



Release Notes for Cisco Unified Contact Center Express Solution, Release 12.0(1)

First Published: 2019-01-11

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2000–2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Introduction 1

- Release Notes for Contact Center Solutions 1
- Cisco Security Advisories 1

CHAPTER 2

Cisco Unified Contact Center Express 3

- New Features 3
 - Advanced Supervisor Capabilities 3
 - New Historical Report 4
 - Bubble Chat Calendar 4
 - Migration to CentOS Based Voice Operating System 4
 - SHA-256 Support for Single Sign-On 4
 - SHA-256 Support for Cisco Identity Service 4
- Updated Features 4
 - Reporting Enhancements 4
- Deprecated Features 5
- Important Notes 5
- Removed and Unsupported Features 6
- Third Party Software Impacts 11

CHAPTER 3

Cisco Unified Intelligence Center 13

- New Features 13
 - User Experience Changes 13
 - Clone Report Definition 14
 - Set Commands 14
 - Show Commands 14
 - Stock Report - User's Audit Log 14

- Updated Features 15
- Important Notes 16
- Deprecated Features 16
- Removed and Unsupported Features 17
- Third Party Software Impacts 17

CHAPTER 4

Cisco Finesse 19

- New Features 19
 - User Experience Changes in Cisco Finesse 19
 - Desktop Chat 21
 - Team Message 21
 - Active Call Details 21
 - Search Reason Codes 21
 - Workflow for Digital Channels 21
 - Configure Wrap-Up Timer 22
 - Force Wrap-Up Reason 22
 - Multiple Wrap-Up Reasons 22
 - CORS Support for Cisco Finesse APIs 22
 - Gadget Source Whitelisting 22
 - JavaScript APIs 22
- Updated Features 22
 - User Experience Enhancements 22
 - Time in State 23
 - Updates to Default Layout XML 23
 - Call Variables Layout 23
 - Cisco Finesse Administration Console 23
 - Changes in REST APIs 23
- Important Notes 24
- Deprecated Features 24
- Removed and Unsupported Features 25
- Third Party Software Impacts 25

CHAPTER 5

Cisco SocialMiner 27

- New Features 27

Updated Features	27
Important Notes	27
Deprecated Features	27
Removed and Unsupported Features	28
Third Party Software Impacts	28

CHAPTER 6**Caveats 29**

Caveat Queries by Product	29
Bug Search Tool	29
Severity 3 or Higher Caveats for Release 12.5(1)	30



CHAPTER 1

Introduction

- [Release Notes for Contact Center Solutions](#), on page 1
- [Cisco Security Advisories](#), on page 1

Release Notes for Contact Center Solutions

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 Unified Contact Center Express

- [New Features, on page 3](#)
- [Updated Features, on page 4](#)
- [Deprecated Features, on page 5](#)
- [Important Notes, on page 5](#)
- [Removed and Unsupported Features, on page 6](#)
- [Third Party Software Impacts, on page 11](#)

New Features

Calendar Management- Administrators can create calendars, configure business hours, special days, and holidays. Administrators can associate calendars with chat widget by using **Chat Widget Configuration**. Administrators can assign the calendars to supervisors so that supervisors can manage the calendars. Administrators and supervisors (who have access to **Application Management**) can associate calendars with applications by using Application Management.

Calendar Step- The calendars that are created in Unified CCX can be included in a script by using the Calendar Step in the Unified CCX Editor.

Advanced Supervisor Capabilities

The following advanced capabilities are available for a supervisor:

- **Queue Management**

A supervisor can manage resources across the assigned CSQs and teams by using the Queue Management feature.

- **Application Management**

A supervisor can manage the prompts, if any configured, in the Unified CCX IVR script based applications that are assigned by the administrator. Supervisors can also associate calendars with applications.

- **Calendar Management**

A supervisor can manage the business hours, holidays, and off hours in the calendars that are assigned by the administrator.

- **Outbound Campaign Management**

A supervisor can manage the outbound campaigns that are assigned by the administrator.

New Historical Report

A new multichannel historical report has been added. The following report presents the details of the CSQs and agents skills that were modified.

- Queue Management Audit Trail Report

Bubble Chat Calendar

The Service Hours can be configured while configuring the Bubble Chat Widget by selecting an available Calendar.

Migration to CentOS Based Voice Operating System

Unified CCX and its components are migrated to CentOS based Voice Operating System (VOS).

SHA-256 Support for Single Sign-On

Secure Hash Algorithm 2 (SHA-256) is now supported as the signing algorithm for Security Assertion Markup Language (SAML) based user authentication.

SHA-256 Support for Cisco Identity Service

The Security Assertion Markup Language (SAML) 2.0 request can be signed using SHA-1 or SHA-256 as per the value configured in the system.

Updated Features

Reporting Enhancements

The following reports were enhanced in this release:

- Chat Agent Detail Report
- Chat Agent Summary Report
- Chat CSQ Activity Report
- Chat Traffic Analysis Report
- Email Agent Activity Report
- Email Contact Detail Report
- Agent Not Ready Reason Code Summary Report

- Agent Wrap-up Data Summary Report
- Agent Wrap-up Data Detail Report
- Chat CSQ Summary Report

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.

Internet Explorer 11

Support for Internet Explorer version 11 is deprecated.

Mobile Skill Manager

This has been deprecated from Release 12.0(1) onward.

Cisco Context Service

Cisco Context Service has been deprecated from Release 12.0(1) onward.

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 **Customer Journey Platform**, **Unified CCX**, **Unified CCE**, and **HCS-CC**. Please refer to 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.

Important Notes

- The VMware tools get outdated when the applications are on ESXi 6.5. To manually upgrade the VMware Tools, open the **Virtual Machine Properties** window of the application. On the **Options** tab, select **VMware Tools** settings and manually check **Check and upgrade Tools during power cycling**.
- When agents reply to emails, the email responses are always in HTML format irrespective of the format of the emails received.
- The Unified CCX 12.0 license file represents the version as 11.7 instead of 12.0. However, you cannot use this license file with Unified CCX 11.6 or earlier systems.
- Please ensure that you download and install the latest software provided by Cisco in the Contact Center application. This will ensure that all the latest updates are applied to the software applications. For Unified

CCX Compatibility Information see, <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html>.

For latest software download see, <https://software.cisco.com/download/home>.

- Customers who are deploying Unified CCX 12.0 should create a Smart Account. Please visit the following URLs for accessing the materials to enable Smart Account overview and creation:

<https://www.cisco.com/go/smartaccounts>

Smart Accounts FAQ for Partners, Distributors and Customers - <https://communities.cisco.com/docs/DOC-64078>

Removed and Unsupported Features

Removed Features

- Classic Chat feature has been removed in this release. The configuration of the Classic Chat in the previous release will not be migrated during an upgrade to this release. Customers must configure the Bubble Chat widget available in the Cisco Unified CCX Administration.
- The link to the Troubleshooting Tips from the Cisco Unified CCX Administration web page from the **Help** menu has been removed from this release.

Chat Transcript Download in a PDF Format

The chat transcript cannot be downloaded in a PDF format from the Unified CCX Release 11.6(2) onward.

TLS

TLS 1.0 and 1.1 are not supported.

Unsupported Options on Finesse for Direct Preview Outbound

Finesse does not support Skip, Skip-Next, Skip-Close, Reject, Cancel Reservation, and Do Not Call for direct preview outbound calls.

Unsupported Features and Configurations for Progressive and Predictive Agent Outbound

Unsupported Features and Configurations for Progressive and Predictive Agent Outbound

- The “Get Reporting Statistic” step is not supported for progressive and predictive agent-based outbound campaigns.
- Unified CCX does not support the translation or modification of the phone number that it uses to dial outbound calls. If any “voice translation rules” that are configured in the gateway modify the phone number, those rules are not supported.



Note You can use either of the following two supported methods to modify a dialed number in the gateway:

- To remove the initial digits of the phone number, use **forward-digits** or **digit-strip** in the dial-peer configuration.
- To add a prefix to the phone number, use **prefix** in the dial-peer configuration.

-
- For Outbound campaigns outside North America, additional configuration is required to add the area-code-to-time-zone mapping. For more information, see the *Cisco Unified Contact Center Express Administration and Operations Guide*, located at https://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html.
 - For multi-country Outbound campaigns, the area code must also include the country code.
 - Unified CCX dialer will dial outbound contacts only if the publisher database is in the “IN SERVICE” state.
 - Finesse does not support the Do Not Call option.
 - Outbound license usage is not captured in the License Utilization Cisco Unified Intelligence Center report.
 - You must enable Agent AutoAnswer manually for agent-based progressive and predictive calls when you upgrade from an older Unified CCX release.

Unsupported Configuration for IPv6

- Cisco Unified Communications Manager does not support SIP IPv6 signaling over UDP where the maximum transmission unit (MTU) is greater than 1500. To ensure that you do not experience intermittent call failure, change the transport protocol to TCP.

For more information, see the “Important Notes” section of the *Release Notes for Cisco Unified Communications Manager*, located at:

<https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html>

Also, see “CSCuo71306” for details on this limitation.

- When using IPv6 and Outbound dialer, use a voice gateway IOS that contains the fix for “CSCu143754”.

Unsupported Configurations and Scenarios for Unified CCX

Unified CCX does not support the following configurations:

- CTI route points with directory numbers (DNs) that are members of line groups and, by extension, that are members of hunt lists of Unified CM.
- Shared lines for CTI ports and CTI route points.
- Agent devices cannot be shared with any other Directory Number, irrespective of the configured partition. (the Agent device and Directory Number must have 1:1 relationship).

- ICD call answer or ICD call transfer using any third-party attendant console desk software.
- Within the same script, using the “Place Call” step to generate a call and then placing the call, back into the same queue (creating a call loop).
- SIP REFER between a switchboard and Unified CCX if the transfer is completed after the call is answered on the Unified CCX CTI port because of media reestablishment issues.
- During TTS prompt playback, if the call is put on hold and then retrieved, the prompt does not continue from the position at which it was left.
- Use of “Consult Transfer”, “Direct Transfer”, or “Redirect” to a translation pattern that maps back to a route point.
- Use of “Consult Transfer”, “Redirect”, and “Place Call” steps to invoke or dial into "Conference Now" conferences.
- The following scenarios have issues:
 - External -> Redirect to Unmonitored device -> Call Forward No Answer (CFNA) to UCCX RP
Use of Redirect Step to an unmonitored device which then uses CFNA to a UCCX route point.
 - External -> Consult Transfer to RP -> Consult Transfer to RP -> Redirect to Unmonitored device
 - External -> Redirect to RP -> Consult Transfer to RP -> Redirect to Unmonitored device
 - External -> Consult Transfer to RP -> Redirect to RP -> Redirect to Unmonitored device
 - External -> Consult Transfer to RP -> Redirect to Unmonitored device
Thus, use the Call Redirect Step in the script instead of Call Consult Transfer.
- Unified CCX doesn't completely support E.164 numbering plan for route point directory numbers (DN).
This limitation is because of the Unified CM limit on device name length set as 15 characters. We add "_" between the device name prefix and the DN. So we support a maximum of 13 characters in the DN as device name prefix is mandatory and hence at least one character is needed there. For example, (Device name prefix) + '_' + (length of DN) = 15 ==> [(1 + '_' + 13) = 15].
- Cisco Unified CCX system does not support modification, addition or deletion of the CTI ports and the CTI Route Points from the Cisco Unified Communication Manager. Performing the same can lead to issues with non-contiguous DN range for which Cisco Tomcat on Unified CCX Server needs to be restarted.
- When the supervisor monitors the Team Performance report and during the time if there is any update or modification done to the team, this doesn't get updated automatically. The supervisor should refresh the browser page or select the respective team again to view the Team Performance report.
- Use of two(2) wildcard CTI Route Points that overlap with each other is not supported. For example, Route Point 1: 123XXXX and Route Point 2: 1234XXX overlap with one another and is not supported.
However, a wildcard CTI Route point can overlap with a full DID (best match pattern) that doesn't contain a wildcard. For example, Route Point 1: 123XXXX and Route Point 2: 1234567 is supported.
- A discrepancy in reports is observed when a call is transferred using Cisco Jabber by multiple agents in the same call flow. Use the Cisco Finesse desktop to transfer calls.
- SIP URI dialing for CTI route points, CTI ports, and agent extensions.

- SIP URI dialing for CTI route points, CTI ports, and agent extensions.
- Mid Call Caller ID updates when call is routed to Unified CM via MGCP gateway.



Note When incoming calls are routed to Unified CM via MGCP gateway, any mid call caller ID updates are reflected only after the call is connected.

Unsupported Actions for Unified CCX Agents

Use of the following softkeys on a Cisco Unified IP Phone is not supported:

- Barge
- cBarge
- DND
- GPickup
- iDivert
- Conference Now
- Park
- Pickup

Unsupported Configurations for Agent Phones

The following configurations are not supported for agent phones:

- Two lines on an agent phone that have the same extension but exist in different partitions.
- Unified CCX extension that is assigned to multiple devices.
- Configuring the same Unified CCX extension in more than one device profile, or configuring the same Unified CCX extension in any combination of device profiles and devices. (Configuring a Unified CCX extension in a single device profile is supported.)
- Silent Monitoring by supervisors who are logged in with Extend and Connect.
- In the Unified Communications Manager Administration Directory Number Configuration web page for each Unified CCX line, setting Maximum Number of Calls to a value other than 2.
- In the Unified Communications Manager Administration Directory Number Configuration web page for each Unified CCX line, setting Busy Trigger to a value other than 1.
- No Cisco Unified Communications Manager device can be forwarded to the Unified CCX extension of an agent.
- The Unified CCX extension of an agent cannot be configured to forward to a Cisco Unified CCX Trigger or CTI route point.
- Configuring the Unified Communications Manager Intercom feature.
- Configuring the Hold Reversion feature.

- Agent extensions cannot be added to hunt lists or hunt groups. If an agent has only one line, the agent phone cannot be part of a hunt list or hunt group. In the case of multiple lines, none of the first four configured lines must be part of the hunt group. For more details on multiple lines support and number of monitored lines, see the *Cisco Unified Contact Center Express Design Guide*, located at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html>.
- Call Forward All to extensions which Unified CCX does not have control over. For example, if an agent extension has Call Forward All to a PSTN extension or Directory Number on another cluster which Unified CCX is unaware of.
- All the Cisco IP Phones for Cisco Finesse IP Phone Agent currently do not support the Simplified New Call UI.

Supported Configurations for Agent Phones

To determine the phone devices that are supported by Cisco Finesse and for use by Cisco Finesse IP Phone agents, see the Unified CCX Compatibility related information located at: <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html>.

The following configurations are supported on agent phones:

- A Unified CCX extension that is configured on a single device (but not on multiple devices).
- A Unified CCX extension that is configured in a single device profile (but not in multiple device profiles).
- Multiple agents sharing the same Unified CCX extension, which you can set up as follows:
 - Configure the Unified CCX extension to a single phone (not in a device profile).
 - Associate the phone with all the agents who will use this extension.
 - Select the appropriate directory number (DN) as the Unified CCX extension for each agent.

In this configuration, only one agent at a time can be logged in.



Note All agents who currently have the Unified CCX extension to be shared must log out before you configure additional agents to share that extension.

- Video is now supported if you are using Cisco Jabber for Windows as agent phone. The agent desktop where Jabber is used for Video should comply to the Cisco Jabber hardware requirements listed in the *Cisco Jabber for Windows 11.0.x and 11.1.x Release Notes*, located at:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/Windows/11_0/RN/JABW_BK_C5E7828C_00_cisco-jabber-windows-11-release-notes.html.

Unsupported and Supported Configurations for Remote Agents

Unified CCX supports Cisco Expressway 8.7.1 from the release 11.5(1) onward. The current version of Cisco Expressway does not support BiB and thus the contact center cannot achieve silent monitoring and recording functionalities.

Unsupported Features in Unified Communications Manager and Cisco Business Edition 6000

The following Unified Communications Manager features are not supported by Unified CCX. These features are disabled by default and you should not enable them for Unified CCX. For more information about these features, see Unified Communications Manager documentation, located at:

https://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

- Block External to External Transfer.
- DSCP IP CTIManager to Application service parameter.
You can enable this service parameter for Unified Communications Manager, but doing so does not affect Unified CCX.
- Advanced Ad Hoc Conference Enabled service parameter.
- Drop ad hoc conference when the creator leaves the conference.
- Signaling (QSIG) Path Replacement (PR).
This feature must be disabled when Unified CCX is deployed. To disable this feature, set the Unified Communications Manager service parameters Path Replacement Enabled and Path Replacement on Tromboned Calls to False.
- Forced Authorization Code and Client Matter Code.
Because these features can be enabled per route pattern, you should turn them off for all route patterns in the Unified Communications Manager cluster that Unified CCX might use. Enabling these features for route patterns that Unified CCX does not use does not affect Unified CCX.
- Multilevel precedence and preemption (MLPP).
You can enable this feature for devices in the cluster that do not interact with Unified CCX.
- Do not use Unified Communications Manager Administration to add or change CTI ports or route points that are used by Unified CCX or application users that are created by Unified CCX.

Unsupported Features in Custom Reports

- The **Do Not Call** field is no longer available in Unified CCX 11.0(1) release onward. While upgrading to Unified CCX 11.5(1), report will not be generated if the **Do Not Call** column is present in the custom report. You can generate the report by removing the **Do Not Call** column from the custom reports in Unified CCX 11.5(1).
- A Custom report that was created from a Unified CCX Stock Report may not work as expected if the report definition of the original Stock Report is modified in the new release.

Third Party Software Impacts

See the Unified CCX Compatibility related information located at:

<https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html> for information on third-party software.



CHAPTER 3

Cisco Unified Intelligence Center

- [New Features, on page 13](#)
- [Updated Features, on page 15](#)
- [Important Notes, on page 16](#)
- [Deprecated Features, on page 16](#)
- [Removed and Unsupported Features, on page 17](#)
- [Third Party Software Impacts, on page 17](#)

New Features

User Experience Changes

This release provides an improved user experience to create, edit, and manage the following entities:

- Report Definitions
 - This feature is available only in Cisco Unified Intelligence Center (CUIC) standalone system.
- Value Lists and Collections
- Schedules
- Configuration of:
 - Data Sources—Data Sources are now represented in the form of cards and can easily switch over nodes (Primary and Secondary).
 - Users and User Roles—The following User Roles are displayed on the **Users** listing page based on the user role assignments:
 - SC—System Configuration Administrator
 - SA—Security Administrator
 - RD—Report Definition Designer
 - R—Report Designer
 - VL—Value List Collection Designer
 - D—Dashboard Designer

- User Groups
- User Permissions

For more information, see *Cisco Unified Intelligence Center Report Customization Guide* and *Cisco Unified Intelligence Center User Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html>.

Clone Report Definition

This release allows you to clone a Report Definition that is associated with the report being saved during the **Save As** action. Click the **Clone Report Definition** check box if you want to create a copy of the Report Definition and its associated reports.



Note This feature is available only in Cisco Unified Intelligence Center (CUIC) standalone system.

Set Commands

The following Set Commands have been introduced in this release:

- set cuic properties http-cache <on|off>

For more information, see *Administration Console User Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html>.

Show Commands

The following Show Commands have been introduced in this release:

- show cuic properties user-audit-logging
- show cuic properties http-cache

For more information, see *Administration Console User Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html>.

Stock Report - User's Audit Log

This release provides a new stock report, User's Audit Log using which you can view the audit log data of users such as, Logged In User Detail (name and role), Event Detail, Updated Column, User Detail, and other modified details.

For more information on this report, click the "?" icon (Template Help) from the report in the run mode.

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>.

Important Notes

Variable Permalink - Encode Back Slash

After upgrading to Unified Intelligence Center 12.0, ensure to encode the character "\" in variable permalinks with "%5C".

For example:

```
https://localhost:8444/cuicui/permalink/?
```

```
viewId=2C3EA4BA10000166000000170A4E5A53&linkType=htmlType&viewType=Grid&refreshRate=3600
&userName=Domain\John
```

to

```
https://localhost:8444/cuicui/permalink/?
```

```
viewId=2C3EA4BA10000166000000170A4E5A53&linkType=htmlType&viewType=Grid&refreshRate=3600
&userName=Domain%5CJohn
```

Migration Limitations

- **Maximum Length for SFTP Password**—In this release, for schedules, the maximum length for the Remote Location (SFTP) password is set to 50 characters. Hence, after upgrade, upon editing a schedule, you may be prompted to change your password for the SFTP settings in the **Schedules > Destination Setting** tab.
- **Schedules during Upgrade**—In this release, schedules that are supposed to run during the upgrade time frame are not triggered. Hence, you need to run these schedules manually after the successful upgrade.

CUIC, Release 11.6(1) ES11

Before you upgrade Cisco Finesse to Release 12.0(1) in a CCE solution, install the CUIC, Release 11.6(1) ES11, patch to ensure that reporting gadgets continue to work on the Finesse desktop after the Cisco Finesse, Release 12.0, upgrade.

Microsoft Edge Limitations

Microsoft Edge can consume considerably higher memory for the same use cases when compared to Chrome or Firefox. Hence, users with Microsoft Edge should use a system with minimum configuration of 8 GB RAM.

Deprecated Features

None

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 4

Cisco Finesse

- [New Features](#), on page 19
- [Updated Features](#) , on page 22
- [Important Notes](#), on page 24
- [Deprecated Features](#) , on page 24
- [Removed and Unsupported Features](#), on page 25
- [Third Party Software Impacts](#), on page 25

New Features

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 and Non SSO mode)**

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. 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 Unified Contact Center Express Administration and Operations 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.

Force Wrap-Up Reason

The administrator can configure Force Wrap-Up Reason for agents.

Force Wrap-Up Reason ensures that an agent provides a wrap-up reason before ending the call.

Multiple Wrap-Up Reasons

You can apply up to five Wrap-Up reasons to a call.

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.

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.

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.

- **Dialog API:** The `wrapUpItems` and `wrapUpItem` payloads indicate the list of multiple wrap-up reason codes associated with a Dialog and the description of a call.
- **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.

Important Notes

-
- Layout is upgraded to insert the new headers and replace the default gadgets with new ones.
- 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

None

Removed and Unsupported Features

The following features are no longer available:

Feature	Effective from Release	Replacement
MediaSense	12.0(1)	None

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 5

Cisco SocialMiner

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

Access to Cisco SocialMiner Administration UI is restricted. To access the UI, the IP from which the UI will be accessed has to be Whitelisted.

- [New Features, on page 27](#)
- [Updated Features, on page 27](#)
- [Important Notes, on page 27](#)
- [Deprecated Features, on page 27](#)
- [Removed and Unsupported Features, on page 28](#)
- [Third Party Software Impacts, on page 28](#)

New Features

None.

Updated Features

None.

Important Notes

None.

Deprecated Features

None.

Removed and Unsupported Features

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.

Access to Cisco SocialMiner Administration UI is restricted. To access the UI, the IP from which the UI will be accessed has to be Whitelisted.

Third Party Software Impacts

None.



CHAPTER 6

Caveats

- [Caveat Queries by Product](#), on page 29

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 12.5(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 Unified Intelligence Center

[https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282163829&rls=12.5\(1\)&sb=anfr&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=282163829&rls=12.5(1)&sb=anfr&bt=custV)

Cisco Unified Customer Voice Portal

[https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=270563413&rls=12.5\(1\)&sb=anfr&svr=3nH&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=270563413&rls=12.5(1)&sb=anfr&svr=3nH&bt=custV)

Cisco Finesse

[https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=283613135&rls=12.5\(1\)&sb=anfr&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=283613135&rls=12.5(1)&sb=anfr&bt=custV)

Cisco SocialMiner

[https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=283613136&rls=12.5\(1\)&sb=anfr&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=283613136&rls=12.5(1)&sb=anfr&bt=custV)

Cisco Enterprise Chat and Email

[https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=280810493&rls=12.5\(1\)&sb=anfr&svr=3nH&bt=custV](https://bst.cloudapps.cisco.com/bugsearch/search?kw=&pf=prdNm&pfVal=280810493&rls=12.5(1)&sb=anfr&svr=3nH&bt=custV)