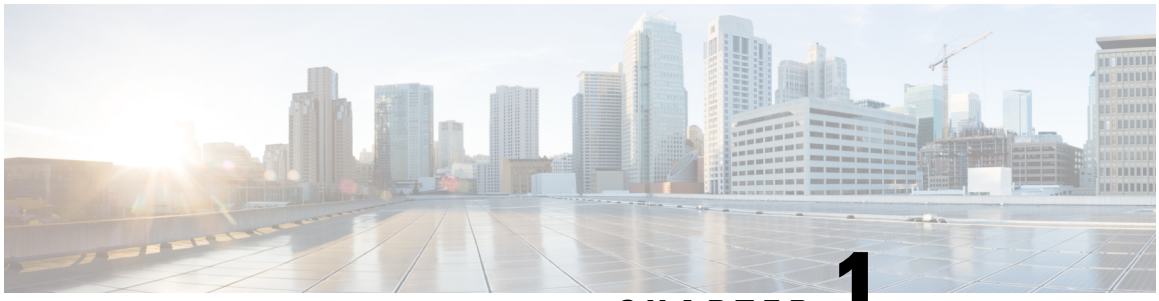
Release Notes for Cisco Unified Contact Center Express Solution, Release 12.5(1) SU2

First Published: 2022-04-11

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

Introduction

Release Notes for Contact Center Solutions

Release introduces release note compilations for each of the contact center solutions. The compilations contain all of the release notes for one solution type and the components that you can use with that contact center.

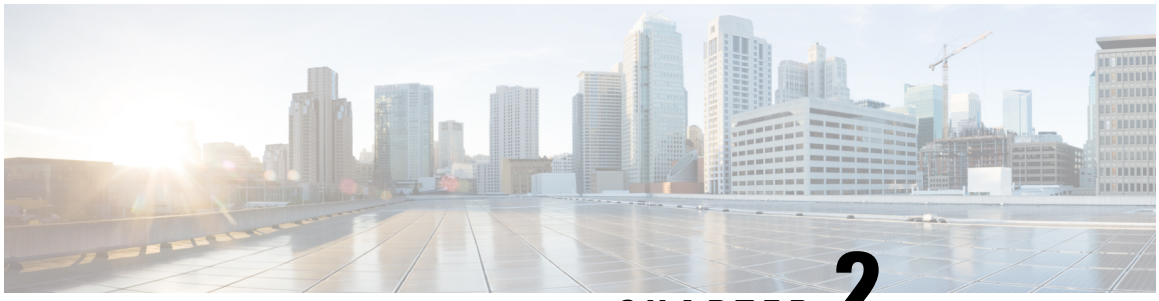
This document includes updates on the Cisco Unified Contact Center Express (Unified CCX) solution and all related components such as Cisco Unified Intelligence Center (CUIC), Cisco Finesse, Customer Collaboration Platform (CCP).

Note Cisco SocialMiner has been renamed as Customer Collaboration Platform (CCP).

Cisco Security Advisories

The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that relates to Cisco products and networks.

For information on existing security issues, see *Cisco Security Advisories, Responses, and Alerts* at https://tools.cisco.com/security/center/publicationListing.x.



CHAPTER 2

Cisco Unified Contact Center Express

New Features

VPN-less Access to Finesse Desktop

This feature provides the flexibility for agents and supervisors to access the Finesse desktop from anywhere through the Internet without requiring VPN connectivity. To enable this feature, a reverse-proxy pair must be deployed in the DMZ.

Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents and supervisors can use Cisco Jabber or Webex over Mobile and Remote Access (MRA). They can also enable the Extend and Connect feature in this deployment.

Cisco Unified CCX supports Historical and Real Time report gadgets in agent and supervisor desktops in VPN-less deployments. The provided reverse-proxy configuration enables authentication of all requests at the proxy, along with other security enhancements.

For more information on this feature, see the *VPN-less Access to Finesse Desktop* sections in the following guides:

- *Solution Design Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html
- *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html

Note For Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, see the *Reverse-Proxy Selection and Configurations* section in the *Cisco Unified Contact Center Express Administration and Operations Guide*. Any reverse-proxy supporting the required criteria (as mentioned in the *Reverse-Proxy Selection Criteria* section of the *Cisco Unified Contact Center Express Administration and Operations Guide*) can be used in place of Nginx for supporting this feature.

ECDSA Certificates

Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography. ECDSA is an alternate algorithm to RSA.

Unified CCX now supports ECDSA and you can make it the default signature algorithm.

For details on how to enable ECDSA, see the `show` and `set` commands in the *Command Line Interface* in *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html

Note WxM does not support Elliptic Curve (EC) certificates. Customers who have deployed WxM must use RSA certificates with Unified CCX.

Support for OpenWebStart in RTR and Script Editor

Oracle is deprecating the Java Network Launch Protocol (JNLP) functionality and support for Java 9 and beyond for Java Web Start. Real Time Reporting (RTR) Tool and Script Editor now support OpenWebstart, an open source reimplementation of the Java Web Start technology.

For more information on OpenWebstart in RTR, see the *Tools Menu* chapter in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

For more information on OpenWebstart in Script Editor, see the *How To Use CUCCX Editor* chapter in *Cisco Unified Contact Center Express Getting Started with Scripts* at https://developer.cisco.com/docs/contact-center-express/#!scripting-and-development-guide.

OAuth 2.0 Support for IMAP

Effective October 1, 2022, Microsoft will permanently disable Basic authentication regardless of usage, with the exception of SMTP authentication. For more information, see https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-september-2021-update/ba-p/2772210.

With this announcement from Microsoft, Unified CCX will support OAuth 2.0 for IMAP protocol (receiving the email) in the current Microsoft Office 365 integrations. SMTP (sending the email) may continue to use Basic authentication until Microsoft supports Basic authentication with SMTP.

Note This feature is available from 12.5(1)SU2 ES03 onwards.

Updated Features

The general updates are as follows:

- Unified CCX now supports RSA key length of 4096 bits in the Certificate Signing Request (CSR). For ECDSA, P-384 key size is recommended, which is roughly equivalent to 7680 bits.
- Specific License Reservation (SLR) is now available by default. You do not have to send any requests to the Cisco Global Licensing Operations team to enable the feature in Cisco SSM.

Deprecated Features

None.

Important Notes

- Before upgrading to Release 12.5(1) SU2, you must download the preupgrade COP from https://software.cisco.com/download/home/270569179.

  The following table lists the COP files that you need to apply prior to performing an upgrade:

Table 1: Release Versions and COP Files for Unified CCX

Version	Release 12.5(1) SU2 Pre-Upgrade COP Name
11.6(2)	ciscouccx.1162.1251SU2PREUPGRADE.41.cop.sgn ucos.keymanagement.cop.sgn
12.0(1)	ciscouccx.1201.1251SU2PREUPGRADE.3.cop.sgn ucos.keymanagement.cop.sgn
12.5(1)	ciscouccx.1251.1251SU2PREUPGRADE.3.cop.sgn ucos.keymanagement.cop.sgn
12.5(1) SU1	ciscouccx.1251.SU1.1251SU2PREUPGRADE.37.cop.sgn

Table 2: Release Versions and COP Files for Customer Collaboration Platform

Version	Release 12.5(1) SU2 Pre-Upgrade COP Name
11.6(2)	ciscosm.keymanagement.cop.sgn
12.0(1)	ciscosm.keymanagement.cop.sgn

Version	Release 12.5(1) SU2 Pre-Upgrade COP Name
12.5(1)	ciscoccp.keymanagement.cop.sgn

Note There is no specific order you must follow while installing the preupgrade COP files.

You must install the COP files on both the publisher and the subscriber nodes. The changes take effect immediately after you install the preupgrade COP files. Reboot is not needed.

- Unified CCX now supports Chromium-based Microsoft Edge and does not support the earlier versions of Edge. For the list of browsers and operating systems that are supported, see Unified CCX Software Compatibility Matrix.
- With the announcement from Microsoft to disable Basic authentication, Unified CCX supports OAuth 2.0 IMAP protocol (receiving the email) in the current Microsoft Office 365 integrations. Simple Mail Transfer Protocol (SMTP) may continue to use Basic authentication until Microsoft supports Basic authentication with SMTP. This feature is available from 12.5(1) SU2 ES03.
- Unified CCX now supports Private Network Access (PNA) in Chrome from 12.5(1) SU2 ES04.
- FIPS 140-2 mode is supported only on releases that have been through FIPS compliance.
- In a HA setup, FIPS 140-2 mode must be first enabled or disabled on the publisher and then on the subscriber. Before enabling or disabling FIPS 140-2 mode on the subscriber, ensure that all the services are running on the publisher.
- Ensure that SRTP is disabled before enabling or disabling FIPS 140-2 mode in Unified CCX. You can enable SRTP after enabling or disabling FIPS 140-2 mode in Unified CCX.
- When FIPS 140-2 mode is enabled or disabled, the keys and certificates are regenerated, and the Unified CCX server reboots. While rebooting, the system performs the cryptographic modules integrity check, and runs certification self-tests.
- Back up the system before and after enabling FIPS 140-2 mode.
- When SRTP is disabled on your system and if you are restoring from a backup that was taken when SRTP was enabled, you must disable SRTP in the System Parameters page after the restore.
- When SRTP is enabled on your system and if you are restoring from a backup that was taken when SRTP was disabled, you must disable and enable SRTP again in the System Parameters page after the restore.
- You can localize most of the messages by using Unified CCX Administration. However, some of the accessibility messages that are read by the screen reader on the Bubble Chat interface have to be localized in the HTML code snippet.
- An SRTP-enabled HA setup requires distinct RmCm provider users. So, the system generates a separate RmCm Provider User Id with the suffix "**_ccxsub**" for the subscriber node.
- Associate devices and device profiles only with the RmCm Provider User that is configured in the Cisco Unified CM Configuration page (primary RmCm user).

- Agent desktops must be synchronized with NTP server so that the time in the auto incrementing fields of Live Data reports match the server time.
- From Unified CCX Release 12.5(1), the 300 agent deployment model is not supported. Deployments that require more than 100 agents have to use the 400 agent OVA profile. The vRAM required for the 400 agent OVA profile has increased from 16GB to 20GB. Customers who want to use Cloud Connect services with the BE6000 must increase the vRAM from 10GB to 14GB. For information about Resource Requirements, refer to the Virtualization Wiki.

Note As the OVA profile is changed for 400 agent model deployments, if you do not change the OVA settings, the upgrade fails at Switch Version. For fresh install, the new OVA must be used for deployment. For more information, see *Cisco Unified Contact Center Express Design Guide*.

Caution Ensure that the reservation of CPU and memory adhere to the specification mentioned in the Virtualization Wiki.

- After upgrading Unified CCX, the CAs that are not approved by Cisco are removed from the platform trust store. However, you can add them back, if necessary.
  - For information about the list of CAs that Cisco supports, see Cisco Trusted External Root Bundle in https://www.cisco.com/security/pki.
  - For information about adding a certificate, see the procedure from step 5 onwards under the *Obtain and Upload CA Certificate* section in Cisco Unified Contact Center Express Administration and Operations Guide.
- You can download the Chat Transcript in only HTML format.
- You can configure the maximum number of concurrent sessions for a user of the following applications: Cisco Identity Service Management, Disaster Recovery System, Cisco Unified CCX Administration, Cisco Finesse Administration, Cisco Unified Serviceability, Cisco Unified CCX Serviceability, Cisco Unified OS Administration, and Cisco Unified Intelligence Center.

  If a user reaches the configured limit, further login attempts are rejected. The maximum number of concurrent sessions is configured by using the **set webapp session maxlimit** command. For more information about this command, see the Command Line Interface chapter in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.
- The DataConn container consumes CPU resources. If DataConn is not being used, use the **utils cloudconnect stop dataconn** command to shut the container down. This command needs to be executed after every reboot from each of the nodes.

Removed and Unsupported Features

Removed Features

- Classic Chat feature has been removed. The configuration of the Classic Chat in the previous release will not be migrated during an upgrade to this release. Customers must configure the Bubble Chat widget available in the Cisco Unified CCX Administration.

Unsupported Features

From Unified CCX release 12.5(1) SU1, the following commands are not supported:

- utils uccx notification-service log
- utils uccx notification-service log disable
- utils uccx notification-service log enable
- utils uccx notification-service log status

Chat Transcript Download in a PDF Format

The chat transcript cannot be downloaded in a PDF format.

Mobile Skill Manager

Mobile Skill Manager is not supported.

TLS

TLS 1.0 and 1.1 are not supported.

Cisco Context Service

Cisco Context Service is not supported.

Customer Journey Analyzer

The trial of Customer Journey Analyzer feature has been concluded. This feature is not available from release 12.5(1) SU1.

Internet Explorer

Support for Internet Explorer is removed.

Unsupported Options on Finesse for Direct Preview Outbound

Finesse does not support Skip, Skip-Next, Skip-Close, Reject, Cancel Reservation, and Do Not Call for direct preview outbound calls.

Unsupported Features and Configurations for Progressive and Predictive Agent Outbound

Unsupported Features and Configurations for Progressive and Predictive Agent Outbound

- The “Get Reporting Statistic” step is not supported for progressive and predictive agent-based outbound campaigns.
- Unified CCX does not support the translation or modification of the phone number that it uses to dial outbound calls. If any “voice translation rules” that are configured in the gateway modify the phone number, those rules are not supported.

Note You can use either of the following two supported methods to modify a dialed number in the gateway:

- To remove the initial digits of the phone number, use **forward-digits** or **digit-strip** in the dial-peer configuration.
- To add a prefix to the phone number, use **prefix** in the dial-peer configuration.

- For Outbound campaigns outside North America, additional configuration is required to add the area-code-to-time-zone mapping. For more information, see the *Cisco Unified Contact Center Express Administration and Operations Guide*, located at https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html.
- For multi-country Outbound campaigns, the area code must also include the country code.
- Unified CCX dialer will dial outbound contacts only if the publisher database is in the “IN SERVICE” state.
- Finesse does not support the Do Not Call option.
- If you are not on Smart Licensing, outbound license usage is not captured in the License Utilization Cisco Unified Intelligence Center report.
- You must enable **Agent AutoAnswer** manually for agent-based progressive and predictive calls when you upgrade from an older Unified CCX release.

Unsupported Configuration for IPv6

- Cisco Unified Communications Manager does not support SIP IPv6 signaling over UDP where the maximum transmission unit (MTU) is greater than 1500. To ensure that you do not experience intermittent call failure, change the transport protocol to TCP.

  For more information, see the “Important Notes” section of the *Release Notes for Cisco Unified Communications Manager*, located at:

  https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html

  Also, see “CSCuo71306” for details on this limitation.
- When using IPv6 and Outbound dialer, use a voice gateway IOS that contains the fix for “CSCul43754”.

Unsupported Configurations and Scenarios for Unified CCX

Unified CCX does not support the following configurations:

- CTI route points with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists of Unified CM.
- Shared lines for CTI ports and CTI route points.
- ICD call answer or ICD call transfer using any third-party attendant console desk software.
- Within the same script, using the “Place Call” step to generate a call and then placing the call, back into the same queue (creating a call loop).
- SIP REFER between a switchboard and Unified CCX if the transfer is completed after the call is answered on the Unified CCX CTI port because of media reestablishment issues.
- During TTS prompt playback, if the call is put on hold and then retrieved, the prompt does not continue from the position at which it was left.
- Use of “Consult Transfer”, “Direct Transfer”, or “Redirect” to a translation pattern that maps back to a route point.
- Use of “Consult Transfer”, “Redirect”, and “Place Call” steps to invoke or dial into "Conference Now" conferences.
- The following scenarios have issues:
  - External -> Redirect to Unmonitored device -> Call Forward No Answer (CFNA) to UCCX RP

    Use of Redirect Step to an unmonitored device which then uses CFNA to a UCCX route point.
  - External -> Consult Transfer to RP ->Consult Transfer to RP -> Redirect to Unmonitored device
  - External -> Redirect to RP -> Consult Transfer to RP -> Redirect to Unmonitored device
  - External -> Consult Transfer to RP -> Redirect to RP -> Redirect to Unmonitored device
  - External -> Consult Transfer to RP -> Redirect to Unmonitored device

    Thus, use the Call Redirect Step in the script instead of Call Consult Transfer.
- Unified CCX doesn't completely support E.164 numbering plan for route point directory numbers (DN).

  This limitation is because of the Unified CM limit on device name length set as 15 characters. We add "_" between the device name prefix and the DN. So we support a maximum of 13 characters in the DN as device name prefix is mandatory and hence at least one character is needed there. For example, (Device name prefix) + '_' + (length of DN) = 15 ==> [(1 + '_' + 13) = 15].
- Cisco Unified CCX system does not support modification, addition or deletion of the CTI ports and the CTI Route Points from the Cisco Unified Communication Manager. Performing the same can lead to issues with non-contiguous DN range for which Cisco Tomcat on Unified CCX Server needs to be restarted.
- When the supervisor monitors the Team Performance report and during the time if there is any update or modification done to the team, this doesn't get updated automatically. The supervisor should refresh the browser page or select the respective team again to view the Team Performance report.
- Use of two(2) wildcard CTI Route Points that overlap with each other is not supported. For example, Route Point 1: 123XXXX and Route Point 2: 1234XXX overlap with one another and is not supported.

However, a wildcard CTI Route point can overlap with a full DID (best match pattern) that doesn't contain a wildcard. For example, Route Point 1: 123XXXX and Route Point 2: 1234567 is supported.

- A discrepancy in reports is observed when a call is transferred using Cisco Jabber by multiple agents in the same call flow. Use the Cisco Finesse desktop to transfer calls.
- SIP URI dialing for CTI route points, CTI ports, and agent extensions.
- Mid Call Caller ID updates when call is routed to Unified CM via MGCP gateway.

Note When incoming calls are routed to Unified CM via MGCP gateway, any mid call caller ID updates are reflected only after the call is connected.

Unsupported Actions for Unified CCX Agents

Use of the following softkeys on a Cisco Unified IP Phone is not supported:

- Barge
- cBarge
- DND
- GPickup
- iDivert
- Conference Now
- Park
- Pickup

Unsupported Configurations for Agent Phones

The following configurations are not supported for agent phones:

- Two lines on an agent phone that have the same extension but exist in different partitions.
- While signing in to the Finesse desktop, the agent chooses one of the devices that share the same extension. The selected device becomes the active device for that session on Finesse desktop. Any actions on the inactive agent devices are not supported on Finesse desktop during that session.
- Silent Monitoring by supervisors who are logged in with Extend and Connect.
- In the Unified Communications Manager Administration Directory Number Configuration web page for each Unified CCX line, setting Maximum Number of Calls to a value other than 2.
- In the Unified Communications Manager Administration Directory Number Configuration web page for each Unified CCX line, setting Busy Trigger to a value other than 1.
- No Cisco Unified Communications Manager device can be forwarded to the Unified CCX extension of an agent.

- The Unified CCX extension of an agent cannot be configured to forward to a Cisco Unified CCX Trigger or CTI route point.
- Configuring the Unified Communications Manager Intercom feature.
- Configuring the Hold Reversion feature.
- Agent extensions cannot be added to hunt lists or hunt groups. If an agent has only one line, the agent phone cannot be part of a hunt list or hunt group. In the case of multiple lines, none of the first four configured lines must be part of the hunt group. For more details on multiple lines support and number of monitored lines, see the *Cisco Unified Contact Center Express Design Guide*, located at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html.
- Call Forward All to extensions which Unified CCX does not have control over. For example, if an agent extension has Call Forward All to a PSTN extension or Directory Number on another cluster which Unified CCX is unaware of.
- All the Cisco IP Phones for Cisco Finesse IP Phone Agent currently do not support the Simplified New Call UI.

Supported Configurations for Agent Phones

To determine the phone devices that are supported by Cisco Finesse and for use by Cisco Finesse IP Phone agents, see the Unified CCX Compatibility related information located at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

The following configurations are supported on agent phones:

- A Unified CCX extension that is configured on a single device (but not on multiple devices).
- A Unified CCX extension that is configured in a single device profile (but not in multiple device profiles).
- Multiple agents sharing the same Unified CCX extension, which you can set up as follows:
  - Configure the Unified CCX extension to a single phone (not in a device profile).
  - Associate the phone with all the agents who will use this extension.
  - Select the appropriate directory number (DN) as the Unified CCX extension for each agent.

    In this configuration, only one agent at a time can be logged in.

Note All agents who currently have the Unified CCX extension to be shared must log out before you configure additional agents to share that extension.

- Video is now supported if you are using Cisco Jabber for Windows as agent phone. The agent desktop where Jabber is used for Video should comply to the Cisco Jabber hardware requirements listed in the *Cisco Jabber for Windows 11.0.x and 11.1.x Release Notes* , located at:

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/Windows/11_0/RN/JABW_BK_C5E7828C_00_cisco-jabber-windows-11-release-notes.html.

Unsupported and Supported Configurations for Remote Agents

Unified CCX supports Cisco Expressway 8.7.1. The current version of Cisco Expressway does not support BiB and thus the contact center cannot achieve silent monitoring and recording functionalities.

Unsupported Features in Unified Communications Manager and Cisco Business Edition 6000

The following Unified Communications Manager features are not supported by Unified CCX. These features are disabled by default and you should not enable them for Unified CCX. For more information about these features, see Unified Communications Manager documentation, located at:

https://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

- Block External to External Transfer.
- DSCP IP CTIManager to Application service parameter.

  You can enable this service parameter for Unified Communications Manager, but doing so does not affect Unified CCX.
- Advanced Ad Hoc Conference Enabled service parameter.
- Drop ad hoc conference when the creator leaves the conference.
- Signaling (QSIG) Path Replacement (PR).

  This feature must be disabled when Unified CCX is deployed. To disable this feature, set the Unified Communications Manager service parameters Path Replacement Enabled and Path Replacement on Tromboned Calls to False.
- Forced Authorization Code and Client Matter Code.

  Because these features can be enabled per route pattern, you should turn them off for all route patterns in the Unified Communications Manager cluster that Unified CCX might use. Enabling these features for route patterns that Unified CCX does not use does not affect Unified CCX.
- Multilevel precedence and preemption (MLPP).

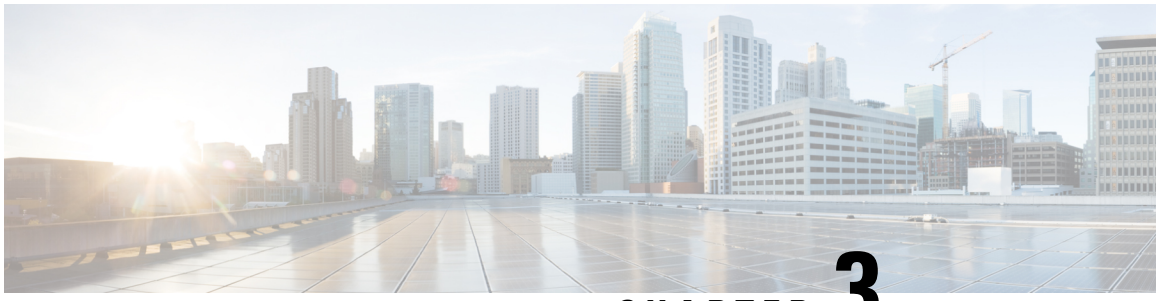
  You can enable this feature for devices in the cluster that do not interact with Unified CCX.
- Do not use Unified Communications Manager Administration to add or change CTI ports or route points that are used by Unified CCX or application users that are created by Unified CCX.

Unsupported Features in Custom Reports

- The **Do Not Call** field is no longer available. While upgrading, report will not be generated if the **Do Not Call** column is present in the custom report. You can generate the report by removing the **Do Not Call** column from the custom reports.
- A Custom report that was created from a Unified CCX Stock Report may not work as expected if the report definition of the original Stock Report is modified in the new release.

Third Party Software Impacts

See the Unified CCX Compatibility related information located at:
https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html
for information on third-party software.



CHAPTER 3

Cisco Unified Intelligence Center

New Features

Accessibility Compliance

This release ensures that the Cisco Unified Intelligence Center reporting application complies with Web Content Accessibility Guidelines (WCAG) 2.0. For more information on the supported JAWS version, see Voluntary Product Accessibility Templates (VPAT) report for Contact Center at https://www.cisco.com/c/en/us/about/accessibility/voluntary-product-accessibility-templates.html.

Custom Logon Messages

You can configure custom logon messages for Cisco Unified Intelligence Center. The custom messages appear in a pop-up box during the sign-in process. The user has to acknowledge this message to proceed further. It is not mandatory to have custom messages. Administrators can set up the logon messages in Cisco Unified OS Administration. For more information, see the Configure Custom Logon Messages section in the Administration Console User Guide for Cisco Unified Intelligence Center at: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge). For information about supported versions, see the *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Commands

The following commands have been introduced:

Allow External Links

The administrator can enable or disable the external links in Unified Intelligence Center dashboard using the **set cuic properties allow-external-links** {*on*|*off*} command.

CUIC Logging

In this release, the log trace setting in OAMP interface is removed. The administrator must use the **utils cuic logging** commands to set the log traces. To change the log level configuration on each node in the cluster, the command must be run separately on each node.

Updated Features

Important Notes

Allow External Links

After the upgrade, the external links in the Unified Intelligence Center dashboard will be disabled. If required, the administrator can enable the external links again using the set cuic properties allow-external-links command.

If enabled, the contents from external links are rendered within the HTML iFrame in the dashboard. This will include the `frame-src*` directive in the Content Security Policy of the Unified Intelligence Center web pages.

Gadget URL

JSP format is not supported for Unified Intelligence Center gadgets (Live Data and Historical). To change the JSP format references to XML format, the administrator must run the following commands on the primary Cisco Finesse server.

- utils finesse layout updateCuicGadgetUrl 12.6.1+—Updates the CUIC URL configured in the Cisco Finesse desktop layout to work with Release 12.6(1) and later versions. For more information, see the *Upgrade* section in the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

HTTP Access

Cisco Unified Intelligence Center is not accessible using port 8081 in any manner. From this release, port 8081 is disabled and does not redirect to HTTPS.

Deprecated Features

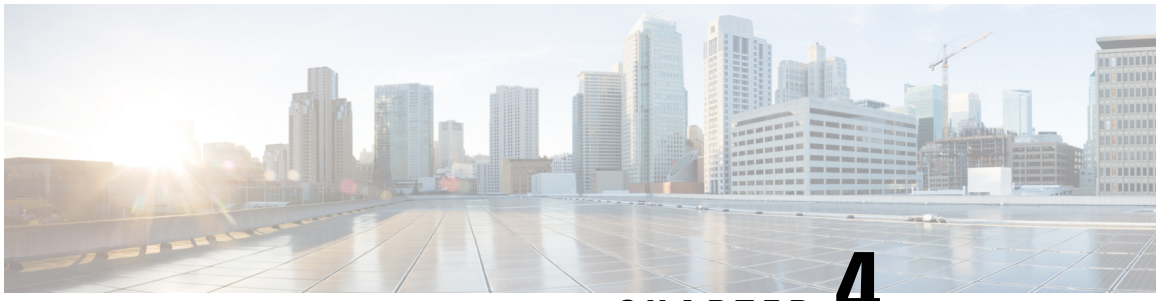
None.

Removed and Unsupported Features

None.

Third Party Software Impact

None.



CHAPTER 4

Cisco Finesse

New Features

View Locked Out Users

To view the locked out users, a new CLI **utils finesse locked_out_users list** command is added. For more information, refer to the **Desktop Properties** section in the Cisco Finesse Administration Guide.

Desktop Interface APIs

Three new APIs are introduced. These APIs can be used for desktop development. The new APIs are as follows:

- **Desktop Configuration**
- **Languages List**
- **Verify Desktop and Third-Party URLs**

For more information on the APIs, see the **Cisco Finesse Desktop Interface API Guide** on DevNet.

Updated Features

SystemInfo API is now authenticated when accessed through VPN-less reverse-proxy. To use alternatives in nonauthenticated mode, refer to the **Cisco Finesse Desktop Interface API Guide** on DevNet.

Important Notes

None.

Deprecated Features

Notifications over BOSH (Long Polling)

In this release, support for notifications over BOSH (long polling) is deprecated. Notifications over direct XMPP (over TCP) and Websocket-based transports are the replacements.

Removed and Unsupported Features

Cisco Finesse Trace Logging

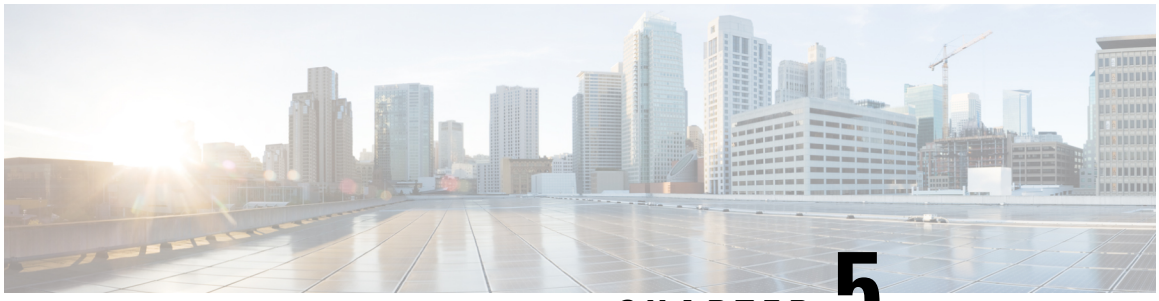
In this release, the following CLIs are removed:

- utils finesse trace enable
- utils finesse trace disable

The replacement is the **utils finesse log** commands that are used to add, delete, update, or view a custom log configuration in the Cisco Finesse system.

Third Party Software Impacts

None.



CHAPTER 5

Cisco Customer Collaboration Platform

New Features

VPN-less Access to Finesse Desktop

This feature provides the flexibility for agents and supervisors to access the Finesse desktop from anywhere through the Internet without requiring VPN connectivity. To enable this feature, a reverse-proxy pair must be deployed in the DMZ.

When deployed with VPN-less reverse-proxy, Customer Collaboration Platform can be deployed within the DMZ or can be moved within the enterprise.

For more information on this feature, see the *VPN-less Access to Finesse Desktop* sections in the following guides:

- *Solution Design Guide for Cisco Unified Contact Center Express* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html
- *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html

ECDSA Certificate Support

Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography. ECDSA is an alternate algorithm to RSA.

Customer Collaboration Platform now supports ECDSA and you can make it the default signature algorithm.

For details on how to enable ECDSA, see the `show` and `set` commands in the *Command Line Interface* in *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html

Note WxM does not support Elliptic Curve (EC) certificates.

Updated Features

None.

Important Notes

After upgrading Customer Collaboration Platform, the CAs that are not approved by Cisco are removed from the platform trust store. However, you can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see *Cisco Trusted External Root Bundle* section in https://www.cisco.com/security/pki
- For information about adding a certificate, see the *Customer Collaboration Platform Configurations* section in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html

Deprecated Features

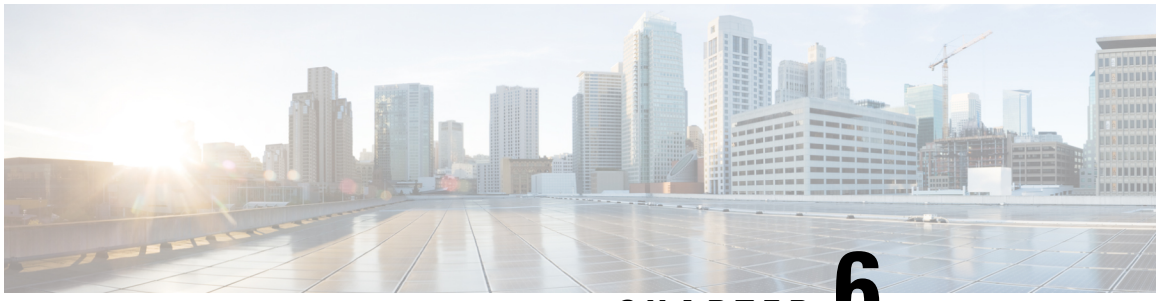
None.

Removed and Unsupported Features

The standalone Customer Collaboration Platform features such as Facebook page, Twitter, RSS Feeds, Standalone single session chat, associated features like filters and notifications have been removed.

Third Party Software Impacts

None.



CHAPTER 6

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 for Release 12.5(1)SU2

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.

Cisco Unified Contact Center Express

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=270569179&rls=12.5(1)SU2&sb=anfr&svr=3nH&bt=custV

Cisco Unified Intelligence Center

None.

Cisco Finesse

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&rls=12.5(1)SU2&sb=anfr&svr=3nH&bt=custV&prdNam=Cisco%20Finesse

Cisco Customer Collaboration Platform

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613136&rls=12.5(1)SU2&sb=anfr&svr=3nH&bt=custV