Cisco Unified Contact Center Enterprise

New Features

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

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

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

To use VPN-less access to Finesse desktop, you must upgrade Finesse, IdS, and CUIC to Release 12.6(1) ES02 or above. If you are using Unified CCE 12.6(1), you must upgrade Live Data to 12.6(1) ES02 or above. You can access the 12.6(1) ES03 Release and Readme from the following locations:

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

Note

- For Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, refer to the Nginx TechNote article. Any reverse-proxy supporting the required criteria (as mentioned in the **Reverse-Proxy Selection Criteria** section of Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1)) can be used in place of Nginx for supporting this feature.
- If CORS status is "enabled", you must explicitly add the reverse-proxy domain name to the list of CORS trusted domain names.

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge) . For more information, see the *Supported Browsers* section in the *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Note

To enable this browser support in **Administration Client Setup for Cisco Unified ICM/Contact Center Enterprise**, install the ICM_12.0(1)_ES65.

Platform Updates

For information about the supported devices for this release, see the *Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Platform Upgrades

This release supports both Common Ground and Technology Refresh upgrades.

This release allows in-place operating system upgrades to Microsoft Windows Server 2016 Standard and Datacenter Editions with Desktop Experience and Microsoft SQL Server 2017 Standard and Enterprise Editions, followed by upgrade of Unified CCE from previous releases. For further information, see https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Hardware and Platform Support

Cisco UCS C240 M5SX Server Support

Cisco Unified CCE, Release 12.0(1), must be installed on Cisco UCS C240 M5SX servers *for TRC deployments*.

Other servers are supported for specification based deployments.

Note Upgrade to Cisco Unified CCE from an earlier release installed on an earlier server platform such as Cisco UCS C240 M4SX is supported.

On Cisco UCS C240 M4SX servers:

- When you upgrade to Release 12.0(1), on deployment types with 4000 Agents, add 16 GB RAM hardware memory to the Cisco UCS C240 M4SX server that is hosting the virtual machine on which Cisco CVP, Release 12.0(1), is installed.
- If you want to upgrade to Cisco Unified Communications Manager (CUCM), Release 12.5, you need to move all the upgrading CUCM virtual machines on to separate servers (off-box deployment).

  The CUCM, Release 12.5 software includes updates made to address the following Critical Vulnerabilities and Exposures (CVE):

  - CVE-2017-5753 and CVE-2017-5715, collectively known as *Spectre*.
  - CVE-2017-5754, known as *Meltdown*.

  Due to these updates, there is an overall decrease in performance of CUCM 12.5 system, requiring additional CPU resources to be allocated to the VM in order to compensate for the performance degradation. These additional resources require the CUCM VM to be moved off-box in order to stay in compliance with TRC requirements for the UCS servers hosting the Contact Center applications.

  You must manually configure 4 vCPU and 7200 MHz CPU reservations on the off-box deployment of CUCM, Release 12.5.

For more information about the server platform and deployment information for Cisco Unified CCE, see the Solution Design Guide for Cisco Unified Contact Center Enterprise

Upgrade VM to Hardware Version 11

Before you install this release, ensure that the Virtual Machine (VM) version installed is version 11.

Note Before you upgrade the VM version to version 11, **Power off** the VMs.

If you are upgrading the CCE deployment to Release 12.0(1), follow the steps provided in the Virtual Machine client documentation to upgrade the VM Compatibility to version 11 by selecting *ESXi 6.0 Update 2 or later*. *ESXi 6.0 Update 2 or later* provides the upgrade compatibility for VM version 11.

Important Selecting an option other than *ESXi 6.0 Update 2 or later* may not upgrade the VM version to version 11.

Note Power on the VMs after upgrading the VM compatibility to version 11.

Reference Design Layouts

The Reference Design layouts for the following Reference Designs have been modified for the Cisco UCS C240 M5SX server:

- 2000 Agents
- 4000 Agents
- 12000 Agents

For more information about support for various Reference Designs introduced in this release, see the New Deployment Types, on page 4 topic.

New Deployment Types

This release includes new deployment types to enable increased scale in contact center enterprise solutions:

- Unified CCE solution deployment type that supports 24000 Agents.

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

Secured Connections

The CCE solution manages customer sensitive information such as Personally Identifiable Information (PII) that is susceptible to internal and external exploitation. CCE solutions ensure security of PII in two ways: firstly, by not storing the PII in internal logs created in the solution and secondly, by securing the transport channels that carry PII, thus protecting it from external threats.

This release provides an end-to-end security of the transport channels that carry PII.

With this release, you can enable secured connections for:

- **Self-service communications**: By enabling secured connections in CVP and VRU PG.
- **Outbound Options**: By enabling secured connection in the CTI server, Dialer, and Media Routing PG.
- **Agent Desktop Communications**: By enabling mixed-mode connection in the CTI server and secured connection in the Cisco Finesse Server or in CTI OS, as applicable.
- **Third-party integration**: By enabling secured connection in the application gateway servers and clients.
- **Multi-channel communications**: By enabling secured connection between:
    - ECE (Server) and MR PG (Client)
    - CTI server and ECE (Client)

Certificate Management and Monitoring

This release provides a new utility called *CiscoCertUtil* to manage the security certificates that are required to establish secured connections.

This release also includes a new service called the *Unified CCE Certificate Monitor* that monitors the SSL and TLS based certificates and keys. This service helps the system administrator to ensure that the systems are installed with valid security certificates without interrupting the Unified CCE services that are running. It alerts the system administrator about the validity and expiry of these certificates through Event Viewer.

For information, see the following guides:

- For more information about the Certificate Monitoring service, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.
- *Solution Design Guide* for your solution.
- *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Default Domain Name

This release includes a new option, **Default domain name**, on the Configuration Manager's **System Information** dialog. With this option, you can choose a default domain name to add to usernames in a non-SSO environment. If a username is not in UPN (or SAM account) format, Unified CCE attaches this global domain name to the username when required.

In non-SSO solutions, Unified CCE does not require a username to be in UPN format. However, activities like supervisor sign-in for multiple PGs might require you to sign in with UPN-formatted usernames.

Non-SSO solutions had to add the required domain names to be added to usernames in Release 11.5 or 11.6. Those solutions can now set a **Default domain name** and then remove the domain name from the usernames with the **Bulk Editor** tool. For detailed instructions on this process, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise*.

Contact Director Supports 3 Unified CCE Targets

This release increases the number of supported Unified CCE targets in the Contact Director Reference Design from 2 to 3. The Contact Director can handle up to 24,000 agents across a maximum of 3 target Unified CCE instances.

Expanded Call Context Payloads

This feature expands the flexibility of Expanded Call Context (ECC) variables. An *ECC payload* is a defined set of ECC variables with a maximum size of 2000 bytes. ECC payloads to a CTI client include an extra 500 bytes for ECC variable names that are included in the CTI message.

In earlier releases, you can only define 2000 bytes of ECC variables system wide. In this release, you can define as many ECC variables as necessary. You can create ECC payloads with the necessary information for a given operation. You can include a specific ECC variable in multiple ECC payloads. The particular ECC variables in a given ECC payload are called its *members*.

You can use several ECC payloads in the same call flow, but only one ECC payload has scope at a given moment. For information on support of ECC payloads by interface, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise*.

Default ECC Payload

The solution includes an ECC payload named *Default* for backward compatibility. If your solution does not require more ECC variable space, you only need the Default payload. The solution uses the Default payload unless you override it.

If your solution only has the Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.

Note You cannot delete the Default payload, but, you can change its members.

In a fresh install, the Default payload includes the predefined system ECC variables. When you upgrade to Release 12.0, a script adds your existing ECC variables to the Default payload.

Important During upgrades, when the system first migrates your existing ECC variables to the Default payload, it does not check the CTI message size limit. The member names might exceed the extra 500 bytes that is allocated for ECC payloads to a CTI client. Manually check the **CTI Message Size** counter in the **Expanded Call Variable Payload List** tool to ensure that the Default payload does not exceed the limit. If the Default payload exceeds the limit, modify it to meet the limit.

If you use an ECC payload that exceeds the CTI message size limit in a client request, the CTI Server rejects the request. For an OPC message with such an ECC payload, the CTI Server sends the message without the ECC data. In this case, the following event is logged, `CTI Server was unable to forward ECC variables due to an overflow condition.`

Note The ECC payload feature is not available for Non Reference Designs.

For more information, see the following documents:

- *Solution Design Guide for Cisco Unified Contact Center Enterprise*
- *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*
- *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise*
- *List Tools Online Help*
- *Script Editor Online Help*

ECC Payload API

The ECC Payload feature includes an API. For details, see the *Cisco Unified Contact Center Enterprise Developer Reference Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-programming-reference-guides-list.html.

Business Hours

The Business Hours feature lets you create schedules for regular working hours and extra working hours, and to close the contact center for holidays or emergencies. It provides the mechanism for routing these contacts to specific support teams based on the configured work hour schedules, holidays, emergency closures, or extra working hours. You can create Business Hour schedules for various scenarios for various contact center teams.

This feature helps you create and apply several Business Hour schedules to the same team. On the other hand, you could apply the same Business Hour schedule to several support teams. When a customer contacts the contact center, the response by the contact center is based on the status of the support team. This status is evaluated using the Business Hour configured for the team.

Use this feature to:

- Configure default working hours (regular hours) for contact center teams for each day of the week. This option is not applicable to 24x7 support teams.
- Configure the special hours for the contact center team or teams for any special days such as Sale days or holidays.
- Force Close the contact center for any emergency such as a natural calamity.
- Force Open the contact center on a holiday or a non-working day to cater to specific business requirements such as Sale days.
- Create and deploy customer notifications that are based on Business Hour status.

For more information about Business Hours, see the Cisco Unified Contact Center Enterprise Features Guide.

PCM (G.711) A-law Support

This release adds support for Pulse Code Modulation (PCM) A-law encoding to SIP dialers.

Now, SIP dialers support both the G.711 encoding laws, A-law and µ-law. The SIP dialers for Outbound Option do not require DSP transcoder resources on the CUBE for initial negotiation between the SIP Dialer and the SIP service provider. CUBE auto-negotiates the encoding law between the SIP dialer and SIP service provider.

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

Updated Features

Increased PG Agent Capacity for Mobile Agents

Added on May 14th, 2021

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

- 2000 with nailed-up connections (1:1)

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

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

NPA NXX Database Update

Unified CCE Release 12.0(1) contains an updated version of the North American local exchange (NPA NXX) database based region prefix data, released on Oct 3rd, 2018. If you are upgrading your systems and employing North American dialing plan for Outbound calls, run the Region Prefix Update Tool (RPUT) for this update. For more information see the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

Outbound Option Predictive Algorithm Enhancements

Note To enable these Outbound Option enhancements, you must install the ICM_12.0(1)_ES87 on 12.0(1).

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

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

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

Configuration Limit Changes

For all the updated configuration limits, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

Required System CLI Update

This release includes changes to the System CLI. Our installers update the System CLI on all of our VMs.

However, you can copy the System CLI and run it on an outside machine. Earlier versions of the System CLI do not operate correctly when used to monitor Unified CCE 12.0. Replace any earlier versions of the System CLI on outside machines with the Release 12.0 version.

Platform Updates for CTI OS

Visual Studio 2015 Redistributable

This release includes Visual Studio 2015 Redistributable on the server side and on Microsoft Windows 10 client.

Software updates

The CTI OS platform has been updated to the following:

Software	Version
.NET Framework	4.7.1
Java JRE	1.8 Update 161

Note For information on Microsoft Windows platforms for CTI OS clients and servers, see *Contact Center Enterprise Compatibility Matrix, Release 12.0(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

Integrated Digital Multi-tasking

This release enhances CCE routing for interruptible Media Routing Domains (MRDs) supporting ECE. The new functionality enables agents to do the following:

- **Pick tasks**—Get specific tasks from either a Unified CCE queue or an external application's queue.
- **Pull tasks**—Get the next *n* tasks from either a Unified CCE queue or an external application's queue, based on the queue's ordering.
- **Transfer tasks**—Transfer specific tasks to or from another agent or queue.

Important This feature requires all components in the call flow to be on Release 12.0(1).

Pick and Pull Integration

An agent can pick an email task from the available email tasks. The agent can also pull email tasks from the available email tasks in the queues. The pick or pull activity can be executed even when:

- the agent is busy on a voice call.

- the agent's maximum task limit for emails is reached and the agent is working on a voice call or chat activity.
- the call is queued in a queue that is not available in the pick or pull request.

These enhancements are available on the ECE gadget on Cisco Finesse, Release 12.0(1).

ECE Task Transfers

ECE task transfers are managed as follows:

- ECE tasks transferred to agents or back to queues are counted as transfer statistics (i.e. Transfer In / Transfer Out / TransferInCallsTime) in *Agent_Skill_Group_Interval* and *Skill_Group_Interval* historical tables.
- ECE tasks transferred to agents or back to queues generate Termination Call Detail (TCD) records with the Peripheral Call Type classified as *Transfer In(4)*.

Enhancements to Active Directory and Service Account Manager

Decouple Authorization from Microsoft Active Directory

The Unified CCE separates authentication and authorization functions. Until Release 12.0(1), Unified CCE uses Microsoft Active Directory Security Groups to control user access rights to perform setup and configuration tasks. Unified CCE solution administration required write permissions to Microsoft AD for authorization.

Decoupling authentication and authorization removes the need to use Microsoft AD to manage authorization in Unified CCE components. User privileges are provided by memberships to local user groups in the local machines. Microsoft AD is only used for authentication.

This release introduces following enhancements to decouple authorizations from Microsoft AD:

- Websetup no longer be used to create service accounts for Logger, Distributor, and HDS services. As an administrator, you can create service account domain users prior to setup. Websetup accepts and verifies an existing domain user for service access.
- Setup users only require local admin privileges to run setup utilities. The ICM_Setup security group in AD is deprecated.
- To run Unified CCE configuration tools such as the Configuration Manager or Script Editor, Config users no longer require local admin privileges, and do not need to be assigned to the ICM_Config security group in AD, although you can continue to use the old Config security group if it is convenient. This behavior of the security group usage is managed by the **ADSecurityGroupUpdate** registry key.
- The ICM OU structures are still required in AD to allow for a consistent instance naming across components.
- As part of the upgrade process, there is a one-time migration of user roles from AD to the Unified CCE local configuration tables. See the *User Role Update tool* section.

ADSecurityGroupUpdate Registry Key

This Registry key allows or disallows updates to the Config and Setup security groups in the Domain under an instance Organizational Unit (OU). By default, upgrading to Release 12.0(1) sets this key to OFF (0), which disallows updates.

For more information on the registry key, see the *Decouple CCE Authorization from Active Directory* section in the *Solution Security* chapter of the Solution Design Guide for Cisco Unified Contact Center Enterprise.

User Health in Service Account Manager

After the upgrade to Release 12.0(1), the Service Account Manager checks the users in the `UcceService` local group. If the users are not in the local security groups, the Service Account Manager displays the status as *Unhealthy*. Select the *Unhealthy* service account and click the **Fix Group Membership** button to make the status healthy or provide the new domain user in the Service Account Manager (SAM) tool or in `Websetup`.

For more information, see the *Decouple CCE Authorization from Active Directory* section in the *Solution Security* chapter of the Solution Design Guide for Cisco Unified Contact Center Enterprise.

User Role Update tool

The Active Directory based authorization enhancements now require the use of a tool to migrate User Authorization role from Microsoft AD to Database.

For more details, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Database Schema Changes

Unified CCE Database Schema Changes

Release 12.0 (1) includes several changes to the database schema for the main database. The release adds the following new tables:

- Business_Hours
- Business_Hours_Real_Time
- Business_Hours_Reason
- ECC_Payload
- ECC_Payload_Member
- Location
- Location_Member
- Peripheral_Set
- Peripheral_Set_Controller
- Peripheral_Set_Host
- Routing_Pattern
- SIP_Server_Group

- SIP_Server_Group_Elements
- Special_Day_Schedule
- Time_Zone_Location
- Week_Day_Schedule

The release added new fields to the following tables:

Table	Changes
Dialed_Number	Added these new fields: • PCSPattern • RingtoneName
Machine_Service	Added the *OutOfSyncTimestamp* field.
Application_Gateway	Added the *TLS* option to the encryption field.
Agent_Interval	Added these new fields: • PickRequests • PullRequests • PickErrors • PullErrors
Call_Type_Interval	Added these new fields: • PickRequests • PullRequests • PickErrors • PullErrors
Reason Code	Added these new fields: • Reason Type • IsGlobal
Campaign	Added these new fields: • StartDate • EndDate • TZDisplayName

Table	Changes
Router_Queue_Interval	Added these new fields: • RedirectNoAnsCalls • CallsHandled • PickRequests • PullRequests • PickErrors • PullErrors • FutureUseInt1 • FutureUseInt2
Call_Type_SG_Interva	Added these new fields: • PickRequests • PullRequests • PickErrors • PullErrors
Dialer_Interval	Added *FutureUseInt3* as a new field.
Dialer_Real_Time	Added *FutureUseInt3* as a new field.
System_Capacity_Real	Added these new fields: • FutureUseInt1 • FutureUseInt2
User_Group	Added the *UserRole* field.

The release includes datatype change to the following table:

Table	Changes
Machine_Host	Changed datatype of *MachineName* to **`NULL`**.

Important Notes

Install Release 12.0(1)

Platform Updates

Note Ensure that Microsoft Windows Update is not running in parallel when you install Release 12.0(1).

Installing or Upgrading to Cisco Unified CCE, Release 12.0(1)

The following considerations apply when you want to install or upgrade to Cisco Unified CCE, Release 12.0(1):

- Do not run the installer remotely. Mount the installer ISO file only to a local machine.
- The installer, previously called ICM-CCE-CCHInstaller, has been renamed as ICM-CCE-Installer. This installer is a full installer. Roll-back to the previously installed release is not supported. Backup the Virtual Machines (VMs) for use as restore points.
- The minimum disk space required to perform the upgrade is 2175 MB.
- Before you upgrade the Cisco VOS based servers such as the Live Data server, power on the VM. Before you power on the VM, ensure the VM is set to check and upgrade VM Tools when powered on.

  For more information on VMware Tools upgrade, see the *VMware documentation*.
- If you install or upgrade to CUCM, Release 12.5, install JTAPI using the procedure provided in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*.

  For details about JTAPI compatibility with the CUCM versions, see the ***JTAPI CUCM Compatibility Matrix*** at: https://d1nmyq4gcgsfi5.cloudfront.net/site/jtapi/documents/jtapi-ucm-compatibility-matrix/

Note When you install Release 12.0(1) using the 12.0(1) base installer, ensure that all other existing applications such as Microsoft Windows sessions are closed. Any applications that may need to be updated by the installation or upgrade process, if left inadvertently left open or active, may prevent the installation or upgrade processes from running smoothly. The installer logs provides the details of the files that are locked during the upgrade.

To resolve the issues that arise during installation or upgrade, close all the applications and re-run the 12.0(1) base installer.

For more information about installing or upgrading to Cisco Unified CCE, Release 12.0(1), see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*

Uninstall Unified CCE Release 12.0(1)

Uninstallation of Release 12.0 using the ICM-CCE-Installer ISO is not supported.

If you need to revert to the previous version that existed before you upgraded to Release 12.0(1), do one of the following before you upgrade to Release 12.0(1):

1. Take a Virtual Machine Snapshot in the powered off state before the upgrade.
2. Clone the Virtual Machine before the upgrade.

Delete these snapshots or clones after the upgrades are successfully completed to avoid performance issues.

Uninstallation and re-installation of other packages like Administration Client and Internet Script Editor (ISE) are supported.

Script Editor Changes Can Disable Existing Script Monitors

In this release, some of the new features, like Integrated Digital Multi-tasking and ECC Payload, added monitors to several existing nodes in the Script Editor. With these new monitors, your existing scripts might exceed the limit of 900 monitors in a script.

If your script exceeds the limit, some of the real-time monitors stop working. In this case, you see periodic messages in the Router log and Event report that the script exceeds the monitor limit. If you edit a script that is over the limit, a warning displays when you attempt to save the script.

Drop Call Participants from a Conference Call

This release resolves the following caveats:

- CSCvb42182
- CSCvb52840
- CSCve48564

The resolution allows dropping any conference call participants with appropriate logs and events with caller information and gadget status updates for Unified CCE solution and components.

A conference call participant may be dropped when a call was queued in the CVP and is redirected to an agent. In a scenario where a call is redirected from CVP to an agent, the following additional event messages are sent from the CTI server to the CTI clients:

- CALL_CONNECTION_CLEARED_EVENT with cause code 28 (CEC_REDIRECTED) occurs for the connection device that is released from CVP.
- CALL_ESTABLISHED_EVENT with cause code 50 (CEC_CALL_PARTY_UPDATE_IND) occurs for a new connection added in to the call.

In a Parent/Child deployment, this function is disabled by default. To enable this function, both the parent and child deployments must be upgraded to Release 12.0. For information on enabling this function in a Parent/Child deployments, see the *Cisco Contact Center Gateway Deployment Guide for Cisco Unified ICME/CCE*.

Supported Login Formats

Login formats are explained using below user’s attributes.

User Details	
UserName	John.Kim
Domain FQDN	cce.local
User's SAM Name	C012345
DC's NetBios	CSS
Alternate Suffix Available	cce.com

The following table illustrates supported login formats in Unified CCE Administration and Web Setup for Cisco Unified ICM/Contact Center Enterprise.

S. No.	Login Format	Supported in Unified CCE Administration	Supported in Unified CCE Websetup
1	Login in UPN format where UPN created with username@DomainFQDN. Example: john.kim@cce.local	Yes	Yes
2	Login in UPN format where UPN created with username@ALTSuffix. Example: john.kim@cce.com	Yes	Yes
3	Login in UPN format but with SAM@DomainFQDN. Example: C012345@cce.local	Yes	Yes
4	Login in UPN format but with SAM@NetBIOS. Example: C012345@CSS	No	Yes
5	Login in NetBIOS format NetBIOS\SAM. Example: CSS\C012345	No	Yes
6	Login just SAM name. Example: C1012345	No	Yes

Note Login with SAM@AlternateSuffix is not supported.

Other Important Considerations

Administration Client Tools Display

Some tools in Configuration Manager may not be displayed properly. On Microsoft Windows 10 clients, turn on the appropriate setting to *Fix scaling for apps* in **Settings**.

For more information about fixing scaling for apps that appear blurry, see the Client OS documentation.

Outbound Option HA Replication

This release changes the replication protocol for Outbound Option High Availability from Named Pipes to TCP/IP to improve replication performance based on Microsoft guidelines.

Microsoft SQL replication is best effort technology, and can result in large replication delays for outbound campaigns depending on your deployment and dialing use case. Warm standby Campaign Manager can be enabled without replication.

For more information about the replication protocol, see the Solution Design Guide for Cisco Unified Contact Center Enterprise.

Deprecated Features

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

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

Deprecated Feature	Announced in Release	Replacement	Notes
Internet Explorer 11	Not applicable[1]	Edge Chromium (Microsoft Edge v79 and later)	None
Cisco MediaSense	12.0(1)	None.	Cisco MediaSense is not supported in the Contact Center Enterprise solutions from Release 12.0(1). Cisco MediaSense is only supported for earlier releases such as Release 11.6(x).

Deprecated Feature	Announced in Release	Replacement	Notes
Context Service	12.0(1)	None.	We will continue to support Cisco Context Service and will provide critical bug fixes as needed. We will be building a new and improved cloud based customer journey capability to replace Cisco Context Service. This capability would be common across all Cisco Contact Center solutions such as the Customer Journey Platform, Unified CCX, Unified CCE, Packaged CCE, and HCS for Contact Center. Please see the published roadmap or contact Cisco for more details. **Note** Existing Cisco Context Service customers can continue to use this capability until the new customer journey capability is available.
Integrity Check Tool	12.0(1)	None.	None.
External Script Validation	12.0(1)	None.	None.
Translation Route Wizard	12.0(1)	None.	None.
Symposium ACD	12.0(1)	None.	None.
MIB Objects: • cccaDistAwWebViewEnabled • cccaDistAwWebViewServerName • cccaSupportToolsURL • cccaDialerCallAttemptsPerSec	11.6(1)	None.	None.
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 PG and VRU PG	None

Deprecated Feature	Announced in Release	Replacement	Notes
ECSPIM	11.5(1)	TAESPIM	Avaya SEI/CVLAN protocol was deprecated by vendor.
"Sprawler" deployment	10.0(1)	A Packaged CCE deployment	A "Sprawler" was a Progger with an Administration & Data Server on a single box. It was used for lab deployments.

[1] Based on external communication from Microsoft

Removed and Unsupported Features

The following features are no longer available:

Feature	Effective from Release	Replacement	
CTI OS deployment on Citrix environment.	12.0(1)	None	
Microsoft Windows 7 Support as Client OS for Administration Clients in the CCE solutions. Support is removed based on Microsoft's product lifecycle milestones for Windows 7.	12.0(1)	Microsoft Windows 10.	

Third Party Software Impacts

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