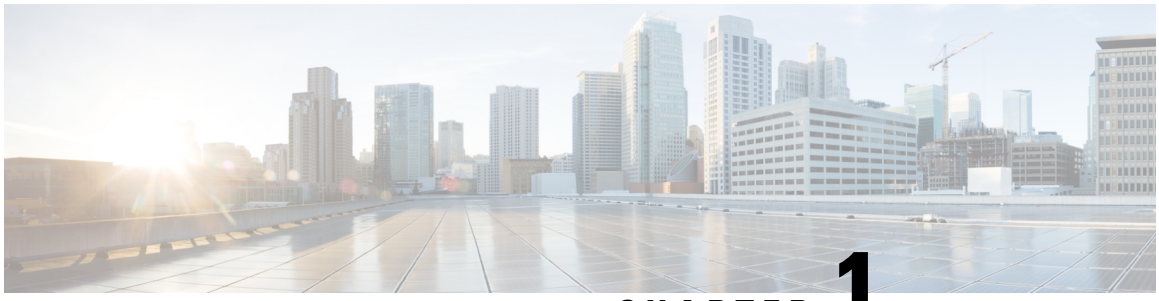
Release Notes for Cisco Contact Center Enterprise Solutions Release 12.6(1)

First Published: 2021-05-14

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 Enterprise Solutions

These release notes describe new and updated features and other changes for Release of the following contact center solutions and their components:

- Cisco Unified Contact Center Enterprise
- Cisco Packaged Contact Center Enterprise

Information in this document applies to the contact center solutions listed above, except where otherwise noted.

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.

Contact Center Enterprise Software Release Delivery Model

Cisco introduces a new software release delivery model for Contact Center Enterprise products. Starting from Release 12.6(1), Contact Center Enterprise issues two types of releases:

- Long Term Release (LTR)
- Dynamic Release (DR)

We recommend the LTR delivery model if you prefer infrequent upgrade cycles over faster adoption of new features. This model includes support for bug fixes through engineering specials.

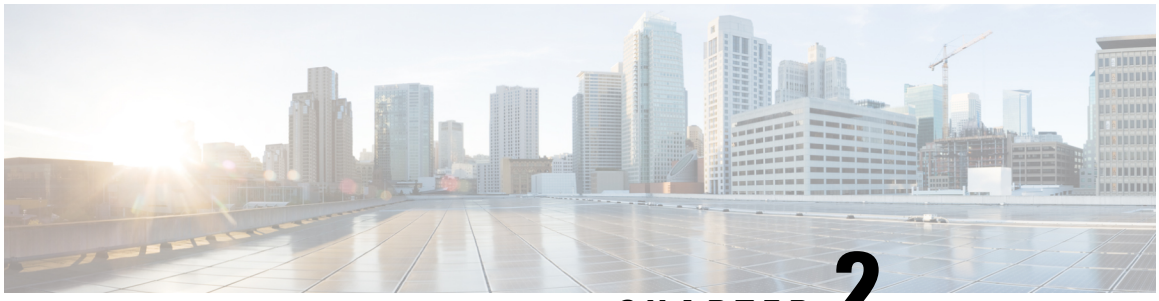
We recommend the DR delivery model if you want faster feature adoption. With this model, both new feature and bug fixes are delivered through engineering specials and maintenance releases. This model also offers simplified patch upgrades through automated notification, orchestrated patch application, and minimal downtime.

For more information about the new delivery models, see the product bulletin *Cisco's Contact Center Enterprise Software Release and Sustaining Lifecycle*. Release 12.6 is a dynamic release and will follow the sustaining process as outlined in this product bulletin.

Multi-server SAN Certificates

Multi-server Subject Alternate Name (SAN) certificates are supported by the following solution components: Cisco Finesse, Cisco Unified Intelligence Center (CUIC), Live Data, IdS, and Cisco Virtualized Voice Browser (VVB).

For more information, see *Configuration of CA-Signed Multi-Server Subject Alternate Name in CVOS Systems*.



CHAPTER 2

Contact Center Enterprise Solutions

New Features

The following table lists the new features available for each Contact Center Enterprise solution in Release 12.6(1).

Table 1: New Features for Contact Center Enterprise Solutions

Feature	Unified CCE	Packaged CCE
VPN-less Access to Finesse Desktop (For Agents and Supervisors), on page 4	Yes	Yes
Agent Answers, on page 5	Yes	Yes
Edge Chromium Browser Support, on page 6	Yes	Yes
Simplified Upgrade, on page 6	Yes	Yes
Graceful Shutdown, on page 7	Yes	Yes
AppDynamics Native Integration with CCE, on page 7	Yes	Yes
Support for 36000 Agents, on page 7	Yes	
Custom Truststore to Store Component Certificates, on page 8	Yes	Yes

Feature	Unified CCE	Packaged CCE
vMotion, on page 8	Yes	Yes
Dual Platform Support, on page 9	Yes	Yes
ECDSA Certificates, on page 9	Yes	Yes
Webex Workforce Optimization (WFO) Support with Contact Center Enterprise (CCE) Solutions	Yes	Yes

Authentication for Reverse-Proxy Connections (ES02 Update)

Finesse introduces authentication at the edge for the reverse-proxy. Authentication is supported for both SSO and Non-SSO deployments. Authentication is enforced for all requests and protocols that are accepted at the proxy before they are forwarded to the respective component servers (Finesse, IdS, CUIC, and IdP). The component servers also enforce authentication locally. All authentications made at the proxy use the Finesse login credentials, irrespective of the component server to which the requests are made. For more information on authentication, see the **Authentication** topic under the **VPN-Less Access to Finesse Desktop** section in the Cisco Unified Contact Center Enterprise Features Guide. For complete list of enhancements to the VPN-Less configuration, refer to the Nginx TechNote article.

Configurable Reverse-Proxy Host Verification (ES03 Update)

You can enable and disable SSL certificate verification for connections that are established from reverse-proxy hosts to Cisco Web Proxy Service by using the **utils system reverse-proxy client-auth** CLI command. For more information about reverse-proxy host authentication see the **Configure Reverse-Proxy Host Authentication** section in Cisco Unified Contact Center Enterprise Features Guide.

VPN-less Access to Finesse Desktop (For Agents and Supervisors)

This feature provides the flexibility for agents and supervisors to access the Finesse desktop from anywhere through the Internet without requiring VPN connectivity to the enterprise data center. To enable this feature, a reverse-proxy pair must be deployed in the DMZ. For more information on this feature, see the Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1) and Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1).

Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents and supervisors can use Cisco Jabber over MRA or the Mobile Agent capability of Contact Center Enterprise with a PSTN or mobile endpoint.

To use VPN-less access to Finesse desktop, you must upgrade Finesse, IdS, and CUIC to Release 12.6(1) ES02 or above. If you are using Unified CCE 12.6(1), you must upgrade Live Data to 12.6(1) ES02 or above. You can access the 12.6(1) ES03 Release and Readme from the following locations:

- Finesse 12.6(1) ES
- CUIC/LD/IdS 12.6(1) ES

Note

- For Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, refer to the Nginx TechNote article. Any reverse-proxy supporting the required criteria (as mentioned in the **Reverse-Proxy Selection Criteria** section of Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1)) can be used in place of Nginx for supporting this feature.
- If CORS status is "enabled", you must explicitly add the reverse-proxy domain name to the list of CORS trusted domain names.

Agent Answers

Unified CCE leverages Artificial Intelligence (AI) and Natural Language Understanding (NLU) to provide services that assist agents. These Contact Center AI services are available for the agents through the Agent Answers gadget and the Call Transcript gadget on the Cisco Finesse desktop.

The Agent Answers gadget displays relevant suggestions and recommendations in real time for the agent to consider. The suggestions and recommendations are based on the ongoing conversation between the caller and the agent. Agent Answers enhances the customer experience because the timely suggestions improve the ability of the agent to respond.

The Call Transcript gadget dynamically converts the ongoing voice conversation to text and presents the text to an agent for real-time viewing and reference.

For details on how to configure the Agent Answers and Call Transcription features, see the *Agent Answers* and the *Call Transcription* chapters in the following documents:

- *Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html
- *Cisco Packaged Contact Center Enterprise Features Guide, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

For information on the design considerations of the Agent Answers and Call Transcription features, see the *Contact Center AI Services Considerations* section in following documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html
- *Solution Design Guide for Cisco Packaged Contact Center Enterprise, Release 12.6* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html

Note To enable Agent Answers or Call Transcript features, ensure your Cisco Unified CVP is on 12.6(1) ES 06, Cisco Finesse is on 12.6(1) ES 01, and Cloud Connect is on 12.6.

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge) . For more information, see the *Supported Browsers* section in 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.

Simplified Upgrade

The Orchestration feature provides partners and administrators an option to automatically download software updates and simplify the installation and rollback processes. Integration of Graceful Shutdown feature within the Orchestration framework ensures that the software updates are updated with minimal downtime. The Orchestration framework is built within the Cloud Connect server that connects to the Cisco-hosted cloud software repository. This framework provides the ability to check and download new software updates as and when they are available and notify the administrators via email about the new updates along with the release notes. Orchestration currently supports installation and rollback of Cisco Engineering Specials (ES), Service Updates (SU), Minor Releases (MR), and Microsoft Patches.

Cloud Connect server version 12.6(1) supports Orchestration in the following scenarios:

- CCE 12.5(x) ES, 12.6(x) ES and Windows Updates can be orchestrated from 12.6(x) Cloud Connect server
- CCE 12.5(1) to 12.5(2) or 12.6(1) software upgrade can be orchestrated from 12.6(x) Cloud Connect server

Note ICM 12.5(2) to 12.6(1) upgrade is not supported either manually or via orchestration.

Apply the mandatory patch on Cloud Connect to Orchestrate 12.5(2) ES and software upgrade.

The following are the known limitations:

- Orchestration is not supported for Tech Refresh and fresh install.
- Orchestration is not supported for Cisco Customer Collaboration Platform (CCP), Cisco Enterprise Chat and Email (ECE), Cisco Unified Contact Center Domain Manager (CCDM), Cisco Unified Contact Center Management Portal (CCMP), and non-Contact Center Cisco products such as Cisco Unified Communications Manager (CUCM), IM&P etc.
- The administrators should read the release notes specifically for ES releases that are notified via email to understand the dependency on each component. The Orchestration framework does not track this aspect automatically. For example, if an ES of Finesse has a dependency on an ES of Live Data and has to be installed in a specific order, then the administrator should consider this before initiating the patch installation from the Cloud Connect server.
- Only Microsoft Exchange Server is supported for email notification; Office 365 and Gmail are not supported as of now.

Note Orchestration is not supported for 12000, 24000, and 36000 agent deployment models.

Graceful Shutdown

Graceful shutdown allows you to perform firmware upgrades, apply security patches, and apply Engineering Specials (ES) without the need for a maintenance window. With this feature, active calls and sessions are transitioned over to secondary or redundant components before an upgrade process is initiated on the target system. Agent states, call states, and call context are maintained. Operations such as reskilling and changing an agent's team membership are not affected.

For more information, see the following documents:

- *Administration Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html
- *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

AppDynamics Native Integration with CCE

For Cisco Contact Center Enterprise solution, it is important to have continuous and seamless monitoring of the deployed solution and automated alerting when anomalies are detected. AppDynamics provides a solution for application and platform performance monitoring that helps to achieve the following:

- Platform, application, and End User Monitoring (EUM) through dashboards and metrics.
- Automated alerting mechanism in case of anomaly detection.

For ordering and setting up AppDynamics SAAS controller, please contact appd_ucce_sales@cisco.com

Note **For AppDynamics, CCE supports SaaS and On-Prem controller (version 21.4.10-24683) over secure connection only.**

Support for 36000 Agents

You can modify your existing 24000 agent reference design to scale up to 36000 agents. This is accomplished by adding more peripheral VMs and peripheral gateways to the deployment and modifying specific configuration limits. You must also modify the OVA files for Live Data and Cisco Identity Service (IdS).

For more information about configuring your solution for 36000 agents, see the following documents:

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

- *Solution Design 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-implementation-design-guides-list.html.

For more details, see the *Scale up to 36000 Agents* topic in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

Custom Truststore to Store Component Certificates

Starting Unified CCE 12.6(x), a new custom truststore is created under the Unified ICM Installation directory `<ICM install directory>\ssl\cacerts` to store all the component certificates. With this new custom truststore, you don't need to export and import the certificates each time Java is updated in the system.

After upgrading from Unified CCE 12.5(x) to Unified CCE 12.6(x), you should export the certificates from the Java truststore to the custom truststore under the Unified ICM Installation directory `<ICM install directory>\ssl\cacerts`.

Export the certificate from the Java truststore:

- Run the command at the command prompt: `cd %JAVA_HOME%\bin`.

Important Use CCE_JAVA_HOME if upgrading from Unified CCE 12.5(1a) or Unified CCE 12.5(1) with ES55 (mandatory OpenJDK ES).

- Export the certificates of all the components imported into the truststore.

  The command to export the certificates is *keytool -export -keystore <JRE path>\lib\security\cacerts -alias <alias of the component> -file <filepath>.cer*
- Enter the truststore password when prompted.

Import the certificate to the custom truststore:

- Run the command at the command prompt: `cd %CCE_JAVA_HOME%\bin`.
- Import the certificates for all the components that you exported from the Java truststore.

  The command to import certificates is *keytool -import -keystore <ICM install directory>\ssl\cacerts -file <filepath>.cer -alias <alias>*.
- Enter the truststore password when prompted.
- Enter 'yes' when prompted to trust the certificate.

vMotion

Cisco Contact Center Enterprise solution components now support vMotion of live virtual machines (VMs) on Cisco Hyperflex servers. VMware vMotion enables the live migration of running VMs from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. vMotion is a key enabling technology for creating dynamic, automated, and self-optimizing data centers.

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 Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html

ECDSA Certificates

This release supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificate, which can be enabled in Unified CCE, Cisco Unified CVP, Cisco Finesse, Cloud Connect, CUIC, Cisco VVB, Cisco IdS, and ECE.

For details on how to enable ECDSA, see *Enabling ECDSA for Unified CCE Solution* in *Security 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

To enable ECDSA certificate, the following solution components in the specified versions, and the respective Engineering Specials (ES) are required. You have to install the below ESes in the order listed:

- Cloud Connect 12.6(1) ES1
- Cisco VVB 12.6(1) ES1
- Cisco CVP 12.6(1) ES6
- CUIC 12.6(1) ES1
- Cisco Finesse 12.6(1) ES1
- ICM 12.6(1) ES9

Webex Workforce Optimization (WFO) Support with Contact Center Enterprise (CCE) Solutions

The Contact Center Enterprise (Unified CCE/Packaged CCE/Webex CCE) solutions supports the Webex Workforce Optimization offering. See https://www.cisco.com/c/en/us/support/contact-center/webex-workforce-optimization/series.html.

Updated Features

The following table lists the updated features available for each Contact Center Enterprise solution in Release 12.6(1).

Table 2: Updated Features for Contact Center Enterprise Solutions

Feature	Unified CCE	Packaged CCE
Webex Experience Management Integration with Post Call Survey, on page 10	Yes	Yes
SMS and Email Survey after Voice, on page 11	Yes	Yes
Non-Production System (NPS), on page 12	Yes	Yes
Database Schema Changes, on page 12	Yes	Yes
Password Hashing, on page 13	Yes	Yes
Diagnostic Framework Portico, on page 13	Yes	Yes
Increased PG Agent Capacity for Mobile Agents, on page 11	Yes	Yes
Enable or Disable Outbound Dialer from Redialing Failed Personal Callbacks (ES65 Update), on page 14	Yes	Yes
Inactivity Timer	Yes	Yes

Webex Experience Management Integration with Post Call Survey

The Voice surveys can be triggered through Webex Experience Management or by using the traditional Post Call Survey (using CVP IVR).

Webex Experience Management surveys use the same scripting and call flows as Post Call Survey, except that the Questionnaire is provided by the cloud-based Experience Management service. The Call Studio survey application, to be invoked, is configured in the router script that runs during the survey leg of the call, and is passed to the CVP through an ECC variable.

The Call Studio application fetches the questions from the Experience Management service, collects the answers from the caller, and submits them to the Experience Management service over REST APIs.

For more information on how to configure Experience Management, see the *Webex Experience Management Integration* chapter in the following documents:

- *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html
- *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Experience Management is supported in all the deployment types. For more information on the call flow and design considerations, see the following documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html
- *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html

Increased PG Agent Capacity for Mobile Agents

The mobile agent capacity on the PG are as follows:

- 2000 with nailed-up connections (1:1)
- 1500 with nailed-up connections if the average handle time is less than 3 minutes, or if agent greeting or whisper announcement features are used with the mobile agent (1.3:1)
- 1500 with call-by-call connections (1.3:1)

For more details, see the *PG Agent Capacity with Mobile Agents* section in the *Sizing and Operating Conditions for Reference Designs* chapter in the following documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html
- *Solution Design Guide for Cisco Packaged Contact Center Enterprise, Release 12.6* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html

SMS and Email Survey after Voice

Cisco Webex Experience Management (referred to as Experience Management), introduced in 12.5(1), is a Customer Experience Management (CEM) solution that allows you to see your business from the perspective of your customers.

In 12.6(1), this feature is extended to SMS and Email. Customers can participate in surveys using the links sent over SMS or email. The survey results help the agents and the supervisors to offer more personalized and contextual experience to the customers.

Administrators can configure and customize the survey in the **Experience Management** console. The responses are displayed on the **Customer Experience Journey** gadget in the Finesse.

For more information, refer to the section *Webex Experience Management Integration* in the following documents:

- *Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html
- *Cisco Packaged Contact Center Enterprise Features Guide, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Non-Production System (NPS)

In this release, Non-Production System (NPS) usage mode is introduced to give you more control on license usage. With NPS, you can switch from production deployment to other deployment types such as lab, testing, and staging.

For more information, refer to the section *Smart Licensing* in one of the following documents:

- *Administration Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html
- *Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Database Schema Changes

Unified CCE Database Schema Changes

This release introduces minor database schema changes. The release includes changes to these tables:

Table	Changes
Smart_License_Server	Added the following columns to the existing table. **1.** UsageMode **2.** SlrEnabled **3.** SlrStatus
As part of Agent Answers added new tables: **1.** Default_Configuration **2.** Agent_Service_Enabled	-
Call_Type	Added a new column called CCAIConfigParamter.
Termination_Call_Detail	Added the following columns to the existing table. **1.** AgentAnswersEnabled **2.** AgentTeamID
ICR_Globals	Added a new column called GlobalSecureFlag.

Password Hashing

This release includes a key security update which allows more secure hashing for agent and supervisor passwords in the non-SSO mode.

A Global switch is introduced in the **Manage Security** tab on Unified CCE Administration console to enforce SHA-256 hashing. When the switch is turned on, the MD5-based hashes are removed. The administrator must re-enter the passwords in the Unified CCE Administration console/Configuration Manager. Then the passwords are hashed with SHA-256 algorithim. For more information on how to enable or disable the global switch see one of the following documents:

- *Cisco Unified Contact Center Enterprise Developer Reference Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-programming-reference-guides-list.html
- *Cisco Packaged Contact Center Enterprise Developer Reference Guide* at https://d1nmyq4gcgsfi5.cloudfront.net/site/packaged-contact-center/documentation/

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

Enhanced Database Migration Tool (EDMT) Support

EDMT is used for seamlessly migrating data across different versions.

During the upgrade from 12.0(1) and 12.5(1) to 12.6(1), you can use EDMT 12.6(1) for data migration and synchronization.

You can also use EDMT 12.6(1), during the Technology Refresh migration from Windows Server 2016 to Windows Server 2019 on 12.6(1).

For more information on EDMT, see the following documents:

- Cisco Unified Contact Center Installation and Upgrade Guide: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
- Cisco Packaged Contact Center Installation and Upgrade Guide: https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html

Enable or Disable Outbound Dialer from Redialing Failed Personal Callbacks (ES65 Update)

You can now update the Dialer registry settings to enable or disable the outbound Dialer from retrying or redialing failed personal callbacks with dialing errors (where the CallResult value is 2).

For more information, see the **Dialer Registry Settings** section in the Cisco Unified Contact Center Enterprise Outbound Options Guide.

Inactivity Timer

Note This feature requires ICM_12.6(2) _ES9 to be installed on the 12.6(2) target system.

Administrators can now configure the inactivity timeout for a session to avoid being logged out after 30 minutes of inactivity. Navigate to the **Unified CCE Administration Portal** > **Call Settings** > **Miscellaneous** tab to set the inactivity time.

For instructions, see the *Miscellaneous* section in the Cisco Packaged Contact Center Enterprise Administration and Configuration Guide.

For instructions, see the *System Setting for Unified CCE Deployment* section in the Administration Guide for Cisco Unified Contact Center Enterprise.

Important Notes

IdS Upgrade

If you are upgrading Cisco Identity Service (IdS) to 12.6(1) and above, after the upgrade, you must reestablish trust relationship between the Identity Provider (IdP) and the IdS. This step is not required if you are using Microsoft ADFS as the IdP.

OpenJDK Java Runtime Update

CCE has transitioned from Oracle to OpenJDK for the Java runtime environment (JRE). The CCE 12.6(1) installer will install the required OpenJDK version. If the existing Oracle JRE is not needed, you may uninstall it from the system manually.

For more information, see the following documents:

- *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
- *Security 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

- *Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html

For information about supported Java 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.

SQL Server Execution Plan Issue

Microsoft SQL Server 2016 and later includes a set of query optimizer enhancements. Under rare circumstances, queries against the Logger historical data have shown higher bandwidth and disk utilization. Interaction with the Logger VM becomes sluggish and the Windows Resource monitor shows close to 100 percent active time on the SQL Server database drive.

If you observe this issue, upgrade Microsoft SQL Server to the latest service pack. If you still experience this issue, run the following query against the database to set compatibility to Microsoft SQL Server 2014:

```
"Alter Database <dbname> set COMPATIBILITY_LEVEL = 120"
```

You can run this query while the system is in operation. For more information about this issue, refer to CSCvw51851.

Tomcat Utility Changes

The `-revert` command, which was used to revert Tomcat to its previous version, is removed. To revert Tomcat to a previous version, run the Tomcat utility with the installer of that Tomcat version.

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

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 3: Deprecated Features

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

Deprecated Feature	Announced in Release	Replacement	Notes
Translation Route Wizard	12.0(1)	Translation Route Explorer	None
Generic PG	11.5(1)	Agent PG and VRU PG	None
ECSPIM/Avaya (Definity) PG using CVLAN interface	11.5(1)	TAESPIM/Avaya (Definity) PG using TSAPI interface	CVLAN interface is deprecated by vendor with limited or no active development support
Webex Experience Management	14 November, 2022	None	Experience Management integration planned.

Removed and Unsupported Features

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

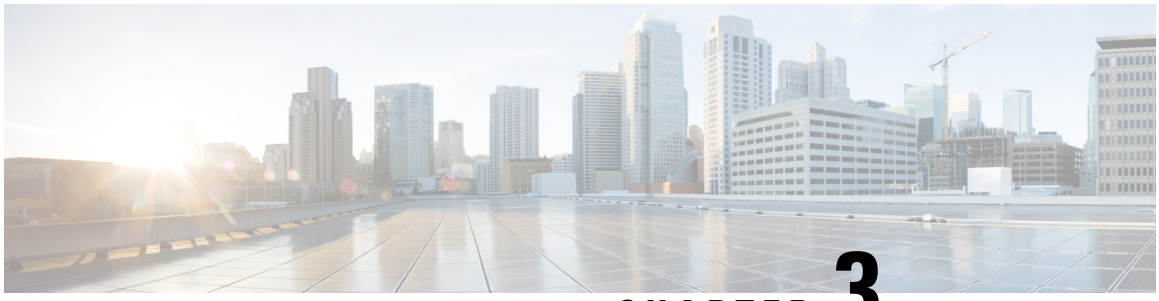
Table 4: Removed and Unsupported Features/Solution

Feature	Effective from Release	Replacement
Internet Explorer 11	12.6(1)	Edge Chromium (Microsoft Edge)
Avaya Aura Contact Center (AACC - formerly Symposium) PG	12.6(1)	Migrate to Contact Center Enterprise or Webex CCE.
Aspect PG	12.6(1)	Migrate to Contact Center Enterprise or Webex CCE.
Symposium ACD	12.6(1)	Migrate to Contact Center Enterprise or Webex CCE.
MIB Objects: • cccaDistAwWebViewEnabled • cccaDistAwWebViewServerName • cccaSupportToolsURL • cccaDialerCallAttemptsPerSec	12.6(1)	None
"Sprawler" deployment	12.6(1)	Packaged CCE deployment

Feature	Effective from Release	Replacement
Customer Journey Analyzer for Business Metrics (Trials)	12.6(1)	None **Note** Customer Journey Analyzer was available for trials only in Release 12.5(1). The trials have been discontinued.
Shared ACD Line	12.6(1)	Agent Device Selection **Note** For more information on device selection, see the *Agent Device Selection* section in *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.
Cisco Hosted Collaboration Solution for Contact Center (HCS-CC)	12.6(1)	Unified CCE / Packaged CCE / Webex CCE.

Third Party Software Impacts

For information about third-party software, 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.



CHAPTER 3

Cisco Unified Customer Voice Portal

New Features

The following features are available in this release:

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.

Virtual Agent–Voice: Onboarding for OEM Customers

Virtual Agent–Voice (VAV), was formerly referred to as Customer Virtual Assistant (CVA) in 12.5(1) release. This feature now provides enhanced onboarding experience to OEM customers (customers who use Cisco's contract, billing, and support for Google's speech services) via Webex Control Hub. OEM customers can use Cisco services coupled with Google's cloud-based AI-enabled speech services.

For details on how to configure VAV onboarding for OEM customers, see the *Virtual Agent–Voice* chapter in the following documents:

Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1) at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

Cisco Packaged Contact Center Enterprise Features Guide, Release 12.6(1) at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Virtual Agent–Voice for Dialogflow CX

Virtual Agent–Voice for Dialogflow CX leverages Google's Dialogflow CX service that allows designing virtual voice agents and creating and connecting complex IVR call flows.

Using Google Dialogflow CX, multiple agents can be created under the same Project ID and can be accessed and managed for different lines of business with a single Google account. For more information, refer to the Google Dialogflow CX documentation at https://cloud.google.com/dialogflow/cx/docs.

Cisco Unified Call Studio's DialogflowCX element is used to engage Google's Dialogflow CX service. For more information, refer to the *DialogflowCX Element* chapter in the *Element Specifications for Cisco Unified CVP VXML Server and Call Studio, Release 12.6(1)* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html.

To use Virtual Agent–Voice for Dialogflow CX on 12.6(1), Assessment to Quality (A2Q) process for Contact Center AI (CCAI) must be completed.

For details on how to configure Google Dialogflow CX for OEM customers, see the *Virtual Agent–Voice for Dialogflow CX* chapter in the following documents:

- *Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html
- *Cisco Packaged Contact Center Enterprise Features Guide, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

The following table lists the minimum version of components required in Unified CCE solution for this feature.

Component	Version
CVP	12.6(1) ES-08
VVB	12.6(1) ES-03
Call Studio	12.6(1) Patch
Cloud Connect	12.6(1)
CCE Components	12.5(1) and higher
ICM	12.5(1) and higher

Note Packaged CCE provides this feature only from release 12.6(1).

Removed and Unsupported Features

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

Deprecated Feature	Announced in Release	Replacement	Notes
Internet Explorer 11	Not applicable[1]	Edge Chromium (Microsoft Edge)	None.

[1] Based on external communication from Microsoft

Important Notes

OpenJDK Java Runtime Environment Update

The 12.6(1) release installs OpenJDK JRE in the CVP installations if the existing installation has Oracle JRE.

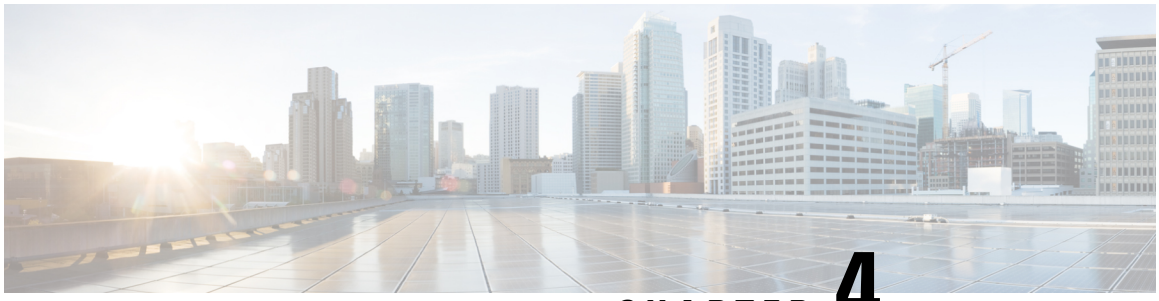
For more information, refer to the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

For more information on JRE minor update, refer to the *Java Runtime Environment Minor Update* section in the *Configuration Guide for Cisco Unified Customer Voice Portal, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

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.

Password Hashing

This release uses salted SHA-256 hashing on user passwords in OAMP, NOAMP, and Serviceability CLI interfaces. The usage of this scheme requires the user to log in once to OAMP, NOAMP, and Serviceability CLI after upgrading to 12.6(1).



CHAPTER 4

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

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.

Maximum Session Count

If a Unified Intelligence Center user reaches the maximum configured session count, that user can log in to another session only after signing out from an active session or if an active session times out due to inactivity. The session timeout duration is configured by using the **set cuic properties session-timeout** command. The maximum session count is configured by using the **set webapp session maxlimit** command. For more information, see the *Command Line Interface* chapter 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.

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.

Report Query Timeout

The administrator can set the report query execution timeout value using the **set cuic properties report-query-timeout** *number of seconds* command. This command is applicable when you run the report using the interface and does not apply to scheduled reports.

For more information, see the *Command Line Interface* chapter 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.

Updated Features

SMTP Settings

If you select the **Use TLS** check box (**Cluster Configuration** > **SMTP Settings**), the communication between the Cisco Unified Intelligence Center and the mail server is encrypted with TLS. By default, SMTP TLS port 465 is used to connect to the mail server. For more information, see the *Cluster Configuration* chapter 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.

All Users Group Access

The administrator can enable or disable the parameter using the set cuic properties allow-allusers-group-ui command.

When this parameter is set to *on*, **AllUsers** group will be visible in the permission modal for non-administrative entity owners to assign permissions.

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.

Live Data

- If Cisco Unified Intelligence Center is upgraded to version 12.6(1) and your Live Data (standalone) server remains on an earlier version (11.6(1), 12.0(1), or 12.5(1)), ensure that you update the Live Data server with the latest ES for that release. This is required for the Live Data gadgets to work in Finesse desktop.
- Live Data 12.6(1) requires a new OVA for all deployments except the 2000 Agent deployment.

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

Log Trace

In this release, the log trace setting in OAMP is removed. The administrator must use the **utils cuic logging** commands to set the log traces.

The following commands are removed:

- **set cuic trace**
- **show cuic trace**
- **utils cuic authorize_remote_node**

Internet Explorer 11

In this release, support for Internet Explorer version 11 is removed. Edge Chromium (Microsoft Edge) is the replacement. For more information about supported browsers, 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.

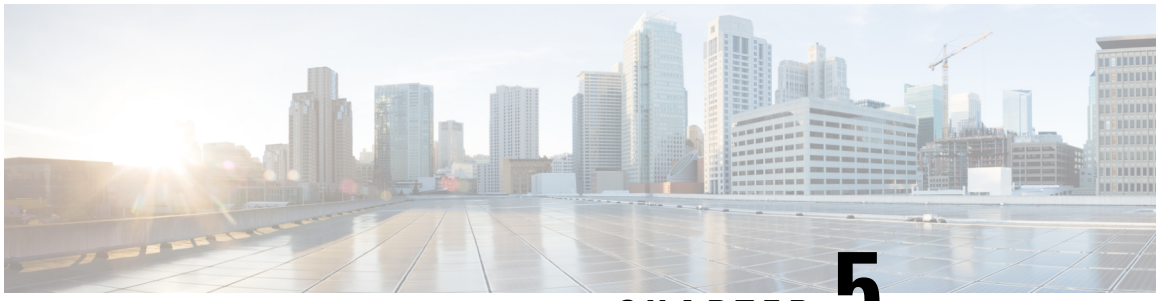
SNMP Object Identifiers (OIDs)

The following SNMP OIDs are removed:

- cuicGeneralInfoServerName
- cuicGeneralInfoServerDescription
- cuicGeneralInfoVersion
- cuicGeneralInfoStartTime
- cuicGeneralInfoTimeZoneName
- cuicGeneralInfoOpsConsoleURL
- cuicReportingTotalKickedOffHistoricalReports
- cuicReportingTotalKickedOffRealTimeReports
- cuicSchedulerStatus
- cuicSchedulerEmailServerStatus
- cuicSchedulerJobsCompletedCount
- cuicSchedulerJobsRunningCount
- cuicSchedulerJobsFailedCount
- cuicSecurityLoginFailedAttempts
- cuicThreadsMaxAvailable
- cuicThreadsRunning
- cuicQueuedTasks
- cuicQueuedTasksMax

Third Party Software Impact

None.



CHAPTER 5

Cisco Finesse

New Features

Locked Out Users (ES02 Update)

A new CLI **utils finesse locked_out_users list** has been added to view the list of locked out users. For more information on the CLI, see the Finesse Administration guide.

Desktop Interface APIs (ES02 Update)

Three new APIs have been introduced, which are primarily used for Finesse desktop development. The 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.

Agent Device Selection

When agents and supervisors need to use different devices that are configured with the same extension, the administrator must enable the Agent Device Selection feature for them. Agents and supervisors can select one of the endpoints (Desk Phone with Extension Mobility, Desk Phone without Extension Mobility, Jabber, and so on) on the shared Automatic Call Distribution (ACD) lines as the active device while signing in to Finesse desktop. This informs the solution to ignore the other devices and use the indicated device as the only source for call interaction. This allows effective control of the call irrespective of from where the user connects

to the system. The user can switch the device based on where they are working, across shifts in an office, moving from one office to another across various locations, or working from home.

When the user signs in with the desired extension, the device selection screen displays a list of devices that share the same extension. If the required device is not listed, the user can refresh the list of devices (if the required device is not listed) and select the device that has to be used as the active device for the current desktop session.

For more information about how to enable or disable the feature, see the *Agent Administration Tasks* section in *Administration Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html.

For more information on device selection, see the *Agent Device Selection* section in *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-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.

Agent PG Maintenance Mode

This release supports peripheral gateway (PG) maintenance mode, which allows the Cisco Finesse server to reconnect to the alternate PG without interrupting the current operations. When the Agent PG maintenance mode is initiated, Finesse desktop users and the Finesse IPPA users do not see any interruption during sign in, state operations, or call operations.

Note This feature is supported with Unified CCE deployments 12.6(1) and above.

For more information see *Agent PG Maintenance Mode* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html

Finesse Maintenance Mode

This release supports transitioning live Cisco Finesse nodes into a maintenance mode for performing administrative tasks, without causing any disruption to contact center activities. This feature is implemented in an automatic phased migration of the Cisco Finesse desktops from the primary node to the secondary node with minimal disruption to the agent activities.

Note This feature is supported with Unified CCE deployments 12.6(1) and above.

For more information, see *Finesse Maintenance Mode* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html

Multi-Tab Gadgets

Finesse desktop supports accessing multiple gadgets through tabs within a single gadget called Multi-Tab gadget. The Multi-Tab gadget allows the desktop to render more gadgets in a single desktop view and thus allows the contact center to efficiently utilize the desktop area. It enables more information to be presented to the agent in a concise and readily accessible manner, without forcing the user to scroll the page or switch the Finesse gadget container to see additional information.

The Multi-Tab gadget can host most gadgets supported by Cisco Finesse desktop. Multiple instances of Multi-Tab gadget containing different groups of gadgets are also supported, which helps users to stack groups of gadgets as required to customize their desktop.

Note The Multi-Tab gadget cannot host the following gadgets:

- Manage Chat and Email gadget (Finesse Agent desktop and Supervisor desktop)
- Advanced Supervisor Capabilities gadget (Finesse Supervisor desktop)

The Multi-Tab gadget functionality supports the maximize and collapse options when configured as a page-level gadget or as a desktop container tab level gadget in the default layout setting.

For more information about this feature, see *Multi-Tab Gadgets* section in *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html

For more information about configuration, see *Configure Multi-Tab Gadgets* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html

Agent Answers

Agent Answers feature provides relevant suggestions and recommendations in real time for the agent to consider. The suggestions and recommendations are based on the ongoing conversation between the caller and the agent.

Note Agent Answers can be configured within the Multi-Tab gadget.

For more information about contact center AI gadgets, see *Contact Center AI Gadgets* in *Cisco Finesse Agent and Supervisor Desktop User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html.

For more information on how to configure Agent Answers gadget, see section *Add Agent Answers Gadgets* in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html

Custom Logon Messages

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 login

messages in the Cisco Unified OS Administration console. For more information, see *Configure Custom Logon Messages* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Change IP Address and Hostname

This release allows the administrator to change the IP address or hostname or domain name of the Cisco Finesse cluster nodes in your deployment.

For more information, see the *Manage IP Address and Hostname* chapter in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Supported Content Security Policy Directives

This release allows the administrator to use the following CLI commands to view, add, or delete the frame-access sources in the response header of Cisco Finesse. This ensures that only the configured sources can embed the Cisco Finesse in an iFrame within their HTML pages.

- **utils finesse frame_access_allowed_list add***[source1,source2]*
- **utils finesse frame_access_allowed_list delete**
- **utils finesse frame_access_allowed_list list**

For more information, see *Supported Content Security Policy Directives* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Set Commands

The following CLIs have been introduced in this release:

Log Configuration

The administrator can use the following CLIs to add, delete, update, or view the logger configuration in the system for Finesse.

utils finesse log configuration {add|update|delete|list}

Secure XMPP Socket Port 5223

The administrator can set the **utils finesse set_property webservices enableExternalNotificationPortAccess** to *true* to enable the external access to the Cisco Finesse Notification Service XMPP port (5223).

Restricting Access to the External XMPP Notification Port 5223

The administrator can restrict the IP addresses from accessing the TCP-based XMPP notification port (5223) available for external client connectivity. The administrator can add, delete, or view the configured IP addresses using the following CLIs:

utils finesse notification external_port_access {add|delete|list}

For more information see, the *Service Properties* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

CUIC Gadget URL

The administrator can use the following release-specific CLIs to change the .jsp references of Cisco Unified Intelligence Center (CUIC) gadgets to .xml in the Finesse desktop layout.

- utils finesse layout updateCuicGadgetUrl 12.5.1
- utils finesse layout updateCuicGadgetUrl 12.6.1+

For more information see, the *Upgrade* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Connected Users Summary

The administrators can view the list of connected users in the current Finesse server.

- utils finesse show_connected_users summary
- utils finesse show_connected_users detail

REST APIs

The following APIs have been added.

- Device—Get List of Devices for Extension—This API allows a user to retrieve the list of devices associated with an extension.
- Finesse MaintenanceMode—This API allows the user to request Finesse to move to maintenance mode. The following are the new Finesse MaintenanceMode APIs:
  - Finesse MaintenanceMode—Get
  - Finesse MaintenanceMode—Update
- ConnectedUsersInfo — This API allows the user to request for the details of the connected users information. The following are the new Connected APIs:
  - ConnectedUserInfo—Summary
  - ConnectedUserInfo—Get Connected Users Information

jQuery

The jQuery version hosted by Finesse has been upgraded from 3.4.1 to 3.5.1.

For more information, see *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!javascript-library.

API Authentication changes for VPN-Less Deployment (ES02 Update)

For changes related to the authentication model when running in VPN-Less deployment, refer to the Cisco Unified Contact Center Enterprise Features Guide. The authentication changes made for VPN-Less deployment, primarily impacts third-party desktops and external API access. It does not impact the Finesse user authentication model and the functionality of the default desktop.

SystemInfo API (ES02 Update)

SystemInfo API is now authenticated when accessed via VPN-Less proxy. For alternatives to be used in non-authenticated mode, refer to the Cisco Finesse Desktop Interface API Guide.

Restricting Access to the External XMPP Notification Port 5223

You can restrict the IP addresses from accessing the TCP-based XMPP notification port (5223) available for external client connectivity. You can add, delete, or view the configured IP addresses only when the `enableExternalNotificationPortAccess` property is enabled on all the Finesse nodes in the cluster. For more information about restricting the access to the port, see the *Restricting Access to the External XMPP Notification Port 5223* section in Cisco Finesse Administration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Updated Features

Reports (ES02 Update)

Historical and Realtime report gadgets are supported in supervisor desktop. The Stock reports can be viewed in the supervisor desktop. To configure custom reports as gadgets, you must run the CLI **set cuic properties allow-proxy-custom-report** command. The report execution dataset size for Historical and Realtime reports can be configured using the CLI **set cuic properties vpnless-response-size-ht** command. For more information, see the CUIC Administration guide.

Drop Participants from Conference

The release allows an agent or a supervisor, who is the participant in a conference call, to drop other agents, supervisors, or non-agents from the conference call. The administrator can customize the desktop property value (`enableDropParticipantFor` and `dropParticipant`) of this feature through the desktop layout:

- Default layout (**Desktop Layout**)
- Team-specific layouts (**Manage Team Resources** > **Desktop Layout**)

Alternatively, the administrator can also set the permission using the CLI **utils finesse set_property webservices enableDropParticipantFor** or the `Dialog—Drop Participant from Conference` API.

For more information on how to set the permissions, see *Drop Participants from Conference* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html and *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!javascript-library.

Dual-Tone Multi-Frequency (DTMF) Updates

This release throttles the number of back-to-back DTMF requests that can be sent by the desktop, to prevent CTI errors. The administrator can configure the number of outstanding DTMF requests and the timeout duration. The administrator can customize the desktop property value (`pendingDTMFThresholdCount` and `dtmfRequestTimeoutInMs`) of this feature through the desktop layout:

- Default layout (**Desktop Layout**)
- Team-specific layouts (**Manage Team Resources** > **Desktop Layout**)

Alternatively, the administrator can also use the following CLIs:

- **utils finesse set_property desktop pendingDTMFThresholdCount** <*value*>
- **utils finesse set_property desktop dtmfRequestTimeoutInMs**<*value*>

Changes in REST APIs

The following changes are made to the payloads.

- User APIs—The following fields are added to the payload:
  - deviceSelection—Indicates whether the CTI device selection is enabled for the agent.
  - activeDeviceId—A unique ID of the active device associated with the extension to which the agent is signed in.
  - Devices—Information about the list of devices associated with an extension.
  - skillTargetId—Indicates the unique identifier for the skill target assigned to the agent in the Unified CCE database.
  - services—Indicates the services that are configured for a user.
- Dialog—Drop Participant from Conference—This API allows an agent or supervisor to make a request to drop other participants from a conference based on the permission set by the administrator. The following fields are added to the payload:
  - ccaiConfigId—Unique configuration ID that is created by the AI service.
  - services—Indicates the services that are configured for a user.
- Single Sign-On APIs—The optional parameters are added in the Fetch Access Token and Refresh Existing Access Token APIs
- SystemInfo APIs—The following fields are added to the payload:
  - ctiTimeInMMode—The total time (in seconds) that the CTI server is in maintenance mode.
  - ctiMMode—Indicates whether the CTI server is in maintenance mode.
  - ctiServers—Information about the list of CTI servers that the Cisco Finesse is connected to.
  - finesseTimeInMMode—The total time (in seconds) that the Finesse server is in maintenance mode.
  - finesseMMode—Indicates whether the Finesse server is in maintenance mode.

For more information, see *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Changes in JavaScript APIs

The following changes are made to the payloads.

- Gadget Configuration—Added the skillTargetId field which refers to the skill ID of the user.
- User—The following functions are added:
  - getSkillTargetId—Retrieves the Id for the skill target assigned to the user in the Unified CCE database.
  - isDeviceSelectionEnabled—Retrieves whether the device selection is enabled for the user.
  - getServices—Retrieves the list of services that are configured for the user.
- SystemInfo—The following functions are added:
  - getCtiMMode—Retrieves the CTI server in maintenance mode.
  - getCtiTimeInMMode—Retrieves the total time (in seconds) that the CTI server is in maintenance mode.
  - getCtiServers—Retrieves the list of CTI servers that Cisco Finesse is connected to.
  - getfinesseMMode—Indicates whether the Finesse server is in maintenance mode.
  - getfinesseTimeInMMode—The total time (in seconds) that the Finesse server is in maintenance mode.

For more information, see *Cisco Finesse JavaScript APIs* chapter in *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!javascript-library.

Serviceability Improvements

This release provides the following serviceability improvements:

- Trace level logging support (*utils finesse log*)
- Fine-grained logging control for critical services (*utils finesse log*)
- ConnectedUsersInfo API to retrieve the list of users signed in to a specific node
- Finesse Maintenance Mode Services (*utils finesse maintenance initiate* and *utils finesse maintenance status*)

For more information about logging improvements and Finesse Maintenance Mode Services, refer to 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 about the ConnectedUsersInfo API, see the *ConnectedUsersInfo* section in the *Cisco Finesse Web Services Developer and JavaScript Guide* at https://developer.cisco.com/docs/finesse/.

Connected Agents Gadget

This release introduces the Connected Agents gadget for administrators that lists all the agents currently signed in to Cisco Finesse. You can use this gadget to determine which agents are signed in to the Publisher and the

Subscriber. You can use this gadget also to filter the client types and identify the client type through which an agent has signed in.

For more information, see the *Manage Connected Agents* section in the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Important Notes

- Finesse desktop now connects to the Notification service using WebSocket or BOSH with https port 8445 instead of 7443. The advantage is that it reduces the number of certificates that needs to be accepted by the desktop during log in.
- Third-party client software can connect to the Notification service using WebSocket or BOSH with either 7443 or 8445 https port.
- The Phonebook container width is increased to 170 pixels in the desktop UI so that more characters are shown without the ellipsis. Any contact name exceeding the preset width (170 pixels) will have an ellipsis and a tool tip next to it to show the full name.
- With the upgrade to Tomcat 9, the "reason phrase" parameter, which provides additional information about the http response according to the status code, is not sent. If the third-party applications that use Finesse APIs build their logic based on the "reason phrase" parameter, the logic will fail.
- Cisco Finesse provides Java Management Extensions (JMX) counters with associated threshold values that can be used to monitor the health of the Finesse. For more information, see the **JMX Counter Thresholds** section in the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.
- The following are some of the new restrictions due to Java version upgrade and CiscoJCE provider:
  - Expired certificates are not supported. All the components in Unified CCE should contain valid certificates.
  - Gadget hosting server's certificate must contain "Digital Signature" as one of the KeyUsage purposes.

Deprecated Features

Notifications over BOSH (Long Polling)

In this release, support for notifications over BOSH (long polling) is deprecated. Applications that require notifications are recommended to use WebSocket-based notifications (Finesse desktop) or notifications over direct XMPP (over TCP).

The usage of port 7443 is deprecated and the port 8445 should be used instead. For the details on how to use port 8445 for WebSocket notifications, refer to the *Managing Notifications in Third-Party Applications* section of the *Cisco Finesse Web Services Developer and JavaScript Guide*.

Removed and Unsupported Features

Internet Explorer 11

In this release, support for Internet Explorer version 11 is removed. Edge Chromium (Microsoft Edge) is the replacement.

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.

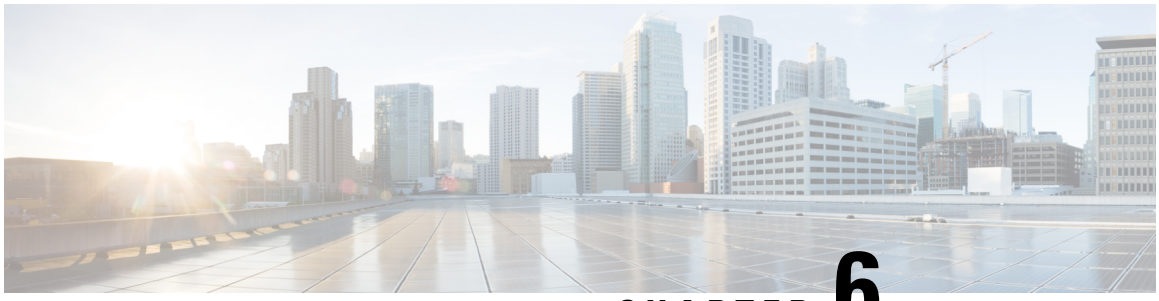
CLIs

The following CLIs are removed:

- utils finesse trace enable
- utils finesse trace disable
- utils finesse trace status
- utils finesse notification logging status

Third Party Software Impacts

None.



CHAPTER 6

Cisco Enterprise Chat and Email

New Features

Support for 2500 Concurrent Agents and Reduced Application and Web Servers for Fully Distributed Model

Note Available starting ECE 12.6(1) ES3 only.

- No change in VMs or agent support for existing 1500 agent deployment.
- For 2500 concurrent agents with 3 Web/App support, use the 2500 Agent OVA.
- For 1500 concurrent agents with 2 Web/App support, use the 2500 Agent OVA.
- The ‘not-required’ application and web servers can be uninstalled and removed by following the appropriate guides.

Decoupled ECE Login/Logout of SSO Agents From Finesse

Note Available starting ECE 12.6(1) ES3 only.

As per previous design, if SSO is configured at Finesse and ECE side and when the agent logs in to Finesse agent desktop, the agent gets logged in automatically to digital channels offered by ECE and doesn't have an option to log out of ECE gadget. This results in consuming a premium license for the agent though the agent doesn't want to work on ECE tasks for that day or session. This results in additional cost on the customers adapting to Smart Licensing. With ECE 12.6(1) ES3, agents will only be logged in to ECE, when they click on ECE gadget and also will be able to log out from only ECE, if they want to. A new logout option is enabled inside the ECE gadget. For more details, refer the Enterprise Chat and Email Agent's Guide, Release 12.6(1).

New Settings for Auto-Completion of Real-Time and Asynchronous Chat Activities

Note Available starting ECE 12.6(1) ES3 only.

- Auto-complete unselected and abandoned real-time chat activities.
- Auto-complete unselected and abandoned asynchronous chat activities.

Platform

Infrastructure

All new installations and systems upgrading to 12.6(1) should use Microsoft Windows and Microsoft SQL Server versions and combinations documented in Compatability Matrix 12.6(1).

Cross-Browser Support

The Administration Console and Agent Console are now supported only on Chrome, Edge, and Firefox browsers. Administration Console and Agent Console are not supported on Internet Explorer. Only the Reports Console is supported on Internet Explorer. The latest version of each browser was tested at time of release.

User Interface in Polish and Czech

The user interface for all consoles is now available in Polish and Czech languages. Note that Dictionary support is not available for these two new languages.

Simplified Administration Console

Simplified Administration Console for Unified CCE

The Administration Console has been fully redesigned to be more contemporary and efficient. The new console streamlines administrative tasks by merging actions that were previously distributed across the Administration, System, and Tools Consoles.

Consolidation of Consoles into the Administration Console

- System Console functions have been consolidated into the new Administration Console. This group of features is available only to users who have system-level view permissions and system-level manage permissions.
- Tools Console functions have been consolidated into the new Administration Console. Some of the utilities within the Tools Console are available only to users who have system- level view permissions and system-level manage permissions.

Reorganization of Configurations and Settings

- Settings and the configuration processes necessary to setup and maintain the product have been restructured and reorganized to improve the user experience.
- Settings that are specific to particular apps or features of the application can be configured within the same space.
- Apps and their configuration elements have been combined to reduce the number of mouse-clicks and navigation necessary to complete an app's configuration process.

Pagination and Filters

- The Administration Console has been restructured to use pagination to improve the user experience. This removes clutter from the console and allows users to navigate through the different functions of the console with ease.
- A filtering search feature is available to help users to quickly find the functions they want. This search feature works across the pagination and auto-completes as the user types in the feature name. Filtering search functionality is available in the List and Properties pages to quickly locate objects in the system and save time during the configuration process.

Enhanced Administration Console for Packaged CCE

As a part of overall Administration Console enhancements, several additions have been made to the ECE administration console that is hosted as a gadget within the Packaged CCE web admin console., This includes the ability to create workflows and supervision monitors, manage storage and purge configuration, and so on. Administrators now do not have to navigate away from the Packaged CCE Administration interface to manage anything specific to ECE, apart for the Reports console.

New Administrator Privileges

System Administrator Privileges

- New privileges have been created for system administrators that supersede all other roles, permissions, and actions: the Manage System Resource and View System Resource privilege.

  When combined, these privileges form a full-fledged system administration user. System administrators can only be created by other system administrators.

- System administrators are granted the View Partition Resource action, by default. This allows them a read-only view of all partition-level and department-level nodes.
- System administrators are now users who can perform system-level tasks. This reassignment of the system administrator's access and permissions reduces the effort required for business users to configure the application to meet their needs.

For details about configuring this feature, see the *Enterprise Chat and Email Administrator's Guide to System Resources* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Partition Administrator Privileges

Two new privileges have been created for partition administrators that supersede other roles, permissions, and actions: The Manage Partition Resource privilege and View Partition Resource privilege.

When combined, the privileges form a full-fledged partition administration user. These users can only be created by other partition administrators.

For details about configuring this feature, see the *Enterprise Chat and Email Administrator's Guide to Administration Console* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Chat Throttling

A security feature has been added to web chat to prevent a single chat client from creating multiple chats and flooding chat queues with spam chats.

- The feature limits the number of chats that can be created from one IP address in one hour.
- This feature is configured in the Security configuration section (Security > Access Restrictions > Blocked Visitors) of the Administration Console and is disabled by default.

For details about configuring this feature, see the Enterprise Chat and Email Administrator's Guide to Administration Console at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html

Audit Reporting for Administration Actions

- All actions performed by an administrator in the application are logged and can be viewed in the Administration Console.
- The new audit interface can be used to view, filter, and trace any specific administrator action performed in the last four weeks.
- This feature ensures that any actions performed in the application can be reviewed and any unintended results can be resolved easily.

For details about configuring this feature, see the *Enterprise Chat and Email Administrator's Guide to Administration Console* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Aria Chat Template

A new chat template, Aria, is available with this release. Aria uses an updated template structure that separates the core and custom components that allows for the styles, appearance, and formatting of the template to be further customized easily.

For more information about personalizing chat templates, see the Enterprise Chat and Email Administrator's Guide to Chat Resources at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Support for Grammarly in the Agent Gadget

The Grammarly browser plugin is now supported in the Agent Console.

APIs

Improved Interaction APIs

Interaction APIs is enhanced to provide the following functionality:

- Users can compose activities with an active queue.
- Users do not need the View Tools Console action to mask the activity if the users with Manage Utilities action is assigned.
- Users assigned with Manage Utilities action can complete activities.
- Users can create a contact point of the apple opaque ID type using the following APIs:
  - Create Individual Customer
  - Edit Individual Customer
- Users can retrieve purge flags and the contact points of the apple opaque ID types using the Get activity by ID and Activity Search APIs.
- Users can edit the content of completed email and chat activities.

With ECE 12.6(1) ES2, the following changes are made to ECE APIs to enhance the experience of obfuscation of customer data:

- Customer search API: Enhanced to incorporate the date of customer creation. The API has a range parameter and returns a list of customers in the specified range.
- Obfuscate customers API: Introduced to obfuscate customers asynchronously. Only one customer information is processed at any given time. As part of running this API, the information of customers that are provided in the request is obfuscated from the application.
- Get Obfuscate Request Status API: Allows users to retrieve the status of a CSV file that is used in the obfuscate customer request. The status helps to identify the successful and failed transactions in the obfuscate customer API request.

Before running the obfuscation APIs, consider the following recommendations:

- Run the APIs during nonbusiness hours.

- Have the number of customers to be obfuscated. The time taken will be high when the number of customers is more.
- To estimate the time taken to run the APIs, refer to the time guidance calculator.
- Run these APIs when there are no maintenance tasks scheduled.

Messaging APIs

New Messaging APIs have been added to allow users to deactivate the webhook callback URL.

- The following new message types are now supported: Delivered, Read and Geolocation
- Customers can retrieve the contact points of the apple opaque ID type by using the Get Conversation Details API.

Routing

Preferred Agent for Chats

Agents can now be set as the preferred agent for a particular customer during chat interactions. After the preferred agent is set, the routing of incoming chat activities from the same customer is configured by Unified CCE scripts to consider the preferred agent for the incoming chat.

- Administrators must add and configure the Queue to Agent node in the Unified CCE script by referencing Call.PreferredAgentID. For more information, about Configuring Queue to Agent Node, see the Scripting and Media Routing Guide at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/User/guide/ucce_b_scripting-and-media-routing-guide_12_6.html.
- The following settings are added to the ECE Administration Console to allow administrators to refine their routing methods for chats in the application.
  - Enable preferred agent assignment—To enable the preferred agent feature in the application.
  - Set last assigned agent as preferred agent—Automatically sends the skill target ID of the agent who most recently handled a customer's chat or messaging activity as the preferred agent ID for the customer to Unified CCE.
  - Allow agent to set preferred agent—Allows agents to mark themselves as the preferred agent for a customer.
  - Allow agent to reset preferred agent—Allows agents to clear the selected preferred agent for a customer.
  - Assign to preferred agent—Determines when to send the preferred agent ID to Unified CCE. One of the following options can be selected: Always, Logged In, and Available.
  - Ignore maximum load for preferred agent assignment—The preferred agent ID is sent to Unified CCE even if an agent has reached the maximum concurrent task limit for chat activities.
  - Preferred agent assignment duration—Determines the length of time for which an agent can be marked as preferred agent for a customer. This duration starts after an activity for which the preferred agent is set gets completed. After this duration is passed, standard routing method is used to assign chat activities.

- Preferred agent assignment duration in days—Determines the number of days for which an agent can be marked as preferred agent for a customer. This duration starts after an activity for which preferred agent is set gets completed.
- Auto-pushback chats from preferred agent—Decides whether to automatically push back chat activities from the preferred agent's inbox if the agent does not click the activity in the time defined in the Expiry time for auto-pushback for chats setting.

Updated Features

Administration

Storage Purge Management and Reporting

The Purge Job feature has been enhanced to the application, providing a self-serve method of purging data. The feature provides centralized reporting of allocated and used data across email and chat in the installation.

- The feature ensures businesses to reduce storage costs.
- The purge jobs process only needs to be configured once, allowing automatic purge jobs to run without any intervention from an administrator.
- The purge jobs process can operate with no service disruptions.
- Diagnostic information and audits are maintained for all purge jobs, ensuring that purge job errors and alerts are handled gracefully.

For more information, see the *Enterprise Chat and Email Administrator's Guide to Administration Console* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Custom Attributes

The system now allows adding custom attributes to the Contact Person Data and make them visible in the Agent Gadget.

Shortcut Settings

A new Enable Shortcuts setting is now available, which can be used to enable or disable the keyboard navigation shortcuts in the Agent Console.

For details about configuring these features, see the *Enterprise Chat and Email Administrator's Guide to Administration Console* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Object Limits

Maximum limit is introduced in the objects creation for performance reasons.

For more details about the object limits, see the *Enterprise Chat and Email Administrator's Guide to Administration Console* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

Agent Gadgets

Conversational View Improvements

- Agents and supervisors can now easily view all communication that has transpired between a customer and an agent through the Reply pane. The following activity types are included in the conversation view: Email, Chat.
- For activities selected from the Main Inbox, an agent can view the most recent communication to and from a customer by clicking the View Conversation option.
- From the Chat Inbox, an agent can scroll up through the chat transcript in the Reply pane. All messages that a customer has sent to and received from the application are displayed. This includes previous chat interactions with other agents.

For details about this features, see the *Enterprise Chat and Email Agent's Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-user-guide-list.html

Chat Monitors

Supervisors can now select multiple agents and queues for monitoring in the Agent Console.

For details about this features, see the *Enterprise Chat and Email Agent's Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-user-guide-list.html

Platform

Note To enable this enhancement in ECE 12.6(1), install the ECE 12.6(1) ES1 patch or the latest ECE ES patch.

ECDSA Support

ECDSA certificates are now supported across secured interfaces (internal and external) and Unified CC Enterprise web services.

Security

Several improvements are made to security and stability. The following vulnerabilities are addressed:

- CVE-2015-5182
- CVE-2020-13920
- CVE-2020-13947
- CVE-2020-1941
- CVE-2021-26117

- CVE-2021-21290
- CVE-2021-21295
- CVE-2021-23899
- CVE-2021-23900
- CVE-2021-20227
- CVE-2020-1945

For more details, refer to Cisco ECE 12.6(1) ES1 readme file.

OAuth2.0 Email Support

Microsoft deprecates Basic authentication. Hence, ECE application uses OAuth 2.0 for authentication through POP and IMAP protocols.

Reports Console

Edge Certification

If the support for Internet Explorer ends, then the reports can be accessed in the compatibility mode of Microsoft Edge.

Important Notes

All the interaction and messaging APIs will be restructured after ECE 12.6(1) release. This release adheres to OpenAPI Specification (OAS) and that results in:

- Standardized API URL formats across all APIs.
- Semantic versioning of the APIs.
- RESTful resource CRUD-based operations.
- Standardized request and response payloads.
    - Error formats, and Page Info.
- Consistent header and query string parameter naming.
    - Paging, Filtering, and Sorting.
- Adopting open standards.

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 5: Deprecated Features

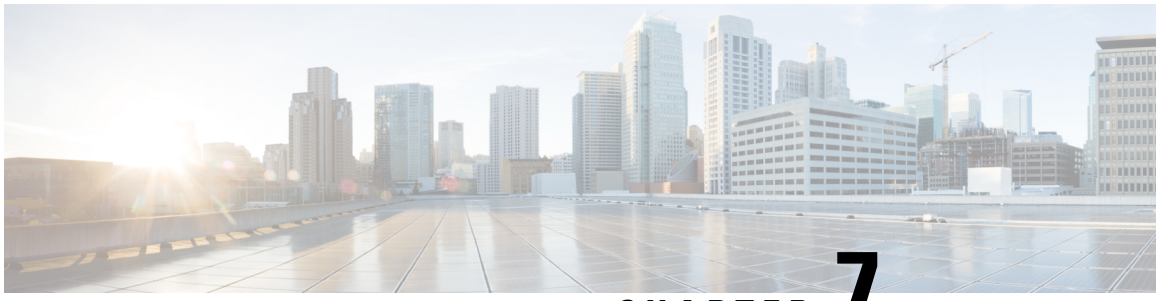
Deprecated Feature	Announced in Release	Replacement	Notes
1500 agent OVAs	12.6 ES2	None	1500 agent OVAs stand deprecated and will be removed post 12.6.
Aqua Chat Template	12.6(1)	None	Aqua template for chat is deprecated in ECE 12.6(1) release. Upgraded customers can continue to use the template. But no new features will be available on these templates.
Reports Console	12.6(1)	None	None

Removed and Unsupported Features

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

Table 6: Removed and Unsupported Features

Feature	Effective from Release	Replacement
Abandoned Chat Notifications for partition users	12.6(1)	None **Note** The abandoned chat notifications can only be sent to department users.
Context Service	12.6(1)	None
Users administration section for PA administrator: • Business • Personal • Miscellaneous	12.6(1)	None **Note** If any of these fields are used in ECE 12.5, it will no longer be accessible in 12.6(1).



CHAPTER 7

Cisco Unified Contact Center Management Portal

New Features

None.

Updated Features

Platform—Infrastructure

All new installations and systems upgrading to Release 12.6(1) must use Windows 2019 and Microsoft SQL Server 2019.

Agent Desk Settings Enhancements

Agents can now use multiple device types or shared lines while accessing the Cisco Finesse desktop. For example, an agent can use a physical phone while working at the contact center and a softphone, such as Jabber, while working at home.

Agent Desk Settings has two new options:

- **ACD shared line usage:** If enabled, this option allows agents to participate in a shared line experience.
- **Tone for auto answer:** This option enables a zip tone when the agent connects. The zip tone can only be enabled if auto-answer is enabled in the desk settings.

Agent Assist Services Enhancements

Agent Assist services can now be enabled per agent. Agent Assist services allow agents to use Cisco Answers and provide seamless responses and suggestions to customer queries.

Call Manager Provisioning Enhancements

This release includes enhanced provisioning for CUCM person, controlled devices and IP Phone provisioning with owner person, and controlled device mapping.

Deletion of Unified CCE Resources Referenced in Scripts

When you attempt to delete Unified CCE resources from the Resource Manager gadget, the system now checks whether the resources are referenced in any scripts. If so, a message is displayed, prompting you to remove the resource from any scripts before proceeding.

Supported Browsers

This release supports the following browsers:

- Microsoft Edge (Chromium)
- Google Chrome
- Mozilla Firefox

Unified CCMP Release 12.6(1) does not support any version of Internet Explorer.

Improved Version Information for Application

The About Unified CCMP page in the application now shows more detail and in a more user-friendly format. The page includes information about the release name, release version number, and the patch history for the installation.

Deprecated Features

The following features are deprecated in this release.

SOAP Support for Resource Manager APIs

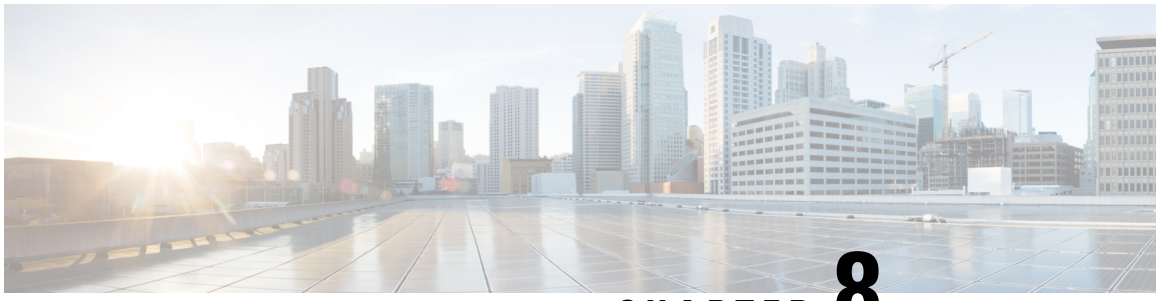
SOAP support for resource manager APIs will be removed post release 12.6(1). Only REST-based access will be supported.

Legacy Resource Manager

Legacy Resource Manager, the traditional three-pane view to manage and maintain resources on Unified CCE, will be removed post release 12.6(1). There will be no new features, enhancements, or bug fixes for Legacy Resource Manager. We recommend that you use the Resource Manager gadgets available with Unified CCMP for resource management-related tasks.

XML Format Support for Web Service APIs

Web Service APIs will now only support the JSON format as the support for the XML format will be removed post release 12.6(1).



CHAPTER 8

Cisco Unified Contact Center Domain Manager

New Features

None.

Updated Features

Platform—Infrastructure

All new installations and systems upgrading to Release 12.6(1) must use Windows 2019 and Microsoft SQL Server 2019.

Agent Desk Settings Enhancements

Agents can now use multiple device types or shared lines while accessing the Cisco Finesse desktop. For example, an agent can use a physical phone while working at the contact center and a softphone, such as Jabber, while working at home.

Agent Desk Settings has two new options:

- **ACD shared line usage:** If enabled, this option allows agents to participate in a shared line experience.
- **Tone for auto answer:** This option enables a zip tone when the agent connects. The zip tone can only be enabled if auto-answer is enabled in the desk settings.

Agent Assist Services Enhancements

Agent Assist services can now be enabled per agent. Agent Assist services allow agents to use Cisco Answers and provide seamless responses and suggestions to customer queries.

Call Manager Provisioning Enhancements

This release includes enhanced provisioning for CUCM person, controlled devices and IP Phone provisioning with owner person, and controlled device mapping.

Deletion of Unified CCE Resources Referenced in Scripts

When you attempt to delete Unified CCE resources from the Resource Manager gadget, the system now checks whether the resources are referenced in any scripts. If so, a message is displayed, prompting you to remove the resource from any scripts before proceeding.

Supported Browsers

This release supports the following browsers:

- Microsoft Edge (Chromium)
- Google Chrome
- Mozilla Firefox

Unified CCDM Release 12.6(1) does not support any version of Internet Explorer.

Improved Version Information for Application

The About Unified CCDM page in the application now shows more detail and in a more user-friendly format. The page includes information about the release name, release version number, and the patch history for the installation.

Deprecated Features

The following features are deprecated in this release.

SOAP Support for Resource Manager APIs

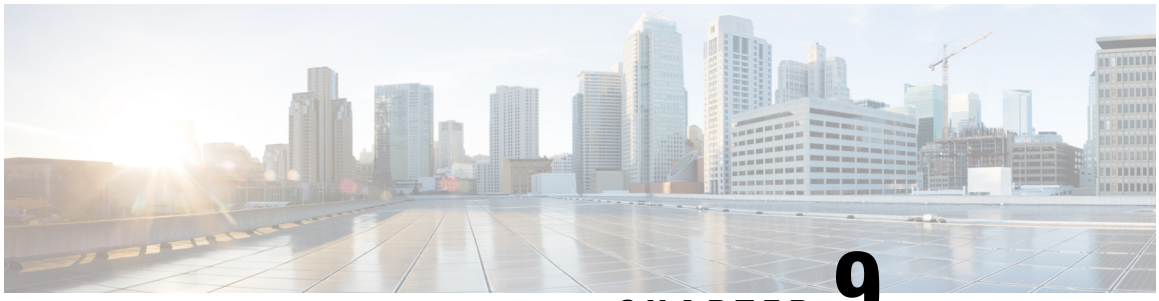
SOAP support for resource manager APIs will be removed post release 12.6(1). Only REST-based access will be supported.

Legacy Resource Manager

Legacy Resource Manager, the traditional three-pane view to manage and maintain resources on Unified CCE, will be removed post release 12.6(1). There will be no new features, enhancements, or bug fixes for Legacy Resource Manager. We recommend that you use the Resource Manager gadgets available with Unified CCDM for resource management-related tasks.

XML Format Support for Web Service APIs

Web Service APIs will now only support the JSON format as the support for the XML format will be removed post release 12.6(1).



CHAPTER 9

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 12.6(1)

Use the following links to the Bug Search Tool to view a list of Severity 3 or higher caveats for each solution 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 Enterprise

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=268439622&rls=12.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Packaged Contact Center Enterprise

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284360381&rls=12.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Unified Intelligence Center and Cisco IdS

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282163829&rls=12.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Cloud Connect

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&rls=12.6(1)&sb=anfr&bt=custV

Cisco Unified Customer Voice Portal

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=270563413&rls=12.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Finesse

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613135&rls=12.6,12.6(1)&sb=anfr&bt=custV

Cisco Customer Collaboration Platform

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613136&rls=12.6(1),12.6&sb=anfr&bt=custV

Cisco Unified Contact Center Management Portal

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286325298&rls=12.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Unified Contact Center Domain Manager

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286281169&rls=12.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Enterprise Chat and Email

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286311237&rls=12.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Virtualized Voice Browser

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286290211&rls=12.6(1)&sb=anfr&svr=3nH&bt=custV