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 2	Yes	Yes
Virtual Agent-Voice Call Transcription, on page 3	Yes	Yes
Preflight request for Private Network Access, on page 3	Yes	Yes
License Reservation, on page 4	Yes	Yes
HTTP Strict Transport Security Support for Unified CCE Web Applications, on page 4	Yes	Yes
Custom Truststore to Store Component Certificates, on page 4	Yes	Yes

Feature	Unified CCE	Packaged CCE
JTAPI credentials encryption (ES 35)	Yes	Yes
Support for 48000 Agents (ES04 and ES 25), on page 5	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 6	Yes	Yes
AppDynamics built-in integration with CCE, on page 7	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).

SQL Server Execution Plan Issue

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

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

```
“Alter Database <dbname> set COMPATIBILITY_LEVEL = 120”
```

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

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.

Deprecated Feature	Announced	Replacement	Notes
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.