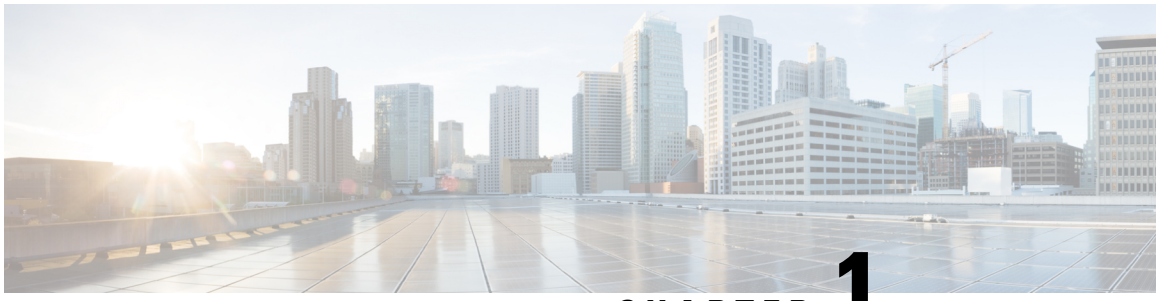
Release Notes for Packaged Contact Center Enterprise Solution Release 11.6(1)

First Published: 2017-08-24

Last Modified: 2018-06-11

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

CONTENTS



CHAPTER 1

Introduction

Release Notes for Contact Center Solutions

Release 11.0 introduced release note compilations for each of the contact center solutions. The compilations contain all of the release notes for one solution type and the components that you can use with that contact center. In addition to the release notes in this document, see the release note compilations for the other contact center solutions at 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 Enterprise Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/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.

Customer Documentation Updates for This Release

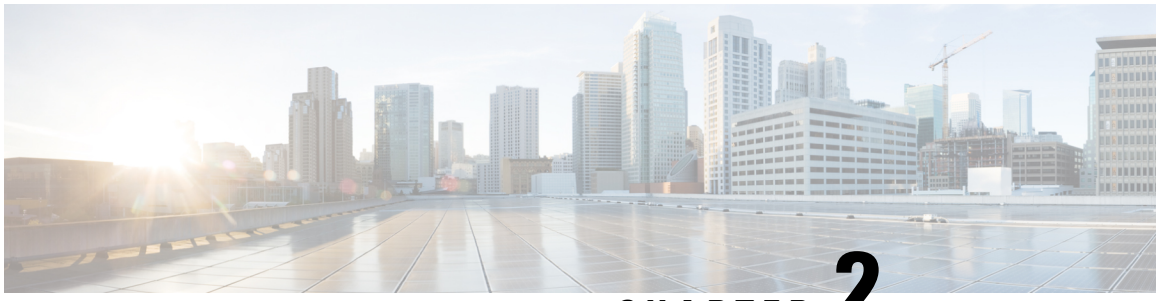
Our Documentation Guides identify the documents that changed for this release:

- **Packaged CCE**—https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-documentation-roadmaps-list.html
- **HCS for Contact Center**—https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-documentation-roadmaps-list.html
- **Unified CCE**—https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-documentation-roadmaps-list.html
- **Unified CCX**—https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-documentation-roadmaps-list.html

Updated documents are also listed under Customer Collaboration in *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

This service lists new and revised Cisco documentation since the last release of this monthly publication.

You can also subscribe to the *What's New in Cisco Product Documentation* RSS feed to deliver updates directly to an RSS reader on your desktop. To subscribe, paste this URL into your RSS reader: http://www.cisco.com/cdc_content_elements/rss/whats_new/



CHAPTER 2

Cisco Packaged Contact Center Enterprise

New Features

Platform Updates

This release requires the following prerequisites made to the platform:

- Ensure that you are running Microsoft SQL Server 2014 SP2 (64-bit).
- If your Administration Clients run on Microsoft Windows 7, upgrade to a minimum of Microsoft Windows 7 SP1.

Important Ensure that these prerequisites are in place before upgrading to Release 11.6(1).

Cisco UCS C240 M5 Server Support

Cisco UCS C240 M5SX server is supported for deployment of Release 11.6(1).

Application Gateway

An application gateway is an optional Cisco Unified Contact Center Enterprise feature that allows you to invoke an external application from within a script (using a Gateway node). You can pass data to the application and receive data in return, which you can then examine and use for routing decisions.

Note Packaged CCE supports only custom application gateways.

Global Deployment

Global Deployments enable the service provider to deploy a single contact center worldwide with a central controller and remote peripheral gateways. This reduces deployment costs by eliminating multiple customer instances. Packaged CCE solution supports the following remote peripheral gateways:

- Agent
- VRU
- Multichannel

In global deployment topology, for on-box, the Packaged CCE solution supports only one local Agent PG and for off-box, three remote Agent PGs are supported. You can use each Agent PG (local or remote) to connect to an independent Unified CM cluster.

Outbound Option High Availability

This release includes enhancements to Outbound Option to provide High Availability.

Campaign Manager High Availability

This release supports the Outbound Option High Availability feature that allows the Campaign Managers and the Outbound Option Import on both Loggers to operate in active/standby mode. It ensures replication of the Outbound Option databases on both sides. The dialers automatically connect to the active Campaign Manager.

When the Unified CCE system starts, the Campaign Manager on Logger Side A functions as the active Campaign Manager, while the Campaign Manager on Logger Side B fuctions as the standby Campaign Manager.

The Outbound Option import is synchronized on each Logger side with the Campaign Manager on same Logger side. Therefore, the Outbound Option import and the Campaign Manager on each side work in tandem. Together with two-way replication and dialer high availability, this provides a robust fault tolerant Outbound Option experience with continuous operation even if the active Campaign Manager fails.

For more information, see the *Outbound Option High Availability* section in the available at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Two-Way Replication

Outbound Option High Availability supports two-way replication between the Outbound Option database that you create on Logger Side A and the Outbound Option database that you create on Logger Side B. Two-way replication offers a High Availability solution in which a failure on the active side of a server allows continuation of outbound dialing and imports on the standby side. All data is replicated between the two sides using Microsoft SQL Server replication.

Enable the Outbound Option High Availability two-way replication on both Logger sides by using Web Setup.

For more information, see the available at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

License Consumption Report

License Consumption

This release introduces the License Consumption Report. This report uses VRU and dialer port monitoring and utilization statistics.

Use this report to monitor the agent license consumption and other resources such as the VRU-IVR ports and the outbound dialer ports. You can generate this report for specific intervals such as hourly, daily, weekly, monthly or quarterly. This further helps you ensure that you have adequate license allocation to cover the peak or maximum license usage during the license agreement period.

The License Consumption report displays the following for a specific interval:

- Total Agents, Enterprise Agents, and ICM Agents logged in
- Maximum VRU ports utilized
- Maximum Dialer ports utilized

Note The VRU and Dialer port, and ICM Agent data will not be available until the Routers, Loggers and PGs are upgraded.

In this release, the Cisco Unified Intelligence Center (CUIC) reports are updated to present the license consumption data from the updated Database tables.

Spikes in license consumption could occur in events such as shift changes when agents of the outgoing shift have not logged out while the agents of the incoming shift have logged in. The Spike Suppression feature included in the License Consumption report allows you to suppress the steep spikes using the standard 95 percentile algorithm. This makes it convenient to view the report while ignoring the spikes.

The changes made in the Database Schema tables provide the License Consumption report updates. For more information, see the Database Schema Changes topic.

Download and import the License consumption report (Templates_CCE_11.6.1_LC_11.6.1.zip file) from Cisco.com.

Note While importing the report, do the following:

- In the Data Source for ReportDefinition field, select **`UCCE Historical`**
- In the Data Source for ValueList field, select **`CUIC`**.

For more information, see the .

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

TLS Versions Support

This release supports Transport Layer Security (TLS) v1.2 and uses it as the default option. The older versions of TLS/SSL are disabled by the Installer.

Note In case there are third party applications installed on CCE VMs that are impacted when the older versions of TLS/SSL are disabled, re-enable the required TLS/SSL versions. For more information, see Microsoft documentation about enabling TLS/SSL provided by Secure Channel (Schannel security support provider) authentication protocol suite.

Similarly, third party applications must use TLS v1.2 while creating connections to CCE VMs or CCE database.

Note For Microsoft Windows 7 client systems, install the Microsoft Windows Update KB3080079 to ensure that the remote desktop connection over TLS v1.1 or 1.2 is supported.

The following components support TLS v1.2:

TLS Options for Cisco Unified CCE and Other Components

Configure TLS v1.2 on all the components and Unified CCE. Internet Script Editor (ISE), and other web applications require TLS v1.2 for HTTPS connections.

Note TLS v1.2 is installed by default on all Cisco VOS based deployments.

For Live Data, CUIC, and Cisco IdS to interoperate with older versions of Unified CCE, run the **set tls client min-version** command on these components to set the minimum TLS version to v1.0 or v1.1 as required.

See the individual component sections for more details on upgrade considerations and default behavior of TLS v1.2 in that component.

Component	Default Option
Cisco Unified CCE	TLS v1.2
Cisco Unified Intelligence Center	TLS v1.2
Cisco Finesse	TLS v1.2
Cisco CVP and VVB	TLS v1.2
Cisco SocialMiner	TLS v1.2
Enterprise Chat and Email	TLS v1.2

ISE Client Requires Manual Upgrade because of TLS v1.2

This release supports only TLS v1.2 between the Internet Script Editor server and ISE clients. ISE client versions before Release 11.6(1) cannot properly establish a TLS v1.2 connection with the server. This prevents an automatic upgrade of the ISE client to the current release.

You can manually upgrade the ISE client installer by entering the following URL in your browser:

`https://<DistributorHost/addr>/install/upgradescripteditor.htm`

This URL reaches the upgrade web page for the ISE client. You can then upgrade the ISE client normally.

ESXi Support

This release supports VMware vSphere Hypervisor (ESXi) 6.5.

Cisco Packaged CCE supports only the VMFS 5 file system.

Feature Updates for Outbound Option

Dialer High Availability

With the Campaign Manager High Availability, all the active dialers connect to the active Campaign Manager. During a Campaign Manager fail-over, the dialers try to connect to the last known active Campaign Manager during the configurable interval (EMTClientTimeoutToFailover), after which the standby Campaign Manager becomes active and the dialers connect to the newly active Campaign Manager.

EMTClientTimeoutToFailover is the interval at which the active Campaign Manager sends the failover message to the router if the Dialer or BAImport do not connect with the Campaign Manager.

Note Upgrade the Peripheral Gateway to Release 11.6(1) to utilize the Outbound Option High Availability feature. This upgrade is mandatory to enable the Dialers to connect to the Campaign Managers on side A and side B.

For more information, refer to the at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Outbound Option Records Handling

When dialer initiates a call for a customer record, the Campaign Manager moves the CallStatus of the customer record to an intermediate Dialed state in the DialingList table. This new state allows the active Campaign Manager to ensure that the customer records for calls that were disconnected due to a failure or fail-over are not dialed again.

Do Not Call Cache Update

To support Outbound Option High Availability and replication between Logger Side A and Logger Side B, Do Not Call data now resides in a Do_Not_Call database table. Previously, the Do Not Call data was stored in the DoNotCall.restore file on Logger Side A. The DoNotCall.restore file is a text file that contains a comma-delimited list of phone numbers and extensions (if extensions exist).

When you upgrade to the current release and enable Outbound Option (whether or not you enable High Availability), the Do_Not_Call table is initially empty, as it is newly created on each Logger side. Populate the Do_Not_Call table on Side A and Side B by importing the DoNotCall.restore file, just as you would perform any other import of customer contact information. You do this only once, when you perform an upgrade.

See the guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

NALENND™ (Region Prefix and Member Data) Database Updates

This release includes new NALENND™ (North American Local Exchange NPA NXX Database) updates for Outbound Option.

Other Notes

The following considerations are important for Outbound Option:

- Outbound Option high availability has specific requirements for the disk size where the outbound database resides, for CCE deployments.
- Optional Outbound High Availability has specific requirements for the *SQL Server Agent* account configuration.

For more information about the specific requirements, see the guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

Reports

Agent State Trace Historical Report

This release includes an enhancement to the Agent State Trace Historical report. If the Agent State is Ready or Not Ready, the Precision Queue/Skill Group field displays the ALL SG/ALL PG value.

ALL SG/ALL PG value indicates that the agent is associated to several skill groups (SGs) within a PG and has picked one of the SGs for a call.

New Languages Supported in Reports

New Languages

All the stock reports are available in the following new languages:

- Bulgarian
- Catalan
- Czech
- Croatian
- Hungarian
- Slovak
- Slovenian
- Serbian
- Romanian

Live Data Reports

This release provides three new Live Data reports for agent and supervisor call and state logs. See the updates in the Cisco Finesse section for the *View Recent Call History*, *View Recent State History*, and *View My History* updates.

See the for more details about the *Recent Call History* and *Recent State History* reports.

Java Version Update

This release supports Java JRE version 1.8 (32-bit) Update 121. Do not remove Java 7.

For more information, see the *Cisco Packaged CCE Software Compatibility Matrix* at .

Database Schema Changes

Unified CCE Database Schema Changes

This release introduces minor database schema changes. Therefore, do not use the Enhanced Data Migration Tool for this release. The Unified CCE, Release 11.6(1) installation performs the database migration.

The release includes changes to these tables:

Table	Changes
NALENND™ (Region Prefix and Member Data) Database Updates	Added new NALENND™ (North American Local Exchange NPA NXX Database) updates for Outbound Option.

Table	Changes
Configuration_Limit	Added several new values for the ConfigLimitName field. Removed the notes on actual values for the configuration limits. The *Solution Design Guide* is the primary source for that information.
Congestion_Control	Added the new deployment type.
Dialer_Interval	Added description for the FutureUseInt3 field.
Dialer_Real_Time	Added description for the FutureUseInt3 field.
System_Capacity_Interval	Added descriptions for FutureUseInt1 and FutureUseInt2 fields.
System_Capacity_Real_Time	Added description for the FutureUse2 field.

SSO Federation

Microsoft AD FS (Active Directory Federation Services)	2.0, 2.1, and 3.0
PingFederate	8.2.2.0
OpenAM	10.0.1
Shiboleth	3.3.0
F5	13.0

Cisco Unified Contact Center Enterprise, Release 11.6(1) supports SAML v2.0.

This release supports an increased number of agents of 12000 SSO users from 4000 SSO users. This release also removes the restrictions imposed by the global deployment model.

In SSO implemented in a single domain environment, this release supports Cisco IdS for Integrated Microsoft Windows Authentication.

Important Notes

Upgrade to Release 11.6(1)

You can upgrade to Cisco Packaged CCE, Release 11.6(1) from Release 11.0(1), 11.0(2) or 11.5(1) directly. To upgrade from a release earlier than Release 11.0(1), upgrade to Release 11.0(1) and then upgrade to Release 11.6(1). If there are other 11.x Maitenance Releases installed, then uninstall these maintenance releases before installing Release 11.6(1).

Note Before upgrading to Release 11.6(1), the peripheral gateways should be named as MR_PG, VRU_PG, and CUCM_PG.

An upgrade to Release 11.6(1) requires the latest Microsoft Windows KB patches and Service Packs.

If you applied a Microsoft Windows update since March 2014, the Windows Update KB2919355 (Hotfix) should be installed. To determine if this Microsoft Windows Hotfix is installed, from your Control Panel go to **Programs** > **Programs and Features**. Click **View installed updates**.

Make sure that Microsoft Windows Update is not running when you install the Release 11.6(1) patch.

Note On the Microsoft Windows 7 based administration client systems, install the Microsoft Windows Update KB3080079 to ensure that the remote desktop connection over TLS v1.1 or 1.2 is supported.

Deprecated Features

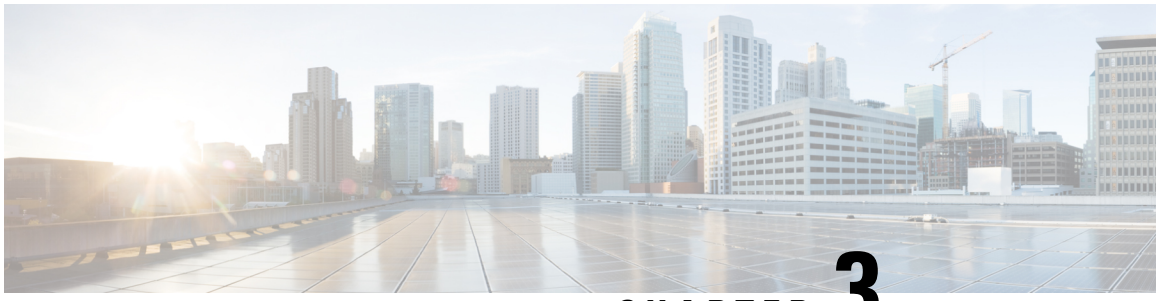
None.

Removed and Unsupported Features

This release does not support Remote Silent Monitor (RSM). The RSM component is replaced with Unified CM-based Silent Monitoring.

Third-Party Software Impacts

See the Packaged CCE Compatibility related information located at for information on third-party software.



CHAPTER 3

Cisco Enterprise Chat and Email

New Features

Attachments to Email, Chat and Knowledge Base Articles

You must be an administrator to configure this feature.

As an administrator, you can specify the file types that can be attached to emails, chat messages, and articles in the knowledge base. You can choose to allow or block specific file types by creating a white list or black list. Additionally, for Chat, you can enable attachments, and specify maximum size for each attachment. Lastly, you can control the attachments for chat using queues and limit file sharing to chats received through specific queues.

Customers and agents can now send files to each other during a chat. The customers and agents can use the paper clip attachment button to browse to a file and attach it. Customers can also drag and drop files into the chat text editor.

Agent Not Ready Codes

This release supports the Not Ready reason codes in the Administration Console. This allows you as an Administrator, to configure the deployments to require a reason from agents for not being available to handle activities, such as breaks, meetings, meals, or training.

When you enable this setting, it displays a popup to agents when they mark themselves not available for any of the channels for which they had previously marked themselves as available.

Localization of Custom Attributes

You can localize the custom attribute names created from the Tools Console, using the user interface. In the cases where the custom attributes use enumerated values, you can localize the enumerated values also.

Customer Facing API for Chat

This release provides new Chat Web Services APIs to hide or show the chat on the web sites, based on the availability and capacity of agents to handle new chats.

REST Based Adapters

Enterprise Chat and Email supports new REST based Data Adapters. These data adapters provide capabilities to fetch information by executing RESTful Web Services exposed by third party applications.

Encrypted Logs

This release supports encrypting all the logs. To enable encryption, update the Encrypt Logs setting at the partition level in the System partition, as a system administrator.

By default, the logs are not encrypted by the application. To decrypt the logs, use the logs_decryption_utility, available in the Utilities folder on the services server.

SDK Support for Chat

This release provides JavaScript based SDK support for Chat, Callback, and Delayed Callback.

Factory Reset of Custom Attributes

This Release provides the Factory Reset option for the Context Service feature. You can, as an administrator, reset the configuration files of the service to the original state and remove all the updates that have been installed by the service automatically. The configuration files are updated again to the latest version when you restart the Context Service.

Updated Features

TLS V1.2 Support

Enterprise Chat and Email supports TLS v1.2. As an Administrator, you can now configure email aliases with TLS authentication from the Administration Console.

You can also configure the partition setting or the Default SMTP server setting to use TLS, SSL or Plain text.

Enhanced Chat Management

This release adds the following chat enhancements:

- A new chat template set called Aqua that enables the website visitors to conduct chat interactions with the agents using a docked chat window within the same browser window that they are currently viewing.

  The chat window remains in place while the customer moves from page to page. This feature offers seamless escalation from virtual assistant to chat agent.

- Alternative engagement options to contact the business (such as **Send an email**, **Visit the FAQ** page) can now be displayed to chat customers while they are waiting for agent to join the chat. Once an agent joins the chat, the options are removed from the chat window. You can display these options as soon as the customer starts the chat, or after a delay.

- Sharing files during chat as attachments.

- SAML v2 authentication for chat login helps you configure the chat entry points to transfer customer context information from the company website to ECE. This allows customers (who are already recognized on the company website to use a SSO-enabled entry point) to chat with an agent without the need to provide repetitive information.

  This feature is available for auto-login configuration only.

Callback and Delayed Callback Enhancements

In this release, you need not configure the voice MRD in the Import Wizard.

This release provides a queue for the voice MRD. Configure this queue with a script selector to use it to process the Callback and Delayed Callback activities.

Enhanced SMTP Settings

This release adds the following enhancements to the SMTP settings:

- Default SMTP server settings is a new setting available at the partition level. Administrators can configure the server from this one setting. The following settings are available through this new setting.
  - Default SMTP Server
  - Default SMTP Protocol
  - SMTP Flag
  - Default SMTP User Name
  - Default SMTP Password
- The Maximum Email Size for Dispatcher (MB) setting has been adjusted to allow the minimum value of the setting to be as low as 1.
- This release supports displaying 24-hour date/time format in the application. Configure this feature in the Date and time format setting at the department and user level.
- A new setting **Allow Activity Transfer to Agents Who Are Not Logged In** is now available to allow users to transfer activities to other agents who are not logged in to work on activities.
- The setting **Allow activity transfer to agents who are not available** has been split into two settings: **Allow chat transfer to agents who are not available** and **Allow email transfer to agents who are not available** to allow separate control for email and chat activities.

Exception Queue for Additional Emails

Emails that the Retriever does not parse, are now routed to the Default exception queue.

The following settings are no longer required and have been removed:

- Action on exception emails.
- Exception mail redirection from address.
- Exception mail redirection to address.

Important Notes

None.

Deprecated Features

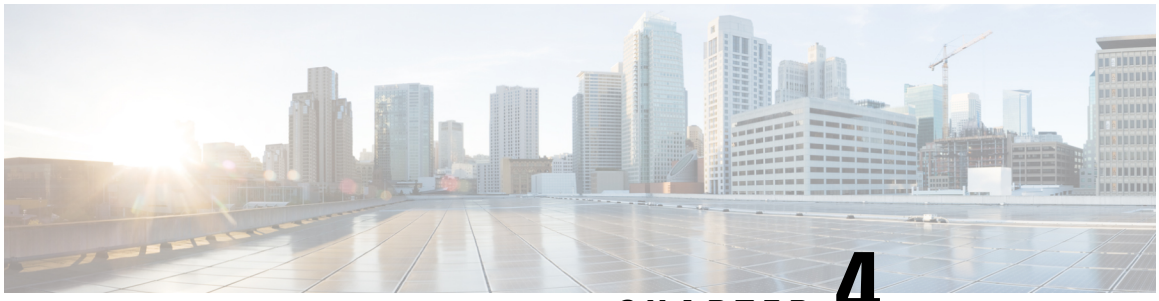
None.

Removed and Unsupported Features

None.

Third-Party Software Impact

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 4

Cisco Unified Customer Voice Portal

New Features

Security Enhancements

Unified CVP has the following new security capabilities:

- SIP over TLS for securing call control over the IVR and agent call legs.
- Log masking of sensitive user DTMF input on Unified CVP Call Studio applications.
- TLSv1.2 enforced for secure communications across solution components.
- Unified CVP Call Studio supports sFTP-based transfer of recorded files.
- The Web Service element of Unified CVP Call Studio supports strong ciphers.

Enforce Maximum Number of Calls

This feature allows administrators to configure maximum number of calls that Unified CVP can handle. This is configurable from OAMP.

vCUBE support

The solution is certified with the virtual Cisco Unified Border Element (vCUBE), enabling a broader range of deployment options and making it possible for businesses to deploy the CVP with less router hardware.

Standalone Application Builder (SAB)

The Standalone Application Builder utility has been restored. This utility allows the deployment of an application through the command-line interface.

Updated Features

Call Studio Enhancements

Unified CVP Call Studio has the following enhancements:

- Install the Unified CVP Call Studio on the Microsoft Windows 10 desktop operating system now.
- Easier addition of comments to Unified CVP Call Studio elements and tooltip display of comments.
- Supports the autopopulation of the subflow parameter and the return parameter of a subflow in the Subflow Call elements to avoid errors.
- Supports the display of spatial coordinates for elements in the script editor.
- Faster loading of the decision element in large Unified CVP Call Studio applications.

Context Service Serviceability Enhancements

Context Service (CS) serviceability improvements make it easier to track and ensure the flow of customer context information into and out of Unified CVP. These improvements include:

- Access to Context Service is validated during registration and de-registration for an enhanced user experience.
- Context Service access status is displayed on the management console, allowing administrators a view of service availability from all component hosts.
- Context Service activity statistics are available and refreshed every 30 minutes, allowing improved performance debugging.

Important Notes

None.

Deprecated Features

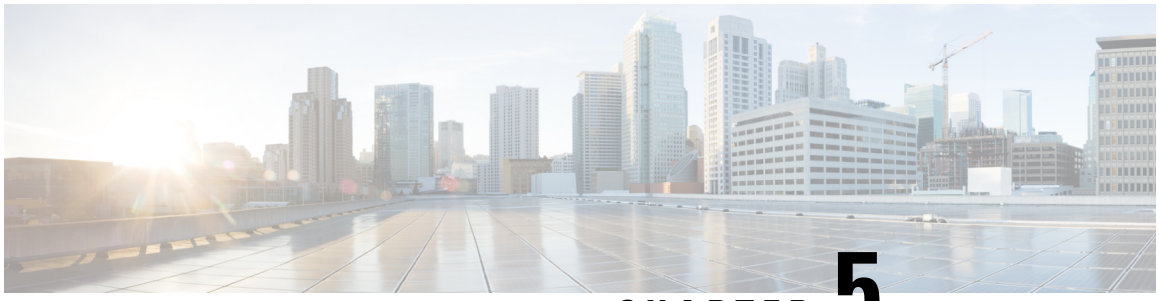
The Key PressMarkup Language (KPML) feature for Cisco unified Customer Voice Portal is deprecated from Release 10.5(1).

Removed and Unsupported Features

None.

Third-Party Software Impact

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 5

Cisco Virtualized Voice Browser

New Features

Security Enhancements

Cisco Virtual Voice Browser (VVB) has the following new security capabilities:

- SIP over TLS for securing call control over the IVR and agent call segments.
- SRTP media support over Cisco VVB to secure the IVR voice media stream.

Note Customers in countries that have local government regulations about using software that allows SRTP voice communication, can alternately use the export unrestricted image of Cisco VVB that does not support SRTP. See the *CCBU Ordering Guide* for more details on ordering options available for the Cisco VVB software.

Support for Cisco VVB on Cisco Integrated Service Routers 4000 Series

Cisco VVB can now be installed on the Kernel-based Virtual Machine (KVM) that is available natively on the Cisco Integrated Service Routers 4000 Series. This allows a small-to-medium-sized edge deployment to use the VVB natively on the router hardware by removing the need to host an add-on UCS E module.

Support for Non-Reference VRU

Cisco VVB now supports the Type 2, 3, 7, and 8 VRU non-reference call flow models.

Optimized Hard Disk Size for OVA

Cisco VVB OVA hard disk size is reduced from 2x146 GB to 1x146 GB. Upgrade from 11.5.1 to 11.6.1 is supported for profiles having 1x146 GB disk size OVA.

Change Hostname or IP Address

You can now change the hostname or IP address of Cisco VVB post installation. This feature allows you to clone Cisco VVB instead of installing it afresh for each new deployment.

CLI-based HTTP Timeout Configuration

This release introduces a new CLI command to configure the HTTP timeout. This configuration allows Cisco VVB to wait for a user-specified time interval to receive a response from the HTTP server.

Support for G.729 Codec

Cisco VVB now supports the G.729 codec with a sampling rate of 8kb/s for the IVR call segment.

Note The G.729 codec does not support the ASR-TTS service.

Fetchaudio

This feature uses the *fetchaudio* attribute for enhancing user experience when there may be noticeable delays during the next document retrieval. This feature can be used to play background music or a series of announcements while the document is being retrieved.

Updated Features

Performance Improvement

With this release, Cisco VVB has been scaled up to support a maximum of 20 calls per second.

Important Notes

None.

Deprecated Features

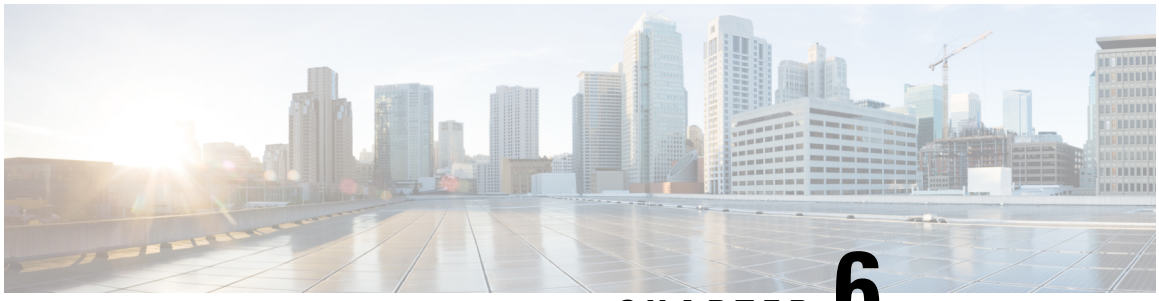
None.

Removed and Unsupported Features

None.

Third-Party Software Impact

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 6

Cisco Finesse

Important Notes

None.

Deprecated Features

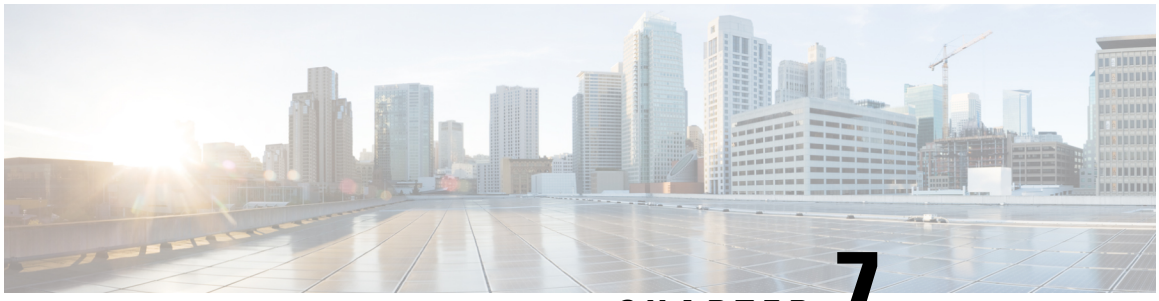
None

Removed and Unsupported Features

None

Third-Party Software Impacts

None



CHAPTER 7

Cisco Unified Intelligence Center

Updated Features

TLS v1.2 Support

This release supports Transport Layer Security (TLS) version 1.2 as the default version for both incoming and outgoing SSL connections.

Deprecated Features

None

Removed and Unsupported Features

Dashboards

The Dashboards drawer from the legacy interface is disabled.

Dashboards - Slideshow

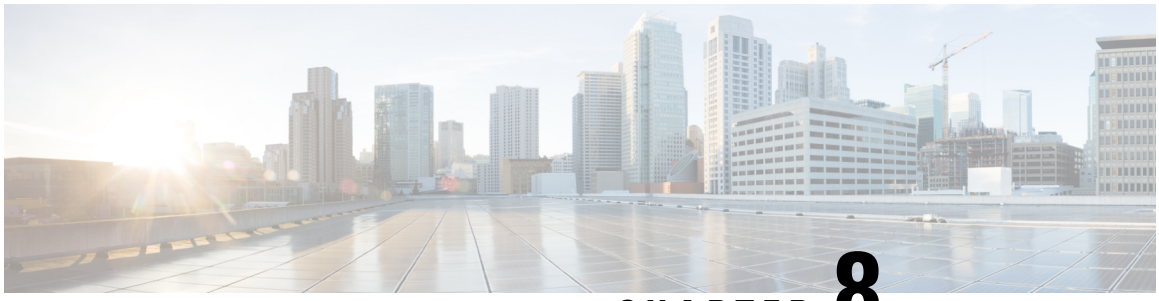
The Dashboard slideshow feature that was used to move through items on the dashboard is removed.

Scheduled Reports on Dashboards

You can no longer add scheduled reports on Dashboards. If there are existing Dashboards with scheduled report widgets in versions prior to 11.6, those widgets (not the Dashboards) will be dropped on upgrade to 11.6.

Third-Party Software Impacts

None



CHAPTER 8

Cisco Remote Expert Mobile

New Features

Application Partitioning

Cisco Remote Expert Mobile now supports application partitioning. This feature enables you to pause and resume the co-browse session.

Horizontal Scroll Buttons

This feature provides sideways scroll buttons to change the area viewed in the window, when the co-browse area extends beyond the viewable window.

IE/Edge Touch Support

Cisco Remote Expert Mobile supports the desktop version of Opera.

Note Cisco Remote Expert Mobile does not support the mobile version of Opera.

Opera Browser Support

Cisco Remote Expert Mobile supports touch gestures in Internet Explorer and Edge browsers.

Zoom Feature

The Agent Consoles now have a zoom feature to enable them to magnify their view of the customer's desktop.

Consumer Shadow Pointer

The mouse pointer on the customer's screen is now displayed on the Agent Console during co-browse.

Disabling Agent Features

You can now disable the Specific Expert Assist features in the Exper Assist Configuration.

Audio-Only Calls

Applications can now make audio-only or video-only calls by setting the appropriate flags when making the call.

Updated Features

Android Device Support

Cisco Remote Mobile Expert now supports Android 7.0.

Cisco Remote Mobile Expert also supports the revised Android 6.0 permissions feature. Android changed its permissions setup to enable you to grant permissions to applications while the application is running. For more details, see the Android documentation at the following URL: https://developer.android.com/training/permissions/requesting.html

Consumer-side Logging

You can disable the consumer-side logging.

This allows you to manage the logs that are collected and control the published logs more effectively.

Important Notes

Safari 10.1 Support

The Safari 10.1 WebSockets implementation has a limit on how much data can be sent in a single frame. This is a known issue https://bugs.webkit.org/show_bug.cgi?id=170463 with Safari 10.1. This link contains a patch for the browser.

CLI

After upgrading to Remote Expert Mobile, Release 11.6 from Release 11.5, you need to disable startup tasks in the CLI:

- Load the file `/opt/cisco/cli/Configuration.properties` into a text editor.
- The file has a standard format for a configuration file. Find the *run.startup.tasks* property and either set it to false or comment it out by adding a hash sign (#) at the start of the line.
- Save the file.

You must do this on each node.

Unauthorized URLs

A malicious Agent can push an unauthorized URL to a customer using the Agent Console. This requires the Agent to be logged into their account in the Agent Console. Only authorized Agents can perform such operations outside the scope of normal usage.

Finesse Gadget and Console

The following caveats for the Finesse Gadget and Console apply to this release:

- The mouse pointer image does not show in the Finesse Console.
- On Safari/iOS, video does not resume after hold.
- There is no video after a call is transferred.

Remote Expert Mobile Client SDK

This release includes the following updates:

iOS

- Supports only iOS version 7 or later.
- When CSDK is used for Voice and Video, a red banner displays at the top of the device's screen when the application is put into the background. This is an iOS feature, and cannot be controlled by the application. It permits the user to tap the banner to return to the application.

Plug-ins

- Supports VP8 and H.264 video.
- To configure this, see Cisco Remote Expert Mobile—Install and Config Guide > Configuring IE and Safari Plug-Ins:

Browser	Last Released Version	Minimum Acceptable Version
Internet Explorer	3.2.2	3.2.2

Browser	Last Released Version	Minimum Acceptable Version
Safari	3.2.2	3.2.2

Deprecated Features

None.

Removed and Unsupported Features

Other Features Removed

Feature	Effective from Release	Replacement
Instant Messaging and Presence (IM&P)	Cisco Unified Contact Center Enterprise, Release 11.5(1)	None.

Third-Party Software Impact

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.

Patching the OS

See the *Guidelines for Updating Security Patches* section in the *Cisco Remote Expert Mobile Design Guide*.

Supported iOS

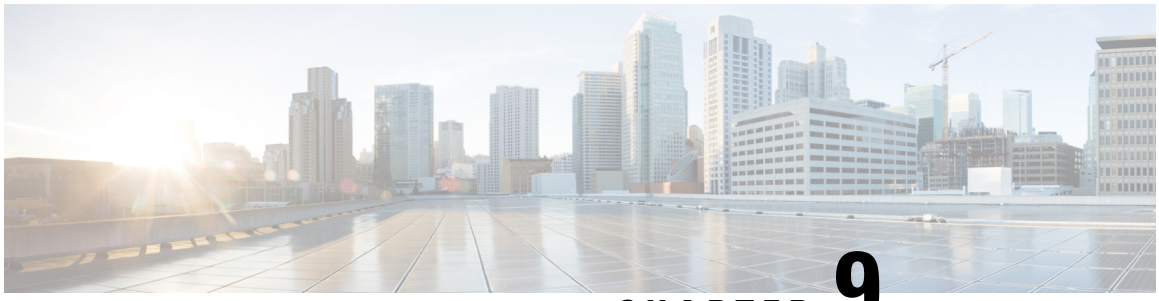
Only iOS version 7 or later are supported.

Supported Web Browsers

The Cisco Remote Expert Mobile Design Guide provides the details of the supported browsers:

- Versions of browsers late than the ones stated in the Cisco Remote Expert Mobile Design Guide may not be compatible.
- Some versions of Internet Explorer are not supported for consumers.
- Web browsers are not supported on iOS or Android.

- Opera v.42 is compatible with REM, but the `isBrowserSupported` function returns `false` for all the versions of Opera. Do not call the `isBrowserSupported` function unless it is verified that the browser is not Opera.



CHAPTER 9

Cisco SocialMiner

The standalone SocialMiner 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 SocialMiner interface to encrypt MR.

New Features

AUDIT Log Support for all Config changes

Cisco SocialMiner, Release 11.6(1) provides audit log capabilities for all its administrative operations.

CORS Support

The Cross Origin Resource Sharing support has been included in SocialMiner 11.6(1) for all public REST APIs including chat APIs.

Updated Features

TLS v1.2 Support

Cisco SocialMiner, Release 11.6(1) supports TLS v1.2 as the default protocol for secure incoming connections as a server and for secure outgoing connections as a client. However, support for earlier TLS versions can be configured. For more information, see the *Cisco SocialMiner User Guide*.

Important Notes

SocialMiner Installation displays "Installing Cisco SocialMiner component" freezing the screen momentarily

While the SocialMiner installation is in progress, the message `Installing Cisco SocialMiner component` causes the screen to freeze. Do not abort the process. Wait for the installation to complete, although it might appear that the system has frozen momentarily.

Deprecated Features

None

Removed and Unsupported Features

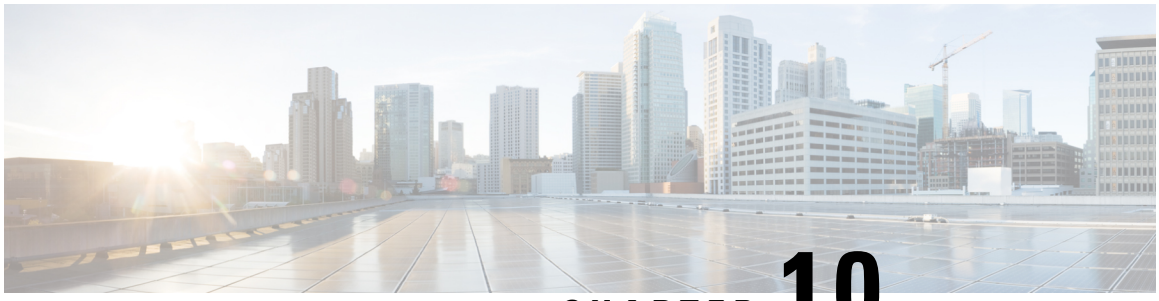
Ability to Browse and Download Logs via HTTP

Effective with Cisco SocialMiner, Release 11.6(1), the ability for administrators to browse system logs from browsers (using the System Logs -> Log Directory option in SocialMiner Administration interface) has been removed.

Standard mechanisms of accessing and downloading system logs are available through Real-Time Monitoring Tool (RTMT) and through the application CLI commands. For more information on RTMT, see the *Cisco SocialMiner User Guide*, available at, http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-user-guide-list.html.

Third-Party Software Impacts

None



CHAPTER 10

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://www.cisco.com/cisco/psn/bssprt/bss. 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.