Cisco Packaged 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.

Desktop Layout Editors

This feature requires ICM12.5(1)_ES7. This release provides the following Desktop Layout editors in the **Teams** and **Resources** pages of the **Unified CCE Administration**.

- **Text Editor**— Allows you to view and edit code in text format. It is the default editor.
- **XML Editor**— Allows you to view and edit code in XML format. However, you cannot add or edit comments (<!-- -->) in this editor.

For more information, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Smart Licensing

Note To manage CVP 12.5(1) licenses in Packaged CCE 12.0(1), install ICM12.0(1)_ES37.

This release introduces Smart Licensing that delivers visibility into your license ownership and consumption. Smart Licensing helps you to procure, deploy, and manage licenses easily and report license consumption. It pools license entitlements in a single account and allows you to move licenses freely through the virtual accounts.

Smart Licensing registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager On-Prem.

For more information, see *Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Command Execution Pane

Note To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES 37 patch or higher.

In this release, a new user interface called **Command Execution Pane** has been added in the Infrastructure Settings page of Unified CCE Administration. This interface allows System Administrators to execute REST API calls to the Unified CVP, Unified CVP Reporting, and Virtualized Voice Browser.

For more information, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Platform Common Ground Upgrade

This release supports Common Ground upgrade.

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 Packaged CCE from previous releases. For further information, see the *Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html.

Third-Party Integration

Note To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES26 patch or higher.

Third-party integration feature enables you to add user interfaces of third-party components your Contact Center employs in to Unified CCE Administration. You can add custom gadgets such as an agent reskilling gadget or third-party pages such as a browser-based CRM tool. Integrate the user-interfaces and administer multiple third-party components from Unified CCE Administration.

For information on how to integrate a third-party gadget or page to Unified CCE Administration, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide, Release 12.0 (1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Avaya Support

Note To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES26 patch or higher.

In this release, support for Avaya Automatic Call Distribution (ACD) integration has been provided in the Packaged CCE 4000 and 12000 Agent deployments.

For more information about the feature, see the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

ICM-to-ICM Gateway Support

Note To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES26 patch or higher.

In this release, support for ICM-to-ICM Gateway has been provided in the Packaged CCE 4000 and 12000 Agent deployments.

For more information about the feature, see the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Unified CVP Statistics

Note To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES15 patch on Packaged CCE 12.0 and CVP ES5 on CVP 12.0.

In this release, the Packaged CCE 2000, 4000, and 12000 Agent deployments will enable the administrators to view statistics for the following in the **Unified CCE Administration > Infrastructure > Inventory** page:

- Unified CVP
  - Call Server: ICM, SIP, and Infrastructure statistics
  - VXML Server: VXML, Infrastructure, and IVR statistics
- Unified CVP Reporting:
  - Reporting statistics
  - Infrastructure statistics

For more information, see the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Hardware and Platform Support

Cisco UCS C240 M5SX Server Support

Cisco Packaged 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 Packaged 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 Packaged CCE, see the *Solution Design Guide for Cisco Packaged 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 7 topic.

New User Interface

Packaged CCE 12.0 has a new user interface which is in accordance with other contact center applications. The user interface allows you to configure the solution through one application. Sign in to the new Unified CCE Administration at https://<IP Address>/cceadmin. <IP Address> is the address of the Side A or B Unified CCE AW or the optional external HDS.

Note Unified CCE Administration requires full screen view of the browser with the minimum resolution of 1366 x 768.

In this release, the Unified CCE Administration interface allows you to configure the following:

- Campaigns
- Courtesy Callback
- SIP Server Groups
- File Transfers: File transfer is possible only through Principal AW (Side A AW in 2000 agent deployment and configured AW in 4000 agent and 12000 agent deployments).
- Routing Patterns: Dialed number pattern in Unified CVP Operations Console is now called Routing Pattern in Unified CCE Administration.
- Locations: In Unified CCE Administration, Routing Code is now the location prefix instead of Site ID.
- Device Configuration: Unified CCE Administration allows you to configure the following devices: CVP Server, CVP Reporting Server, VVB, Finesse, Identity Service (Single Sign-on Setup).

- Team Resources: Unified CCE Administration allows you to define and associate the following resources for agent teams: Call Variables Layout, Desktop Layout, Phone Books, Workflows, Reasons (Not Ready, Sign Out, Wrap-Up).
- Email and Chat

New Deployment Types

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

- Packaged CCE solution deployment types that support 4000 Agents and 12000 Agents respectively.

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

Business Hours

Business hours are the working hours during which you conduct business. You can create and modify business hours and set weekly and daily schedules for each business hour. You can create different business hour schedules for regular working days and holidays. You can also open or close the business hours if there is an emergency.

You can define the status reasons for business hours and assign codes for each status reason. Status reason is required when you force open or force close a business hour, and when you add special hours and holidays.

Synchronization

In this release, the Unified CCE Administration interface supports synchronization of configuration to other machines (Unified CVP Server, Unified CVP Reporting Server, Finesse, CUIC, ECE) from AW Database in real time basis.

In case of synchronization failure, the respective machine is marked out-of-sync and a new out-of-sync icon appears on the Unified CCE Administration interface. All configuration made while a machine is in out-of-sync, is synchronized periodically every 10 minute or by manual trigger from the Inventory page.

The Full Sync option for Unified CVP on the Inventory allows redeployment and synchronization of all configuration data.

VMware Foundation License

Packaged CCE qualifies with VMware Foundation license.

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.

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 Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html

CVP Configuration for Media Server

Note To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES34 patch on Packaged CCE 12.0 and CVP ES6 on CVP 12.0.

In this release, support for the following has been provided in the **Inventory** page of **Unified CCE Administration**:

- Addition, modification, and deletion of external Media Servers
- Access to FTP configuration in external Media Servers
- Access to FTP configuration in CVPs where Media Servers are installed

Note Any configuration change in Media Server gets propagated to all CVPs across sites.

For more information, see *Media Server* section in the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Enhancements to Active Directory and Service Account Manager

Note **Note**: To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES34 patch. After installing ES34, ensure that you change the AW registry "ADSecurityGroupUpdate" to 1 to disable this feature. Change the registry key value back to 0 if you want to enable this feature.

Decouple Authorization from Microsoft Active Directory

The Packaged CCE separates authentication and authorization functions. Until Release 12.0(1), Packaged CCE uses Microsoft Active Directory Security Groups to control user access rights to perform setup and configuration tasks. Packaged 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 Packaged CCE components. User privileges are provided by memberships to local user groups in the local machines. Microsoft AD is only used for authentication.

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 Packaged 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`.

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.

External Machines

In this release, Unified CCE Administration allows you to add the following external machines:

- Cisco Virtualized Voice Browser
- Cisco Unified SIP Proxy
- Gateway

- ECE Web Server

Configuration Manager Tools

Following is the list of Configuration Manager tools that are enabled for Packaged CCE 4000 agents and 12000 agents deployments:

- Explorer Tools: DB Lookup Explorer, ICM Instance Explorer, Network VRU Explorer, PG Explorer
- List Tools: Agent Desk Settings List, Label List
- Miscellaneous Tools: Unreferenced Objects

Dialed Number Configuration

In this release, the Unified CCE Administration interface enables you to configure the Post Call Survey Dialed Number and ringtone media file for external type Dialed Number.

Reason Labels

In this release, the Unified CCE Administration interface allows you to configure the Not Ready, Sign Out, and Wrap-Up reason labels for Cisco Finesse across all sites. Reason labels appear in the Cisco Unified Intelligence Center reports, and helps identifying agent work behavior. For more information about pre-defined reason codes, see Reason_Code table in the *Database Schema Handbook for Cisco Unified ICM/Contact CenterEnterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-technical-reference-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.

Configuration Limit Changes

For all the updated configuration limits, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-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.

Important Notes

SocialMiner Name Change

Cisco Social Miner is renamed to Customer Collaboration Platform.

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

S. No.	Login Format	Supported in Unified CCE Administration	Supported in Unified CCE Websetup
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.

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*.

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).
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.

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 PG and VRU PG	None
"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	
Unified CVP Operations Console (OAMP)	12.0(1)	Unified CCE Administration interface	You can configure CVP components, VVB, Gateway, CUSP, and related configurations through Unified CCE Administration interface.
UCS B-Series Fabric Interconnects Validation Tool	12.0(1)	None.	None.

Third Party Software Impacts

See the *Contact Center Enterprise Compatibility Matrix* for this release at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for information on third-party software.