



What's New in Cisco IOS XE Dublin 17.12.x

- [Hardware Features in Cisco IOS XE Dublin 17.12.3, on page 1](#)
- [Software Features in Cisco IOS XE Dublin 17.12.3, on page 1](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3, on page 1](#)
- [Hardware Features in Cisco IOS XE Dublin 17.12.2, on page 1](#)
- [Software Features in Cisco IOS XE Dublin 17.12.2, on page 2](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2, on page 2](#)
- [Hardware Features in Cisco IOS XE Dublin 17.12.1, on page 2](#)
- [Software Features in Cisco IOS XE Dublin 17.12.1, on page 3](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1, on page 6](#)

Hardware Features in Cisco IOS XE Dublin 17.12.3

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.3

There are no new software features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.2

There are no new hardware features in this release.

Software Features in Cisco IOS XE Dublin 17.12.2

Feature Name	Description
ASAc Firewall-Application Hosting	Application hosting Infrastructure on Cisco Catalyst 9300 series switches can now host Cisco Adaptive Security Virtual Appliance (ASAc) Firewall for stateful inspection of traffic in a network without changing the network architecture. This allows to seamlessly add firewall services to the existing network.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2

There are no behavior changes in this release.

Hardware Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
Cisco QSFP28 to SFP28 Adapter Module on Cisco Catalyst 9300X Series Switches	Supported transceiver module product number: <ul style="list-style-type: none"> • CVR-QSFP28-SFP25G Compatible switch models: <ul style="list-style-type: none"> • C9300X-12Y • C9300X-24Y • C9300X-48HX • C9300X-48TX • C9300X-24HX

Software Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
BGP EVPN VXLAN <ul style="list-style-type: none"> • ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs) • BGP EVPN VRF Auto RD and Auto RT 	<p>The following BGP EVPN VXLAN features are introduced in this release:</p> <ul style="list-style-type: none"> • ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs): BGP EVPN VXLAN fabric now supports ARP inspection and DHCP Rogue Server Protection. To configure these features, enable ARP inspection and DHCP Snooping on the VTEPs of the EVPN VXLAN fabric. • BGP EVPN VRF Auto RD and Auto RT: BGP EVPN Layer 3 overlay VRF configuration is simplified with the introduction of new CLIs to auto generate the route distinguisher (RD) and route target (RT) for a VRF. <p>You can enable the auto generation of RD either at a global level, using the vrf rd-auto command or specifically for a VRF, using the rd-auto [disable] command in the VRF submenu.</p> <p>To enable auto assignment of RT for a VRF, use the vniid vni-id command in the VRF submenu.</p> <p>You can also choose to disable the auto RD and RT features by using the no form of the command.</p>
DSCP marking for RADIUS packets for administrative sessions	Allows you to configure DSCP marking for RADIUS packets for administrative sessions such as SSH and Telnet.
EPC support of AppGigabitEthernet	Introduces support for configuring the AppGigabitEthernet port as an interface for Embedded Packet Capture (EPC).
Interface ID Option in DHCPv6 Relay Message	Introduces support for interface ID option in DHCPv6 Relay message. With this, the physical interface details of the client interface are included along with the VLAN number in the message.
Interface Template Support for IPv6 DHCP Guard	Enables you to add the ipv6 dhcp guard attach-policy policy_name global configuration command to an interface template. IPv6 DHCP Guard is then enabled and the policy is applied, wherever the template is applied.
IP DHCP Server Changes to Limit IP Assignment to Next Hop only	Allows you to assign DHCP IP address only to the neighbouring device in an interface using the ip dhcp restrict next hop command. When this command is enabled, the DHCP server in the interface uses the MAC addresses in the DHCP packet and compares it with the addresses in the Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) cache table. If the MAC addresses match, then the DHCP IP address is assigned to that device.

Feature Name	Description
Modified Trustpoints for Secure Unique Device Identity (SUDI) Certificates	

Feature Name	Description
	<p>Starting from Cisco IOS XE Dublin 17.12.1, the following changes have been introduced for trustpoints.</p> <ul style="list-style-type: none"> Trustpoint names for existing SUDI certificates <p>If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows.</p> <ul style="list-style-type: none"> For <i>Cisco Manufacturing CA III</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI For <i>Cisco Manufacturing CA SHA2</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI <p>If your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled using no platform sudi cmca3 command, the trustpoint names are as follows.</p> <ul style="list-style-type: none"> For <i>Cisco Manufacturing CA SHA2</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI For <i>Cisco Manufacturing CA</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI Hardware SUDI certificates <ul style="list-style-type: none"> If your device supports <i>High Assurance SUDI CA</i> certificate, this certificate is loaded under CISCO_IDEVID_SUDI trustpoint. If your device does not support <i>High Assurance SUDI CA</i> certificate, <i>ACT2 SUDI CA</i> certificate is loaded under CISCO_IDEVID_SUDI trustpoint. show wireless management trustpoint command output <p>If Cisco Catalyst 9300 Series Switch is used with a Cisco Embedded Wireless Controller for wireless deployments, the trustpoint name in the output of show wireless management trustpoint command is updated to the modified trustpoint name as mentioned previously.</p> <p>The following example shows a sample output of show wireless management trustpoint command. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the Trustpoint Name in the below output displays CISCO_IDEVID_CMCA2_SUDI.</p> <pre>Device# show wireless management trustpoint Trustpoint Name : CISCO_IDEVID_CMCA3_SUDI Certificate Info : Available Certificate Type : MIC Certificate Hash : <SHA1 - hash> Private key Info : Available FIPS suitability : Not Applicable</pre> show ip http server status command output <p>If you configure the trustpoint for the HTTP server as CISCO_IDEVID_SUDI, the output of show ip http server status command displays the operating trustpoint along with the configured trustpoint.</p> <p>The following example shows a sample output of show ip http server status command with</p>

Feature Name	Description
	<p>both the configured and the operating trustpoint names. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the operating trustpoint in the below output displays CISCO_IDEVID_CMCA2_SUDI.</p> <pre>Device# show ip http server status ... HTTP secure server trustpoint: CISCO_IDEVID_SUDI HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI</pre>
Programmability: <ul style="list-style-type: none"> • NETCONF-SSH Algorithms • YANG Data Models 	The following programmability features are introduced in this release: <ul style="list-style-type: none"> • NETCONF-SSH Algorithms: The NETCONF-SSH server configuration file contains the list of all supported algorithms. From this release onwards, you can enable or disable these algorithms at runtime by using Cisco IOS commands or YANG models. • YANG Data Models: For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/17121.
request tech-support command	The request tech-support command was introduced. It generates an archive of tech support file and system report.
show idprom tan command	The show idprom tan command was introduced. It displays the top assembly part number and top assembly part revision number for the identification programmable read-only memory.

New on the WebUI

There are no new WebUI features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1

Behavior Change	Description
BDPU Guard and Root Guard Syslogs	The BDPU guard and root guard syslogs have been modified to include client bridge ID information.
system env fan-fail-action shut command	The expected behavior of the system env fan-fail-action shut command is fixed. When the command is enabled, the device automatically shuts down if more than one fan stops working or are removed.