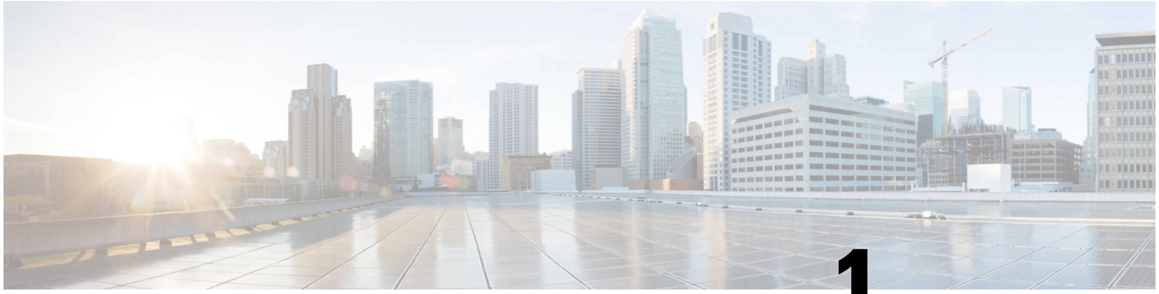
Release Notes for Cisco Hosted Collaboration Solution for Contact Center Solution, Release 12.5(2)

First Published: 2022-07-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Hosted Collaboration Solution for Contact Center

All features that were introduced in 12.5(1) and 12.5(1) ES releases are included as part of 12.5(2).

New Features

Dual Platform Support

Contact Center Enterprise (CCE) components supports the following platforms:

- Microsoft Windows Server 2016 and Microsoft SQL Server 2017
- Microsoft Windows Server 2019 and Microsoft SQL Server 2019

Note The cross combination of platforms is not supported. For example, Windows Server 2016 with SQL Server 2019 or Windows Server 2019 with SQL Server 2017 is not supported.

For more information, see the *Install Microsoft Windows Server* section in the Installing and Upgrading Guide for Cisco Hosted Collaboration Solution for Contact Center at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html

HTTP Strict Transport Security Support for HCS for CC Web Applications

In this release, the HCS for CC web applications such as Diagnostic Portico, CCE Administration, and Websetup will support HTTP Strict Transport Security (HSTS). The HCS for CC web applications will use the HSTS header to instruct the browsers to use only the HTTPS connections.

The Internet Script Editor (ISE) will use the HTTPS connection to communicate with the Administration and Data Server.

The interface to download the ISE client from the Administration and Data Server will happen only over the HTTPS connection and any attempt to download using an HTTP connection will be forbidden.

The following additional security hardening measures are added on the ISE installer location:

1. Disabled directory and wildcard listing.
2. Disabled anonymous authentication, and enabled basic or windows authentication.
3. Disabled the following unused HTTP methods: `PUT`, `POST`, and `DELETE`.

For more information, see the *Internet Script Editor* section in the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

Updated Features

The following are the updated features available for each Contact Center Enterprise solution in Release 12.5(2).

Diagnostic Framework Portico

The Unified ICM/Unified CCE Diagnostic Framework Portico has moved to form-based authentication for login. It has a new login page, an option to log out, and a 30 minute session timeout.

Note The **GetMenu** URL is now deprecated.

Note For more information, see *Diagnostic Tools*section in the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Important Notes

OpenJDK Java Runtime Environment Update

12.5(2) MR installs OpenLogic's OpenJDK JRE as the runtime support for all the CCE java applications. If you uninstall CCE 12.5(2) MR, the applications will use the following JRE versions:

- OpenJDK JRE that was installed on 12.5(1a) base installer or 12.5(1) ES55 and above.

  Or

- Oracle JRE that was installed on 12.5(1).

Before you install or upgrade to 12.5(2), make sure to export the certificates of all the components. For more information, see the *Certificate management requirements* section in the Installing and Upgrading Guide for Cisco Hosted Collaboration Solution for Contact Center at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Tomcat Upgrade

In ICM 12.5(2), Tomcat is upgraded from 9.0.44 to 9.0.62 .

Cloud Connect Update

Starting release 12.5(2), Cloud Connect 12.5(1) is not supported. If you are using Cloud Connect 12.5(1) in your deployment and you want to upgrade to ICM 12.5(2), make sure that you upgrade to Cloud Connect 12.6.

24 Character Hostname Support for ICM nodes

CCE hostname (Router, Logger, AW/AW-HDS/AW-HDS-DD, PG) can now be configured up to a maximum of 24 characters.

Deprecated Features

Deprecated features are fully supported. However, there is no additional development for deprecated features. These features may be scheduled to be removed in a future release. Plan to transition to the designated replacement feature. If you are implementing a new deployment, use the replacement technology rather than the deprecated feature.

Table 1: Deprecated Features/Solution

Deprecated Feature	Announced in Release	Replacement	Notes
UCC Enterprise Gateway PG (Parent PG in Parent-Child deployments)	12.5(1)	None	None
Integrity Check Tool	12.0(1)	None	None
External Script Validation	12.0(1)	None	None
Translation Route Wizard	12.0(1)	Translation Route Explorer	None
MIB Objects: cccaDistAwWebViewEnabled cccaDistAwWebViewServerName cccaSupportToolsURL cccaDialerCallAttemptsPerSec	11.6(1)	None	None

Deprecated Feature	Announced in Release	Replacement	Notes
Generic PG	11.5(1)	Agent PG and VRU PG	None
"Sprawler" deployment	10.0(1)	A Packaged CCE deployment	A "Sprawler" was a Progger with an Administration & Data Server on a single box. It was used for lab deployments.
Cisco Hosted Collaboration Solution for Contact Center (HCS-CC)	12.5(2)	Unified CCE / Packaged CCE / Webex CCE	None

Removed and Unsupported Features

The features listed in the following table are no longer available.

Table 2: Removed and Unsupported Features

Feature	Effective from Release	Replacement
Internet Explorer 11	12.5(2)	Edge Chromium (Microsoft Edge v79 and later)
Avaya Aura Contact Center (AACC - formerly Symposium) PG	12.5(2)	Migrate to Contact Center Enterprise or Webex CCE.
ECSPIM/Avaya (Definity) PG using CVLAN interface	12.5(2)	TAESPIM/Avaya (Definity) PG using TSAPI interface
Customer Journey Analyzer for Business Metrics (Trials)	12.5(2)	None **Note** Customer Journey Analyzer was available for trials only in Release 12.5(1). The trials have been discontinued.

Third Party Software Impacts

Other Software Upgrades

The following softwares are upgraded in this release:

- JRE—Upgraded to 1.8 (32 bit), Update 332.
- Perl—Upgraded to version 5.32.1.
- Apache Tomcat—Upgraded to version 9.0.62.
- OpenSSL—Upgraded to version openssl-1.1.1m.
- Apache Struts—Upgraded to version 2.5.30.
- Jackson—Upgraded to version 2.13.2.
- Spring—Upgraded to version 5.2.20.
- Hibernate—Upgraded to version 5.6.7.
- Log4J—Upgraded to version 2.17.2.
- Xerces—Upgraded to version 2.12.2.
- Xstream—Upgraded to version 1.4.19.

CHAPTER 2

Cisco Finesse

In This Release

There are no release notes for this component.

CHAPTER 3

Cisco Unified Customer Voice Portal

In This Release

There are no release notes for this component.

CHAPTER 4

Cisco Unified Intelligence Center

In This Release

There are no release notes for this component.

CHAPTER 5

Cisco Enterprise Chat and Email

In This Release

There are no release notes for this component.

CHAPTER 6

Cisco Unified Contact Center Management Portal

In This Release

There are no release notes for this component.

CHAPTER 7

Cisco Unified Contact Center Domain Manager

In This Release

There are no release notes for this component.

CHAPTER 8

Caveats

Caveat Queries by Product

Bug Search Tool

If you have an account with Cisco.com, you can use the Bug Search tool to find caveats of any severity for any release. Access the Bug Search tool at https://bst.cloudapps.cisco.com/bugsearch/. Enter the bug identifier in the search box, and press return or click **Search**.

To access a list of open caveats and resolved caveats (rather than an individual caveat) for a particular product or component, see the relevant sections later in these notes.

You can also choose your own filters and criteria in the tool to see a specific subset of caveats, as described in the following table.

If you choose this in Releases	And you choose this in Status	A list of the following caveats appears
Affecting or Fixed in these Releases OR Affecting these Releases	Open	Any caveat in an open state for the release or releases you select.
Fixed in these Releases	Fixed	Any caveat in any release with the fix applied to the specific release or releases you select.
Affecting or Fixed in these Releases	Fixed	Any caveat that is either fixed or occurs in the specific release or releases you select.
Affecting these Releases	Fixed	Any caveat that occurs in the release or releases you select.

Severity 3 or Higher Caveats

Use the following links to the Bug Search Tool to view a list of Severity 3 or higher caveats for each product or component for the current release. You can filter the result by setting the filter values in the tool.

Note If the list of caveats does not automatically appear when you open the browser, refresh the browser.