Release Notes for Unified Contact Center Enterprise, Release 12.5(1)

First Published: 2020-01-21

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** 1

Release Notes for Contact Center Solutions 1

Cisco Security Advisories 1

Multi-server SAN Certificates 2

CHAPTER 2 **Unified Contact Center Enterprise** 3

New Features 3

VPN-less Access to Finesse Desktop (For Agents and Supervisors) 3

Agent Answers 4

Support for 36000 Agents 4

Edge Chromium Browser Support 5

Smart Licensing 5

Cloud Connect 5

Cisco Webex Experience Management 5

Experience Management Voice Surveys 6

Experience Management Email/SMS Surveys 6

Agent Summary Live Data Report 6

Encryption Support for External DBLookUp Registry Configuration 6

Campaign Skillgroup Dialing Mode 7

Live Data CLIs 7

Agents Placing Outbound Calls in Available State 7

Shared ACD Line 8

Customer Journey Analyzer for Business Metrics (Trials) 8

Webex Workforce Optimization (WFO) Support with Contact Center Enterprise (CCE) Solutions 9

Updated Features 9

Increased PG Agent Capacity for Mobile Agents 9

Non-Production System (NPS) 9
Security Enhancements 9
Tomcat Upgrade 10
Configuration Limit Changes 10
Replication Enhancements 10
Outbound Option Predictive Algorithm Enhancements 10
Database Schema Changes 11
Important Notes 14
OpenJDK Java Runtime Environment Update 14
SocialMiner Renamed 14
Certificate Validation 14
Outbound Option Import Rule 14
Deprecated Features 14
Removed and Unsupported Features 15
Third Party Software Impacts 16

CHAPTER 3 **Cisco Unified Customer Voice Portal** 17
New Features 17
Edge Chromium Browser Support 17
Customer Virtual Assistant 17
Smart Licensing 18
Send DTMF 18
DTMF Tone Overlay 18
Voice Activity Detection (VAD) 18
Waveform URI 18
VVB Media Streaming 19
Updated Features 19
Important Notes 19
Informix Upgrade 19
OpenJDK Java Runtime Environment Update 19
Certificates Removed on Upgrade 19
TLS Version Support 20
Cisco VVB 12.5(1) SU 20
Deprecated Features 20

Removed and Unsupported Features 20
Third Party Software Impacts 20

CHAPTER 4 Cisco Unified Intelligence Center 21
New Features 21
Edge Chromium Browser Support 21
User Experience Changes 21
CUIC CORS Enablement 22
Updated Features 22
User Role Changes 22
Enable or Disable Custom Widgets in Dashboards 22
Important Notes 23
Deprecated Features 23
Removed and Unsupported Features 24
Third Party Software Impacts 24

CHAPTER 5 Cisco Finesse 25
New Features 25
Edge Chromium Browser Support 25
Improvements to Finesse Failover 25
Keyboard Shortcuts 27
Desktop Chat Search 27
Edit Call Variables 27
Drag-and-Drop and Resize Gadget or Component 27
Gadget Expand and Collapse 28
Desktop Layout Editors 28
Customize Desktop Properties 28
Configuration for Cloud Connect 28
WebProxy Service 29
Security Banner Message 29
Automatic Desktop Login Retries 29
Finesse IP Phone Agent Certificate Management 29
HTTP Secure Support 30
HTTP/2 Support 30

Enhanced Log Collection 30
Set Commands 30
REST APIs 32
JavaScript APIs 32
Updated Features 33
Security Enhancements 33
Failure Message for Login 33
Prevent Non-Voice Task RONAs during CTI Reconnect 34
Team Performance Gadget 34
Queue Statistics Support 34
Phone Book Contact Limit 35
Changes in REST APIs 35
Changes in JavaScript APIs 35
Important Notes 35
Deprecated Features 35
Removed and Unsupported Features 36
Third Party Software Impacts 36

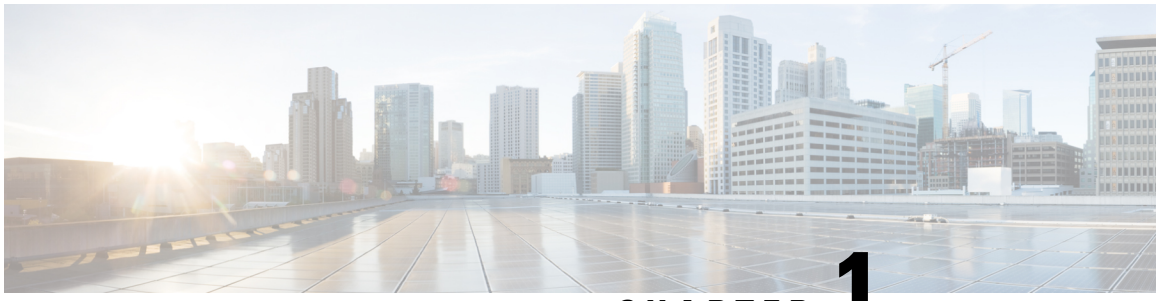
CHAPTER 6 **Cisco Enterprise Chat and Email** 37
New Features 37
Edge Chromium Browser Support 37
Ability to Block Chat Customers 37
Finesse Shortcuts 37
Messaging Hub 38
Calltrack 38
APIs 38
Login and Logout APIs 38
Interaction APIs 39
Messaging APIs 39
Updated Features 39
Headers, Footers, Greetings, Signatures, and Auto-Acknowledgements Limitation 39
Popover Configuration Improvements 39
Agent Efficiency Improvements 40
Chat Monitors 40

Deprecated Features 40
Kiwi Chat Template 40
Third-party Software Impacts 40

CHAPTER 7 Cisco Customer Collaboration Platform 41
New Features 41
Updated Features 41
Important Notes 41
Deprecated Features 41
Removed and Unsupported Features 42
Third Party Software Impacts 42

CHAPTER 8 Cisco Unified Contact Center Management Portal 43
Legacy Resource Manager Deprecated 43

CHAPTER 9 Caveats 45
Caveat Queries by Product 45
Bug Search Tool 45
Severity 3 or Higher Caveats for Release 12.5(1) 46



CHAPTER 1

Introduction

- Release Notes for Contact Center Solutions, on page 1
- Cisco Security Advisories, on page 1
- Multi-server SAN Certificates, on page 2

Release Notes for Contact Center Solutions

In addition to the release notes in this document, see the release note compilations for the other contact center solutions at the following links:

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

For Release Notes of other Contact Center solutions from Cisco, refer to the following links:

- *Release Notes for Cisco Packaged Contact Center Enterprise Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html
- *Release Notes for Cisco Hosted Collaboration Solution for Contact Center* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-release-notes-list.html
- *Release Notes for Cisco Unified Contact Center Express Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-release-notes-list.html

Cisco Security Advisories

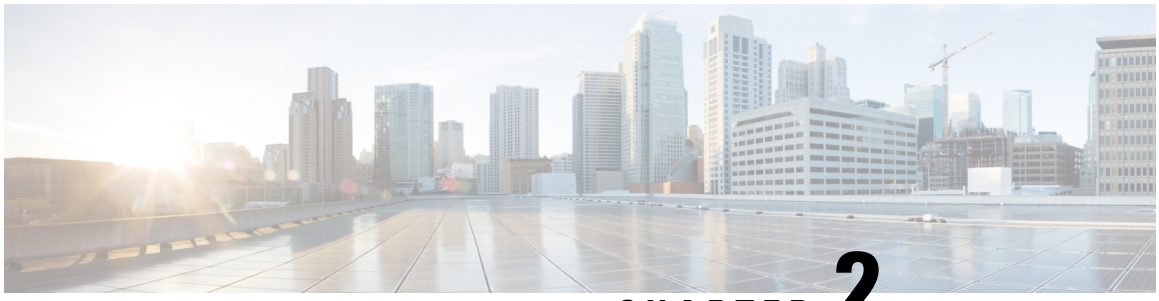
The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that relates to Cisco products and networks.

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

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

Unified Contact Center Enterprise

- New Features, on page 3
- Updated Features, on page 9
- Important Notes, on page 14
- Deprecated Features, on page 14
- Removed and Unsupported Features, on page 15
- Third Party Software Impacts, on page 16

New Features

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 solution 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 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-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 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

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).

Note The following engineering specials are required to support 36000 agents:

- ICM_12.5(1)_ES45
- CUIC_12.5(1)_ES07 if you are using Live Data

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.

Note To enable this browser support in **Administration Client Setup for Cisco Unified ICM/Contact Center Enterprise**, install the ICM_12.5(1)_ES30.

Smart Licensing

This release introduces Smart Licensing that delivers visibility into your license ownership and consumption. Smart Licensing helps you to procure, deploy, and manage licenses easily and report license consumption. It pools license entitlements in a single account and allows you to move licenses freely through the virtual accounts.

Smart Licensing registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager On-Prem.

For more information, see *Configuration 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.

For more information, see *Administration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Cloud Connect

Cloud Connect is an infrastructure component that hosts services that enable integration with Cisco Webex Cloud Services, such as Cisco Webex Experience Management.

Cisco Webex Experience Management

Cisco Webex Experience Management (referred to as Experience Management) is the platform for Customer Experience Management (CEM), integrated with powerful tools that allow you to see your business from your customer's perspective.

With Experience Management integrated with Unified CCE:

- Administrators can configure post call surveys to collect feedback directly from customers.
- Administrator can configure and initiate digital channel surveys when the agent responds to an email or chat from a customer by using the Enterprise Chat and Email gadget.
- Administrators can configure analytical gadgets, which can be viewed on the Finesse desktop.
- Agents and Supervisors can view pulse of the customers through industry standard metrics such as NPS, CSAT, and CES, or other KPIs.

See Experience Management Voice Surveys, on page 6

See Experience Management Email/SMS Surveys, on page 6

Experience Management Voice Surveys

The voice surveys can be triggered through Experience Management, using CVP IVR. Experience Management surveys use the same scripting and call flows as Post Call Survey, with the exception that the questionnaire is provided by the cloud-based Experience Management service. The Call Studio survey 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 CVP Call Studio survey 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* chapter in the *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

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

Experience Management Email/SMS Surveys

This feature allows customers to participate in the post-call surveys using links sent over SMS or Email.

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

For more information on the list of tasks required to integrate Experience Management, refer to the section *Experience Management Task Flow* in *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

Agent Summary Live Data Report

This release adds the Agent Summary Live Data report which displays real-time agent statistics such as not ready time, total number of calls handled, and wrap-up time. This report is also available in a Finesse gadget and displays agent statistics to an agent and team statistics to a supervisor. The report is useful when monitoring the performance of an agent.

For details see the *Cisco Unified Contact Center Enterprise Reporting User Guide, Release 12.5* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

Encryption Support for External DBLookUp Registry Configuration

External DBLookUp registry configuration will support only encrypted value, the CCEDataProtect Tool is used to encrypt and decrypt sensitive information that the Windows registry stores in it. After upgrading to Release 12.5, if the DBLookUp is configured, then you must reconfigure the external DBLookUp registry value using the CCEDataProtect Tool to encrypt the data in the registry. For more information, refer to the **Configure External DBLookUp Registry Value using CCEDataProtect Tool** procedure 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.

Campaign Skillgroup Dialing Mode

Configure the mode and percentage of the Campaign Skillgroup directly from the Campaign Skillgroup tab. This eliminates the need to use an administrative script to update the skill groups dynamically. An administrative script, if used, will override the configuration changes made from the Campaign Skillgroup tab.

For more details, see the Administrative Scripts for Outbound Option and Set Up an Administrative Script sections in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

Live Data CLIs

Live Data HSTS Configuration

This release allows an Administrator to turn on or off HTTP Strict Transport Security (HSTS) on live-data and also show the current status of the HSTS property.

HSTS is a web security policy mechanism that helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that the web browsers (or other complying user agents) interact with it using only secure HTTPS connections, and never through the insecure HTTP protocol.

For more information, see *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.

Live Data HTTP Configuration

This release allows an Administrator to turn on or off HTTP access to live-data and also show the current status of the http-enabled property.

Any changes to http-enabled status needs a restart of CCE Live Data NGINX Service.

Note By default, HTTP is disabled. You can enable HTTP (if required) using the `set live-data properties http-enabled on` command.

For more information, see *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.

Agents Placing Outbound Calls in Available State

If agents in Available state place outbound calls, the Unified CCE system sets the agent's state to NotReady before allowing the call (without manually setting the agent's state to NotReady from the CTI interface). The system changes the agent's state back to Available when the call ends or fails to connect.

For details on the reason code, see the *Database Schema Handbook for Cisco Unified ICM/Contact Center Enterprise, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/

unified-contact-center-enterprise/products-technical-reference-list.html. For details on the call manner type, see the *CTI Server Message Reference Guide (Protocol Version 23) for Cisco Unified Contact Center Enterprise, Release 12.5(1)*.

This enhancement also enables the Finesse Make Call from Ready feature via the Finesse API. For details, see Changes in REST APIs, on page 35 and the *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Shared ACD Line

Note Shared ACD line feature introduced in an ICM_12.5(1)_ES4, will require additional configuration in case you want to use it on 12.6(1). The behavior changes are: in that you will now select which device to use when you log into Finesse. It also requires a change in agent desk settings to enable for the agent.

1. When you log in to Finesse, you will now select which device to use.
2. Additional changes are required in agent desk setting incase you want to enable it for the agents.

This release includes shared ACD lines support for up to two devices. The support enables an agent with devices at different locations to utilize the same extension.

Note UCM auto-answer and Agent Desk Settings auto-answer are not supported when shared ACD lines are in use.

For more information, see the *Call Type Considerations for Phone Extensions* section in the *Solution Design Guide for Cisco Unified Contact Center Enterprise, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Customer Journey Analyzer for Business Metrics (Trials)

Customer Journey Analyzer is a cloud service that processes historical contact center data from on-premise deployment to generate specific Business Metrics across the contact center. It displays trends to help you identify patterns and gain insight for continuous improvement. You can view the Abandoned Contacts dashboard on the Customer Journey Analyzer which enables supervisors and business analysts to identify where contacts are being abandoned and take appropriate action. You can use Customer Journey Analyzer to create visualizations using Customer Activity Records, Customer Session Records, and Agent Activity Records.

Note Customer Journey Analyzer is available as Trials. Please contact your Cisco Support to get started on Trials.

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

Increased PG Agent Capacity for Mobile Agents

Added on May 14th, 2021

The mobile agent capacity on the PG has increased 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 at *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

Non-Production System (NPS)

Note This feature requires ICM_12.5(1)_ES25 to be installed on the 12.5(1) target system to enable the Non-Production System (NPS) .

Non-Production System (NPS) usage mode gives 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, see the *Smart Licensing* section in the *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.

Security Enhancements

This release introduces following security enhancements for CCE Administration:

- It is mandatory to import self-signed certificates (if CA-signed certificates are not used) of Solution components into the AW machines.

For more information, see the *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.

- HTTP Security headers (Content-Security-Policy (CSP), X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, and Strict-Transport-Security) have been introduced in the browser response to prevent cross-site scripting (XSS) vulnerabilities.

Tomcat Upgrade

Tomcat is upgraded from 7.0.x to 9.0.21.

Configuration Limit Changes

The following configuration limits have increased from this release:

- Outbound dialer maximum calls per second per dialer increased from 20 to 60 for the 2000 agent deployment and from 30 to 60 for the 4000 agent, 12000 agent, and 24000 agent deployments.
- Outbound dialer maximum ports per SIP dialer increased from 1500 to 3000 for all the deployment types.
- Number of campaigns per system increased from 600 to 1500 for all the deployment types.

For more details see the *Outbound Campaign Limits* section in the *Solution Design Guide for Cisco Unified Contact Center Enterprise, Release 12.5* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Replication Enhancements

With Outbound Option High Availability, replication of data is managed by the Campaign Manager running on the standby side, through a series of files in a replication folder. For more information, see *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

Note Direct access to the Personal_Callback_List table is not supported with Outbound Option High Availability enabled. Use the Outbound API to insert customer records directly into the Personal_Callback_List table. For information on Outbound APIs, see the *Cisco Unified Contact Center Enterprise Developer Reference* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-programming-reference-guides-list.html

Outbound Option Predictive Algorithm Enhancements

Note To enable these Outbound Option enhancements, you must install the ICM_12.5(1)_ES90 on 12.5(1).

The following enhancements have been made to the Outbound Option feature:

- *EnhancedPredictiveDialing*, a new registry setting is added to reduce the idle time when there is a low hit rate for voice customers and when the agent idle times are long. This change adapts to the dialing rate more aggressively, irrespective of the configured abandon limit. This feature is disabled by default.
- The logic associated with the existing *ReclassifyTransferFailures* registry setting is modified so that the answering machine calls that are abandoned due to lack of agent or IVR resources are not counted as abandoned voice calls but as answering machine calls. *ReclassifyTransferFailures* registry setting is enabled by default on fresh installs and disabled by default in upgraded systems.

For more information, see the *Dialer Registry Settings* section in the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

Database Schema Changes

Unified CCE Database Schema Changes

Release 12.5.1 includes several changes to the database schema for the main database. The release adds the following new tables:

- Smart_License_Server
- Smart_License_Info
- Smart_License_Entitlements
- Smart_License_Product

The release includes datatype changes to the following tables:

Table	Changes
Config_Message_Log	Changed datatype of ConfigMessage to varbinary(max).
Event	Changed datatype of BinData to varbinary(max).
Application_Event	Changed datatype of BinData to varbinary(max).
Feature_Control_Set	Changed datatype of FeatureSetData to varbinary(max).
Route_Call_Detail	Changed datatype of CallTrace to varbinary(max).
Machine_Connection_Profile	Changed datatype of Password to varbinary(max).
Machine_Service	• Changed datatype of EnablePassword to varbinary(max). • Changed datatype of Password to varbinary(max).
Script_Real_Time	Changed datatype of ScriptMeters to varbinary(max).
Script_Data	Changed datatype of ScriptData to varbinary(max).
System_Capacity_Interval	Changed datatype of DbDateTime to DBDATETIME NULL.

The release added new fields to the following tables:

Table	Changes
ICR_Globals	Added these fields: • AnalyzerIntegrated • CVPCxSurveyAppName
System_Capacity_Interval	Added these fields: • MaxVoiceAgentsLoggedIn • MaxNonVoiceAgentsLoggedIn • MaxAgentsHandledPrevOB • MaxAgentsHandledPredProgOB • MaxPerpetualPremiumAgentsLoggedIn • MaxFlexStdAgentsLoggedIn • MaxFlexPremiumAgentsLoggedIn • CustomerDefinitionId
System_Capacity_Real_Time	Added these fields: • MaxVoiceAgentsLoggedIn • MaxNonVoiceAgentsLoggedIn • MaxAgentsHandledPrevOB • MaxAgentsHandledPredProgOB • MaxPerpetualPremiumAgentsLoggedInNow • MaxStdAgentsLoggedInNow • MaxPremiumAgentsLoggedInNow • MaxCVPCallControlPorts • MaxVRUPorts • CustomerDefinitionId • FutureUseInt3 • FutureUseInt4

Table	Changes
Agent_Event_Detail	Added these fields: • RouterCallKey • RouterCallKeyDay • PeripheralCallKey • AgentDialedNumber • EventDateTimeUTC • DialedNumber • TaskIndex • AgentSessionId • AgentState • RouterCallKeySequenceNumber • Direction • PrecisionQueueID • SkillGroupID • WrapupData
Route_Call_Detail	Added the CallStartDateTimeUTC field.
Termination_Call_Detail	Added these fields: • AnsweredDateTimeUTC • WrapUpStartDateTimeUTC • ConsultStartDateTimeUTC • ConsultEndDateTimeUTC • ConferenceStartDateTimeUTC • ConferenceEndDateTimeUTC • TransferredDateTimeUTC • CallTerminatedDateTimeUTC • AgentSessionId
User_Group	Added the EmailAddress field.

The release removed this field from the following table:

Table	Changes
ICR_Globals	Removed the ContextServiceConnectionData field.

Important Notes

OpenJDK Java Runtime Environment Update

A new 12.5(1a) base installer is available for customers, which has OpenJDK JRE as the supporting Java runtime for all CCE applications. It is no different from the preceding 12.5(1) installer except for the Java runtime environment installed on the CCE virtual machines (VMs).

You can continue to use Oracle JRE if you installed CCE 12.5(1) before the release of 12.5(1a). Further Java security updates and fixes can be downloaded and installed from the Oracle website.

There is no requirement to redeploy/reinstall existing 12.5 CCE VMs using the 12.5(1a) installer to switch to OpenJDK. Download and install ES55 (mandatory OpenJDK ES) instead, as needed.

However, if you want to install any ESs released after ES55 on 12.5(1), then you must first install ES55 (mandatory OpenJDK ES) on the relevant VMs as a prerequisite.

SocialMiner Renamed

SocialMiner will be referred to as Customer Collaboration Platform from release 12.5(1) onwards.

Certificate Validation

All components now enforce certificate validations. If you use any third-party Certificate Authority (CA) signed or self-signed certificates for any components that are not trusted by the platform by default, then the certificates must be mandatorily imported into the dependent component server trust store.

For more information, see *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.

Outbound Option Import Rule

In Outbound Option Import Rule, when you add or modify a field in the import rule table, change the target table name to save your changes to the import rule. After the name change, the old table remains in the database, but the system does not use it.

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.

Please review the applicable notes for details about exceptions or other qualifiers.

Deprecated Feature	Announced in Release	Replacement	Notes
Internet Explorer 11	Not applicable[1]	Edge Chromium (Microsoft Edge v79 and later)	None.
Avaya Aura Contact Center (AACC - formerly Symposium) PG	12.5(1)	None.	None.
UCC Enterprise Gateway PG (Parent PG in Parent-Child deployments)	12.5(1)	None.	None.
Aspect PG	12.5(1)	None.	None.
Integrity Check Tool	12.0(1)	None.	None.
External Script Validation	12.0(1)	None.	None.
Translation Route Wizard	12.0(1)	None.	None.
Symposium ACD	12.0(1)	None.	None.
MIB Objects: • cccaDistAwWebViewEnabled • cccaDistAwWebViewServerName • cccaSupportToolsURL • cccaDialerCallAttemptsPerSec	11.6(1)	None.	None.
Generic PG	11.5(1)	Agent PG and VRU PG	None
ECSPIM	11.5(1)	TAESPIM	Avaya SEI/CVLAN protocol was deprecated by vendor.
"Sprawler" deployment	10.0(1)	A Packaged CCE deployment	A "Sprawler" was a Progger with an Administration & Data Server on a single box. It was used for lab deployments.

[1] Based on external communication from Microsoft

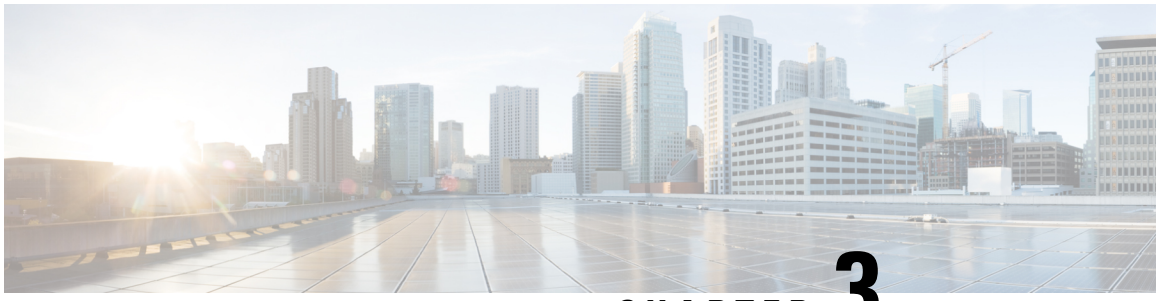
Removed and Unsupported Features

The following features are no longer available:

Feature	Effective from Release	Replacement
Context Service	12.5(1)	None.
Cisco MediaSense	12.5(1)	None.
SHA-1 certificate	12.5(1)	SHA-256
TLS 1.0 and TLS 1.1	12.5(1)	TLS 1.2
Cisco Remote Expert Mobile	12.5(1)	None.

Third Party Software Impacts

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



CHAPTER 3

Cisco Unified Customer Voice Portal

- New Features, on page 17
- Updated Features, on page 19
- Important Notes, on page 19
- Deprecated Features, on page 20
- Removed and Unsupported Features, on page 20
- Third Party Software Impacts, on page 20

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.

Customer Virtual Assistant

Customer Virtual Assistant (CVA) enables the IVR Platform to integrate with cloud-based speech services. CVA provides the following speech services:

- **Text to Speech**: Integration with cloud-based TTS services in your application for Speech Synthesis operations. CVA currently supports Google Text to Speech service.
- **Speech to Text**: Integration with cloud-based ASR services in your application for Speech Recognition operations. CVA currently supports Google Speech to Text service.
- **Speech to Intent**: CVA provides capability of identifying the intent of customer utterances by processing the text received from Speech to Text operations. CVA offers this service by using cloud-based Natural Language Understanding (NLU) services CVA currently supports Google Dialogflow service.

For more information, see *Customer Virtual Assistant* chapter in *Feature Guide for Cisco Unified Contact Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html.

Smart Licensing

This release introduces Smart Licensing that delivers visibility into your license ownership and consumption. Smart Licensing helps you to procure, deploy, and manage licenses easily and report license consumption. It pools license entitlements in a single account and allows you to move licenses freely through the virtual accounts.

Smart Licensing registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager On-Prem.

For more information, see *Configuration 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.

For more information, see *Administration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Send DTMF

This feature supports playing a Dual Tone Multi Frequency (DTMF) tone as a prompt in VVB.

For more information, see *Developer Guide for Cisco Virtualized Voice Browser* at https://developer.cisco.com/site/customer-voice-portal/documents/virtual-voice-browser/.

DTMF Tone Overlay

DTMF tone overlay provides the capability to enable injection of DTMF tones (overlay) on the caller stream at random intervals during the recognition of sensitive data. For more information, see *Digits* chapter in *CVP Element Specification Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Voice Activity Detection (VAD)

VAD enables VVB to handle events like start of speech, end of speech, total recording duration to reduce the initial silence duration based on configuration from Call Studio. It also enables configuring Cisco VVB to various levels of silence sensitivity.

For more information, see *Record* chapter in *CVP Element Specification Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Waveform URI

Record utterance uses Waveform URI to enable application developers to collect URI for the recordings done in the ASR systems. A new parameter `recordutterance` is introduced in the `Form` element in Call Studio. When the value of this parameter is set to `true`, the recordings are done in the ASR systems and the URI of the recording is sent back to VXML server for further use.

For more information, see *Form* chapter in *CVP Element Specification Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

VVB Media Streaming

VVB now supports continuous streaming of media through HTTP(S) from a streaming URL.

For more information, see *Audio* chapter in *CVP Element Specification Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Updated Features

None.

Important Notes

Informix Upgrade

The 12.5(1b) base installer is now available for customers, which has support for IBM Informix 14.10 FC8 version for the Unified CVP application. This release is supported on Windows Server 2016 and Windows Server 2019.

For more information, refer to the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

OpenJDK Java Runtime Environment Update

The 12.5(1b) base installer has OpenJDK JRE as the supporting Java runtime for the Unified CVP application. It is the same as the preceding 12.5(1) installer, except that in the 12.5(1b) base installer, the Java runtime environment is installed on the Unified CVP virtual machines (VMs).

Note For JRE update post installation of 12.5(1b), refer to the OpenLogic OpenJDK site (https://www.openlogic.com/openjdk-downloads) to download the JREs.

For more information, refer to the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.5(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 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Certificates Removed on Upgrade

After the successful upgrade to VVB 12.5(1) and CVP 12.5(1), the CAs that are unapproved by Cisco are removed from the platform trust store. However, you can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see the *Cisco Trusted External Root Bundle* at https://www.cisco.com/security/pki.
- For information about adding a certificate, see *Insert a New Tomcat-trust Certificate* section in the *CUCM Certificate Management and Change Notification* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-tech-notes-list.html.

TLS Version Support

This releaae supports only TLS 1.2. For more information, see *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html.

Cisco VVB 12.5(1) SU

A new Service Update (SU) release is available for Cisco Virtualized Voice Browser 12.5(1). You can perform a fresh installation or upgrade from 12.5(1) version to Cisco VVB 12.5(1) SU on supported virtual machines. For more information, see the ReadMe.

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.

Deprecated Feature	Announced in Release	Replacement	Notes
Internet Explorer 11	Not applicable[2]	Edge Chromium (Microsoft Edge v79 and later)	None.

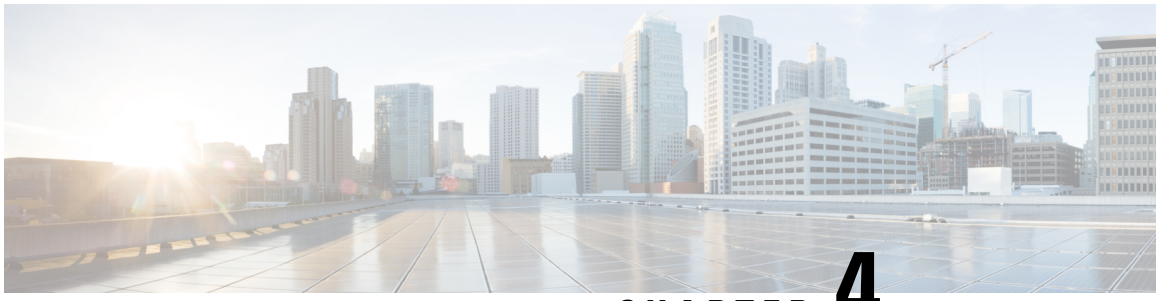
[2] Based on external communication from Microsoft

Removed and Unsupported Features

TLS 1.0 and TLS 1.1 are not supported in this release. However, these versions have not yet been removed completely in order to prevent backward compatibility breakage.

Third Party Software Impacts

None.



CHAPTER 4

Cisco Unified Intelligence Center

Note A new Service Update (SU) release is available for Cisco Unified Intelligence Center 12.5(1). You can perform a fresh installation or upgrade to Cisco Unified Intelligence Center 12.5(1) SU on supported virtual machines from previous versions. For more information, see the ReadMe.

- New Features, on page 21
- Updated Features, on page 22
- Important Notes, on page 23
- Deprecated Features, on page 23
- Removed and Unsupported Features, on page 24
- Third Party Software Impacts, on page 24

New Features

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.

User Experience Changes

This release provides an improved user experience to configure, edit, and manage the following Administration Console entities:

- User Management
- Device Configuration
- Log and Trace Settings
- Control Center Management
- Cluster Configuration

- Tools Management

For more information, see *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.

CUIC CORS Enablement

In this release, an administrator can perform the following actions for Cross-Origin Resource Sharing (CORS) on Unified Intelligence Center:

- Enable, disable, and view CORS status
- Add, delete, and list the allowed headers
- Add, delete, and list the exposed headers
- Add, delete, and list the allowed origin URLs

For Unified Intelligence Centre gadgets (Live Data and Historical) to load in Cisco Finesse, you must:

- Enable CORS using the **utils cuic cors enable** command.
- Set the Finesse host URL in the **utils cuic cors allowed_origin add URLs** command.

For Live Data gadgets, in addition to the above settings, ensure to enable CORS using the **utils live-data cors enable** command and set the Finesse host URL in the **utils live-data cors allowed_origin add URLs** command. For more information, see *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

User Role Changes

- When you modify the user account information of a user who is currently signed in, that user gets signed out automatically.
- When the signed in user is in the Run As mode of another user, modifying the user account information of either of the users stops the Run As mode.

Enable or Disable Custom Widgets in Dashboards

In this release, to address injection vulnerabilities, the **Custom Widget** feature in **Dashboards** is disabled by default. If any custom widgets were added to the **Dashboards** in versions earlier to Unified Intelligence Center 12.5, those widgets are visible in the read-only mode post upgrade to version 12.5. You can opt to retain or delete them.

An administrator can enable or disable the **Custom Widget** feature using the **set cuic properties dashboard-customwidget-enabled** CLI.

For more information, see *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.

Important Notes

Access Administration Console

The URL to access the Administration Console is https://<HOST ADDRESS>/oampui, where HOST ADDRESS is the IP Address or Hostname of your server.

You must access the legacy OAMP user interface (https://<HOST ADDRESS>/oamp) to configure **Policy Information** for the user.

Certificate Removed on Upgrade

After the successful upgrade, the CAs that are unapproved by Cisco are removed from the platform trust store. You can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see the Cisco Trusted External Root Bundle at https://www.cisco.com/security/pki.
- For information about adding a certificate, see Insert a new tomcat-trust certificate.

Large Schedules Frequency on Upgrade

After upgrade to Unified Intelligence Center version 12.5, all large schedules with frequency more than once per day will be converted to run only once per day.

Report Thresholds - Image Location

This release supports only image URLs that are reachable from Unified Intelligence Center server. Maximum size limit that is allowed for an image is 5MB.

Install Language ES

After successful install or upgrade, if you want to use the Cisco Unified Intelligence Center interface in a language other than English, you have to download and install the language pack ES.

Deprecated Features

Internet Explorer 11

In this release, Internet Explorer version 11 is deprecated. Edge Chromium (Microsoft Edge v79 and later) is the replacement.

Removed and Unsupported Features

Cisco Unified Intelligence Center Licenses

In this release, the application of Cisco Unified Intelligence Center licenses during fresh install or upgrade is removed.

By default, Cisco Unified Intelligence Center is provisioned with licenses when you install or upgrade to version 12.5.

HTTP Support for Unified Intelligence Center

In this release, the HTTP support for Unified Intelligence Center has been removed. The users can now securely communicate to Unified Intelligence Center over HTTPS.

The following CLIs are removed from Unified Intelligence Center release 12.5:

- show cuic properties http-enabled
- set cuic properties http-enabled
- show cuic properties hsts
- set cuic properties hsts on [max-age value in seconds]
- set cuic properties hsts off

Authenticated Excel Permalink on Office 365

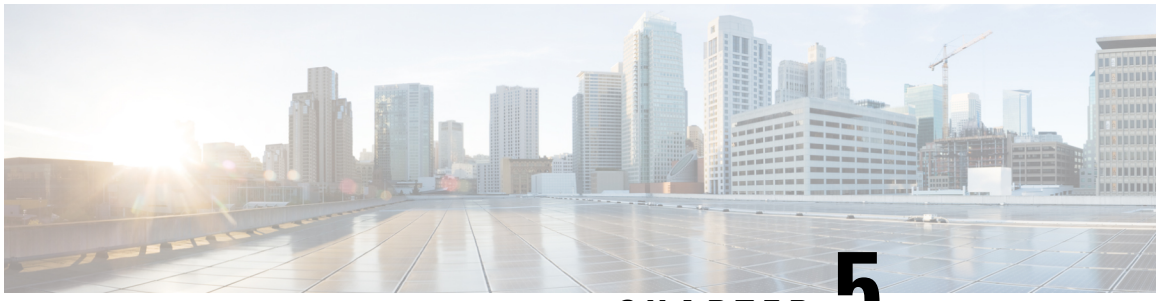
Authenticated Excel report permalink is not supported on Office 365.

MediaSense Reports

In this release, MediaSense reports are removed and users cannot run MediaSense reports.

Third Party Software Impacts

None.



CHAPTER 5

Cisco Finesse

Note A new Service Update (SU) release is available for Cisco Finesse 12.5(1). You can perform a fresh installation or upgrade to Cisco Finesse 12.5(1) SU on supported virtual machines from previous versions. For more information, see the ReadMe.

- New Features, on page 25
- Updated Features, on page 33
- Important Notes, on page 35
- Deprecated Features, on page 35
- Removed and Unsupported Features, on page 36
- Third Party Software Impacts, on page 36

New Features

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.

Improvements to Finesse Failover

This release optimizes the Cisco Finesse CTI failover and Desktop failover performances.

- CTI Failover—When deployed with Agent PG 12.5(1), CTI server/Agent PG failover varies approximately from 35 seconds to 75 seconds. When deployed with Agent PG 12.0(1) or 11.6(1), CTI server/Agent PG failover varies approximately from 75 seconds to 120 seconds.
- Desktop Failover—When deployed with Agent PG 12.5(1), desktop failover with the default desktop layout varies approximately from 50 seconds to 110 seconds. When deployed with Agent PG 12.0(1) or 11.6(1), desktop failover is approximately 40 seconds more when compared to Agent PG 12.5(1).

When OVA with 8 vCPUs is configured for Cisco Finesse, the time taken for CTI server/Agent PG failover and desktop failover improves by 20 percent. This configuration is supported on all deployment types including the 24000 Agent deployment type. For more information on OVA with 8 vCPUs, see *Virtualization for Cisco Finesse* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-finesse.html.

The total failover time varies depending on the WAN bandwidth, the number of signed-in users, network latency, number of vCPUs configured, Agent PG version, and the number of gadgets configured on the Finesse desktop. Most of the desktop failover improvements (as opposed to CTI failover) are also available with earlier versions of the Agent PG.

For more information on deployment practices and guidelines to ensure optimal failover performance, see *Guidelines for Optimal Desktop Failover* and *Failover Planning* sections in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

For more information on ensuring how the custom gadgets improve failover performance, see *Best Practices for Gadget Development* section in *Cisco Finesse Web Services Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Desktop Performance Improvements

This release optimizes the Finesse desktop performance in the following areas:

- Uses HTTP/2 by default for loading resources. This provides significant improvement when starting up the desktop compared to the older HTTP 1.1.
- Consumes significantly lesser desktop bandwidth when reloading the Finesse desktop (without gadgets) from the cache.
- Uses fewer requests for loading resources.
- Serves static resources much faster using client-side resource caching.
- Provides cached REST responses at a team-level for configuration data to improve the desktop loading.
- Improves gadget loading by caching the gadget definitions.

Finesse Server Performance Improvements

This release optimizes the Finesse server performance in the following areas.

- Significantly reduces the average CPU consumption while the server is under load.
- Optimizes the server performance by avoiding dynamic server pages, using SSL termination, faster CTI message parsing, and cached static resources.
- Provides access to more memory and reduces GC latencies as the Cisco Finesse server uses 64-bit Java 8.
- Optimizes CTI request processing to reduce the latencies in sending requests to the server.
- Reduces overall latencies for CTI communication.

Keyboard Shortcuts

This release provides keyboard shortcuts for easy access to the Finesse desktop features. The keyboard shortcuts define an alternate way to perform a specific action on the Finesse agent and supervisor desktop. The administrator can set the **utils finesse set_property desktop enableShortCutKeys** to *true* to enable this feature.

For more information, see *Access Keyboard Shortcuts* 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.

Desktop Chat Search

This release allows you to refine the desktop chat search to display the user details based on the Organization Unit (OU) defined in Cisco Unified Communications Manager IM and Presence Service. The administrator can use the following CLIs to configure the OU-based user search in Cisco Finesse.

- **utils finesse set_property desktop desktopChatOUSearchFieldKey** <*value*>
- **utils finesse set_property desktop desktopChatOUSearchFieldValue** <*value*>

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

Edit Call Variables

This release allows agents and supervisors to edit the call variable values from the Finesse desktop. The administrator can configure any of the callVariable values, including ECC variables as editable. The agent and the supervisor can edit the call variable values during an active call or in the wrap-up state.

Note Call variables edit operation updates the values of the variables within the particular call. All entities listening to dialog events receive the updated call variables through the Cisco Finesse notifications. If any CTI clients are connected to the same Agent PG, they also receive notifications of the changed call data though CTI call events. However, application scripts or databases that are used to populate the call variables are not directly affected by this edit.

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

Drag-and-Drop and Resize Gadget or Component

This release allows agents and supervisors to drag-and-drop or resize the gadgets or components in the Finesse desktop. The administrator can customize the desktop property value of these features through the desktop layout:

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

Alternatively, the administrator can also set the **utils finesse set_property desktop enableDragDropAndResizeGadget** to *true* to enable these features.

For more information, see *Drag-and-Drop and Resize Gadget or Component* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Gadget Expand and Collapse

This release supports to expand and collapse of gadgets dynamically in the Finesse desktop to optimize available screen space.

For more information, see *Container Services* section in JavaScript Library at https://developer.cisco.com/docs/finesse/#!javascript-library.

Desktop Layout Editors

This release provides two types of editors in the **Desktop Layout** and **Team Resources** of the Cisco Finesse administration console.

- **Text Editor**—A plain text editor. It is the default editor. Use the **Expand All** option to see all the code details and **Search** box to refine results.
- **XML Editor**—An XML editor. The administrator cannot add or edit comments (<!-- -->) in this editor.

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

Customize Desktop Properties

This release allows the administrator to customize the desktop properties for individual Teams through the desktop layout using the following layouts:

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

For more information, see *Customize Desktop Properties* and *Customize Desktop Properties at Team Level* sections in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Configuration for Cloud Connect

This release allows the administrator to configure the Cloud Connect server settings in the Finesse administration console to contact the Cisco Cloud Services, such as Cisco Webex Experience Management.

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

WebProxy Service

This release introduces WebProxy Service within the Finesse server to provide SSL termination and caching services to the Finesse service to reduce latency and improve performance. For more information, see *WebProxy Service* section in *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html.

Gadget developers must bypass the proxy to access the updated gadget responses for testing purposes. For more information, see *Best Practices for Gadget Development* section in *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/#!rest-api-dev-guide.

Security Banner Message

This release provides custom banner messages in the administrator and desktop Sign In pages. The administrator can use the following CLIs to define the custom security banner message.

- **utils finesse set_property desktop desktopSecurityBannerMessage** <*value*>
- **utils finesse set_property admin adminSecurityBannerMessage** <*value*>

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

Automatic Desktop Login Retries

This release supports automatic desktop login retries when the desktop login fails due to device-related errors. The administrator can use the following CLIs to enable, define the number of attempts and intervals in seconds for the retry login mechanism. By default, the value of this property is set to true.

- **utils finesse set_property desktop enableRetryLoginFeature** {*true*|*false*}
- **utils finesse set_property desktop loginFailureRetryAttempts** <*value*>
- **utils finesse set_property desktop loginFailureRetryInterval** <*value*>

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

Finesse IP Phone Agent Certificate Management

This release requires HTTPS for Finesse IP Phone Agent (IPPA) to address the security vulnerabilities across the solutions. The administrator must ensure to import the following certificates and configuration changes to use the FIPPA functionality.

- Import the Cisco Unified Communications Manager (CUCM) certificate to the trust store as **tomcat-trust**.
- Import the Cisco Finesse certificate to the CUCM trust store as **Phone-trust**.

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

HTTP Secure Support

This release supports only HTTP Secure (HTTPS). Support for HTTP is disabled for the administration console, desktop (agent and supervisor), Web Services, Desktop Modules (gadgets), and Finesse IPPA. All the HTTP requests are automatically redirected to HTTPS.

For HTTPS access, enter: `https://FQDN of Finesse server:8445/`

For more information on disabled ports, see Cisco Finesse Important Notes, on page 35.

HTTP/2 Support

This release supports HTTP/2 protocol by default.

Enhanced Log Collection

3rdpartygadget Log Directory

This release provides the 3rdpartygadget log directory, which contains information, error, startup, and shutdown-related logs for the Finesse 3rdpartygadget server.

WebProxy Service Logs

The administrator can use the **file get activelog webproxy recurs compress** CLI to obtain logs for the WebProxy Service.

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

Automatic Log Collection for Desktop Users

The administrator can use the following CLI to create, list, and delete automatic desktop log collection schedules for agents and supervisors.

utils finesse desktop_auto_log_collection {*create*|*list*|*delete*}

For more information, see *Log Collection Schedule* 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:

Call Variables Logging

The administrator can use the following CLIs to enable or disable the call variables logging.

- **utils finesse set_property webservices logCallVariables** {*true*|*false*}
- **utils finesse set_property fippa logCallVariables** {*true*|*false*}

Enforcement of X.509 Certificate Trust Validation

The administrator can set the **utils finesse set_property webservices trustAllCertificates** to *false* to enable the validation of the X.509 CA or the self-signed certificate.

Mobile Agent

The administrator can set the **utils finesse set_property desktop enableMobileAgentLogin** to *true* to enable Sign in as a Mobile Agent feature on the Finesse desktop Sign In page.

Preloading of the Secondary Resources

The administrator can set the **utils finesse set_property desktop preLoadSecondaryResources** to *true* to enable the preloading of static resources from the secondary server to ensure faster failover.

XMPP Socket and BOSH/WebSocket (HTTP)

The administrator can set the **utils finesse set_property webservices enableInsecureOpenfirePort** to *true* to enable the Cisco Finesse Notification Service unsecure XMPP port (5222) and HTTP-BOSH/WebSocket port (7071).

Update Cisco Unified Intelligence Center Gadget URL

JSP format for Cisco Unified Intelligence Center gadgets is not supported. To change the JSP format references to the XML format, the administrator can run the CLI **utils finesse layoutupdateCuicGadgetUrl** on the Finesse server.

User Authentication Discovery API

The administrator can set the **utils finesse set_property webservices enableUserAuthMode** to *true* to enable the `UserAuthMode` API.

For more information, see *User APIs* section in *REST API Developer Guide* at https://developer.cisco.com/docs/finesse/.

WORK Mode Retention for Non-Voice

The administrator can set the **utils finesse set_property desktop enableAutoWorkModeStateChange** to *false* to enable the agent to retain WORK mode after CTI reconnection (non-voice).

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

WebProxy Service

The administrator can use the following CLIs to clear, set access log-level and log-severity for the logs that are generated by the WebProxy Service.

- **utils webproxy cache clear**
- **set webproxy access-log-level**
- **set webproxy log-severity**
- **show webproxy access-log-level**

- **show webproxy log-severity**

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

REST APIs

The following APIs have been introduced in this release:

- CompressedClientLog—Post Compressed Log to Finesse
- Cloud Connect Configuration—Get
- Cloud Connect Configuration—Set
- Cloud Connect Integration—Delete
- ECCVariableConfig—Get ECC Variable Configuration
- Media—Change Agent from Work State to Active
- Single Sign-On—Get User Authentication Mode
- TeamResource—Get Reason Codes
- TeamResource—Get Wrap-Up Reasons
- TeamResource—Get Media Properties Layouts
- TeamResource—Get Phone Books
- TeamResource—Get Workflows
- User—Get User Id from loginName

REST API Response Caching

In order to improve login performance, the Finesse webproxy caches the following REST API responses:

- ChatConfig
- ECCVariableConfig
- MediaDomain
- TeamResource APIs include Reason Codes, Wrap-Up Reasons, Media Properties Layouts, Phone Books, and Workflows. The responses of the TeamResource API are cached at the team-level.

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

JavaScript APIs

The following APIs have been introduced in this release:

- finesse.shortcutkey.ShortcutKeyService

- finesse.utilities.DesktopCache

For more information, see *JavaScript Library* at https://developer.cisco.com/docs/finesse/#!javascript-library.

Updated Features

None.

Security Enhancements

This release implements the following security changes:

- By default, Cisco Finesse Notification Service unsecure XMPP port 5222 and BOSH/WebSocket (HTTP) port 7071 are disabled.

  For more information on enabling the ports, see *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.

- Validation of the X.509 certificate is enforced. It is mandatory to have the following valid non-expired X.509 CA or self-signed certificates, which must be imported into the Cisco Finesse trust store.
  - Cisco Finesse node certificates are available by default. The administrator must verify the validity of the certificates, as non-expired certificates are invalid.
    - Valid non-expired Cisco Finesse primary certificate must be present on the secondary Cisco Finesse.
    - Valid non-expired Cisco Finesse secondary certificate must be present on the primary Cisco Finesse.
  - Import the CUCM certificate to both the primary and secondary Finesse nodes.
  - Import the IdS certificate to both the primary and secondary Finesse nodes.
  - Import the Customer Collaboration Platform server certificates to both the primary and secondary Finesse nodes in Unified CCE.
  - Import the LiveData server certificates to both the primary and secondary Finesse nodes in Unified CCE.
  - Import the Cloud Connect server certificates to both the primary and secondary Finesse nodes in the Unified CCE.

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

Failure Message for Login

This release displays detailed error messages corresponding to login failures on the Finesse desktop. This allows the administrator to respond to client login failures without referring to the logs.

The error messages are updated for both UI and API.

- The Finesse desktop UI is updated to include the 2nd Level Text error messages provided by CTI operations for sign-in scenarios.

  Peripheral error codes 12004 and 12005 are replaced with desktop sign-in retries. When the sign-in retry fails, it displays the 2nd Level Text error messages provided by CTI operations.

- The Cisco Finesse API payloads are updated to include the peripheral error codes and 2nd Level Text error messages provided by CTI operations. The newly added parameters are:
  - peripheralErrorCode
  - peripheralErrorMsg
  - peripheralErrorText

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

Example

13036 PERERR_GW_E_JTAPIOBJ_PERFORMANSWERCALL_NO_TERMINAL_CONNECTION

```
1st Level Text = 'JTAPI Gateway - Error on ANSWER operation'
2nd Level Text = 'The routine performAnswerCall in class JTapiObj got a null connection
from a call to 'findTerminalConnection'
```

Prevent Non-Voice Task RONAs during CTI Reconnect

This release provides `Media—Change Agent from Work State to Active` API to signal the availability of media channels explicitly, after CTI reconnection. This can significantly reduce RONAs, since tasks are not routed to the agent until the agent is available in the non-voice MRD.

The CLI command **utils finesse set_property desktop enableAutoWorkModeStateChange** is introduced to enable or disable the feature.

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

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

Team Performance Gadget

In the Team Performance gadget, supervisors can use the **Search** box to refine any agent details by using the search criteria such as Agent Name, State, or Extension.

Queue Statistics Support

The maximum number of agents and supervisors that are supported in Queue Statistics is increased from 1500 to 2000.

Phone Book Contact Limit

The maximum number of contacts per agent across all phone books is increased from 1500 to 6000.

Changes in REST APIs

The following payloads are updated:

- MediaPropertiesLayout APIs—The `uiEditable` payload indicates if the call variable values can be edited in the Finesse desktop (agent and supervisor).

Dialog—Create a New Dialog (Make a Call)

The `MAKE_CALL` API is updated to make a call from Ready state. When an agent goes off-hook to place a call, the Unified CCE changes the agent status to Not Ready with 50006 reason code.

Login Name Support

The `User—Get User Id from loginName` API is updated to accept the **`loginName`** in URI and authentication for both SSO and non-SSO deployments.

Phone Book Contact Limit

The maximum number of contacts per agent is increased from 1500 to 6000 in the `Phone Book` and `Contact` APIs.

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 functions are updated:

- ContainerServices—The `collapseMyGadget` and `expandMyGadget` functions, that hide and display the gadget contents respectively.
- DialogBase—The `updateCallVariables` function updates the dialog's call variables.

For more information, see *JavaScript Library* at https://developer.cisco.com/docs/finesse/#!javascript-library.

Important Notes

Deprecated Features

GET APIs

The following GET User APIs are deprecated. These APIs are available for backward compatibility and have lower performance compared to the TeamResouce APIs.

- ReasonCode
- WrapUpReason
- MediaPropertiesLayout
- PhoneBook
- WorkFlow

Internet Explorer 11

In this release, Internet Explorer version 11 is deprecated. Edge Chromium (Microsoft Edge v79 and later) is the replacement. For more information, see the *Contact Center Express Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html

Notifications over BOSH (Long Polling)

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

Removed and Unsupported Features

Context Service Management

The Context Service Management feature is removed from the Cisco Finesse administration console.

HTTP Support

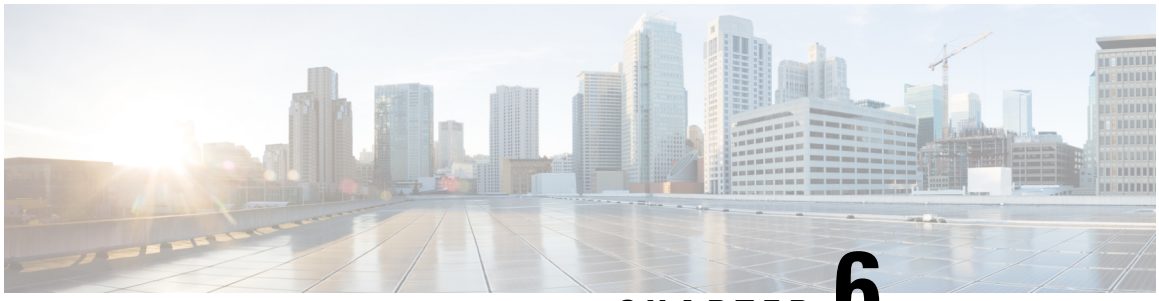
The HTTP support for Cisco Finesse is removed. You can now securely communicate to Cisco Finesse over HTTPS.

The following CLIs are removed:

- **utils finesse application_https_redirect status**
- **utils finesse application_https_redirect enable**
- **utils finesse application_https_redirect disable**

Third Party Software Impacts

None.



CHAPTER 6

Cisco Enterprise Chat and Email

- New Features, on page 37
- Updated Features, on page 39
- Deprecated Features , on page 40
- Third-party Software Impacts , on page 40

New Features

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge v79 and later) for Agent Desktops. For more information, see *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.

Ability to Block Chat Customers

Agents can now block chat customers that appear to be spam bots, or visitors who are trolling the company or the agent. The administrator can enable this feature and configure option to block chat visitors based on Browser Cookie or Visitor IP Address. When the feature is enabled by administrators, agents get the option to block customers per chat. The customer is then blocked from creating chats from that browser instance/IP Address for the number of days set by the administrator. Supervisors have access to the list of customers who are blocked and can unblock them if needed.

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

Finesse Shortcuts

Finesse Shortcuts for availability controls are now available for Agents.

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

Messaging Hub

Messaging is increasingly becoming the most popular way customers are choosing to engage with businesses. With so many messaging platforms and channels, it is important for a business to be able to provide an experience to customers and a consistent experience for their agents. eGain Messaging Hub provides a consistent messaging experience for their customers and agents across all messaging channels (synchronous and asynchronous).

eGain Messaging Hub add-on enables ECE to connect to the messaging platform Facebook Messenger and Twitter Direct Messaging seamlessly. It can also interface with eGain Virtual Assistant for automatic handling of the queries before escalating to an agent assistance.

Calltrack

eGain Calltrack is a case management solution that helps companies provide quick, high-quality, and cost-efficient resolution of customer issues.

eGain Calltrack add-on for ECE makes agents more efficient and productive as it provides them complete customer context across all channels including email, chat and voice, which helps them resolve the cases promptly and correctly. Additionally, agents can categorize and add notes to the Calltrack activity.

APIs

These new APIs were introduced/enhanced in ECE 12.5:

- Login and Logout APIs, on page 38
- Interaction APIs, on page 39
- Messaging APIs, on page 39

Login and Logout APIs

New APIs are provided to achieve the following functionality:

- SAML assertion with bearer token can be used to log a user into the application using Single Sign-On.

Existing APIs have been enhanced to provide the following functionality:

- Authenticate client application enhancements.
- The client application session will now expire after a fixed duration, even if it is not inactive.
- A maximum of 10 concurrent sessions can be created for each client application.
- Supports a query parameter to force a login even if there are 10 concurrent sessions by terminating the earliest session.
- Customer Single Sign-On supports external ID.

For more information about the APIs, see the Enterprise Chat and Email's *Interaction API Developer Guide* at https://developer.cisco.com/docs/enterprise-chat-and-email/#!interaction-api-developer-guide

Interaction APIs

New APIs are provided to achieve the following functionality:

- Users can get the information about the product version and installed licenses using the `Get application details` API.

For more information about the APIs, see the Enterprise Chat and Email's *Interaction API Developer Guide* at https://developer.cisco.com/docs/enterprise-chat-and-email/#!interaction-api-developer-guide

Messaging APIs

New APIs are provided to achieve the following functionality:

- Client applications can invoke an API to activate the webhook callback URL.

Existing APIs have been enhanced to provide the following functionality:

- A new conversation can be initiated for the following social contact types: Facebook, Twitter.
- Get conversation API response will now have message type as text/plain or text/html instead of text.
- The message type text is not supported anymore as part of Send Message API. Instead, the clients can now use text/plain or text/html. This API also supports error type of message.
- The message type text is not supported anymore as part of posting messages on the Webhook Callback URLs. Instead, the application will either use text/plain or text/html.

For more information about the APIs, see the Enterprise Chat and Email's *Interaction API Developer Guide* at https://developer.cisco.com/docs/enterprise-chat-and-email/#!interaction-api-developer-guide

Updated Features

Headers, Footers, Greetings, Signatures, and Auto-Acknowledgements Limitation

The Headers, Footers, Greetings, Signatures, and Auto-Acknowledgements templates text should not exceed beyond 600 characters. Post ECE 12.5, the product will enforce these limits and will not allow users to add more than 600 characters to these templates.

Popover Configuration Improvements

Administrators can now add call variables information in the Finesse popovers displayed to agents from the Administration Console.

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

Administrators can now configure the counter value and counter type for popover notifications.

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

Agent Efficiency Improvements

Agents can now click the **Attachments** icon to access and download attachments from all the places in the Agent Console where the activity information is available. In addition to administrators, supervisors can now pick activities from the default exception queue.

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

Chat Monitors

While monitoring chats, supervisors can now view the name of the agent in the Inbox tile view. The agent information provides the supervisor context on the agent handling the chat and helps them in deciding to monitor chats for specific agents.

For details about using this feature, see the *Enterprise Chat and Email Supervisor's Guide for Unified Contact Center Enterprise and Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-user-guide-list.html

Deprecated Features

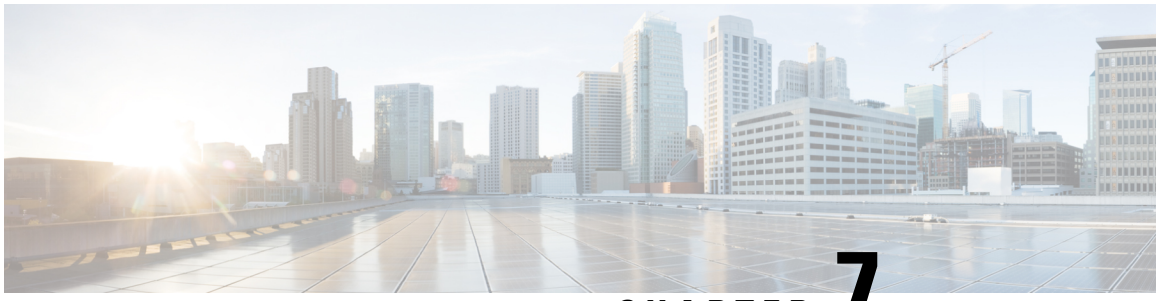
In this release, Internet Explorer version 11 is deprecated. Edge Chromium (Microsoft Edge v79 and later) is the replacement.

Kiwi Chat Template

The Kiwi template for chat is deprecated with ECE 12.5.

Third-party Software Impacts

None.



CHAPTER 7

Cisco Customer Collaboration Platform

The standalone Customer Collaboration Platform features such as Facebook page, Twitter, RSS Feeds, Standalone single session chat, associated features like filters and notifications have been removed from release 12.0. However, you can still use Customer Collaboration Platform interface to encrypt MR.

- New Features, on page 41
- Updated Features, on page 41
- Important Notes, on page 41
- Deprecated Features, on page 41
- Removed and Unsupported Features, on page 42
- Third Party Software Impacts, on page 42

New Features

None.

Updated Features

None.

Important Notes

None.

Deprecated Features

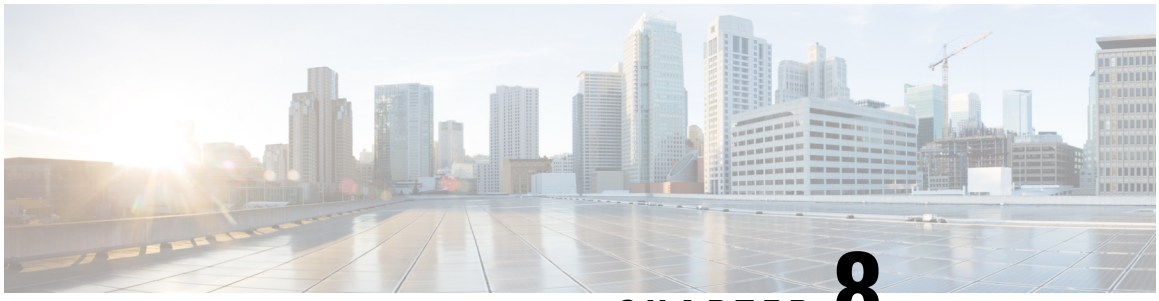
None.

Removed and Unsupported Features

The support for monitoring of Facebook fan pages, Twitter, and RSS feeds from Customer Collaboration Platform for all Customer Journey Solutions customers is removed in Cisco Customer Collaboration Platform 11.6(2) and later. This is applicable ONLY to the social media feed integration to Customer Collaboration Platform. The field notice in this regard is available at, https://www.cisco.com/c/en/us/support/docs/field-notices/702/fn70274.html.

Third Party Software Impacts

None.



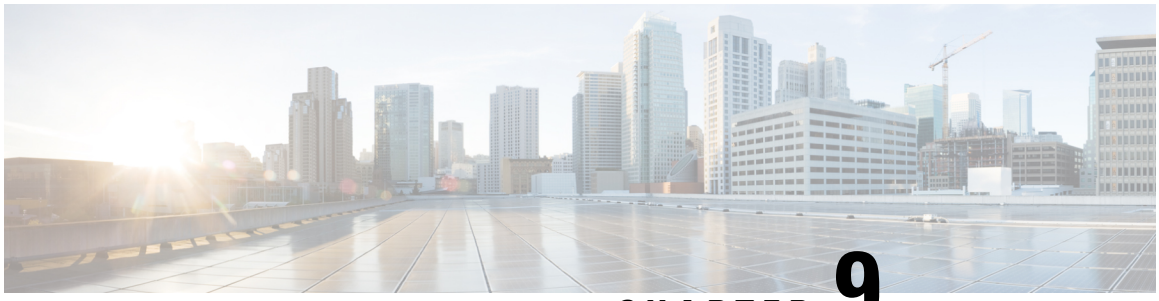
CHAPTER 8

Cisco Unified Contact Center Management Portal

- Legacy Resource Manager Deprecated, on page 43

Legacy Resource Manager Deprecated

Legacy Resource Manager, the traditional three-pane view to manage and maintain resources, is deprecated in Unified CCE 12.5 release. It is recommended that you use the Resource Manager gadgets for all resource management related tasks.



CHAPTER 9

Caveats

• Caveat Queries by Product, on page 45

Caveat Queries by Product

Bug Search Tool

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

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

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

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

Severity 3 or Higher Caveats for Release 12.5(1)

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

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

Cisco Unified Contact Center Enterprise

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=268439622&rls=12.5(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=12.5(1)&sb=anfr&svr=3nH&bt=custV

Cisco Cloud Connect

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

Cisco Unified Customer Voice Portal

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=270563413&rls=12.5(1)&sb=anfr&svr=3nH&bt=custV

Cisco Finesse

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613135&rls=12.5,12.5(1)&sb=anfr&bt=custV

Cisco Customer Collaboration Platform

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

Cisco Unified Contact Center Management Portal

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286325298&rls=12.5(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=12.5(1)&sb=anfr&svr=3nH&bt=custV

Cisco Virtualized Voice Browser

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286325307&rls=12.5(1)&sb=anfr&svr=3nH&bt=custV