Cisco Hosted Collaboration Solution for Contact Center for Contact Center

New Features

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

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

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

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

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

Note For Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, refer to the Nginx TechNote article. Any reverse-proxy supporting the required criteria (as mentioned in the **Reverse-Proxy Selection Criteria** section of Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1)) can be used in place of Nginx for supporting this feature.

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 Solution Design Guide for Cisco Unified Contact Center Enterprise 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 Outbound Option Guide for Unified Contact Center Enterprise available at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

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).

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 Cisco Unified Contact Center Enterprise Reporting User GuideCisco Unified Contact Center Enterprise Reporting User Guide.

CLID Masking Feature at Unified ICM/CCE Level

The CLID masking option allows you to mask the original CLID / Automatic Number Identification (ANI) of the caller from appearing on the agent desktops and getting stored in the Unified CCE or Unified ICM database. You can set up masking to either remove digits or replace digits with another character. The feature traditionally was only available in NAM/CICM deployments or ICM to ICM deployments using the INCRP NIC.

Cisco Unified CCE, Release 11.6(1) introduces the CLID masking feature at the enterprise level. It is possible to configure the masking option that needs to be applied, on a per routing client basis using a configuration parameter. For more details, see the tool help in the System Information tool and the NIC Explorer tool in the Configuration Manager tool.

Updated Features

Increased PG Agent Capacity for Mobile Agents

Added on May 14th, 2021

The mobile agent capacity on the PG has increased as follows:

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

For more details, see the *PG Agent Capacity with Mobile Agents* section in the *Sizing and Operating Conditions for Reference Designs* chapter at *Solution Design Guide for Cisco Hosted Collaboration Solution for Contact Center* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-implementation-design-guides-list.html

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.

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
Cisco Unified Contact Center Domain Manager	TLS v1.2

Use the Transport Layer Security CLI commands to view or change the TLS minimum version for inbound or outbound connections. For product-specific TLS configuration, see *Configuration Guide 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-installation-guides-list.html.

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.

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 Solution Design Guide for Cisco Unified Contact Center Enterprise 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 Outbound Option Guide for Unified Contact Center Enterprise 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 Outbound Option Guide for Unified Contact Center Enterprise 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 *Cisco Unified Contact Center Enterprise Reporting User Guide* 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.

The Unified CCE installation process installs Java JRE version 1.8 (32-bit) Update 121. Previous versions of Java may be removed, if necessary, after ensuring that Java JRE version 1.8 (32-bit) Update 121 is installed on the server.

For more information, see the *Compatibility Matrix for Cisco HCS for Contact Center 11.6(1)* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html. You can also apply newer Java security updates.

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.
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

This release adds support to the following customer IdPs to be federated to the Hosted AD FS 2012 R2 IdP:

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

Documentation is provided only for Microsoft AD FS. For all other customer IdPs, hosting partners must refer to Microsoft and third-party vendor IdP documentation, to create and test Federation trust.

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

Cisco Unified Contact Center Domain Manager 11.6(1) requires Microsoft AD FS 2012 R2.

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.

For more information, see the *Cisco Hosted Collaboration Solution for Contact Center Configuration Guide, Release 11.6(1)*.

ESXi Release 6.5 Support

This release supports VMware vSphere Hypervisor (ESXi) 6.5.

Cisco Unified CCE supports only the VMFS 5 file system.

For more information, see Virtualization for Hosted Collaboration for Contact Center at: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html

Important Notes

Upgrade to Release 11.6(1)

You can upgrade to Cisco Unified 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 later 11.x Maintenance Releases installed, uninstall these maintenance releases before installing Release 11.6(1). You can determine which maintenance releases you have applied, in the Programs and Features list in Control Panel.

Before upgrading or uninstalling Release 11.6(1), close all the open Microsoft Windows Event Viewer instances. This will prevent an installation failure with an error that the following DLLs are locked:

- icrcat.dll
- icrmsgs.dll
- snmpeventcats.dll
- snmpeventmsgs.dll

If the failure occurs, close the Event Viewer and retry the installation or uninstallation.

If the failure persists, restart the Microsoft Windows Event Log service.

COP Files Installation

Before upgrading a standalone deployment of Unified CCE (Release 10.5 or Release 11.0) or Packaged CCE with CUIC to a Release 11.6(1) co-resident `UCCE: 2000 Agents` deployment (CUIC with Live Data and IdS), install the required COP files. See the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide for more information about the installation of the COP files.

Upgrade Utilities

The EDMT, RegUtil, User Migration Tool, and DB Estimator upgrade utilities do not apply in this release. Use the Release 11.0(1) version of the EDMT, RegUtil, User Migration Tool, and DB Estimator upgrade utilities to upgrade to Release 11.0(1), as needed.

For the upgrade utilities, see https://software.cisco.com/download/type.html?mdfid=268439622

Live Data Deployments

In this release, Live Data supports only 12 Agent Peripheral Gateways (PGs). Deployment upgrades from Release 11.0(2) to Release 11.6(1) with more than 12 Agent PGs (UCM PGs and TDM PGs) are only supported if you are not using Live Data.

Microsoft Windows Patches and Updates

An upgrade to Release 11.6(1) requires the latest Microsoft Windows Server 2012 R2 and Microsoft SQL Server 2014 KB patches and Service Packs.

If you applied a Microsoft Windows update since March 2014, the Microsoft 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 Microsoft Windows Update KB3080079 to ensure that the remote desktop connection over TLS v1.1 or 1.2 is supported.

Download and install the necessary Microsoft Patch updates to ensure that the ransomware Wannacry does not affect the Cisco Unified Contact Center deployment.

Upgrade Live Data

Upgrade Live Data and the AW database together. If you restart Live Data after you upgrade the AW database to Release 11.6(1) but before you upgrade Live Data, the Live Data upgrade switch partition step fails. If necessary, resolve this issue by temporarily removing the AW database configuration from Live Data. For the procedure to remove the AW database configuration from Live Data, see CSCvf20136.

Agent Service Logon

For the two-way Outbound Option database replication, it is necessary to create a Microsoft SQL Server user and assign that user the sysadmin privilege. Also, MSSQLSERVERAGENT user must be assigned to the

SQL Server Agent process. If the service is running under a different account, then you must change the account.

Change the Agent service logon using the Microsoft SQL Server Configuration Manager. Do not change it directly using the Services Control Panel application. Ensure that the logon account is included in a SQLSERVERAGENT group on the machine.

Supervisor Sign-on When SSO is Disabled

The login name of a supervisor who is not enabled for single sign-on requires either one of these formats:

- User Principal Name (UPN); for example, user@domain.com
- Security Accounts Manager (SAM); for example, DOMAIN\USER

Note After upgrading to Release 11.6(1), change the supervisor login usernames to comply with the Email ID format (user@domain.com) to ensure that the User List tool functionality does not fail. Alternatively, see the defect CSCvf27253 to apply the necessary updates.

You can change the login name for multiple supervisors at once using the Bulk Edit Person tool.

For supervisors with SSO not enabled, Cisco Unified CCE supports SAM Account Name and User Principal Name format for supervisor login name configuration. However, Cisco Finesse supports only User Principal Name (UPN). Therefore, use only UPN login format for configuring EA (Enterprise Agent) Supervisor login name. As the alternative to using the UPN login format, the supervisors can use the numeric IDs of their peripheral.

Direct Attached Storage (DAS) for Cisco UCS C240 M4 TRC Server

The Cisco Unified Contact Center Enterprise Installation and Upgrade Guide now provides details for mapping Virtual Machines to data stores for the `UCCE: 2000 Agents` deployment for the Cisco UCS C240 M4 Server hardware. This aligns with the Cisco Packaged CCE Virtual Machines mapping.

Check the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide for specific information for product upgrades that may require specific Virtual Machines to datastore placement that may be different from your current design. Check your servers array design and controller settings to ensure that they align with the documented requirements.

For more details about Cisco UCS C240 M4 Server RAID configurations, see https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M4/install/C240M4/raid.html.

Sub-Customer Capacity for Small Contact Centers on UCS TRC Blades

In previous releases, the SCC 100 Agent dedicated sub-customer option supported 10 sub-customers on each blade pair. In Release 11.6, Finesse requires more CPU resources. This reduces the capacity to 6 sub-customers on each blade pair.

Plan your server resources accordingly when upgrading to this release.

Deprecated Features

There is no new development for Deprecated features. These features may be scheduled to be removed in a future release. Plan to transition to the designated replacement feature. If you are implementing a new deployment, use the replacement technology rather than the deprecated feature.

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

Deprecated Feature	Announced in Release	Replacement	Notes
MIB Objects: • cccaDistAwWebViewEnabled • cccaDistAwWebViewServerName • cccaSupportToolsURL • cccaDialerCallAttemptsPerSec	11.6(1)	None	None
SHA-1 certificate	11.5(1)	SHA-256	For more information on SHA-256 compliance, see https://communities.cisco.com/docs/DOC-64548
Generic PG	11.5(1)	Agent, VRU, and MR PGs	None
ECSPIM	11.5(1)	TAESPIM	Avaya SEI/CVLAN protocol was deprecated by vendor.
"Sprawler" deployment	10.0(1)	A Packaged CCE deployment	A "Sprawler" was a Progger with an Administration & Data Server on a single box. It was used for lab deployments.

Removed and Unsupported Features

Feature	Effective from Release	Replacement	Notes
HCS for CC 500 Agent Deployment Model	11.6(1)	HCS for CC 2000 Agent Deployment Model	The 2000 agent deployment model for HCS for CC has a subset deployment for 500 agent capacity allowing for reduced hardware footprint. For more information about 2000 Agent Deployment Model and the migration procedures, see *Cisco HCS for Contact Center Installing and Upgrading Guide* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html and *Solution Design Guide for Cisco HCS for Contact Center* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/tsd-products-support-series-home.html
AAS for Symposium (SEI Interface)	11.5(1)		
CTI OS Agent Desktop **Note** CTI OS Agent Desktop is supported for TDM and System PG only.	11.5(1)	Cisco Finesse.	
CTI OS Supervisor Desktop **Note** CTI OS Supervisor Desktop is supported for System PG only.	11.5(1)	Cisco Finesse	
CTI OS-Based Silent Monitoring **Note** CTI OS-Based Silent Monitoring is supported for System PG only.	11.5(1)		
Cisco Agent Desktop (CAD)	11.0(1)	Cisco Finesse	
Cisco Supervisor Desktop	11.0(1)	Cisco Finesse	

Feature	Effective from Release	Replacement	Notes
Cisco Media Blender	11.5(1)	For Unified WIM & EIM, use the Script Editor to configure dialed number prefixes and filters for Agent Request.	
Database Partitioning	9.0(1)	This feature is discontinued.	
H.323 protocol support	11.5(1)	SIP protocol	
Half Hour database tables: • Agent_Half_Hour • Agent_Skill_Group_Half_Hour • Call_Type_Half_Hour • Call_Type_SG_Half_Hour • Peripheral_Half_Hour • Service_Half_Hour • Skill_Group_Half_Hour **Note** The Half Hour database tables available in the database are not populated because these tables are not supported.	11.5(1)	Interval database tables	
On-Demand Licensing Model for Unified CCE	11.5(1)	Cisco Hosted Collaboration Solution (HCS) for Contact Center	
Jabber Guest	11.6(1)	Cisco Remote Expert Mobile for Android	
Support for Secure Socket Layer (SSL) 2.0 and 3.0	11.5(1)	Transport Layer Security (TLS)	
Unified Intelligent Contact Management Hosted (ICMH) and Unified Contact Center Hosted (Unified CCH)	11.5(1)	Cisco Hosted Collaboration Solution (HCS) for Contact Center	
Unified WIM & EIM	11.5(1)	Enterprise Chat and Email	
Remote Silent Monitor	11.6(1)	None	

Third Party Software Impacts

See the *Compatibilty Matrix for Cisco HCS for Contact Center* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html for information on third-party software.