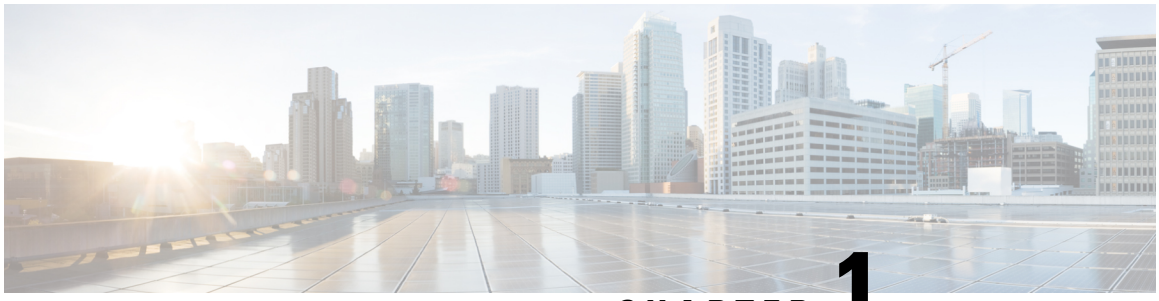
Release Notes for Cisco Contact Center Enterprise Solutions, Release 12.6(2)

First Published: 2023-04-28

Last Modified: 2023-09-20

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 12.6(2) 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.

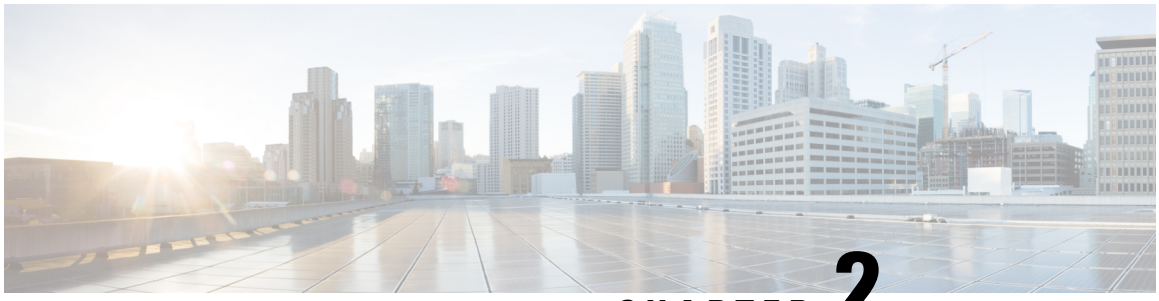
Multi-server SAN Certificates

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*.

Important Notes

- SSO Deployments upgrading to 12.6(2) should ensure that Reverse Proxy Installer (for VPN-Less deployments) 12.6(2) ES02 or later, followed by IdS 12.6(2) ES02 or later, is installed before upgrading any of the components like Cisco Finesse/CUIC to 12.6.(2).
- For 2K Co-Res Deployment model, CUIC, LD and CCE (Router, logger and AW) should be upgraded to in the same maintenance window.



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(2).

Table 1: New Features for Contact Center Enterprise Solutions

Feature	Unified CCE	Packaged CCE
Connect with business through digital channels using Webex Connect, on page 4	Yes	Yes
Virtual Agent-Voice Call Transcription, on page 5	Yes	Yes
Preflight request for Private Network Access, on page 5	Yes	Yes
License Reservation, on page 6	Yes	Yes
HTTP Strict Transport Security Support for Unified CCE Web Applications, on page 6	Yes	Yes
Custom Truststore to Store Component Certificates, on page 6	Yes	Yes

Feature	Unified CCE	Packaged CCE
JTAPI credentials encryption (ES 35)	Yes	Yes
Support for 48000 Agents (ES04 and ES 25), on page 7	Yes	No

Connect with business through digital channels using Webex Connect

Note This feature is available to customers on request and only after necessary review and agreement. Please contact your Partner or Customer Success Manager or Cisco Support for details.

Today's customers want to connect with businesses through any communication channel of their choice. Webex Connect allows the Contact Center business and its customers to interact using digital channels such as email, chat, and SMS.

The Contact Center Enterprise (CCE) solution integrates with Webex Connect to create a seamless omnichannel experience for your agents. This integration helps your customers to interact across voice and digital communication channels as one unified solution.

Webex Connect offers a rich self-service and bot integration to empower your customers to get answers to some common questions. It provides a unified solution for integrated routing, Agent Desktop, and reporting service. Webex Connect provides a simplified framework that helps partners and customers interact through digital channels.

For details on how to configure the digital channel interaction using Webex Connect, see the *Digital Channels Integration Using Webex Connect* chapter in the following documents:

- Cisco Unified Contact Center Enterprise Features Guide
- Cisco Packaged Contact Center Enterprise Features Guide

For information on the design considerations, see the *Digital channels integration using Webex Connect considerations* section in following documents:

- Solution Design Guide for Cisco Unified Contact Center Enterprise
- Solution Design Guide for Cisco Packaged Contact Center Enterprise

For information about how to configure the Manage Digital Channels gadget, see the *Manage Digital Channels gadget* section in the Cisco Finesse Administration Guide.

For information about how to use the Manage Digital Channels gadget, see the *Cisco Contact Center Enterprise Manage Digital Channels Gadget User Guide*.

Virtual Agent-Voice Call Transcription

Note This feature is available to customers on request and only after necessary review and agreement. Please contact your Partner or Customer Success Manager or Cisco Support for details.

Cisco Contact Center Enterprise leverages Artificial Intelligence (AI) and Natural Language Understanding (NLU) to provide transcription services that assist agents. These services are available for the agents in the Cisco Finesse desktop gadgets.

If a customer has interacted with a virtual agent at the beginning of the call and then the call gets routed to an agent, the **Transcript** gadget displays the transcript of the voice conversation between the customer and the virtual agent along with the live transcript. It helps in gathering context from the earlier interaction with the virtual agent and capturing high level summary points for wrapping up the call. In addition, there is a **Highlights** panel that displays the intents and intent parameters based on the customer's query. This helps the agent to assess the overall interaction and how satisfied the customers are.

For details on how to configure VAV call transcription, refer to the following documents:

- *Virtual Agent–Voice Call Transcription* chapter in the Cisco Unified Contact Center Enterprise Features Guide.
- *Virtual Agent–Voice Call Transcription* chapter in the Cisco Packaged Contact Center Enterprise Features Guide.

For instructions about how to view the transcript, see the *Transcript* section in the *Contact Center AI Gadgets User Guide for Cisco Contact Center Enterprise*.

Preflight request for Private Network Access

As browsers like Google Chrome, Microsoft Edge have now deprecated direct access to private network endpoints from public websites, the preflight requests mechanism is enabled by default. This feature provides you a more secure access to web application servers that reside in a private network.

To disable the preflight request feature:

1. In the HKEY_LOCAL_MACHINE root registry, go to SOFTWARE\Cisco Systems, Inc.\ICM\SystemSettings.
2. Create a DisablePnaPreflight string.
3. Set the value of the string to true.

Note The system accepts only the value *true* for disabling the feature or it remains in its default *enabled* state.

For more information, refer to the Field Notice at https://www.cisco.com/c/en/us/support/docs/field-notices/724/fn72432.html

License Reservation

Unified CCE Deployments that are unable to share license utilization data with Cisco SSM on a regular basis due to regulatory requirements can now use the Specific License Reservation (SLR) feature. Using this feature, you can reserve licenses (including add-on licenses) for your product instance and share the license utilization data with Cisco SSM.

For information about Specific License Reservation, see the *Smart Licensing* section in the Administration Guide for Cisco Unified Contact Center Enterprise.

HTTP Strict Transport Security Support for Unified CCE Web Applications

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

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

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

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

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

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

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.

JTAPI credentials encryption (ES 35)

UCCE 12.6(2) ES35 supports Agent PG encrypting the JTAPI credentials which can be configured , if required . To use the Agent PG encryption feature, install UCCE 12.6(2)_ES35 on Agent PG and follow the instructions in the ES35 reference document.

Support for 48000 Agents (ES04 and ES 25)

UCCE 12.6(2), with ES 04 and ES 25 , supports an increased scale of up to 48000 concurrent agents on a single UCCE instance . It is based on the 24000 and 36000 reference models and needs reconfiguration of the router. For more information about moving to the 48000-deployment model, see the ES-specific Release Notes.

- 12.6(2) ES04
- 12.6(2) ES25

Updated Features

The following table lists the updated features available for each Contact Center Enterprise solution in Release 12.6(2).

Table 2: Updated Features for Contact Center Enterprise Solutions

Feature	Unified CCE	Packaged CCE
Simplified upgrade, on page 8	Yes	Yes
AppDynamics built-in integration with CCE, on page 9	Yes	Yes
Inactivity Timer	Yes	Yes
Support for Third Party Gateways	No	Yes

Feature	Unified CCE	Packaged CCE
Agent Multi-Edit Attribute	Yes	Yes

Simplified upgrade

The Orchestration feature provides partners and administrators an option to automatically download software updates and simplify the installation and rollback processes.

The following CLIs are introduced in Release 12.6(2):

- CLI to initiate software download from Cisco hosted software artifactory to Cloud Connect server. This CLI is used to initiate software download before the next scheduled download. The CLI can also be used to enforce the clean-up and download of restricted vs unrestricted software when the usage of restricted vs unrestricted software is changed for the deployment after initial configuration.

Note Software download will not be initiated during Cloud Connect restart.

- CLI to configure the bandwidth, used by orchestration, for downloading software from Cisco hosted software artifactory to Cloud Connect server. Bandwidth control is disabled by default, and you must configure it on Cloud Connect publisher and subscriber separately. Also, you must configure the bandwidth only after the software from Cisco hosted software artifactory is downloaded for the first time locally to the Cloud Connect server. We recommend a minimum of 10 Mbps bandwidth for optimal software download.
- CLI to change the default schedule for software download from Cisco hosted software artifactory or to change the previously configured software download schedule. This is configured on Cloud Connect publisher and subscriber separately.
- CLI to configure the proxy, used by Orchestration, for checking and fetching updates from Cisco-hosted cloud artifactory. Orchestration supports only HTTPS proxy.

For more information on the new CLIs, see the *Orchestration* chapter in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide or Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide.

Orchestration supports upgrade and rollback of 12.5(2) and 12.5(2) ES.

Orchestration supports the recent change in multistage upgrade workflow for 4000 agents and above deployments, where Unified CVP and Cisco VVB moved to Stage 2 and Stage 3 respectively in the updated workflow. For more information, refer to the following documents:

- Unified Contact Center Enterprise: See the *Multistage UpgradeWorkflow for 4000 Agents and above* section in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.
- Packaged Contact Center Enterprise: See the *Upgrade Flowcharts for 4000 Agents and above Deployments* section in the Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide.

Software download via orchestration now validates the digital signature for Unified ICM and Unified CVP software and removes the software from Cloud Connect if the signature validation fails. Email notification is sent if the digital signature validation fails.

Serviceability for software download entitlement failure is enhanced. The logs capture the MDFID along with the product name for which the entitlement failed for the customer.

AppDynamics built-in integration with CCE

For Cisco Contact Center Enterprise solution, it's 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.

CCE 12.6(2) introduces the following enhancements for AppDynamics monitoring:

- Support for Windows Event Log monitoring in Unified ICM 12.6(2). You can enable this monitoring service while enabling AppDynamics monitoring for Unified ICM 12.6(2). If you have configured AppDynamics for Unified ICM 12.6(1), then post upgrade to 12.6(2), you must disable and re-enable AppDynamics to enable Windows Event Log Monitoring. Administrator must provide the AppDynamics controller username and password to enable Windows Event Log Monitoring on Unified ICM. For more information, see the *Enable Performance Monitoring* section in the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise. You can also check if the Windows Event Log Monitoring service is enabled or disabled using the status CLI. For more information, see the *Check Status of Performance Monitoring* section in the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise.
- App Monitoring Proxy Set and Show CLIs introduced in 12.6(1) are removed in 12.6(2). App Monitoring enable CLI now provides an option to configure Proxy Host and Proxy Port. App Monitoring status CLI shows the proxy enabled status. The option to configure Proxy User Name and Proxy Password is removed in 12.6(2). For more information, see the *Enable Performance Monitoring* and *Check Status of Performance Monitoring* sections in the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise.
- If Cloud Connect is on 12.6(2) and the target Windows and VOS nodes are on 12.6(1) during stagewise upgrade, ensure the required ESs and COP are applied in respective 12.6(1) target nodes. For more information, see the *CCE Serviceability and Monitoring using AppDynamics* chapter in Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise.
- When you install CCE 12.6(2)_ES37, the AppDynamics agents deployed on the CCE VMs are upgraded to the following latest versions:

Agent	Version
DotNet	24.3
Machine	24.3
Java	24.3

Note

- If you are installing CCE 12.6(2)_ES37, be sure to disable Federal Information Processing Standard (FIPS) in your registry before enabling AppDynamics.
- CCE supports SaaS and On-Premise AppDynamics controller over secure connection only. For the supported On-Premise AppDynamics controller version, see the *CCE Serviceability and Monitoring using AppDynamics* chapter in Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise.
- AppDynamics monitoring for VVB-Admin and Finesse-Notification Java App Agents is not supported in 12.6(2). Post upgrade from 12.6(1) to 12.6(2), you will still see the VVB-Admin and Finesse-Notification services in the AppDynamics controller. But the metrics will not be received from the respective 12.6(2) nodes. You can right-click these services and remove them from the AppDynamics controller.

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.

Support for Third Party Gateways

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

Administrators can now add third-party gateways to the inventory for routing calls. For instructions, see the *Optional Configurations* section in the Cisco Packaged Contact Center Enterprise Administration and Configuration Guide.

Agent Multi-Edit Attribute

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

Administrators and supervisors can now edit multiple attributes for a set of agents at the same time. Ensure that the agents belong to the same site and department. The agents can also be global agents.

For instructions, see the *Agent Multi Edit Attribute* section in the Cisco Packaged Contact Center Enterprise Administration and Configuration Guide.

For instructions, see the *Manage Agents* section in the Administration Guide for Cisco Unified Contact Center Enterprise.

Important Notes

Mandatory ES for Cloud Connect

Ensure CCE 12.6(2) ES01 or later is installed to optimize the functionality of Cloud Connect 12.6(2).

OpenJDK Java Runtime Update

The CCE 12.6(2) installer installs the OpenJDK version 1.8 (32-bit), update 352. 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
- Security Guide for Cisco Unified ICM/Contact Center Enterprise
- Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide

For information about supported Java versions, see the Contact Center Enterprise Solution Compatibility Matrix.

Tomcat Upgrade

Tomcat is upgraded to 9.0.89. For details on how to apply later security patches on Tomcat 9, refer to the *Upgrade Tomcat Utility* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Account Lockout Support for Active Directory

The account lockout mechanism is now supported for Microsoft Active Directory users of the following applications:

- **Unified Contact Center Enterprise Management** administration portal
- **Web Setup** tool
- **Diagnostic Portico** web service

For more information, see the following documents:

- The *Active Directory Deployment* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.
- The *Active Directory and ICM/CCE* section in the Staging Guide for Cisco Unified ICM/Contact Center Enterprise.

CUIC Co-resident Compatibility

CUIC Co-resident Live Data can be used on 12.6(2) when the CCE Central Controller/AW is on 12.6(1). However, if both Live Data and CCE Central Controller/AW are on 12.6(2), then the ports used in Live Data will change. Releases earlier than 12.6(2) use ports 12005 and 12008; 12.6(2) and later releases use port 443.

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	Replacement	Notes
UCC Enterprise Gateway PG (Parent PG in Parent-Child deployments)	12.5(1)	None	None
Unified Intelligent Contact Management (ICM) deployments including all NICs	12.6(2)	None	INCRP NIC is the only exception, as it will continue to be used for routing calls between two Unified CCE instances and in Contact Director deployments.
TAESPIM/Avaya (Definity) PG using TSAPI interface	12.6(2)	None	None
Unified CCE System PG	12.6(2)	Agent PG and VRU PG	None
CTI OS	12.6(2)	Cisco Finesse on Unified CCE or Packaged CCE deployments	None
Contact Share	12.6(2)	None	None
Microsoft Windows Server 2016	12.6(2)	Microsoft Windows Server 2019	None
Microsoft SQL Server 2017	12.6(2)	Microsoft SQL Server 2019	None
Webex Experience Management	14 November, 2022	None	None

Removed and Unsupported Features

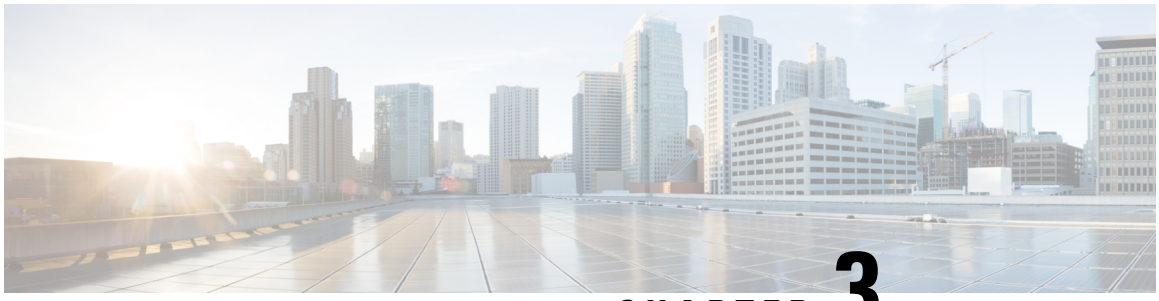
The features listed in the following table are no longer available.

Table 4: Removed and Unsupported Features

Feature	Effective from Release	Replacement
Integrity Check Tool	12.6(2)	None
External Script Validation	12.6(2)	None
Translation Route Wizard	12.6(2)	Translation Route Explorer
Generic PG	12.6(2)	Agent PG and VRU PG
ECSPIM/Avaya (Definity) PG using CVLAN interface	12.6(2)	TAESPIM/Avaya (Definity) PG using TSAPI interface
App Monitoring for VVB-Admin JVM App Agent	12.6(2)	NA

Third Party Software Impacts

For the list of third-party softwares, see Open Source Documents. Filter by **Product/Release Name** and **Version** to download the required Open Source document.



CHAPTER 3

Cisco Unified Customer Voice Portal

New Features

Ability to Host Custom Code Applications on Webex CCE

CVP 12.6(2) ES18 supports hosting and running custom code applications on Webex CCE. You can easily migrate existing CVP applications, whether hosted locally or on remote servers, to Webex CCE without disrupting ongoing calls using VXML and Call servers. This allows you to separate your custom code from the core VXML application, making it easier to identify VXML server crashes and other memory leak issues.

For more information on how to install and configure custom code using remote server, refer to the following documents:

- Installation and Upgrade Guide for Cisco Unified Customer Voice Portal
- Configuration Guide for Cisco Unified Customer Voice Portal

Regionalized Media Support

Contact Center Enterprise (CCE) now extends support for regionalized media to all supported data center locations. Regionalized media allows customers and agent media (audio and SIP signaling) to remain local to a geographic region, regardless of the location of the CCE tenant or home location resides. Keeping media local to a region reduces latency, improves audio quality, meets in-country data residency security compliance requirements, and allows for unique regionalized configurations in multinational deployments.

For example, if the location of the CCE tenant is based in the United States (US) region, calls within the US are localized there, European calls are handled in Europe, and Asian calls are managed in Asia. Only control signals are transmitted from the media endpoint to the US region.

Regional media is available at no additional cost for all WxCCE and on-prem deployment customers who opt for Cisco CCAI services. Ensure that your assigned tenant has been enabled for enhanced media platform capability. For more information, refer to the Solution Design Guide for Cisco Contact Center Enterprise.

Custom SIP header passing to VXML server

You can parse selected SIP headers (custom headers) when using standalone deployment model and SIP trunk termination on VVB. This feature provides you with a great amount of flexibility when sending user-data or context from third-party Automatic Call Distributor (ACD) or service provider to a VXML server for processing. You can send and receive SIP headers only on the initial *SIP Invite* message and not on the reinvite messages.

For more information, see Custom SIP header passing to a VXML server in *Solution Design Guide for Cisco Unified Contact Center Enterprise* and *Solution Design Guide for Cisco Packaged Contact Center Enterprise.*

Virtual Agent–Voice via Cloud-Based Connector

Note This feature is available to customers on request and only after necessary review and agreement. Please contact your Partner or Customer Success Manager or Cisco Support for details.

Virtual Agent–Voice (VAV) via cloud-based connector leverages Cisco's cloud-based Artificial Intelligence (AI) and Natural Language Understanding (NLU) services for designing virtual voice agents and creating complex IVR call flows.

The Webex CCAI services platform enables integration with speech-based services from different vendors. On the premises side, VVB interfaces with the Orchestrator service and connects to the CCAI service via cloud-based connector.

Hybrid IVR with VAV via Cloud-Based Connector

With Cisco's Hybrid IVR functionality, customers who have on-premises applications can leverage their traditional ASR/TTS/CRM integrations, along with cloud-based Dilaogflow CX AI capabilities. They can select a few nodes or sections of their application to be processed in the cloud and few nodes to be processed on-premises. For example, in an application, OTP generation can be performed on-premises, while other tasks can be processed in the cloud.

The above services are enabled through the *VirtualAgentVoice* element of Cisco Unified Call Studio. For more information, see the *VirtualAgentVoice* chapter in the *Element Specifications for Cisco Unified CVP VXML Server and Call Studio, Release 12.6(2)* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html.

For details on how to configure VAV via cloud-based connector and Hybrid IVR, refer to the following documents:

- *Virtual Agent–Voice > VAV via Cloud-Based Connector* section in the *Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(2)* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.
- *Virtual Agent–Voice > VAV via Cloud-Based Connector* section in the *Cisco Packaged Contact Center Enterprise Features Guide, Release 12.6(2)* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/series.html#%7Etab-documents.

Specific License Reservation (SLR)

CVP devices registered with Smart Licenses share device information at regular intervals with Cisco Smart Software Manager (CSSM). However, the devices that are deployed in highly secure networks must not share this information outside the network. Cisco offers specific license reservation as an on-request configuration for these CVP devices.

For details on how to reserve specific licenses for a device, see the *Cisco Unified Customer Voice Portal > Operations Console (NOAMP) > Smart Licensing > Specific License Reservation (SLR)* section in the following guide:

Administration Guide for Cisco Unified Customer Voice Portal 12.6(2) at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.

Partial Response in Virtual Agent—Voice (ES01 Update)

The partial response feature addresses a key aspect of the user experience by engaging a user during a call. It plays an interim message while the Webhook response takes time to process in the background.

An API or Webhook request to an AI application (Dialogflow CX) that requires several parameters often takes longer to receive the correct response. An end user is kept absolutely silent while an API request is being processed. There is a chance that the end-user will hang up the phone. To avoid this, an intermediate response must be sent to the end user informing them that their request is currently being processed.

This feature allows an AI bot developer to create a static response that may be conveyed to the end user while their inquiry is still being processed. In the CX bot agent, static messages can be configured for up to 30 seconds. Once the final API response is received, the flow can be continued.

For configurations instructions, see Configure Partial Response in Dialogflow CX.

To configure this feature, you must upgrade Cisco VVB to Release 12.6(2) ES01 or above. You can access the 12.6(2) ES01 Release and Readme from Virtualized Voice Browser Engineering Specials for Release 12.6(2).

Updated Features

TTS Server Status Update

In this release, you can retrieve the status of the TTS server (Reachable or Unreachable) by invoking the following REST API call:

```
https://<IP address> /adminapi/ttsServer/
```

DecryptKeystoreUtil.bat Utility Update

In this release, you can retrieve the keystore password by running the `DecryptKeystoreUtil.bat` file stored in the `%CVP_HOME%\bin` folder.

Important Notes

The following device/feature are supported in this release:

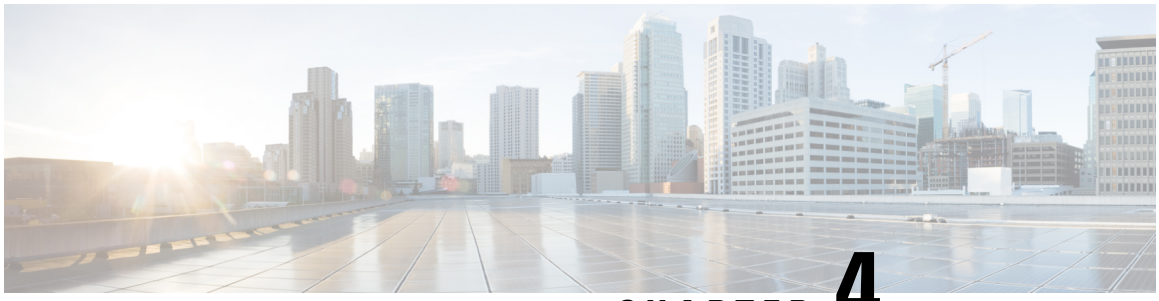
- **Cisco Catalyst 8000 series**
- **Private Network Access (PNA) Compatibility** in Chrome browser

If the Packaged CCE is not in 12.6(2) release, then the following ES has to be applied in Packaged CCE, before upgrading CVP to 12.6(2).

- ES 24 in 12.5(2)
- ES 144 in 12.5(1)

Third Party Software Impacts

For the list of third-party softwares, see Open Source Documents. Filter by **Product/Release Name** and **Version** to download the required Open Source document.



CHAPTER 4

Cisco Unified Intelligence Center

New Features

None.

Updated Features

Logging and Tracing Information

The following utils oamp logging commands are introduced to set the log traces:

- `utils oamp show logging-level`
- `utils oamp update logging-level`

For information, see the *Command Line Interface* section in the Administration Console User Guide for Cisco Unified Intelligence Center.

SNMP Object Identifiers (OIDs)

The following counters related to permalink are added to SNMP:

- cuicReportingHistoricalHTMLPermalinkDataSetRead
- cuicReportingHistoricalEXCELPermalinkDataSetRead
- cuicReportingHistoricalXMLPermalinkDataSetRead
- cuicReportingHistoricalHTMLPermalinkDataSetCreated

- cuicReportingHistoricalEXCELPermalinkDataSetCreated
- cuicReportingHistoricalXMLPermalinkDataSetCreated
- cuicReportingRealtimeHTMLPermalinkDataSetRead
- cuicReportingRealtimeEXCELPermalinkDataSetRead
- cuicReportingRealtimeXMLPermalinkDataSetRead
- cuicReportingRealtimeHTMLPermalinkDataSetCreated
- cuicReportingRealtimeEXCELPermalinkDataSetCreated
- cuicReportingRealtimeXMLPermalinkDataSetCreated

Important Notes

Allow External Links

If you are upgrading from 12.5(1) SU or earlier version, 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

The JSP format is not supported for Unified Intelligence Center gadgets (Live Data and Historical). If you are upgrading from 12.5(1) SU or earlier version, 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 Unified Intelligence Center URL configured in the Cisco Finesse desktop layout to work with Release 12.6(2) and later versions. For more information, see the *Upgrade* section in the Cisco Finesse Administration Guide.

Cisco IdS Upgrade

Cisco IdS 12.6(2) upgrade requires all SSO clients to log out from SSO, before any of the upgraded nodes is brought online. Deployments using VPN-less access to Finesse desktop should also upgrade the reverse proxy to 12.6(2) before Cisco IdS is upgraded to 12.6(2).

Graceful shutdown feature will not be available for Cisco IdS12.6(2) upgrade for the above reasons. Therefore, you must plan for the required downtime for upgrading Cisco IdS to 12.6(2).

Live Data

- If Unified Intelligence Center is upgraded to 12.6(2) and your Live Data (standalone) server remains on the earlier version, 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.

- If you are upgrading Live Data from 12.5(1) ES06 or earlier, the Live Data Virtual Machine(VM) configuration requirement changes for 12.6(2). For information on configuration requirements, see Virtualization Guide.
- AppDynamics monitoring for LiveData-Worker JVM App Agent is disabled by default, because of performance overhead. You can enable it using the set live-data appd-monitoring enable CLI. For more information on the CLI, see the *Live Data CLI Commands* Commands section in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

Unified Intelligence Center Gadgets Failover in VPN-less Setup

In VPN-less setups, if the primary reverse proxy goes down, the Unified Intelligence Center gadget does not render till the primary node comes back online. If you anticipate an extended downtime of the primary reverse proxy, change the gadget URL in the Desktop Settings to point to the Unified Intelligence Center node that is configured with the failover reverse proxy. For instructions, see the *Manage System Settings* chapter in the Cisco Finesse Administration Guide.

Note This issue is addressed in release 12.6(2) ES01. From release 12.6(2) ES01, the Unified Intelligence Center gadget renders when the primary reverse-proxy goes down.

Deprecated Features

None.

Removed and Unsupported Features

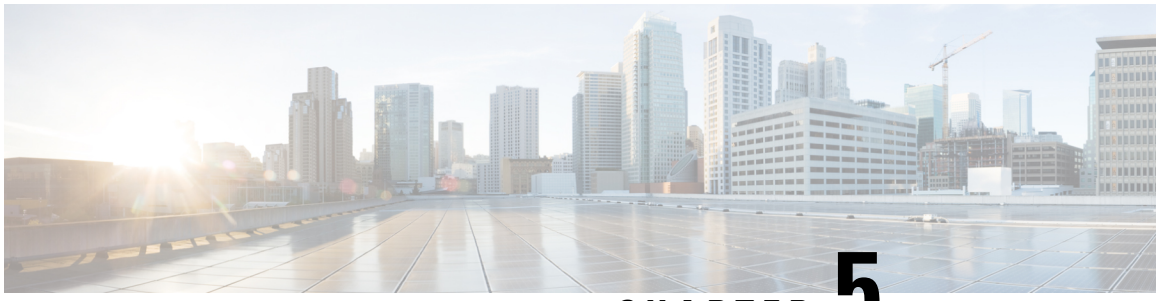
Log Trace

In this release, the log trace setting OAMP Web page is removed. The administrator must use the utils oamp logging commands to set the log traces.

For information, see the *Command Line Interface* section in the Administration Console User Guide for Cisco Unified Intelligence Center.

Third Party Software Impact

For the list of third-party softwares, see Open Source Documents. Filter by **Product/Release Name** and **Version** to download the required Open Source document.



CHAPTER 5

Cisco Finesse

New Features

Manage Digital Channels gadget

This gadget allows agents and supervisors to interact with customers through digital channels. This gadget is available only with SSO login. This gadget is available to agents and supervisors only when an administrator configures and assigns at least one digital channel to them. The following digital channels are available:

- **Chat/Social Channels—**Represents the Chat and SMS media.
- **Email—**Represents the email digital channel.

For information on how to configure this gadget, see the *Manage Digital Channels gadget* section in the Cisco Finesse Administration Guide.

For information on how to use this gadget, see the Cisco Contact Center Enterprise Manage Digital Channels Gadget User Guide.

Customizable gadget behavior

As an administrator, you can now modify the desktop layout entry of a gadget to customize and override the gadget properties. You can modify the gadget properties for a specific team.

For an example on customizing and overriding the gadget properties, see the *Manage Digital Channels gadget properties* section in the *Cisco Finesse Administration Guide*.

Refresh of drag-and-drop and resize gadgets feature

The desktop drag-and-drop and resize behaviors are refreshed to provide new capabilities. The new capabilities that are now available on the desktop are as follows:

- The restrictions on moving and resizing of page level gadgets are removed.
- Each desktop tab can be customized to have a unique layout without affecting other tabs.
- Each desktop tab can be reset to its original layout without affecting the customizations of other tabs.
- If the browser size is reduced, based on the width of the browser, the gadgets in the desktop layout are automatically organized one below the other.
- When the desktop drag-and-drop feature is enabled, Maximize and Collapse features are available in the Multi-Tab gadget.
- Call Control gadget automatically minimizes and restores when the gadgets under Call Control gadget are maximized and restored respectively.

For instructions, see the *Drag-and-Drop and Resize Gadget or Component* section in the *Cisco Finesse Agent and Supervisor Desktop User Guide*.

JMX Counters for Finesse APIs

You can now access the detailed application API performance-related counters through REST APIs. For more information, see the *Finesse Performance API* section in the *Cisco FinesseWeb Services Developer and JavaScript Guide* on *DevNet*.

Finesse REST APIs

The following are the new Finesse REST APIs:

- **/finesse/api/DigitalChannels/Configuration**—This API enables you to get the digital channel configuration.
- **/finesse/api/ScriptSelectors**—This API enables you to get the script-selectors for specific channels (Voice and Non-Voice) or for both the channels.
- **finesse/api/performance**—This API enables you to get the complete list of JMX counters exposed in Cisco Finesse Tomcat service.
- **https://<FQDN>/finesse/api/User/<id>/Media**—A new method **PUT** is introduced, which enables you to update a list of Media objects for all nonvoice Media Routing Domains (MRDs) configured on Unified CCE.
- **https://<FQDN>/desktop/api/ResourceURLs?type=desktop**—Returns in string format the list of all the valid desktop web application file paths that are available on the server.
- **https://<FQDN>/desktop/api/ResourceURLs?type=3rdParty**—Returns in string format the list of all the valid third-party gadget web application file paths that are available on the server.

For more information on the Finesse REST APIs, see the *Cisco FinesseWeb Services Developer and JavaScript Guide* on *DevNet*.

JavaScript APIs

The following is the new JavaScript API that is introduced corresponding to the newly introduced Finesse API:

- **finesse.containerservices.NotificationPopoverService**—This API enables you to create notifications for login failures and show them on the Finesse desktop. You can also capture notifications from any of the gadgets and display them on the navigation bar of the Finesse desktop.

For details about this API, see the *Container Services* section in the *Cisco Finesse Web Services Developer and JavaScript Guide* on *DevNet*.

New Desktop Capabilities

Finesse introduces the following new desktop capabilities for notifications:

- Notification icon on the navigation pane
- Desktop popups for alerting users

The notifications are used to inform the agents about the login failures and incoming messages from various media channels. You can add specific icons, that are supported by Finesse, to the notifications. If you don't add an icon, a default icon is displayed.

A new JavaScript API **NotificationPopoverService** is introduced to publish the notifications. For more information, see the *Cisco Finesse Web Services Developer and JavaScript Guide* on *DevNet*.

Structured Logs

Finesse and Openfire logs are now in JSON format so that the logs can be used more easily with the analytical tools.

Updated Features

VPN-Less Finesse reverse-proxy support

The VPN-less Finesse deployments are made much easier with the support of a new installer that has the following features:

- Installer autodeploys Nginx and separates the configurations from the rules.
- Support for reverse-proxy access through load balancer.
- Support for reverse-proxy access through clients behind a proxy.
- Support for deployments that are larger than 2000 agents.

For more information, see the *Reverse Proxy Automated Installer* chapter in the *Cisco Unified Contact Center Enterprise Features Guide*.

Finesse REST APIs

The following are the updated Finesse REST APIs:

- showMyGadgetNotification—This container services API is updated to accept a new parameter **messageDetails**.
- finesse/api/User/<id>/Media—GET method is updated to return only the non-voice MRDs associated with the user. Previously, it was incorrectly returning all of the non-voice MRDs configured in the system.

Note You can retrieve the complete list of MRDs configured in the system using the existing API – **finesse/api/MediaDomain**.

For more information, see the *Container Services* section in the *Cisco Finesse Web Services Developer and JavaScript Guide* on *DevNet*.

JavaScript APIs

The `channelState` object in the Digital Channel is modified to show login warnings on the respective digital channels. For more information, see the *Digital Channel* section in the *Cisco Finesse Web Services Developer and JavaScript Guide* on *DevNet*.

Support for IdS Asymmetric key-based tokens

Cisco IdS 12.6(2) uses asymmetric keys for token encryption, which can be authenticated independently by clients without requesting the token validity to Cisco IdS. Cisco Finesse 12.6(2) adds support for asymmetric key tokens and switches the authentication mechanisms appropriately, based on the configured IdS. For more information, see the *Single Sign-On* chapter in the following documents:

- *Cisco Unified Contact Center Enterprise Features Guide*
- *Cisco Packaged Contact Center Enterprise Features Guide*
- *Cisco Finesse Web Services Developer and JavaScript Guide* on *DevNet*

Command Line Interface

The following are the new parameters for the **utils finesse set_property webservices** command-line interface (CLI):

- `mrdScriptSelectorPollingInterval`—Time interval in seconds to poll the updates for script-selectors from Unified CCE.
- `drapiStatusPollingInterval`—Time interval in seconds to check the DR-API status.
- `drapiRequestRetryInterval`—Time interval in seconds to retry the DR-API request.
- `drapiMaxTimeToWaitBeforeRequestDiscard`—Time in seconds to discard the DR-API request if there's a failure.

- `drapiRequestRetryIntervalForChat`—Time interval in seconds to retry the DR-API request for Chat conversations.
- `drapiMaxTimeToWaitBeforeRequestDiscardForChat`—Time in seconds to discard the DR-API request if there's a failure for Chat conversations.

For more information about these CLI parameters, see the *Cisco Finesse CLI* chapter in the *Cisco Finesse Administration Guide*.

Important Notes

- After the fresh install, by default the **utils system reverse-proxy client-auth** is enabled. If this is enabled and there are multiple certificates in the client system, when agents login to Finesse through LAN, it forces the agents to select one of the certificates to communicate with the Finesse server. If the deployments aren't configured for VPN-less access to Finesse, disable it by running the **utils system reverse-proxy client-auth disable** command on both the Finesse nodes.
- SSO connectivity requires Cisco IDS to be on version 12.6(2).
- SSO Deployments upgrading to 12.6(2) should ensure that Reverse Proxy Installer (for VPN-Less deployments) 12.6(2) ES02 or later, followed by IdS 12.6(2) ES02 or later, is installed before upgrading any of the components like Cisco Finesse/CUIC to 12.6.(2)
- For 2K Co-Res Deployment model, CUIC, LD and CCE (Router, logger and AW) should be upgraded to in the same maintenance window.

Deprecated Features

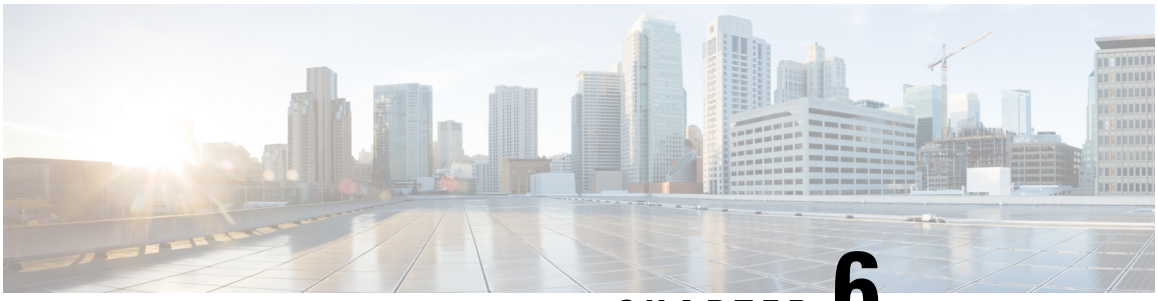
None.

Removed and Unsupported Features

None.

Third Party Software Impacts

For the list of third-party softwares, see Open Source Documents. Filter by **Product/Release Name** and **Version** to download the required Open Source document.

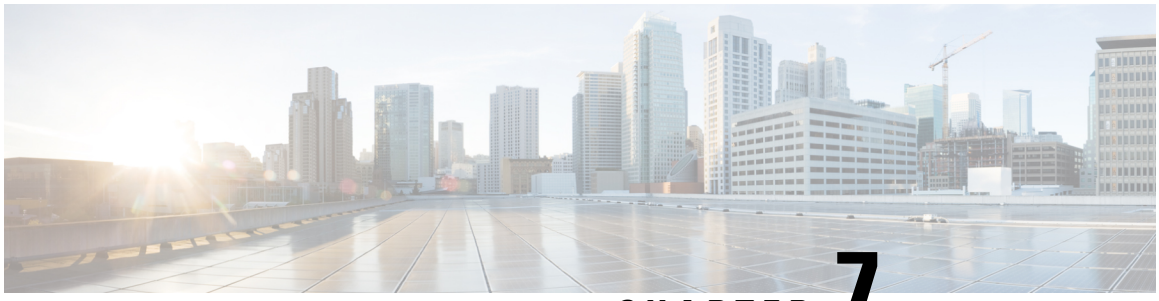


CHAPTER 6

Cisco Enterprise Chat and Email

In This Release

There is no release notes for this component. Refer Release Notes for Cisco Contact Center Enterprise Solutions, Release 12.6(1).

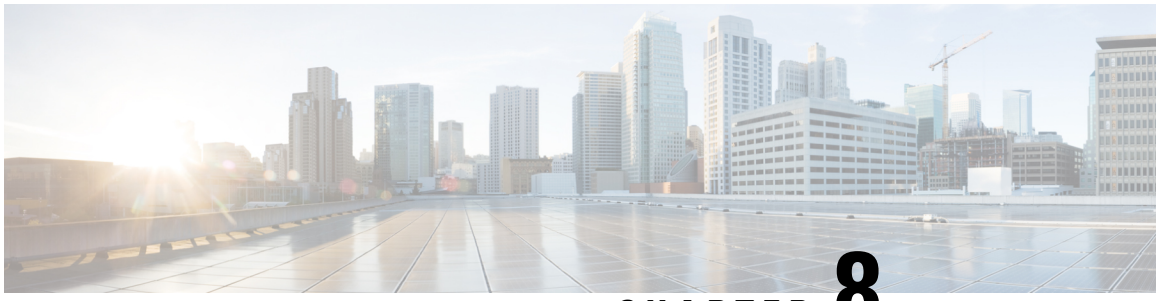


CHAPTER 7

Cisco Unified Contact Center Management Portal

In This Release

There is no release notes for this component. Refer Release Notes for Cisco Contact Center Enterprise Solutions, Release 12.6(1).

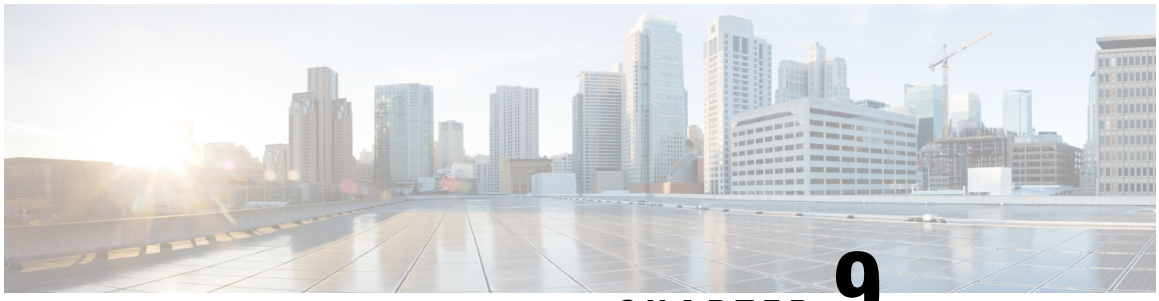


CHAPTER 8

Cisco Unified Contact Center Domain Manager

In This Release

There is no release notes for this component. Refer Release Notes for Cisco Contact Center Enterprise Solutions, 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(2)

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(2)&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(2)&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(2)&sb=anfr&svr=3nH&bt=custV

Cisco Cloud Connect

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&rls=12.6(2)&sb=anfr&bt=custV

Cisco Unified Customer Voice Portal

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=270563413&rls=12.6(2)&sb=anfr&svr=3nH&bt=custV

Cisco Finesse

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613135&rls=12.6(2)&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(2)&sb=anfr&svr=3nH&bt=custV