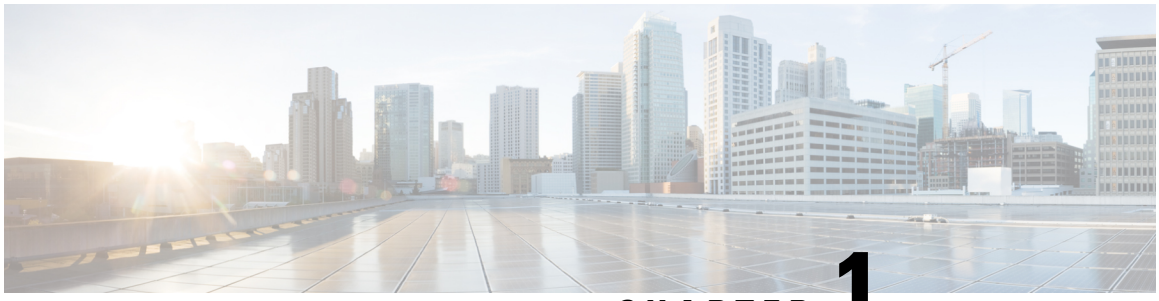
Release Notes for Cisco Hosted Collaboration Solution for Contact Center Solution, Release 12.0(1)

First Published: 2019-01-11

Last Modified: 2021-07-30

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

CONTENTS



CHAPTER 1

Introduction

Release Notes for Contact Center Solutions

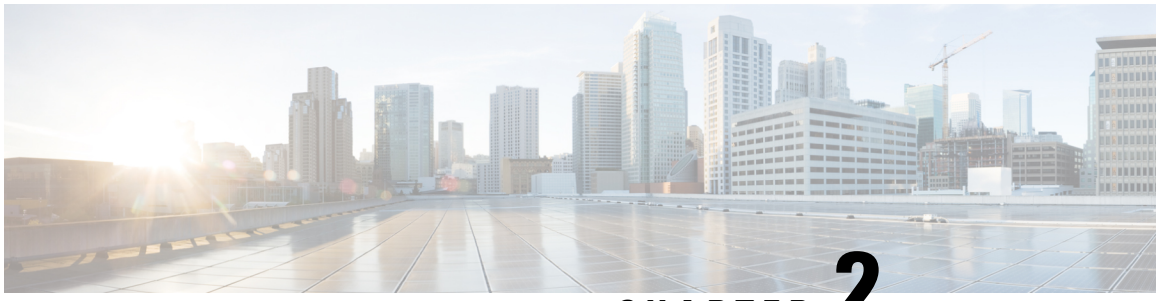
In addition to the release notes in this document, see the release note compilations for the other contact center solutions at the following links:

- *Release Notes for Cisco Packaged Contact Center Enterprise Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html
- *Release Notes for Cisco Hosted Collaboration Solution for Contact Center* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-release-notes-list.html
- *Release Notes for Cisco Unified Contact Center Enterprise Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-release-notes-list.html
- *Release Notes for Cisco Unified Contact Center Express Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-release-notes-list.html

Cisco Security Advisories

The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that relates to Cisco products and networks.

For information on existing security issues, see *Cisco Security Advisories, Responses, and Alerts* at https://tools.cisco.com/security/center/publicationListing.x.



CHAPTER 2

Cisco Hosted Collaboration Solution for Contact Center

All features that were introduced in 12.5(1) and 12.5(1) ES releases are included as part of 12.5(2).

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 the *Installing and Upgrading Guide for Cisco Hosted Collaboration Solution for Contact Center* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/hcs-cc/12_0_1/Install_Upgrade_Guide/hcs-cc_b_installing-and-upgrading-guide-12-0.html.

Hardware and Platform Support

Cisco UCS C240 M5SX Server Support

Cisco Hosted Collaboration Solution for Contact Center, 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 Hosted Collaboration Solution for Contact Center 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.

For more information about the server platform and deployment information for Cisco Hosted Collaboration Solution for Contact Center, see the *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

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 6 topic.

New Deployment Types

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

This release of Cisco Hosted Collaboration Solution for Contact Center supports the 24000 Agent deployment type to enable increased scale in contact center enterprise solutions.

For more information, see the *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 .

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 Cisco Hosted Collaboration Solution for Contact Center, Release 12.0* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/tsd-products-support-series-home.html

- *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. 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 Hosted Collaboration Solution for Contact Center, Release 12.0* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/tsd-products-support-series-home.html

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.

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 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

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 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

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 separates authentication and authorization functions. Until Release 12.0(1), uses Microsoft Active Directory Security Groups to control user access rights to perform setup and configuration tasks. 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 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 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 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.

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.

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

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

Non Support For Business Hours

HCS for Contact Center 12.0 release does not support the Business Hours feature.

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.
Translation Route Wizard	12.0(1)	None.	None.
Symposium ACD	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
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

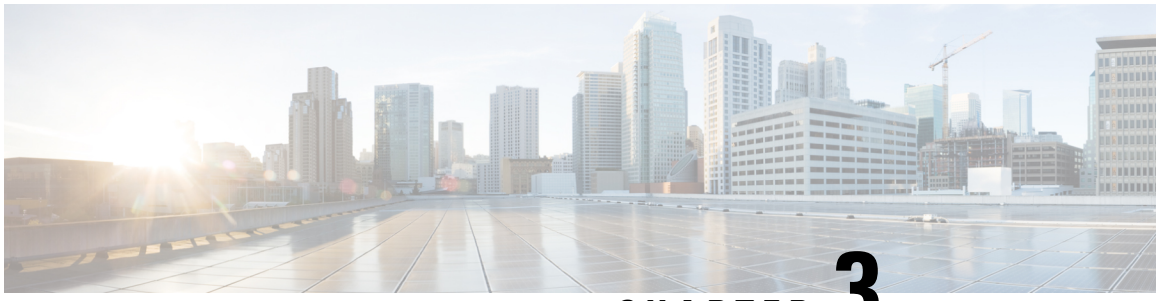
Removed and Unsupported Features

The following features are no longer available:

Feature	Effective from Release	Replacement	
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 *Contact Center Enterprise Compatibility Matrix* for this release at https://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.



CHAPTER 3

Cisco Enterprise Chat and Email

New Features

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.

Utility for Masking Content

Note To enable this enhancement in ECE 12.0(1), install the ECE 12.0(1) ES1 patch or the latest ECE ES patch.

A new utility **Mask Content of Chat and Email Activities** is available in the Tools Console to mask content in completed chats and both open and completed emails. The utility can be run by department users with the **View Tools Console** action.

Secure MR PG and CTI Interface

Secure connections ensure that all personally identifiable information, that passes through these connections, remains secure in the CCE solution. The following connections for ECE can be secured:

- Connection between the external agent assignment service (EAAS) to MRPG interface.
- Connection between the external agent message service (EAMS) to CTI interface.

This ECE release adds validation tools to the interface that allow administrators to do the following:

- enable the secure connections.
- disable the secure connections.
- test the secure connections.

ECE Administrator Gadget for PCCE

This release adds the ECE administrator gadget to the PCCE Admin Console.

This gadget provides a fast, simple interface for ECE administrators that is compatible with multiple compatible and can be accessed through the PCCE web admin interface. This interface provides a single convenient location to complete the post-installation administrative tasks without the need to access multiple administration consoles.

Skill Based Availability

In this release, the method of determining agent availability for activities is enhanced.

The enhanced method determines agent availability based on skill groups or precision queues, instead of determining availability based on Media Routing Domains. This ensures a better customer experience by more efficiently pairing customers with agents who are qualified and capable of handling the customers' requests.

Integrate Supervisor Accounts

This release supports the import and integration of supervisor user accounts from CCE into ECE.

Supervisors that are imported from CCE into ECE are automatically assigned the ECE Supervisor role.

Chat Monitoring for Supervisors

This release adds chat monitoring capabilities for supervisors in ECE.

Chat monitoring allows supervisors to review how agents handle chat interactions. Supervisors can monitor each agent individually, or they can monitor selected queues and the chats coming through them. They can also join chat sessions that are in progress and provide guidance to the agent or further assistance to the customer.

Purge Email Attachments

It is necessary to manage and reduce database storage to accomplish the following:

- Reduce data storage costs.
- Improve application performance.
- Reduce risks related to the handling of older data.

This release adds the purge functionality to manage email attachments that increase database usage. This functionality is a step in accomplishing better management and reduction of database storage.

Updated Features

Updated JDK

Note To enable this enhancement in ECE 12.0(1), install the ECE 12.0(1) ES1 patch or the latest ECE ES patch.

The following versions are now supported. The Updater automatically installs the new version.

- Open JDK version 11 (replaces Oracle JDK (1.8.0))
- Eclipse JETTY 9.4.14
- Apache ActiveMQ 5.15.6

Chat Improvements

Note To enable this enhancement in ECE 12.0(1), install the ECE 12.0(1) ES1 patch or the latest ECE ES patch.

Agents can now authenticate customers while a chat is in progress. To use this feature, SP initiated single sign-on must be enabled for chat. A new button is added to the chat reply area using which the agent can request customer authentication. A new icon is used to indicate authenticated chats in the agent inbox.

A new department level setting Chat - Daily Service Level Timezone is available to define the time zone for Daily Service Level in supervision monitors. The default value of the setting is UTC.

Agent Gadget

Note To enable this enhancement in ECE 12.0(1), install the ECE 12.0(1) ES1 patch or the latest ECE ES patch.

Agent Efficiency Improvements

- Agents can now add notes to activities from the Transfer window. Transfer notes are presented as pop-up notification to the receiving agent upon selection of the activity.
- The system now allows agents to print all case details. The Print Case button is available in the Case Details section of the Information Area.

Search Improvements

- Content search restrictions for email address, customer name, subject, and email content have been eased to include special characters, like $ & * ^ % _ # " ~ ! | + - .
- Search results can now be sorted by Creation Date, Customer name, Email address, Subject, Assigned to, Activity status, Activity sub status, Queue name, and Department name.
- Improvements are made for partial text search. For example, if activity subject or content contains “How do I return my orders”, searching for “return my order” will return that activity in search results.

My Searches Folders

Agents now have the ability to create My Searches folders for cases and activities. Folders can be created to save quick reference for any search criteria you use frequently for activities and cases.

ECE REST API Enhancements and Updates

Note To enable this enhancement in ECE 12.0(1), install the ECE 12.0(1) ES1 patch or the latest ECE ES patch.

Chat Messaging APIs

Chat Messaging APIs are now available. These APIs can be used to build external integrations with custom messaging apps, messaging channels like Facebook Messenger etc. and building custom web templates. The chats created from these Chat Messaging APIs will be routed to agents like regular web chats and will have the web chat features available.

The client applications for the integration are setup from the Administration console. For details, see Administrator’s Guide to Chat and Collaboration Resources. For details about using the APIs, see the Interaction API Reference Guide.

New APIs are provided to achieve the following functionality:

- Create, read and delete notes for activity, case and customer.
- Edit custom attributes of a closed case.

Existing APIs have been enhanced to provide the following functionality:

- Using **Activity Search API**, activities can now be filtered based on type along with one or more additional criterion.
- Partition users can now use Get Activity Attributes and **Get Customer Attributes API** to retrieve the custom attributes for activity and customer object. These can then be used in creating a new activity using existing APIs.
- Users can retain inline attachments while offloading the attachments of a completed email activity using **Delete completed activity attachments API**.
- Users can get the inline attachment data along with content of an email using the **Get activities by IDs API**. This can be used while offloading the content to external systems.

Administration

Note To enable this enhancement in ECE 12.0(1), install the ECE 12.0(1) ES1 patch or the latest ECE ES patch.

Administration for PCCE

The Global space in the ECE Administrator Gadget in PCCE is renamed to Partition.

User Management

Administrators can now create custom roles using the role templates available in the system.

Custom Attributes

Custom Attributes can now be added for Customer and Contact Person objects. This is in addition to the ability to add custom attributes for activities.

Call Variables

Custom Attributes can now be added for Customer and Contact Person objects. This is in addition to the ability to add custom attributes for activities.

Redundancy Across Geographies

This release supports automatic failover capabilities across multiple geographies. For more details see the *Enterprise Chat and Email Design Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-implementation-design-guides-list.html and the *Enterprise Chat and Email Installation and Configuration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-management-portal/products-installation-guides-list.html.

Limit Activities in the ECE Queue

Better queue management is necessary to ensure that higher priority queues offer tasks to the Unified CCE queue over lower priority queues.

This release provides administrators the ability to define the number of activities a queue can have at a given time. This, in turn, provides better queue management.

Alarm Workflow Integration

This release enhances the functionality of alarm workflows by adding routing operations to support integrated queues and users.

Alarm workflows can now transfer activities to/from integrated queues or integrated users. Alarm workflows can also do the following:

- Send notifications to agents regarding the SLA of an activity.
- Modify the activity's properties.
- Allow an assigned activity to be marked as complete .

Integrated Digital Multi-tasking

This release adds enhanced support for Integrated Digital Multi-tasking. The enhancements include improved routing methods for agent activities.

The enhancements include the following:

- Concurrent task limits do not prevent high-priority activities from being assigned and handled quickly.
- Improved efficiency in picking, pulling, and transferring activities.
- Improved handling of the concurrent task limits (CTL) of the agents and queues.

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)*.

Cisco Finesse Integration Enhancements

This release adds support for Cisco Finesse, Release 12.0(1) and enhances its integration with the ECE Agent Console. As Agents, you can now do the following:

- Manage your availability for chat and email activities through the Finesse desktop toolbar.
- Receive toaster and popover notifications on your desktop, ensuring that you are immediately alerted to any new incoming activities, regardless of if the agent is actively working in the ECE Agent Console.

ECE, Release 12.0(1) supports Finesse workflows for email and chat.

Search Functionality

Some search functionality has been changed or removed to improve application performance. The changes include:

- The timeout for searches has been reduced to 30 seconds. Search timing out before completion of the search is an indication that a large number of results were found and that the search criteria should be refined.
- Sorting of search results is enabled only for the following fields:
  - Activity ID.
  - Case ID.
  - Customer First Name.
  - Customer Last Name.

- As applicable, the default operator for search fields has been changed from *Contains* to =
- Validations have been added for the specific search attributes. The validations include:
  - Activity – Subject: A minimum of 5 characters is required when using the operator.
  - Customer - Customer name: A minimum of 2 characters is required when using the *Contains*operator.
  - Contact Point - Phone number: A minimum of 6 characters is required.
- Search operators have been changed for search attributes. Existing saved searches should be edited and saved using an operator that is currently available in the application.

Important Notes

Archive Database

From ECE, Release 12.0(1), the archive database is no longer required.

Note If you have upgraded to ECE 12.0(1) from an earlier version, you can connect to the archive database using data adapters.

Deprecated features

None.

Removed and Unsupported Features

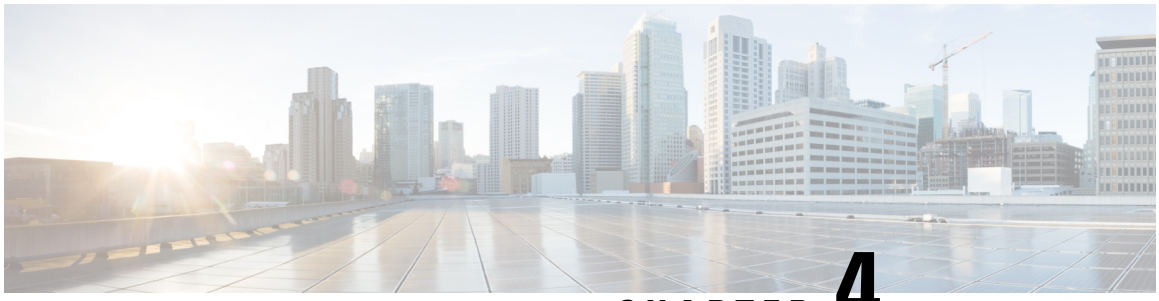
Wrap-Up Role

The Wrap-Up role and the actions specifically associated with the role have been removed for both email and chat, in this release.

Note Agents can still make notes and complete the chat activities after the customer has left the chat.

Third Party Software Impacts

See the *Contact Center Enterprise Compatibility Matrix* for this release at https://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.



CHAPTER 4

Cisco Unified Customer Voice Portal

New Features

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge). For information about supported versions, see 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.

Platform-Updates

In this release, CVP supports Microsoft Windows Server 2016 Standard and Datacenter Editions with Desktop Experience. For more information, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal, Release 12.0(1)* .

Configuration and Administration

Configuration and Administration

- **ORM and WSM process merge:** The ORM and the WSM processes are merged and are now running under WSM process.

Call Studio Licensing

With this release, Call Studio installation does not need a license.

Updated Features

Enhancements

Security

- **Secure Communication with PG:** CVP now supports secured encrypted communication between CVP and VRU PG which encrypts communication of GED 125 protocol.
- **Support for 2048-bit encryption:** CVP now supports 2048-bit encryption.
- **Security Fixes:** Various components upgraded for enhanced security and vulnerability fixes.

Upgrades

- **Java Script Engine:** Java Script engine used in VXML Server upgraded from Rhino to Nashorn.
- **Java Upgrade:** CVP components upgraded to use Java 1.8 from Java 1.7.
- **Tomcat Upgrade:** CVP components upgraded to use Tomcat 9 from Tomcat 8.

SIP Server Group Enhancements

Error response 503 from Call Manager does not result in Call Manager being put in the unreachable list. To achieve this, the unreachable list is optimized.

Others

- This release introduces support for SIP Session timer.
- This release fixes various Statistics parameters to provide more accurate reporting of these Statistics.

Important Notes

None.

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.

Deprecated Feature	Announced in Release	Replacement	Notes
Internet Explorer 11	Not applicable[2]	Edge Chromium (Microsoft Edge v79 and later)	None

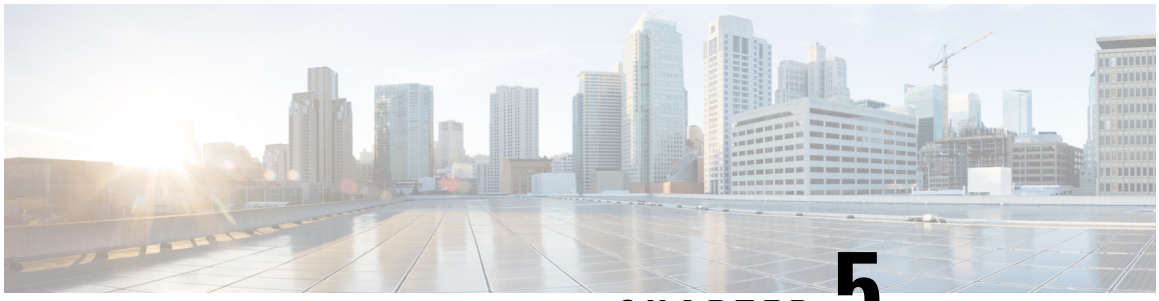
[2] Based on external communication from Microsoft

Removed and Unsupported Features

- TLS 1.0 and TLS 1.1 are not supported in this release. However, these versions have not yet been removed completely in order to prevent backward compatibility breakage.

Third-Party Software Impacts

None.



CHAPTER 5

Cisco Virtualized Voice Browser

New Features

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge). For information about supported versions, see 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.

Bridge Transfer

In earlier releases, Cisco VVB supported blind transfer as a way for VXML applications to transfer an IVR session to a required SIP endpoint. With this release, Cisco VVB adds bridge transfer capabilities to VXML applications. The bridge transfer implementation allows VVB to transfer an IVR session to a SIP endpoint (CUCM, agent, or third-party IVR) while maintaining control of the media path.

Bridge transfer in the connecting or connected state can be terminated by injecting single DTMF digit, as specified in the Call Studio bridge transfer term character. It is recommended that customers do not set term char if bridging to another IVR. The incoming and destination dial peer (or DN) cannot be of the same pattern as it applies to route hunt configured on CUCM.

Note

- Bridge transfer is supported only with G711 u-law and G711 A-law.
- Bridge transfer supports only SIP URI.
- Bridge transfer does not support TLS/SRTP.

Multilingual Support for ASR-TTS

In earlier releases, you could use the VVB integration with ASR-TTS servers only in the *US English* language context. Starting Release 12.0, you can use all locales supported by the integrated ASR-TTS servers with the appropriate locale and encoding settings in Unified Call Studio scripts.

Note

- Support for locales format: ISO639 and ISO639-2
- Support for encoding: ISO-8559-1 and UTF-8. UTF-8 is supported only with MRCPv2.

Support for Record Utterance

Cisco VVB now supports speech recognition and customers can now record the utterance of their speech operations.

Caching

With this release:

- The caching algorithm is optimized to provide faster access to the cached entries.
- HTTP Max-Age attribute is supported for caching.

Updated Features

Enhancements

- For Packaged CCE deployment model, customers can now use the Unified CCE Administration user interface instead of VVB AppAdmin for configuration and administration.
- **NLU Support using Nuance:** Cisco VVB is now compatible with Nuance NR11 that enables the AI IVR-based application based on Speech Recognition/NLU.
- **Support for 2048-bit encryption:** Cisco VVB now supports 2048-bit encryption.
- **Enhanced Security:** Cisco VVB now supports QoS for SIP and RTP.
- REST APIs for configuration and administration:
  - **System Parameter Configuration API:** Cisco VVB now supports configuring the system parameters for TLS/SRTP/ciphers using REST API.
  - **Media Parameter Configuration API:** Cisco VVB now supports configuring the media parameters for codec, MRCP version, overriding system prompts using REST API.
- Enhanced event handling.
- UUI/AAI handling in transfer scenarios.

- FetchAudio attribute for audio now supports *loop* and *starttime* attributes.
- Improvements in VXML 2.0/2.1 compliance.
- Support for transcription grammar.

Important Notes

None.

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.

Deprecated Feature	Announced in Release	Replacement	Notes
Internet Explorer 11	Not applicable[3]	Edge Chromium (Microsoft Edge v79 and later)	None.

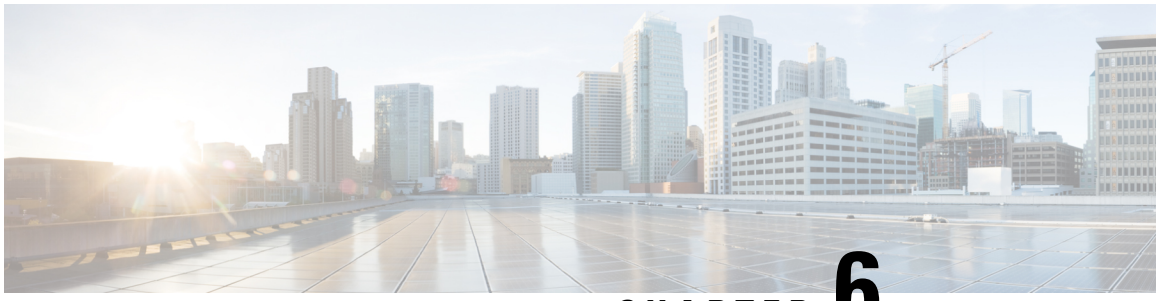
[3] Based on external communication from Microsoft

Removed and Unsupported Features

None.

Third-Party Software Impacts

None.



CHAPTER 6

Cisco Finesse

New Features

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge). For information about supported versions, see 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.

User Experience Changes in Cisco Finesse

Cisco Finesse has undergone a user experience refresh in this release. The Agent and Supervisor desktop layouts have a new look and feel with the following functionalities:

- **Signing in to Cisco Finesse Desktop (SSO mode, Non SSO mode, Hybrid Mode, and Mobile Agent)**

  The login screen for Cisco Agent and Supervisor has a new look and feel. When signing in to Cisco Finesse desktop, choose the language from the drop-down option of the Language Selector screen (the language selector screen does not appear unless a language pack is installed).

  If you do not choose the language, English is the default language.

- **Certificate Acceptance**

  To accommodate browser behavior, the accepting certificates from the SSL certificates popup is changed from opening all certificates in different tabs to certificates appearing as links. Click each link to open and accept the certificate in a new browser tab and the accepted certificates are removed from the SSL certificate popup.

- **User Options Icon**

The User Option in the Finesse header has the Agent details like name, ID, Extension, option to Sign Out with reason codes, and Mobile Agent details. The Send Error report lets you send the desktop logs to your administrator in case of any technical issues.

- **Customized Logo and Product Name**

  The logo and product name appearing on Finesse desktop can be customized by the Administrator in the Manage Desktop Layout.

- **Customized Left Navigation Bar**

  You can customize the left navigation bar by adding icons that indicate the gadgets hosted within them. To understand how to customize the icons, see the *Icons for Custom Cisco Finesse Gadgets* section in *Cisco Finesse Administration Guide*.

  The Navigation bar can be pinned or automatically collapsed to increase or decrease the Finesse desktop area.

- **Desktop Notifications**

  - For incoming voice calls: Popover with configured customer details appear with the Answer button. These customer details (call variables) can be configured via the Finesse Desktop Layout in the Admin console.
  - For campaign initiated outbound calls: Popover with configured customer details appear with the Accept or Decline buttons.
  - For Digital Channels: Popover with configured customer details appear with options to accept or reject the request depending on the gadget behavior.

  When the Finesse desktop window or tab is inactive, you receive toaster notifications for any Voice or Digital Channel requests.

- **Answering an Incoming Call**

  When a call arrives at the Cisco Finesse desktop, a popover notification displays with the following:

  - Options to answer the call.
  - Call context.

- **Making a Call**

  To make a call from the dialpad, either enter the number or use the one-click option in the phone book.

- **Digital Channels**

  The new user experience has the agent state control for Digital Channels added next to the agent Voice state. Agents cannot sign out of Finesse if they are in the Ready state.

- **Accessibility**

  Accessibility is added for the following features:

  - Digital Channels
  - Queue Statistics
  - Agent State Control
  - Team Message

- Desktop Chat

- **Sign Out or Reload**

  When you sign out or reload the Finesse desktop, a confirmation message is prompted to confirm your action.

- **Visual Design Guide**

  The Visual Design Guide provides guidelines to customize the visual experience of the Agent and Supervisor desktop. For information on customizing the visual experience, see https://developer.cisco.com/docs/finesse/#!visual-design-guide.

Desktop Chat

Desktop Chat is an XMPP browser based chat, which is powered by Cisco Instant Messaging and Presence (IM&P) service. Desktop Chat allows agents and supervisors to chat with each other and Subject Matter Experts in the organization.

The Desktop Chat interface is hosted by the Finesse Agent desktop and requires a separate login to the IM&P service. A separate login is required even in SSO deployment.

Desktop Chat's server settings and attachment support can be configured by the administrator.

Team Message

The Team Message feature allows the supervisors to broadcast messages to their respective teams. The messages appear as a banner across the Finesse desktop and the respective agents can view these messages and take necessary action.

Active Call Details

In the Team Performance gadget, the Supervisor can view the active call details of an agent. The active call details shows:

- The call variable header and the call variables configured by the administrator.
- Active Participants
- Held Participants
- Duration
- Call Status
- Queue Name

Search Reason Codes

Administrators can search and select reason code to add or edit them. For more accurate results, Administrators can search by the entering the values of Reason Label, Reason Code, or keywords from Reason Label Name and Reason Code.

Searching with keywords from Reason Label Name and Reason Code is supported only for Not Ready and Sign Out reason codes.

Workflow for Digital Channels

Workflows and Workflow actions can be created for voice and digital channels.

Configure Wrap-Up Timer

Depending on the configuration done by the administrator, the wrap-up timer can either countdown or count up the time.

ShowWrapUpTimer property can be used to show or hide the timer in the wrap-up state.

List of CLIs

You can perform the following functions using CLIs:

Sign out from Digital Channels

- Configure the media channels.
- List all the choices of media channels.
- Display the type of media channels.

View and Update all Configurable Properties

- View any Finesse IPPA, Desktop, and Web Services property's value.
- Update any Finesse IPPA, Desktop, and Web Services property's value.

CORS Support for Cisco Finesse APIs

CORS support to third-party web server is disabled by default for Cisco Finesse and OpenFire. CORS support can be enabled for specific origins and the allowed origin list can be configured by the Administrator using CLIs.

CTI Server Settings

Finesse support Secure CTI connection. In the Admin Console, secure configuration is enabled in CTI Server settings with an SSL encryption checkbox.

Note This functionality is supported only from Unified CCE 12.0 onwards.

CTI connection for the given configuration can be tested with the **Test Connection** button.

Gadget Source Whitelisting

To prevent SSRF, the Administrator can choose to allow outgoing connections for specified sources to be used in the gadgets, by adding URLs to the whitelist using CLIs.

Microsoft Edge Support for Cisco Finesse

For the Agent and Supervisor desktop and the Admin Console, Cisco Finesse supports Microsoft Edge.

JavaScript APIs

JavaScript APIs are provided to add third-party digital channel integrations to the Finesse Desktop. The JavaScript APIs added in this release are Digital Channel APIs, Popover API, and Workflow for Digital Channels APIs. For more information on these APIs see https://developer.cisco.com/docs/finesse/#!javascript-library.

Updated Features

User Experience Enhancements

The following features have been enhanced for this release:

- **Apply Wrap-Up Reason Using Search Option**
  - You can either apply Wrap-Up Reason by selecting from the drop-down list or use the search field provided in the Wrap-Up popup.
  - The reverse wrap-up timer is displayed.
- **State Control for Voice and Digital Channels**

  The look of the state control is enhanced. You can change the state for voice and all other digital channels.
- **Actions Tab**

  In the Team Performance gadget, the functionalities to Monitor an agent, Change the agent state to Ready or Not Ready, and Sign Out the agent are moved to the Actions Tab

Time in State

Beginning with this release, the *Time in State* field in the team performance gadget also displays the total duration since the agent has logged out, in addition to duration of other agent states.

Updates to Default Layout XML

The following attributes are added in the Default Layout XML:

- `managedBy` is added in the Live Data gadget.

- `maxRow` to adjust the height of the team performance gadget.
- `hidden` added to support headless gadgets.

The following attributes are added in the Default Layout XML and can be customized:

- Horizontal Header.
- Title and Logo.
- Icons in the left navigation bar.

Call Variables Layout

In the call layout popover configuration, the admin can configure the call header and upto five call variables in the Call Variable popover layout configuration. These variables are displayed in the agent's call popover and active call details in the Team Performance gadget.

Cisco Finesse Administration Console

The look and feel of the admin console is enhanced as part of user interface refresh.

Changes in REST APIs

The following changes are made to the payloads in the Cisco Finesse REST APIs.

The REST APIs available in 12.0(1) are backward compatible with previous versions.

- **User API**: The `stateChangeTime` payload indicates the time at which the state of the user is changed to the current state.
- **Queue API**: The `agentsBusyOther` and `agentsLoggedOn` payloads indicates the number of agents busy with calls and the number of agents currently logged into the system.
- **Media Properties Layout API**: The `showInPopOver` payload indicates the call variables to be displayed in the call popover based on the set value.
- **Media API**: The `media` payload indicates the media of the workflow.
- **User API**: The user API has been enhanced to support getting the user object with the user name to enable userName to peripheralID translation.

The following new REST APIs are included in Cisco Finesse:

- **ChatConfig APIs**: used to configure the Desktop Chat server settings.
- **TeamMessage APIs**: used to configure Team Message settings.
- **MediaDomain API**: used to get a list of all Media Domain objects configured on Unified CCE.

Important Notes

- Before you upgrade Cisco Finesse to Release 12.0(1) in a Unified CCE solution, install CUIC Release 11.6(1) ES11 to ensure that reporting gadgets continue to work on the Finesse desktop after the upgrade.
- Websockets is now the default notification channel used by Finesse. The port used (7443/7071) is the same for websocket communication. Support for 1500 agents in queue statistics is only available with websockets. They provide better notification throughput and reduce the notification latencies.
- An upgrade scenario will modify the layout where state and call history gadgets are configured. The tab layout and its navigation has been altered within the desktop.
- Layout is upgraded to insert the new headers and replace the default gadgets with new ones.
- Finesse CTI failover times are enhanced and the performance gains is only available with Unified CCE, Release 11.6(1), and later.
- Finesse notification service is upgraded from OpenFire 4.0.3 to 4.3.2.
- Microsoft Edge can consume considerably higher memory for the same when compared to Chrome or Firefox. Hence, users with Microsoft Edge should use a system with a minimum configuration of 8 GB RAM.

Desktop Chat Support

The Desktop Chat feature is supported only on Cisco Unified Communications Manager (CUCM), Release 12.5 and Cisco Instant Messaging and Presence (Cisco IM&P), Release 12.5.

Note This feature will not be supported until CUCM, Release 12.5, and Cisco IM&P, Release 12.5, are available.

Desktop Chat connects to Cisco IM&P servers over port 5280 from the browser that hosts the Finesse Agent desktop. Thus, ensure that the IM&P server is visible and the port is accessible, to use the Desktop Chat feature.

Deprecated Features

Internet Explorer 11

In this release, Internet Explorer version 11 is deprecated. Edge Chromium (Microsoft Edge v79 and later) is the replacement.

Removed and Unsupported Features

Inbuilt Gadgets

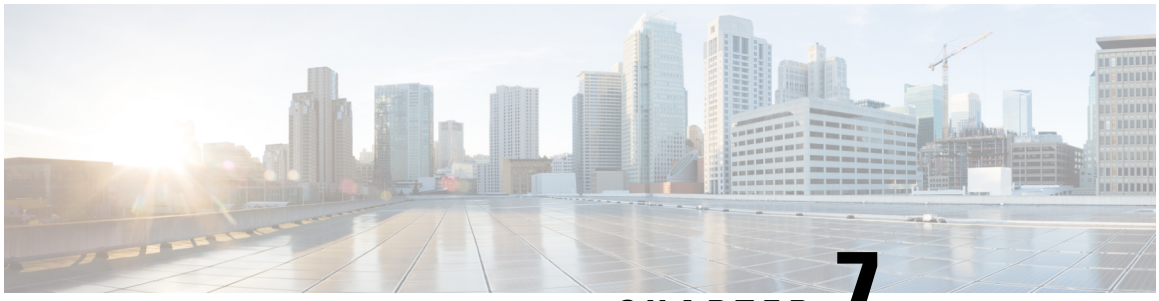
After the upgrade, the Cisco-provided gadgets such as **CallControl**, **TeamPerformance**, and **QueueStatistics** which were **JSP** gadgests change to **JavaScript** components. The path and file names of the gadgets also

change. For more information, see the **Perform Upgrade** section in the Cisco Finesse Installation and Upgrade Guide.

Third Party Software Impacts

Third-party gadgets may have a different look and feel and are encouraged to update their look and feel, to provide a seamless user experience to agents and supervisors.

To address security issues, the supported SSL Ciphers have been restricted or enhanced.



CHAPTER 7

Cisco Unified Intelligence Center

New Features

Edge Chromium Browser Support

This release supports Edge Chromium (Microsoft Edge). For information about supported versions, see 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.

Updated Features

Reports

The report creation now uses tab based wizard. The **Manage Filters** tab is now termed as **Set Default Filter** and is accessible from the ellipsis action menu for each report.

Value List and Collections Config Limits

In this release, the maximum number of Values and Collections per Value List has been increased:

- Maximum number of Values Per Value List = 72000
- Maximum number of Collections Per Value List = 7200

Improved Terminologies

In this release, the following terms are updated:

Previous Terminology	Usage	Updated Terminology
Execute	Permissions	View
Write	Permissions	Edit
Security	Navigation	Configure
Don't show filter while executing a report	Reports-Choose Filters	Skip filter during the report execution
Manage Filters	Filter Dialog box	Set Default Filter
Share	Entity ellipsis Actions	Permissions

Entity Ellipsis Actions - Permissions

In this release, the Share action has been replaced with the Permissions action in the ellipsis actions menu for each of the entity.

Using the Permissions feature:

- Security Administrators can now grant **View** and **Edit** permissions for the entity to various groups.
- Security Administrators can now grant **View** and **Edit** permissions for the entity to various users.
- Entity owners can grant **View** and **Edit** permissions for the entity to groups that they are directly associated with.

Synchronize Cluster

In this release, the Synchronize Cluster link is available below the username on the top-right corner of your user interface screen.

For more information, see *Unified Intelligence Center Cache* section in the *Cisco Unified Intelligence Center Administration Guide* at

https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

Recent Call History Gadget Icons

In this release, the **Call** and the **Edit** icons (**Actions** column) are not disabled for an unknown number on the Recent Call History gadget in Cisco Finesse.

Deprecated Features

Internet Explorer 11

In this release, Internet Explorer version 11 is deprecated. Edge Chromium (Microsoft Edge v79 and later) is the replacement.

Removed and Unsupported Features

Entity Ellipsis Actions - Share

In this release, the **Share** action that helped you in granting **View** and **Edit** permissions for the entities within their group (default group) has been removed.

Permissions, Default Group, and My Group

In this release, the following default group-related features have been removed.

- The **Default Group** selection in the **Groups** tab during the User Group creation process.
- The **Permissions** selection for the **My Group (AllUsers)** and **All Users** in the **General Information** tab during the User creation process.
- The **My Group** selection in the **Groups** tab during the User creation process.

Report Filter Fields in a Grid or a Chart View

This release does not support the display of filter fields in a grid or a chart view. **Report Definition** > **Fields** > **Filter Fields** are used exclusively for setting filter criteria when running reports. Any report view that is created in the previous releases with Filter Fields may fetch wrong results upon upgrading to 12.0 (when the reports are run). Hence, remove the Filter Fields from those views before you run the report.

User Roles - Login User

The **Login User** check box has been removed from the **User Roles** page. The Login User role that is used to sign in to Unified Intelligence Center is now integrated within the system.

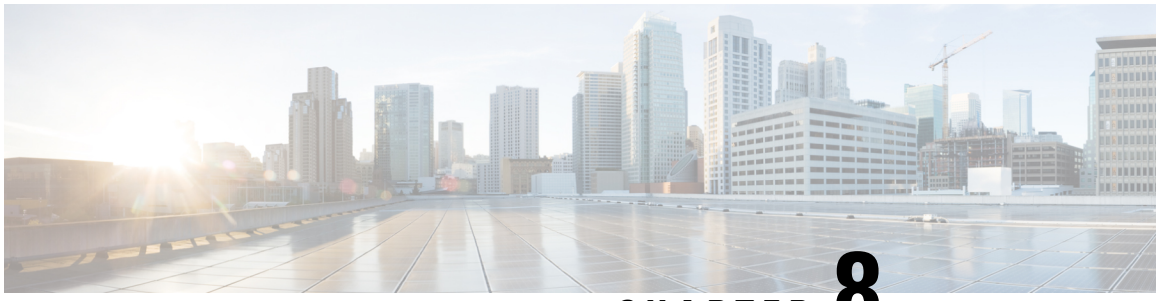
To activate or inactivate a Login User, the administrator can now use the toggle button on the **Configure** > **Users** > **Edit User** > **User Information** tab.

Import and Export Report Definition

This release does not support importing and exporting Report Definition as a separate entity. The corresponding Report Definitions are imported or exported while importing or exporting the reports respectively.

Third Party Software Impacts

None



CHAPTER 8

Cisco Unified Contact Center Domain Manager

New Features

Support for 24000 Agent Deployment Types

This release expands capacity limits and now supports deployments with as many as 24,000 users and up to 48,000 skill groups.

Updated Features

Support for Non-SSO Default Domain for Supervisors

This release adds default domain provisioning for Unified CCE Non-SSO supervisor users. If a default domain is set, a supervisor account can be created or updated without a domain name in the login field. The default domain is appended to the user without changing the user's login name. The system then validates the user's login name against the Global Catalog (GC) that was configured for that UCCE cluster. Once configured, the supervisor can sign into the application without having to provide an email ID or domain in their login.

ECC Payload Provisioning

This release adds support for ECC Payloads. Expanded call context (ECC) variables store values associated with a contact, which are normally determined and recorded during a call. With ECC payloads, a system integrated with Unified CCE can more easily and efficiently send ECC variables over any specific communication path by placing the variables in an ECC payload. An ECC payload can be up to 2000 bytes in size. ECC Payload provisioning is only available via the Resource Manager Gadget.

Deprecated Features

Legacy Resource Manager

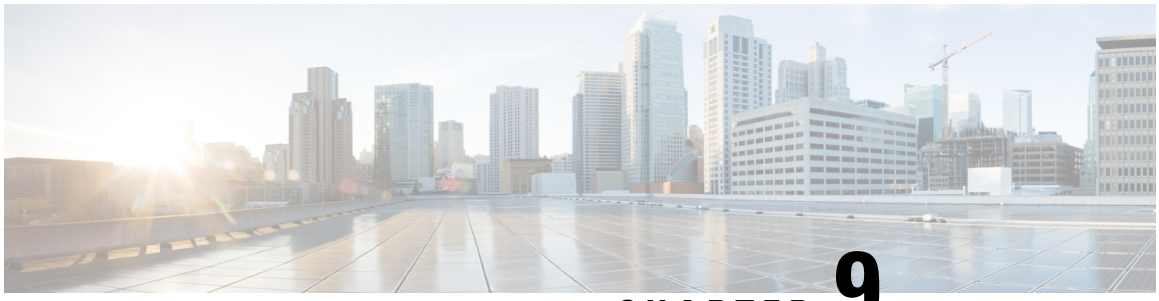
This is the last release for the Legacy Resource manager and there will be no enhancements for it in future releases. All tasks previously performed in the Legacy Resource Manager should now be performed in the current Resource Manager Gadget interface.

Removed and Unsupported Features

There are no removed and unsupported features for this release.

Third-Party Software Impacts

There are no third-party software impacts for this release.



CHAPTER 9

Cisco SocialMiner

The standalone SocialMiner features such as Facebook page, Twitter, RSS Feeds, Standalone single session chat, associated features like filters and notifications have been removed from release 12.0. However, you can still use SocialMiner interface to encrypt MR.

New Features

None.

Updated Features

None.

Important Notes

None.

Deprecated Features

None.

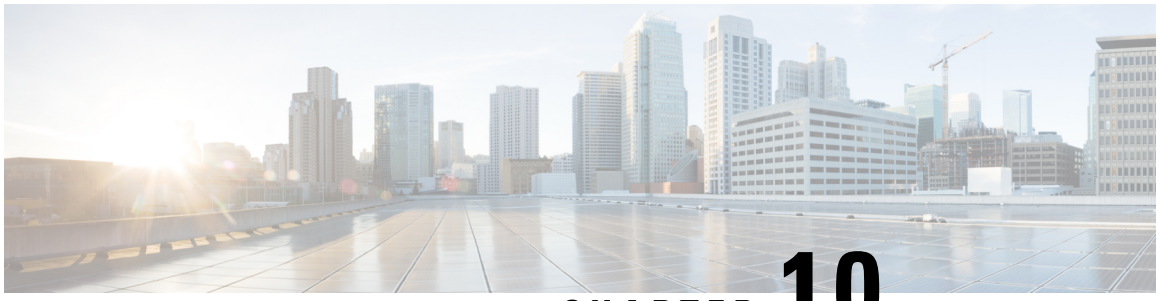
Removed and Unsupported Features

The support for monitoring of Facebook fan pages, Twitter, and RSS feeds from SocialMiner for all Customer Journey Solutions customers is removed in Cisco SocialMiner 11.6(2) and later. This is applicable ONLY to the social media feed integration to SocialMiner. The field notice in this regard is available at, https://www.cisco.com/c/en/us/support/docs/field-notices/702/fn70274.html.

The standalone SocialMiner features such as Facebook page, Twitter, RSS Feeds, Standalone single session chat, associated features like filters and notifications have been removed from release 12.0.

Third Party Software Impacts

None.



CHAPTER 10

Caveats

Caveat Queries by Product

Bug Search Tool

If you have an account with Cisco.com, you can use the Bug Search tool to find caveats of any severity for any release. Access the Bug Search tool at https://bst.cloudapps.cisco.com/bugsearch/. Enter the bug identifier in the search box, and press return or click **Search**.

To access a list of open caveats and resolved caveats (rather than an individual caveat) for a particular product or component, see the relevant sections later in these notes.

You can also choose your own filters and criteria in the tool to see a specific subset of caveats, as described in the following table.

If you choose this in Releases	And you choose this in Status	A list of the following caveats appears
Affecting or Fixed in these Releases OR Affecting these Releases	Open	Any caveat in an open state for the release or releases you select.
Fixed in these Releases	Fixed	Any caveat in any release with the fix applied to the specific release or releases you select.
Affecting or Fixed in these Releases	Fixed	Any caveat that is either fixed or occurs in the specific release or releases you select.
Affecting these Releases	Fixed	Any caveat that occurs in the release or releases you select.

Severity 3 or Higher Caveats for Release 12.0(1)

Use the following links to the Bug Search Tool to view a list of Severity 3 or higher caveats for each product or component for the current release. You can filter the result by setting the filter values in the tool.

Note If the list of caveats does not automatically appear when you open the browser, refresh the browser.

Cisco Hosted Collaboration Solution for Contact Center

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284526699&rls=12.5(1)&sb=anfr&svr=3nH&bt=custV

Cisco Unified Intelligence Center

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282163829&rls=12.0(1)&sb=anfr&bt=custV

Cisco Unified Customer Voice Portal

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=270563413&rls=12.0(1)&sb=anfr&svr=3nH&bt=custV

Cisco Finesse

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613135&rls=12.0(1)&sb=anfr&bt=custV

Cisco SocialMiner

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283613136&rls=12.0(1)&sb=anfr&bt=custV

Cisco Enterprise Chat and Email

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282163829&rls=12.0(1)&sb=anfr&bt=custV