4094" causes watchdog forced crash
CSCvn33844	RATE_11M supported cannot be preserved in config after reboot(no lower datarates set as mand.)

Resolved Caveats in Cisco IOS XE Denali 16.3.7

Caveat ID Number	Description
CSCvj76259	MOSFET fault 3850/3650 suddenly stops providing PoE on certain ports
CSCvc85100	Should not install Policy Map that has a Table-map action in police used with priority feature
CSCvf21673	APs send block ACK packets using disabled data rates
CSCvf94632	AVB stream not forwarded when talker/listeners are connected to different ASICs
CSCvg45950	packet drop seen intermittently if 40G traffic sent via cts interface

Caveat ID Number	Description
CSCvg60743	Switch crashing after configuring CTS on uplink 10G port (2x1G,2X10G)
CSCvg64578	reflects back multicast traffic received from source on the same vlan.
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvh11396	packet drop seen intermittently if 40G traffic sent via cts interface
CSCvh11581	Switch netflow export packet Vlan ID display as "unknown" in packet capture
CSCvh20944	In RSTP during conversion, port Desg.BLK does not to change to forwarding state immediatly.
CSCvh28402	optical signal present on shut interface with "cts manual"
CSCvh66882	sh idprom data not correct for 40G SFP
CSCvh73819	Switch crash on bulk_vlan_stats_msg_stats_set_internal
CSCvh87270	StackWise Virtual not forwarding IGMP traffic over the standby switch.
CSCvi02072	Cisco Wave 2 APs: ETSI 5G adaptive Wi-Fi compliance fix
CSCvi11287	Cisco 2800 AP consistently reboots around 1 second after joining to the WLC
CSCvi14641	Cisco 2802, 3802 APs cannot connect with 100Mbps LAN speed
CSCvi17380	TxFSM stuck on Radio 0 with TCQVerify patch
CSCvi19809	Memory leak in TMS process
CSCvi38191	Memory leak in lman process due to "ld_license_ext.dat" build-up.
CSCvi40033	802.1x authentications are failing if there was interface template config applied before
CSCvi75086	Rapid TDL memory leak in SMD process leads to crash of active switch in stack for ipv6 clients
CSCvi92251	3850 / 16.3.6 / SV stack splits after drops on CPU queue (nif_mgr)
CSCvj41163	Memory size in smand process increases on 3850/3650 without any services, uplinks nor configuration
CSCvj41853	Incorrect Tx power on AP3802P-Q on some channels
CSCvj63612	When PoE interface comes up with specific config, causes High CPU %, IOSd , IOMd crashes
CSCvj70569	Cisco 2800, 3800,4800 APs: Incorrect Tx power on power on till we configure Tx power using Cisco WLC

Resolved Caveats in Cisco IOS XE Denali 16.3.6

Caveat ID Number	Description
CSCuw85826	Evaluation of Cisco IOS and IOS-XEl for NTP_October_2015
CSCux86075	Unexpected crash during SSH operation
CSCva46459	SSH session hangs if it is not closed properly

Caveat ID Number	Description
CSCvb95909	16.3.2: smd crash (CPU hog in SMD:sgacore / cts_authz_session_uninstall_rbacl _authz)
CSCvc23868	IP Phone authorization failing on switch after interface flap
CSCvc47165	SFP port detect link-flap error and it's in error-disabled state on switch
CSCvc61653	Memory leak in btrace thread deletion: cli_agent
CSCvd12100	NGWC guest accounts aren't deleted after lifetime expires
CSCvd20857	3850 Stack may reload when making config changes
CSCve54486	Crash when attempting to assign nonexistent/shutdown VLAN to 802.1x port
CSCve83826	Packet drop due to IGR_MISC_FATAL_ERROR exception
CSCve90160	Observing memory leaks in AAA_STRDUP_GREEN_PARSER_SG_NAME1
CSCvf43271	Traceback: Stack master crash at dot1x authentication
CSCvf60862	Cisco IOS and IOS XE Software IOS daemon Cross-Site Scripting Vulnerability
CSCvf96466	GLC-TE 100M link shows notconnect after SFP reseat or reload switch
CSCvg32105	Memory Leak in fman_fp_image when NBAR is configured
CSCvg34039	Switch : no traffic over tex/1/7 ports
CSCvg37755	Switch does NOT answer arp request for some specific mac addresses
CSCvg43372	incorrect CDP/UDLD neighbors, duplicate entries seen in 16.3.5
CSCvg48154	UDLD error disables the 10G interface when enabling "udld aggresive" on peer
CSCvg53159	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch
CSCvg56727	3850/3650 with 16.3.5/16.6.1 crashes with 'server-key' command using key of 128 characters or more
CSCvg58932	Qos classification issue with NBAR
CSCvg60156	Switch CTS fails to enforce RBACLs on known mappings
CSCvg60288	Device IP address AV pair replaced with 192.168.1.5
CSCvg75380	16.3.5: Unexpected Reboot with Device Classifier enabled
CSCvg74751	Switch - Memory Leak in pvp.sh Process
CSCvg81139	ping failure for more than 10 seconds after REP topo change
CSCvg89791	Configuring "qos queue-softmax-multiplier" causes stackwise-virtual members to split or crash.
CSCvg91169	3850 standby switch reloads due to configuration-mismatch after use "exception crashinfo" command
CSCvg95142	running multicast traffic switch crashed by fed process
CSCvg96399	Hardware OutDrops interface counter is cloned on the Software OutDrops interface counter
CSCvh00038	Device IP address AV pair replaced with 192.168.1.5
CSCvh08380	LLDP attibutes are not seen in accounting messages during config changes
CSCvh21718	DHCP request/inform packets lead to uplink MAC being seen on access ports

Caveat ID Number	Description
CSCvh28573	Switch Memory Leak without any cabling
CSCvh52882	Memory Leak due to nbar config
CSCvh56888	Policer action incorrectly set to MARKDOWN instead of DROP in hardware
CSCvh60088	Unresponsive on save wi th multiple privilege commands
CSCvh60525	CLI 'aaa common-criteria' not available on IPBASEK9 license
CSCvh60757	traffic loss for more than 10 seconds after active member of switch stack reboot (REP topology)
CSCvh85482	memory utilization increasing for tams_proc
CSCvh89372	Memory leak in linux_iosd-image or platfrom_mgr

Resolved Caveats in Cisco IOS XE Denali 16.3.5b

Identifier	Description
CSCvg42682	Key Re-installation attacks against WPA protocol
CSCvg43372	incorrect CDP/UDLD neighbors, duplicate entries seen in Denali-16.3.5

Resolved Caveats in Cisco IOS XE Denali 16.3.5

Identifier	Description
CSCud22987	STANDBY wcm: %OSAPI-4-TIME_SHIFT_DETECTED: Detected backward time shift
CSCur31055	Ten gig links gets err-disable after "UDLD enable" on 3850
CSCuw77959	Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability
CSCva05226	"dot1x pae authenticator" lost from interface once port moved to trunk
CSCva76263	3850-48P switch stack rebooted with a Abort on Chasfs
CSCvb14640	Cisco IOS and Cisco IOS XE Software IPv6 SNMP Message Handling Denial of Service Vulnerability
CSCvb44320	Switch crashes continuously after booting up with autosmartport
CSCvb48912	SNMP crashes getting ntpAssociationEntry with low/fragmented memory condition
CSCvb69066	3650/3850 traffic not passing on the interface with GLC-GE-100FX (3.6.5/3.7.4)
CSCvb91970	Switch Crash in the FED Process
CSCvc07577	Crash in BGP due to regular expressions
CSCvc26787	Interface may flapping unexpectedly or go to err-disabled
CSCvc42037	Setany failed @ifAdminStatus
CSCvc55215	Modified 802.11AC MCS 8 and MCS 9 configurations not pushed to AP

Identifier	Description
CSCvc56873	With 3800/2800 APs, AVC works only for existing WLAN and not for new WLAN when AVC enabled
CSCvc58336	DHCP replies from DHCP server are not forwarded to client when ap link-encryption config
CSCvc62532	HTTP connection may fail when IPv6 address is configured on any interface
CSCvc63975	Ping fails with RSPAN configured when SRC and DEST(remote-span) vlans are allowed on the same trunk
CSCvc76125	Rogue APs must be reclassified by new reports even if they are classified as Malicious
CSCvc86691	When 'dot1x critical eapol' is configured, switch sends EAP failure instead of Success
CSCvc87589	HSRP standby router forwards packets after HSRP preempt
CSCvc88679	SCHED-3-THRASHING: Process thrashing on watched queue 'sep rxQ'. -Process= "SEP_webui_wsma
CSCvc89645	SGACL enforcement under VRF unexpectedly blocking traffic
CSCvc96706	Denali 16.3.2 not providing PoE after bouncing the port.
CSCvc98571	EEM applet will not release the Config Session Lock if it ends when CLI is in configuration mode
CSCvc99468	Observed traceback: "Node not found for wdb type 5"
CSCvd02101	QSFP-40G-SR-BD shows speed as 1000Mb/s
CSCvd02153	router crash due to mpls/ospf config on interface
CSCvd03465	Switch prevents updating MAC address in multi-host mode
CSCvd05280	DBM Crash on Active Switch while changing DCA channels
CSCvd10161	Optimized Roaming is not triggered when client moves beyond Coverage Data RSSI threshold
CSCvd12339	AP not receiving 11AC data rates configuration from wlc
CSCvd12371	SSH logs showing empty username on successful authentication
CSCvd28429	A-MSDU and A-MPDU config reset to defaults after device reloads
CSCvd30006	Controller allows changing 1830 AP mode to monitor
CSCvd33197	3850 Uplink port goes down after reload due to udld err-Disable on remote end
CSCvd33735	WCM crash at reaper_handler_serv on 3850
CSCvd40809	Traffic is not excluded from role-based permissions when enforcement is disabled on interface
CSCvd45069	Cisco IOS XE Wireless Controller Manager DoS Vulnerability
CSCvd45710	Crash seen in IOSXE-RP Punt Service Process
CSCvd45973	Catalyst 3850/3650 - memory leak in platform_mgr process
CSCvd53514	RF channel change not working on 3850
CSCvd53780	Line Protocol on 10G interfaces (on NM modules) may flap on 3850 mGig models
CSCvd66543	Access-session commands can never be removed from port
CSCvd67113	3850 stack startup config sometimes disappear after power cycle

Identifier	Description
CSCvd80714	High CPU Usage on 3850 running Polaris when it received ipv4 packets with options
CSCvd85770	StackWise Virtual 3850-48X MEC switchover traffic black holing
CSCve00087	Line-by-Line sync verifying failure on command: client test01 server-key 0 Password
CSCve30446	User intermittently blocked from local login to WebUI (wrong credentials) 3850
CSCve30905	Nginx Crash when Accessing webui.
CSCve31547	ICMP Time exceed dropped due to uRPF on the MPLS PE (per-ce label) [PE-CE is eBGP]
CSCve44523	%OSAPI-4-TIME_SHIFT_DETECTED: 1 wcm: Detected forward time shift
CSCve47887	Crash in CEF: IPv4 process on Catalyst 3850 and 3650
CSCve54313	Crash in ALPS SNMP code
CSCve56006	FIB has extra prefix when BGP and OSPF receive the same route
CSCve57788	Web authentication clients do not receive redirect URL and HTTP Intercept, Invalid appl_id error smd
CSCve59027	16.3.3 SV stack sometimes results in unpredictable switchover after a few days of operation
CSCve61344	DHCP NAK is observed with Rebind request
CSCve66658	Crash in TN3270E-RT-MIB code
CSCve82129	Different behavior seen in DHCP Init Reboot scenario
CSCve90164	Observing incorrect server state in BINOS
CSCvf01501	NBAR data-plane crash for DNS TXT query with an additional record
CSCvf03228	3850 Denali Wireshark fails to start after stack master switchover
CSCvf05494	Traffic shaping not working with percent command
CSCvf14321	RRM LOG: Radio Resource Management: RRM Import Packet error. Received from 0.0.0.0 length 0 0
CSCvf19274	Observing memory leaks in AAA_MALLOC_LITE after scale test
CSCvf29760	3850 crash with "IOSXE_INFRA-4-NO_PUNT_KEEPALIVE" when mgmt port down/not connected
CSCvf38644	Access-session CLI missing and config-sync error on reload/switchover
CSCvf39811	[IOS] Evaluation of CVE-2017-7529 (NGINX) for IOS Software
CSCvf45112	[AVC]context with name longer than 15 chars assignment fails
CSCvf58092	SV:G48: fail to route pkts when data port and SVL are on same asic and core
CSCvf65643	Unicast ping stops working when "ip pim sparse-mode" removed from SVI
CSCvf69507	Perpetual poe + Fast Poe doesn't work for CREE ONLY with latest firmware
CSCvf71734	Custom Nbar protocol is classifying traffic incorrectly.
CSCvf79882	CREE Light goes to Low Power mode immediately after boot up and stays in low power mode.

Resolved Caveats in Cisco IOS XE Denali 16.3.3

Identifier	Description
CSCvc24401	Downlink port LEDs display green without plugging anything in the port
CSCvc88106	Entropy exhaustion leading to IOSd Crash on Standby Switch with FIPS enabled
CSCvc54604	Unable to configure MACSec and port-channel with IP Base license
CSCvc39894	LOOP packets still can be seen when "no keepalive" configured
CSCvb24904	Port-channel flapping causing REP topology failure in 10 seconds
CSCuy21545	QinQ and L2PT do not work as expected on 3850 and 3650 switches
CSCvc48659	Unicast flooding after rep topology changed
CSCvc90507	Memory leak under fed main event due to multicast
CSCvc51326	port-security // restrict // does not filter traffic after shutdown/no shutdown
CSCvc06109	3650 1G/10G SFP link down if only remove SFP Tx cable
CSCvc57865	3850 stack port use SFP-10G-LR became suspend after show command and stack switchover
CSCvc44041	CRC Errors on Uplink interface of WS-C3650-24PDM & WS-C3650-48FQM-S.
CSCux63166	"no service password-recovery" is seen after reload of 3850
CSCvb65304	Output drops and Output errors increment simultaneously in show interfaces
CSCvb05512	3850 EPC failing under increased CPU load
CSCuz43112	EFP deleted when unconfig otv overlay interface and then config back
CSCvc44133	Polaris 3850 EAP identity response for dot1x NPS client not been processed
CSCvc74968	3850 "snmp-server queue-length" Value Back to Default 10 after Reload
CSCuz97232	3850 SNMP timesout or large delays when polling certain MIBs
CSCva37722	ISG Accounting Accuracy is not worked on disconnecting PPP from client
CSCvb70028	Unable to Access internal-webauth login page when client associated with AIR-AP2802I-B-K9 AP
CSCvc17979	Polaris 16.3.2 wireless PEAP clients fail to auth in NPS if ap link-encryption
CSCvb99355	"wireless management interface" command not disabling mobility agent in 3650
CSCvb95657	Auto-QoS configured wlan, policy validation fails after performing "sh/no sh" on wlan multiple times
CSCvb89106	webui swichview issue : port no. 49-50 as downlink port

Resolved Caveats in Cisco IOS XE Denali 16.3.2

Identifier	Description
CSCvb56482	Autoinstall/ PnP fails - from 16.3.1/ 16.3.1a to 16.3.2; wrkaround: use router as DHCP server.
CSCuz33679	Cat3850: REP LSL PDU counter up on shut down interface

Identifier	Description
CSCva17300	REP Multicast Traffic does not resume after neighbor switch reloaded
CSCva17341	REP Multicast packet loss for 10+seconds during re-convergence
CSCva54058	REP, what will happen when BPA or EPA is lost, TAC SR#680354116
CSCva61031	SVI Ping fails after HA-SSO during REP Topology change
CSCva79145	REP packet drop after 3rd SSO on one of the nodes
CSCvb81117	Cat3850: REP LSL PDU counter incrementing when link is in down state (remote end)
CSCux14425	ACL matching IP option is not working with "no ip unreachables"
CSCva08676	after deleting flex link config, LED of backup port still shows amber
CSCva46457	c3850 stack crash with static mac-address map'd to multiple port-channel
CSCva65105	Cat3650 Stack: specific vlan down when swithcover
CSCva10757	Invalid MAC learning in private VLAN for static MAC addresses
CSCva51684	Ping to SVI fails after breaking link in REP Ring on 3850
CSCuz28295	TCN generate late and mac learn issue on 3650 stack after RSTP TCN
CSCuz98374	3850 incorrectly set more-fragment flag for double fragmentation
CSCuz88403	3850stack stops forward traffic via GRE tunnel after master turning off
CSCuz83883	IPv6 neighbor discovery packet processing behavior
CSCuz11169	High memory utilization observed on catalyst 3650/3850
CSCva69776	PEAP clients cannot get authenticated with NPS server on 16.3.1
CSCuv75864	"octeon_wdt: WDT device closed unexpectedly " error msgs on reload
CSCus49022	Active switch crashes on changing STP mode from RSTP to PVST w/ 128vlans
CSCuu38981	crash observed on high rates of roam @ fman_qos_mark_aom_free
CSCuy19562	3850/3650 intercepts telnet/ssh connections for unknown destinations
CSCva71996	CLNS ping failing to 3850
CSCvb17094	Disable Tunnel IPIP CLI as feature not supported on NG3K
CSCvb49347	NGWC ipsec vpn only support "IPv4 GRE" tunnel mode
CSCuw38877	Static IGMP join-group on VLAN interface is not reachable
CSCva25392	forward trap is generated when shutdown by storm control
CSCuz65463	Storm-control is not working after Cat3850 reload
CSCuz05771	3850 Last reload reason: "Power Failure" when reloaded due to OOM
CSCuw69829	WebUI: Not able to contain rogue AP's using webUI
CSCva33039	"show env rps" display wrong RPS state
CSCuz60623	"snmp-server enable traps transceiver all" is recorded twice.
CSCuz71966	"speed auto 10 100" disappeared from show run after reload
CSCuw41152	'%NGWC_PLATFORM_FEP-1-FRU_PS_SIGNAL_FAULTY' message is not output
CSCup05919	3850 - Power given, but State Machine Power Good wait timer timed out
CSCuz50876	3850 Denali 16.1.1 - Bootflash is missing from system-report
CSCva15754	AC power supply still display OK state even if RPS is providing power

Identifier	Description
CSCva00967	After OIR USB flash on C3850, no trap and syslog output
CSCva13231	CRC/Corrupted packets after a link failure with MACSEC and 802.1q (3850)
CSCva43372	Interoperability - remote side CRC error
CSCva25015	Mode button functionality not working Intermittently
CSCuz08086	PD's not getting PoE on multiple interfaces in 3850 stack
CSCuy97043	Remove invalid data cefcModuleAdminStatus MIB from 3850/3650 switch platform
CSCva69778	Wrong temperature syslog OVERTEMP severity level in 3850
CSCuy70475	Latency increases with low priority background traffic
CSCuz05208	Wireless mobility client data tx via macsec uplink 3850 foreign is drop
CSCuz94565	fqdn acl bypass not taking effect intermittently
CSCva13738	ISR4k dose not send SOLICIT msg in DHCPv6-PD over PPPoE
CSCux98943	Padding for PPPoE over ATM should not be added for accounting
CSCuz17963	plogd tracelogs getting generated causing high cpu in plogd process
CSCuz33638	%IOSXE-4-PLATFORM: R0/0: kernel: EXT2-fs warning:
CSCuz30182	ASR1013: Fails to detect power supply at startup
CSCva90588	Xchassis keeps reloading after installing an RP2 with an old CPLD
CSCuz88340	AN: ULA is configured on ANI & same ANI used for multiple neighbors
CSCva36556	Smart call home crash with debugs enabled
CSCva08096	hostname cannot be retrieved
CSCuz65251	All the UP interfaces displayed as DOWN after wr erase and reload
CSCux60876	Memory corruption due to DHCP
CSCva32903	Tracebacks seen while testing DHCP functionality
CSCuz39061	"logging filter ...tcl" config crashes the router
CSCux99594	EEM Policies May Not Be Able To Send Email
CSCuz81292	IPv6 neighbor discovery packet processing behavior
CSCuv24653	ENH: Specify SSL/TLS Version for HTTP secure-server Feature
CSCuz69005	AP unable to join due to pending destroy IFID state
CSCuz12475	Polaris: fman_rp crash occurs with bgp_pic profile
CSCuu77403	%LINK-4-TOOBIG Messages Seen on ISR 3945 with L2TPv3
CSCur47235	When one vrf deletes with "no vrf definition", ip vrf receive is removed
CSCva15526	PW down after clear mpls ldp neighbor followed by RSP SSO
CSCva17339	LDP session stuck in established with no TCP connection
CSCuz95908	Memory leak due to path querry with Null outgoing interface
CSCva44687	ASR 1K Running IOS-XE 3.16S w/ MPLS Crashes on 'clear ip route *'
CSCva64489	1810w - Invalid Number of supported Power Levels: 0
CSCux09478	sh proc mem platform sorted output is incorrect with low free memory
CSCva56329	DMI - AAA authentication/authorization timeout does not try fallback

Identifier	Description
CSCuz41275	Crash seen with SMD tracing in verbose mode
CSCuy34177	Need 5508 to support sleeping client as single Anchor with NGWC
CSCuz58624	CGM Traceback observed impacting client connectivity
CSCuy16530	Crash after member link re-added to port-channel and clear counters CMD
CSCuu13476	Cisco IOS & IOS XE Software OpenSSH TCP Denial of Service Vulnerability
CSCuu11760	NG3k-QOS: Need to block priority percent command in policy-map
CSCuv92031	Track SNMP Transceiver Sensor Implementation
CSCuw12882	Improper Reporting of FEPs on 3650 with 3.06.01E and others
CSCuw90273	Cannot telnet/ssh(Sessions max out)
CSCuy37943	perpetual POE on per port is working as global command
CSCuz01059	Implement SXP path length override option to limit the SXP database size
CSCuz10706	Infinity: Image name will need to be changed to not have Cisco reference
CSCuz39384	CSCuz10706Upgrade MCU in Amur without changing other silent roll packages
CSCuz39783	Polaris 16.3 :"session port shut-down and session cleared"via COA failed
CSCuz42283	Remove the build path from %IOSXE-3-PLATFORM: R0/0: kernel: logs
CSCuz96994	MAG to MAG, Host to remote MAG ping fail with ISR4000 PMIPv6
CSCva00632	Switch not forwarding traffic after applying the policy-map
CSCva06274	Polaris 163:CPP crash with SGT caching and SGACL interop
CSCva07535	AWS : CSR Crashed after copying config file using kron-policy
CSCva12002	Polaris:DACL entries in ACL LE present for unauth sessions
CSCva20123	ERSPAN pkts not received at destination after source sw reload
CSCva27128	AAA Proxy authentication fail with group TACACS-SERVER, local
CSCva32407	RLDP config does not get saved on reboot or upgrade
CSCva62445	ip tcp adjust-mss is not supported on 3850/3650; it should be removed
CSCva63982	1832 error :Invalid Power Level Index 7. Should be in [1,5]
CSCva69559	Theon system noisy after booting IOS
CSCva72088	3802 AP on CA, link-encryption DS/US stats show 0
CSCva92486	polaris : Getting SOA response for unconfigured SOA record/domain
CSCva98140	Secure Fabric, issuing "show fabric host-pool" is crashing box on C3850
CSCvb05894	Backout CSCux99594 EEM Policies May Not Be Able To Send Email
CSCvb56934	Commit to 3.7.x and 16.3.x Zero RX counters on te1/1/3 port on bootup
CSCvd96372	Stack reloading with Last reload reason: Critical process wcm fault on rp_0_0 (rc=133)

Resolved Caveats in Cisco IOS XE Denali 16.3.1a

The following are the resolved caveats in Cisco IOS XE Denali 16.3.1a. Click on the identifier to view the details of a caveat in the BST.

Identifier	Description
CSCvb29204	BenignCertain on IOS and IOS-XE
CSCvb01730	Leapsec 3.10.7: deadlock test causes wdog timeout - rtr crashes
CSCvb19326	NTP leap second addition is not working during leap second event
CSCvb04298	NTP-PTP: Invalid PTP time during NTP leap second insertion/deletion

Resolved Caveats in Cisco IOS XE Denali 16.3.1

The following is the list of Cisco IOS XE Denali 16.1.x and Cisco IOS XE Denali 16.2.x caveats that are resolved in Cisco IOS XE Denali 16.3.1. Click on the identifier to view the details of a caveat in the BST.

Identifier	Description
CSCuw98808	Empty VLAN ACL sequence with no match causes STP issues
CSCul84467	C3850:Stack:Port-Channel:active mem switch power shut causes traffic loss
CSCuw94814	IEEE8023-LAG-MIB does not work use CISCO-LAG-MIB
CSCuw56706	LACP with 16 ports: after switchover, ports in H state change to D state
CSCuw38877	Static IGMP join-group on VLAN interface is not reachable
CSCux25383	Passwords still encrypted after encryption key is removed
CSCuw69672	WebUI: ACL - "any" option for mask not disabled when it is not supported
CSCux23861	WebUI: Few scenarios - refreshing issue related to AP with 11AC module
CSCux62751	Memory leak seen @ dup_classmap_runtime
CSCux35552	Error on editing RogueRule on user configured SSID
CSCuz20613	IOS-XE : Shell license bypass via LXC (2)
CSCuy06768	Secure LDAP with wired 1k dot1x sessions may reload the system
CSCux35423	TACACS mgmt over wireless not working
CSCux22276	vlan pooling-static ip client is not passing traffic for wireless dot1x
CSCuv47300	CTS: In loopback interface, config of IP SGT map should not be allowed
CSCux89701	CFD QMUL: session comes up after port-security violation
CSCux26381	Match based on username fails for dot1x client with Native Profile WLAN
CSCuy04948	Reauth timer running for unauthorized case
CSCuy21768	Session fails authz after few vlans in group brought down and up
CSCux77357	stuck Session with 0 Mac 0 IP not removed from admission cache output
CSCuy32871	WS-C3850-48XS:'sh inventory FRU' lists fan even after removal/failure
CSCuz11169	High memory utilization observed on catalyst 3650/3850
CSCuw94595	Tracebacks on bootup at "epm_vlan_name_insert_or_delete" w/200+ VLANs
CSCuu38981	crash observed on high rates of roam @ fman_qos_mark_aom_free
CSCuz88340	AN: ULA is configured on ANI & same ANI used for multiple neighbors

Identifier	Description
CSCuy75068	System traceback while Smart Call Home debugs turned on
CSCuz65251	All the UP interfaces displayed as DOWN after wr erase and reload
CSCuy34177	Need 5508 to support sleeping client as single Anchor with NGWC
CSCuy79779	AP flaps for 30 minutes upon changing AP mode after SSO
CSCuy39207	PI3.1 voice diagnostics SNMP GET not working

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

http://www.cisco.com/en/US/support/index.html

Choose **Product Support > Switches**. Then choose your product and click **Troubleshoot and Alerts** to find information for the problem that you are experiencing.

Related Documentation

- Cisco IOS XE Denali 16.x.x documentation at this URL:

  http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html
- Catalyst 3850 switch documentation at this URL:

  http://www.cisco.com/go/cat3850_docs
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes at this URL:

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- Cisco Validated Designs documents at this URL:

  http://www.cisco.com/go/designzone
- Error Message Decoder at this URL:

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Obtaining Documentation and Submitting a Service Request

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/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation*, which lists all new and revised Cisco Technical documentation, as an RSS feed and deliver content directly to your desktop using a read application. The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2020 Cisco Systems, Inc. All rights reserved.