# Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Dublin 17.11.x

**First Published:** 2023-04-06

## Full Cisco Trademarks with Software License

## About Cisco 1000 Series Integrated Services Routers

The Cisco 1000 Series Integrated Services Routers (also referred to as router in this document) are powerful fixed branch routers based on the Cisco IOS XE operating system. They are multi-core routers with separate core for data plane and control plane. There are two primary models with 8 LAN ports and 4 LAN ports. Features such as Smart Licensing, VDSL2 and ADSL2/2+, 802.11ac with Wave 2, 4G LTE-Advanced and 3G/4G LTE and LTEA Omnidirectional Dipole Antenna (LTE-ANTM-SMA-D) are supported on the router.

**Note** Cisco IOS XE Dublin 17.11.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE Dublin 17.11.x release series.

**Note** Starting with Cisco IOS XE Amsterdam 17.3.2 release, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following:

- Cisco Smart Software Manager (CSSM),
- Cisco Smart License Utility (CSLU), and
- Smart Software Manager On-Prem (SSM On-Prem).

## Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

# New and Changed Hardware and Software Features

## New and Changed Software Features

*Table 1: New Software Features*

| Feature | Description | | |
|---|---|---|---|
| Deprecation of Weak Ciphers | The minimum Rivest, Shamir, and Adleman (RSA) key pair size must be 2048 bits. The compliance shield on the device must be disabled using the **crypto engine compliance shield disable** command to use the weak RSA key. | | |
| Enabling the RSRP and RSRQ Parameters for Link Recovery on LTE Modems | This feature enables the RSRP (Reference Signal Received Power) and RSRQ (Reference Signal Received Quality) parameters that detect any network issues or malfunctions as part of the link-recovery feature on LTE modems.<br>To enable these parameters, the user can configure the **lte modem link-recovery rsrp onset-threshold** command for RSRP and **lte modem link-recovery rsrq onset-threshold** command for RSRQ. | | |
| Flex Support on Layer 2 and Layer 3 Ports | This feature enables the flex Layer 2 and Layer 3 capability in the Layer 2 switch ports of the Cisco 1000 Series Integrated Services Routers (ISRs). This allows to add more Layer 3 WAN ports on the device by configuring the last two Layer 2 switch ports to Layer 3 WAN ports using the **no switchport** command.<br>For more information, see Cisco IOS Interface and Hardware Component Command Reference. | | |
| Profile Clean-up on LTE Modems Using Factory Reset Button | To clean the cellular modem completely, users can press the physical factory-reset button on the device, which enables the inbuilt **lte cellular-profile-cleanup** command to erase the configuration setup and profiles. This command is disabled by default, but can be enabled only when the factory-reset button is pressed. | | |

| Feature | Description | | |
|---|---|---|---|
| Redirecting Deprecated LISP Commands to Revised Versions | The following LISP commands have been revised: | | |
| | Old Command | | New Command |
| | **show ip/ipv6 lisp all** | | **show lisp service ipv4/ipv6** |
| | **show ip/ipv6 lisp instance-id alt** | | **show lisp instance-id ipv4/ipv6 alt** |
| | **show ip/ipv6 lisp instance-id database** | | **show lisp instance-id ipv4/ipv6 database** |
| | **show ip/ipv6 lisp forwarding** | | **show lisp ipv4/ipv6 instance-id forwarding** |
| | **show ip/ipv6 lisp instance-id** | | **show lisp instance-id** |
| | **show ip/ipv6 lisp locator-table** | | **show lisp locator-table** |
| | **show ip/ipv6 lisp instance-id map-cache** | | **show lisp instance-id ipv4/ipv6 map-cache** |
| | **show ip/ipv6 lisp instance-id route-import** | | **show lisp instance-id ipv4/ipv6 route-import** |
| | **show ip/ipv6 lisp instance-id smr** | | **show lisp instance-id ipv4/ipv6 smr** |
| | **show ip/ipv6 lisp instance-id statistics** | | **show lisp instance-id ipv4/ipv6 statistics** |
| | **show lisp site** | | **show lisp server** |
| | **show lisp site detail** | | **show lisp instance-id ipv4/ipv6 server detail** |
| | **show lisp site name** | | **show lisp instance-id ipv4/ipv6 server name** |
| | **show lisp site summary** | | **show lisp instance-id ipv4/ipv6 server summary** |
| | **show lisp site rloc** | | **show lisp instance-id ipv4/ipv6 server rloc** |
| **Cube Features** | | | |
| Unified SRST: Concurrent use of Webex Calling Survivability Gateway and Unified SRST | From Cisco IOS XE Dublin 17.11.1a onwards, concurrent use of Cisco Webex Calling Survivability Gateway and Unified SRST is supported on the same router. | | |
| **Smart Licensing Using Policy Features** | | | |

| Feature | Description | | |
|---|---|---|---|
| Snapshots for Product Activation Key (PAK) licenses | Starting with Cisco IOS XE Dublin 17.11.1a, the PAK-managing library is discontinued and the provision to take a snapshot is no longer available. Software images from Cisco IOS XE Dublin 17.11.1a onwards rely only on the snapshotted information about PAK licenses. For more information, see: Snapshots for PAK Licenses.<br><br>If you have a PAK license without a snapshot, and you want to upgrade to Cisco IOS XE Dublin 17.11.1a or a later release, you will have to upgrade twice. First upgrade to one of the releases where the system can take a snapshot of the PAK license and complete DLC, and then again upgrade to the required, later release. | | |

**Note** From Cisco IOS XE Release 17.9.1a, guestshell is removed from the IOS XE software image. As a result, Zero Touch Provisioning (ZTP) python script is no longer supported on Cisco 1000 Series Integrated Services Routers. If you need to use guestshell, then download it from https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloads. For more information, see Guestshell installation procedure.

## Cisco ISR1000 ROMmon Compatibility Matrix

The following table lists the ROMmon releases supported in Cisco IOS XE 16.x.x releases and Cisco IOS XE 17.x.x releases.

**Note** To identify the manufacturing date, use the **show license udi** command. For example:

```
Router#show license udi
UDI: PID:C1131-8PLTEPWB,SN:FGLxxxxLCQ6
```

The xxxx in the command output represents the manufacturing date.

- If the manufacturing date is greater than or equal to 0x2535, the manufactured ROMmon version is 17.6(1r) or higher.
- If the manufacturing date is less than 0x2535, the ROMmon will be automatically upgraded to 17.5(1r) or above when the Cisco IOS XE 17.9.x release is installed.
- The minimal or recommended ROMmon version for devices using Cisco IOS XE 17.5 or later is 17.5(1r) or later.

**Note** To upgrade to Cisco IOS XE Dublin 17.11.x, follow these steps:

1. If you are on a device that is running software version between Cisco IOS XE 16.x to Cisco IOS XE 17.4.x, upgrade to any IOS XE image between Cisco IOS XE 17.5.x to Cisco IOS XE 17.10.x.
2. After performing step a, upgrade to Cisco IOS XE 17.11.x.
3. For devices that are running on software version Cisco IOS XE 17.5.x or later, you can upgrade to Cisco IOS XE 17.11.x directly.

*Table 2: Minimum and Recommended ROMmon Releases Supported on Cisco 1000 Series Integrated Services Routers*

| Cisco IOS XE Release | Minimum ROMmon Release for IOS XE | Recommended ROMmon Release for IOS XE |
|---|---|---|
| 16.6.x | 16.6(1r) | 16.6(1r) |
| 16.7.x | 16.6(1r) | 16.6(1r) |
| 16.8.x | 16.8(1r) | 16.8(1r) |
| 16.9.x | 16.9(1r) | 16.9(1r) |
| 16.10.x | 16.9(1r) | 16.9(1r) |
| 16.11.x | 16.9(1r) | 16.9(1r) |
| 16.12.x | 16.9(1r) | 16.12(1r) |
| 17.2.x | 16.9(1r) | 16.12(1r) |
| 17.3.x | 16.12(2r) | 16.12(2r) |
| 17.4.x | 16.12(2r) | 16.12(2r) |
| 17.5.x | 17.5(1r) | 17.5(1r) |
| 17.6.x | 17.5(1r) | 17.5(1r) |
| 17.7.x | 17.5(1r) | 17.5(1r) |
| 17.8.x | 17.5(1r) | 17.5(1r) |
| 17.9.x | 17.5(1r) | 17.5(1r) |
| 17.10.x | 17.5(1r) | 17.5(1r) |
| 17.11.x | 17.5(1r) | 17.5(1r) |

# Resolved and Open Bugs in Cisco IOS XE 17.11.x

## Resolved Bugs in Cisco IOS XE 17.11.1a

*Table 3: Resolved Bugs in Cisco IOS XE 17.11.1a*

| Bug ID | Description |
|---|---|
| CSCwd47940 | PMTU discovery is not working after interface flap. |
| CSCwd65945 | LR interface which has NAT enabled is chosen for webex traffic. |
| CSCwc79115 | Policy commit failure notification and alarm from vsmart. |
| CSCwd16559 | ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table. |
| CSCwd67198 | uCode crash seen on device after stopping NWPI trace. |
| CSCwe28204 | Control connection over L3 TLOC extension failing as no NAT table entry created. |
| CSCwe24210 | SNMP MIB does not show correct firmware version for LTE module. |
| CSCwd89012 | Tested flap-based auto-suspension - Minimum duration value - no results as expected. |
| CSCwe29430 | Critical process fpmd fault on rp_0_0 (rc=134). |
| CSCwd79089 | Device crash when sending full line rate of traffic with >5 Intel AX210 stations. |
| CSCwd87195 | NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support. |
| CSCwd81357 | QoS classification not working for DSCP or ACL + MPLS EXP. |
| CSCwc99823 | FMAN crash seen in SGACL@ fman_sgacl_calloc |
| CSCwd44439 | Device crashing at fman_sdwan_nh_indirect_delete_from_hash_table |
| CSCwd67654 | FnF stats are getting populated with unknown in egress/ingress interface in VPN0. |
| CSCwd34941 | NAT configuration with no-alias option is not preserved after reload. |
| CSCwc72588 | Device should not allow weak cryptographic algorithms to be configured for IPsec. |
| CSCwd25107 | Interface VLAN1 placed in shutdown state when configured with **ip address pool**. |
| CSCvx89305 | When cellular drops during PnP it never comes back. |
| CSCwe00946 | System crash after disabling endpoint-tracker on tunnel interfaces. |
| CSCwe18058 | Unexpected reload with IPS configured. |
| CSCwd61255 | Data Plane crash on device when making per-tunnel QoS configuration changes with scale. |
| CSCwe01015 | IKEv2/IPSec - phase 2 rekey failing when peer is behind NAT. |

| Bug ID | Description |
|---|---|
| CSCwd85580 | Unexpected reload after set **ospfv3 authentication null** command. |
| CSCwd17272 | UTD packet drop due to fragmentation for ER-SPAN traffic. |
| CSCwe27241 | NBAR classification error with custom app-aware routing policy. |
| CSCwc37465 | Unable to push "no-alias" option on static NAT mapping from management system. |
| CSCwc67625 | OU field is deprecated from CA/B Forum certificate authorities. |
| CSCwe33793 | Memory allocation failure with extended entireplay enabled. |
| CSCwe23276 | Change in the IPsec integrity parameters breaks the connectivity. |
| CSCwd46921 | Device is not connecting to second vSmart after both assigned vSmart is down. |
| CSCwe34808 | FMAN FP leak due to the punt-policer command. |
| CSCwd12330 | Invalid TCP checksum in SYN flag packets passing through router. |
| CSCwd30578 | Wired guest client stuck at IP_LEARN with dhcp packets not forwarded out of the foreign to anchor. |
| CSCwe60059 | Crash when using dial-peer groups with STCAPP. |
| CSCwd15487 | Kernel crash is observed when modem-power-cycle is executed. |
| CSCwd56131 | LTE modem does not show GSM bands. |
| CSCwd38943 | GETVPN: KS reject registration from a public IP. |
| CSCwc68069 | RTP packets not forwarded when packet duplication enabled, no issue without duplication feature. |
| CSCwb59113 | BFD session gets NAT translated with static ip over dialer interface. |
| CSCwe03614 | CWMP: MAC address of ATM interface is not included in inform message. |
| CSCwb46968 | Device template attachment causes PPPOE commands to be removed from ethernet interface. |
| CSCwe19084 | NAT: Traffic is not translated to the same global address though PAP is configured. |
| CSCwe69783 | Device can lose its config during a triggered resync process if lines are in an off-hook state. |
| CSCwd71586 | BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash. |
| CSCwd14973 | Several devices rebooting with the reason 'Power On'. |
| CSCwc42978 | Device looses all BFD sessions with invalid SPI. |
| CSCwd33202 | DHCP behavior issue when BDI interface is enabled on WAN and SVI interface. |

| Bug ID | Description |
|---|---|
| CSCwd06923 | Stale IP alias left after NAT statement got removed. |
| CSCwc48427 | BFD issues with clear_omp -> non-PWK + non-VRRP scenario only. |
| CSCwd28593 | Control connection flap of assigned vSmart after shutting down other assigned vSmart. |
| CSCwe32862 | Router IOS-XE crash while executing AES crypto functions. |
| CSCwe25076 | ALG breaks NBAR recognition impacting application firewall performance. |
| CSCwd68994 | ISAKMP profile does not match as per configured certificate maps. |
| CSCwd79572 | FW policy with app-family rule with FQDN causes traffic drop for other sequences. |
| CSCwe20008 | SNMP MIB OID changing its last index. |
| CSCwe91988 | Need to disable CSDL compliance check for NPE images. |

### Open Bugs in Cisco IOS XE 17.11.1a

*Table 4: Open Bugs in Cisco IOS XE 17.11.1a*

| Bug ID | Description |
|---|---|
| CSCwd42523 | Same label is assigned to different VRFs. |
| CSCwd45508 | Device does not form BFD across serial link when upgrading. |
| CSCwd39219 | Device SMS archive does not work when FTP transaction is of VRF. |
| CSCwe52971 | BFD tunnels via Starlink remain in down state. |
| CSCwe49509 | Some BFD tunnel went down after migrating. |
| CSCwe37123 | Device uses excessive memory when configuring ACLs with large object groups. |
| CSCwe32827 | NIM-LTEA-EA module incorrectly shows "Profile 1 = INACTIVE*". |
| CSCwe19394 | Device may boot up into prev_packages.conf due to power outage. |
| CSCwe18276 | Route-map not getting effect when it is applied in OMP for BGP routes. |
| CSCwd68111 | Device object group called in ZBFW gives error after upgrade. |
| CSCwe49684 | BFD sessions keeps flapping intermittently. |

## Related Information

- Hardware Installation Guide
- Software Configuration Guide
- Smart Licensing using Policy

# Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

### Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

# Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

# Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.