Release Notes for Cisco Catalyst IR1101 Rugged Series Router - Release 17.3.1 through 17.3.4

First Published: 2021-08-03

Last Modified: 2023-05-01

Introduction

The Cisco Catalyst IR1101 Rugged Series Router is a next generation modular industrial router which has a base module with additional Pluggable Modules that can be added. The Pluggable Module provides the flexibility of adding different interfaces to the IR1101 platform, for example, a cellular module.

The IR1101 also has an Expansion Module that adds key capabilities such as dual LTE Pluggables, mSATA SSD FRU, SFP, and Digital GPIO connections.

Important These combined release notes provide information for Cisco IOS-XE Release 17.3.1 through Release 17.3.4. Cisco IOS-XE Release 17.3.5 was the first release that combined the IR1101 with other routing products.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

The Cisco Catalyst IR1101 Rugged Series Router is a next generation modular industrial router which has a base module with additional Pluggable Modules that can be added. The Pluggable Module provides the flexibility of adding different interfaces to the IR1101 platform, for example, a cellular module.

The IR1101 also has an Expansion Module that adds key capabilities to the IR1101, such as mSATA SSD FRU, Ethernet SFP port, and Digital GPIO connections. It also makes the IR1101 dual LTE capable, with one module in the base and the other in the expansion module.

Note The IR-1100-SP Expansion Module is the same as the IR-1100-SPMI module, without the Digital I/O and mSATA components.

Interface Naming Conventions

Port	Naming Convention
Gigabit Ethernet combo port	Gigabitethernet 0/0/0
Gigabit Ethernet SFP port on Expansion Module	Gigabitethernet 0/0/5
Fast Ethernet ports	Fastethernet 0/0/1-0/0/4
Cellular Interface on IR1101 Base	Cellular 0/1/0 and Cellular 0/1/1
Cellular Interface on Expansion Module	Cellular 0/3/0 and Cellular 0/3/1
Asynchronous Serial Interface	Async 0/2/0
USB	usbflash0:
mSATA	msata
IR1101 Base Unit Alarm input	alarm contact 0
GPIO on Expansion Module	alarm contact 1-4

Software Images for IoT Routers

Note You must have a Cisco.com account to download the software.

Cisco IOS-XE includes the following Cisco images:

Table 1: Software Images 17.3.1

Router	Image Type	Filename
IR1101	Universal	ir1101-universalk9.17.03.01.SPA.bin
	NPE	ir1101-universal9_npe.17.03.01.SPA.bin

Table 2: Software Images 17.3.2a

Router	Image Type	Filename
IR1101	Universal	ir1101-universalk9.17.03.02a.SPA.bin
	NPE	ir1101-universal9_npe.17.03.02a.SPA.bin

Table 3: Software Images 17.3.3

Router	Image Type	Filename
IR1101	Universal	ir1101-universalk9.17.03.03.SPA.bin
	NPE	ir1101-universal9_npe.17.03.03.SPA.bin

Table 4: Software Images 17.3.4

Router	Image Type	Filename
IR1101	Universal	ir1101-universalk9.17.03.04.SPA.bin
	NPE	ir1101-universal9_npe.17.03.04.SPA.bin

The latest software downloads for the Routers can be found at:

https://software.cisco.com/download/home/286319772/type

Click on the IR1101 link to take you to the specific software you are looking for.

New Features in Cisco IOS XE 17.3.1

Remote Docker Workflow

Remote Docker workflow is an alternative to traditional app deployment approaches that are using Local Manager or ioxclient tools. Remote Docker workflow is designed for developers, so we recommend that it is used only during application development and not on a production gateway.

You can find the Overview here:

https://developer.cisco.com/docs/iox/#!remote-docker-workflow

Yang Support for IO Ports

This feature increases the compatibility between the Command Line Interface and the Yang Model. Cisco IOS-XE Yang Data Models are found here:

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

Each release has a directory, and the 17.3.1 release is found under 1731. The two modules for Digital IO are Cisco-IOS-XE-digital-io-oper and Cisco-IOS-XE-digitalio.

The following are relevant IOS-XE CLI commands available:

Show Commands

show run

show alarm

show led

Configuration Commands

alarm contact attach-to-iox

no alarm contact attach-to-iox

alarm contact 1 enable enable

no alarm contact <1-4> enable

alarm contact <1-4> application <wet | dry>

no alarm contact <1-4> application

alarm contact <1-4> description <alarm description>

no alarm contact <1-4> description

alarm contact <1-4> severity <critical | major | minor | none>

no alarm contact <1-4> severity

alarm contact <1-4> threshold <1600-2700>

no alarm contact <1-4> threshold

alarm contact <1-4> trigger <closed | open>

no alarm contact <1-4> trigger

alarm contact <1-4> output <1 | 0>

alarm contact <1-4> output relay temperature <critical | major | minor>

alarm contact <1-4> output relay input-alarm <0-4>

no alarm contact <1-4> output

Support for Security-Enhanced Linux (SELinux)

Security-Enhanced Linux is a set of patches to the Linux kernel and some utilities to incorporate a strong, flexible mandatory access control (MAC) architecture into the major subsystems of the kernel. SELinux provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications.

SELinux enforces mandatory access control policies that confine user programs and system servers to the minimum amount of privilege they require to do their jobs. This reduces or eliminates the ability of these programs and daemons to cause harm when compromised (for example, via buffer overflows or mis-configurations). This confinement mechanism operates independently of the traditional Linux access control mechanisms.

The are no additional requirements or configuration steps required to enable or operate the SELinux feature. The solution is enabled/operational by default as part of the base IOS-XE software on supported platforms.

The following are enhanced show commands that have been defined for viewing SELinux related audit logs.

show platform software audit all

show platform software audit summary

show platform software audit switch <<1-8> | active | standby> <FRU identifier from a drop-down list>

Command Examples

The following is a sample output of the **show software platform software audit summary** command:

```
Device# show platform software audit summary

====================================
AUDIT LOG ON switch 1
------------------------------------
AVC Denial count: 58
====================================
```

The following is a sample output of the show software platform software audit all command:

```
Device# show platform software audit all

====================================
AUDIT LOG ON switch 1
------------------------------------
========== START ============
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
 tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc: denied { execute } for pid=8300 comm="sh"
name="id" dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
 tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
========== END ============

(output omitted for brevity)
```

The following is a sample output of the **show software platform software audit switch** command:

```
Device# show platform software audit switch active R0

========== START ============
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
 tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
```

```
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
========== END ============
====================================
```

Syslog Message Reference

Facility-Severity-Mnemonic

%SELINUX-3-MISMATCH

Severity-Meaning

ERROR LEVEL Log

Message Explanation

A resource access was made by the process for which a resource access policy is not defined. The operation was flagged but not denied.

The operation continued successfully and was not disrupted. A system log has been generated about the missing policy for resource access by the process as denied operation.

Recommended Action

Please contact CISCO TAC with the following relevant information as attachments:

The message exactly as it appears on the console or in the system log.

Output of "show tech-support" (text file)

Archive of Btrace files from the box using the following command ("request platform software trace archive target <URL>") For Example: Device# **request platform software trace archive target flash:selinux_btrace_logs**

Support Added for the P-LTEAP18-GL Modem PID

The P-LTEAP18-GL PID uses the Telit modem LM960 modem. Details about all of the IR1101 modems are found here:

https://www.cisco.com/c/en/us/td/docs/routers/access/1101/b_IR1101HIG/b_IR1101HIG_chapter_01.html#con_1161147

Initial Bootup Security Improvements

Enforce Changing Default Password

Previous software versions allowed the user to bypass setting a new enable password. When the device was first booted after factory reset or fresh from the factory, the following prompt is received on the console:

Would you like to enter the initial configuration dialog? [yes/no]:

Previous software versions allowed answering **no** and the device would drop to the **Router>** prompt with a blank enable password. At this point, the router could be configured and brought into service with a blank enable password.

In previous documentation, Cisco recommended using the **enable secret** command instead of the **enable password** command because this offers an improved encryption algorithm.

Starting with 17.3.1, the initial dialog has been changed to force setting a new enable password, and also using the **enable secret** command instead. The following is an example:

```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Router]: router-1

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: ********
Confirm enable secret: ********

The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images.
Enter enable password: **********

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: *********
Configure SNMP Network Management? [yes]: no

Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0

Configuring interface Ethernet0/0:
Configure IP on this interface? [yes]: no

The following configuration command script was created:
hostname router-1
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
.
.
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
.
.
router-1>en
```

```
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1

The following is an example of what happens if you answer no to the initial configuration
dialog:

Would you like to enter the initial configuration dialog? [yes/no]: no

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: ********
Confirm enable secret: ********

Would you like to terminate autoinstall? [yes]: yes

.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
```

After the enable secret is prompted during the first login, and the admin enters a password, the admin entered password will be always masked. If the admin enters a weak password, they will be prompted again to enter strong password (i.e. the standard mix of upper/lower case characters, special characters, numbers etc.). The prompting will continue until the admin enters a strong password. The admin will be prompted to enter the strong secret password twice for confirming that admin is sure that it is the secret that they want to configure.

Telnet and HTTP

There has been a change in the telnet and http boot configuration. When the device is first booted after factory reset or fresh from the factory, the following takes place:

- Disable telnet
- Disable http server. HTTP client works.
- Enable SSH
- Enable https server

Note This only applies to the IR1101, other IoT routers configuration remain the same.

New Features in Cisco IOS XE 17.3.2a

This release does not contain any new features. It is maintenance only.

New Features in Cisco IOS XE 17.3.3

Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy

SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM.

Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to push the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to pull the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem.

Minimum Required SSM On-Prem Version: Version 8, Release 202102

Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3

Note Starting with Cisco IOS XE Amsterdam 17.3.2, 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).

New Features in Cisco IOS XE 17.3.4

This release does not contain any new features. It is maintenance only.

Related Documentation

Cisco Catalyst IR1101 Rugged Series Router

IR1101 documentation landing page.

Product Independent Documentation

Cisco IOS XE 17.x

Cisco SD-WAN

Known Limitations

Release 17.3.1, 17.3.2a, 17.3.3 and 17.3.4

Downgrading from 16.12.1 to 16.11.1 x

Symptoms: If an IR1101 with RJ45 Gig0/0/0 WAN is downgraded from 16.12.1 to 16.11.1 *x* or earlier, it will cause the Gig0/0/0 to fail to come up because its media-type is set to **media-type sfp**. The problem occurs because 16.12.1 or later automatically selects the correct media-type of the Gig0/0/0 interface, while 16.11.1x and earlier does not have that capability.

Workaround: Specifically set the correct media-type for the Gig0/0/0 interface (e.g. media-type rj45) prior to any downgrade.

An IR1101 operating in SDWAN Controller-mode must not downgrade to Cisco IOS XE Release 17.1.1. This is not supported for SDWAN. Instead, use Cisco IOS XE Release 16.12.1.

Note Cisco IOS XE Release 16.12.1 supports separate Autonomous (non-SDWAN) and SDWAN Controller-mode images.

Starting with release 17.3.1, in order for FND to work on the IR1101, each certificate (used in the certificate chain) needs to be installed, including the root certificate.

Release 17.3.4

Downgrading from 16.12.1 to 16.11.1 x

Symptoms: If an IR1101 with RJ45 Gig0/0/0 WAN is downgraded from 16.12.1 to 16.11.1 *x* or earlier, it will cause the Gig0/0/0 to fail to come up because its media-type is set to **media-type sfp**. The problem occurs because 16.12.1 or later automatically selects the correct media-type of the Gig0/0/0 interface, while 16.11.1x and earlier does not have that capability.

Workaround: Specifically set the correct media-type for the Gig0/0/0 interface (e.g. media-type rj45) prior to any downgrade.

An IR1101 operating in SDWAN Controller-mode must not downgrade to Cisco IOS XE Release 17.1.1. This is not supported for SDWAN. Instead, use Cisco IOS XE Release 16.12.1.

Note Cisco IOS XE Release 16.12.1 supports separate Autonomous (non-SDWAN) and SDWAN Controller-mode images.

Starting with release 17.3.1, in order for FND to work on the IR1101, each certificate (used in the certificate chain) needs to be installed, including the root certificate.

Starting with Cisco IOS XE Amsterdam 17.3.2, 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).

Caveats

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

The Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Open Caveats in Cisco IOS XE 17.3.1

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

To view the details of a caveat, click on the identifier.

Identifier	Description
CSCvt95976	dm-log generating dm-log file only once for the first time, modem power-cycle is needed.
CSCvu46609	Cat18 LM960 Modem does not display FirstNet network name.
CSCvu63985	Upon bootup LM960 modem Firstnet SIM gives Error Code 241, no IP when LTE tech AUTO

Resolved Caveats in Cisco IOS XE 17.3.1

There are no resolved caveats with this release.

Open Caveats in Cisco IOS XE 17.3.2a

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

Identifier	Description
CSCvw67128	SL Policy: Purchase information should be protected and shouldn't be able to be erased

Resolved Caveats in Cisco IOS XE 17.3.2a

To view the details of a caveat, click on the identifier.

Identifier	Description
CSCvv41909	Issues with **ip tcp adjust-mss** command added automatically to cellular interface.
CSCvu60481	Throughput exceeds the designed default of 250MB.
CSCvv07529	Traceback for MCU upgrade.
CSCvv13624	boot env var corruption on hard reload.
CSCvv56689	SLE identification added.
CSCvv98043	IOx latency to show running state.

Open Caveats in Cisco IOS XE 17.3.3

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

This release has no open caveats.

Resolved Caveats in Cisco IOS XE 17.3.2a

To view the details of a caveat, click on the identifier.

Identifier	Description
CSCvw57687	Multicast throughput is slower.
CSCvw73603	SNMP MIB ID issue changing dynamically.
CSCvx18288	All features which should be available with only NA License is available from NE.
CSCvx01068	Async: CR gets appended to LF in relay-line mode on Async interface.
CSCvw08412	Edge Intelligence - Issue with serial port access.

Open Caveats in Cisco IOS XE 17.3.4

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

This release has no open caveats.

Resolved Caveats in Cisco IOS XE 17.3.4

To view the details of a caveat, click on the identifier.

Identifier	Description
CSCvw57687	Multicast throughput is slower.

Identifier	Description
CSCvx63341	IR1101 router running in sdwan mode has consistent increase of memory.

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 DevNet.
- 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 gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The 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.