Release Notes for Cisco Unified Contact Center Express Solution, Release 11.6(1)

First Published: 2017-08-24

CONTENTS

CHAPTER 1

Introduction

Release Notes for Contact Center Solutions

Release 11.0 introduced release note compilations for each of the contact center solutions. The compilations contain all of the release notes for one solution type and the components that you can use with that contact center. 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

Addressing security issues in Cisco products is the responsibility of the Cisco Product Security Incident Response Team (PSIRT). The Cisco 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.

Customer Documentation Updates for This Release

Our Documentation Guides identify the documents that changed for this release:

- **Packaged CCE**—https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-documentation-roadmaps-list.html

- **HCS for Contact Center**—https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-documentation-roadmaps-list.html

- **Unified CCE**—https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-documentation-roadmaps-list.html

- **Unified CCX**—https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-documentation-roadmaps-list.html

Updated documents are also listed under Customer Collaboration in *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

This service lists new and revised Cisco documentation since the last release of this monthly publication.

You can also subscribe to the *What's New in Cisco Product Documentation* RSS feed to deliver updates directly to an RSS reader on your desktop. To subscribe, paste this URL into your RSS reader: http://www.cisco.com/cdc_content_elements/rss/whats_new/

CHAPTER **2**

Cisco Unified Contact Center Express

New Features

Unified CCX Qualified in Cisco Hosted Collaboration Solution (HCS)

The Cisco Hosted Collaboration Solution (HCS) enables service providers to offer managed and hosted Unified Communications (UC) and collaboration services to multiple autonomous business customers by hosting UC applications. Using this solution, service providers can manage and deploy new highly reliable and scalable collaboration services to small- or medium-sized businesses and enterprises. This capability allows a service provider to offer differentiated services.

Unified CCX 11.6(1) version onward is qualified to be used in the HCS deployment model.

Email Signature

Administrator can create, modify, delete, and view email signatures.

The email signature can be configured and tagged as Global for all CSQs or Customize for selected CSQs.

The signature is automatically appended to the email reply while being sent.

Editable To, Cc, and Bcc Fields

The agent can add and modify the To, Cc, and Bcc recipients in the email reply and forward.

Email Reply All

The agent has an option to click Reply All to send the email response to all the recipients that were initially included in the email.

Email Forward

The agent has an option to forward the email to one or more recipients including Cc and Bcc.

✎

Note All the new email fields introduced in the release 11.6(1) are included in the respective Email historical reports.

Gmail Integration

Customers can now integrate Gmail as another mail server type.

Wrap-Up Reasons for Chat and Email

Administrator can configure Wrap-Up Reasons and the agent can select upto five (5) Wrap-Up Reasons for chats and emails. The Wrap-Up statistics can be viewed in the respective historical reports.

Agent Alias with Space

Space is now supported in the Agent Alias.

Group Chat

In Group Chat, an agent can involve another agent in an ongoing chat session to support the customer.

A Group Chat enables an agent to:

- Send a chat invite to an available agent of the selected CSQ.

- Enter the summary of the ongoing chat for the other agent.

- Accept or decline, when the Group Chat is offered.

Typing Indicator

This release introduces typing indicator for both the agent and the customer with a delay of 5 seconds on each side.

Scheduler for Chat Web Form

The Administrator can configure a schedule for the chat web form based of the business days, working hours, and holidays.

Direct Transfer

In direct transfer, the agent can transfer the call without a consult leg.

Agent Not Ready State when Non-ACD Line is Busy

This feature enables the agent's state to change from Ready to Not Ready when the monitored Non-ACD lines are used for incoming or outgoing calls. This feature can be enabled from the **System Parameters**.

The agent is moved to Ready after the call on the Non-ACD line is ended.

This is not applicable if the Non ACD lines are shared lines.

Monitor Outbound Calls

The supervisor can now monitor the outbound calls.

Import of Contacts

The administrator can manually import contacts for a campaign, by setting the order of the list of contacts in a CSV file.

The administrator can now automatically import contacts for a campaign. Select one of the two options, SFTP or HTTPS based on the server type.

Historical Reports for Supervisors

The following Historical reports are now available for the Supervisor:

- Chat Agent Detail Report
- Chat Agent Summary Report
- Chat CSQ Activity Report
- Chat CSQ Agent Summary Report
- Email Agent Activity Report
- Email Contact Detail Report
- Email CSQ Activity Report
- Agent Call Summary Report
- Agent Detail Report
- Agent Summary Report
- Agent Login Logout Activity Report
- Agent Not Ready Reason Code Summary Report
- Agent State Detail Report
- Agent State Summary by Agent Report

- Agent State Summary by Interval Report

- Agent Wrap-up Data Summary Report

- Agent Wrap-up Data Detail Report

- Abandoned Call Detail Activity Report

- Common Skill CSQ Activity Report

- Contact Service Queue Activity by CSQ Report

- Contact Service Queue Activity Report

- Contact Service Queue Activity Report by Interval

- Contact Service Queue Call Distribution Summary

- Contact Service Queue Priority Summary

- Contact Service Queue Service Level Priority Summary Report

- CSQ Agent Summary Report

- Detailed Call CSQ Agent Report

- Outbound Agent Detail Performance Report

- Preview Outbound Agent Detail Performance Report

- Reason Code report by Agent grouping

- Reason code report by Reason code grouping

- Contact Service Queue Activity by Window Duration

- Agent All Fields Report

- CSQ All Fields Report

New Historical Reports

Two new Multichannel Historical reports have been added:

- Wrap-Up Reasons for Chat and Email

- Multichannel Agent Summary Report

Recent State History and Recent Call History

Agents can now view their recent state and call history details in the Cisco Finesse gadgets. The following gadgets are available under the My History tab:

- Recent State History.

- Recent Call History. Agents can make an outgoing call to any of the listed phone numbers in the Recent Call History.

Supervisor can view the recent state and call history of an agent available in the Team Performance gadget.

TLS 1.2 Support

This release of Unified Contact Center Express supports by default the Transport Layer Security (TLS) version 1.2.

Note
- For both incoming and outgoing connections, only the TLS version 1.2 is supported.
- Cisco Unified CCX Editor and Real-Time Monitoring Tool must be reinstalled.

Finesse Failover Enhancements

Finesse Desktop can failover independent of the Unified CCX engine mastership status.

This will also enable agents to login to either of the Unified CCX server irrespective of engine mastership status.

Single Sign On Enhancements

Following are the enhancements in the Single Sign-On feature:
- Integrated Windows authentication is available in the Single-Sign On login.
- Cisco Identity Service supports the following Identity Providers:

Microsoft AD FS (Active Directory Federation Services)	2.0, 2.1, and 3.0
PingFederate	8.2.2.0
OpenAM	10.0.1
Shiboleth	3.3.0
F5	13.0

Cisco Identity Service supports the above listed Identity Providers (IdPs) and any other IdPs that comply to generic SAML 2.0 authentication.

Context Service Enhancements

Few of the Context Service feature enhancements in this release are:
- Context Service Logging

  When the Unified CCX or any of its components are registered with Context Service, the Context Service statistics are logged every half an hour in the Unified CCX engine and in the components like SocialMiner, Fusion Management Connector, and Finesse.

- New RTMT Alert

  A new RTMT alert, `ContextServiceStepsExecutionIssue` is triggered when Context Service related step times out or fails due to an error from the Context Service continuously and hits a threshold of X continuous failure.

- Context Service Serviceability

  This displays the status of Context Service integration for the components in the Unified CCX solution.

  The following parameters are displayed for each component:

  - State—Registration state of the component with Context Service
  - Status—Connectivity status of the component with Context Service.
  - Mode—Displays whether the component is connected to the Context Service in Lab mode or in Production mode.
  - Last Fetched at—Time when the last connectivity status was identified.

Infrastructure

The following hardware as part of the infrastructure have been qualified in Unified CCX Release 11.6(1):

- ESXi 6.5 with VMware File System (VMFS) 5. For more information, see the *Virtualization for Cisco Unified Contact Center Express* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_ system/virtualization/virtualization-cisco-unified-contact-center-express.html.

- Hyperflex

- Cisco Business Edition 6000 (BE6K) for Cisco SocialMiner

Updated Features

Enhancement in Real Time Monitoring of Unified CCX Components

Administrator can now connect and monitor Unified CCX solution components using Real Time Monitoring Tool (RTMT) that is installed from any of the Unified CCX 11.6(1) Solution components (Unified CCX, SocialMiner, and Standalone CUIC).

The RTMT client can also monitor a Unified Communication Manager (Unified CM) that is compatible with the Unified CCX 11.6(1) starting from Unified CM 11.0(1).

Reason Code Enhancements

Reason labels are displayed instead of the reason codes .

Administrator can now customize the labels for the system generated Not Ready reasons.

When the system sets the agent's state to Not Ready, the corresponding reason label is displayed on the agent desktop along with the state.

All historical and live data reports now show reason labels for Not Ready and Logout.

Enhanced Email Attachment Size

This release has the following enhanced limits for the email attachment size:

- The total attachment file size limit in an agent's reply has been increased to 20MB.

- The size limit of a single file attachment has been increased to 10 MB.

- The total size limit of attachments in the incoming email from the customer has been increased to 20 MB.

Finesse Workflows based on CSQs

Configure to display the queue details in the call variable layout. A workflow can be defined and triggered based on the queue details available in Call Variable.

Scripting Enhancements

- HTTP Proxy and Header Support in the Make REST Call Step—Provides support for using HTTP proxy and customizing the HTTP headers in the Make REST Call step. This enables to invoke external REST APIs via HTTP proxy.

- Get Reporting Statistics Step—This step is enhanced to be able to obtain the number of agents in the Not Ready state along with the corresponding Reason Code.

- New Document Steps

  Following two new steps have been included:

  - Create JSON Document Step

    This step converts a Text document to JSON Document, if the content of Text document is a valid JSON.

  - Get JSON Document Data Step

    Use the Get JSON Document Data step after the Create JSON Document step to obtain data from a document formatted with JSON.

Deprecated Features

None

Important Notes

- The count of Ring No Answer (RNA) is now incremented only when an agent has not answered the presented call and it rang for the entire configured ring time.

- For certificate regeneration and Certificate Signing Request (CSR) generation the supported key lengths are restricted to 1024 and 2048.

- When you upgrade Unified CCX in an HA deployment ensure that the following conditions are met before Switch version is initiated on Node 2:

    - Switch version of Node 1 is complete and the node is successfully restarted. Otherwise, the upgrade might fail or there might be discrepancy in data.

    - The following services are started on Node 1 after it was restarted (post Switch version):

        - A Cisco DB

        - Cisco Unified Intelligence Center

        - Cisco Finesse

        - Cisco Unified CCX Administration

        - Cisco Unified Cluster View Daemon

        - Cisco Unified CCX Engine

    - Ensure that you are able to log in successfully to Cisco Unified Intelligence Center, on Node 1, using Administrator or Reporting User credentials.

- After the upgrade of Unified CCX, agents and supervisors must clear the browser cache before logging in to Cisco Finesse Desktop and Cisco Unified Intelligence Center.

- When you access the Cisco Unified Contact Center Express Administration and Cisco Unified Intelligence Center in the Single Sign-On mode in Internet Explorer 11 on Windows 7, an error message is displayed. Ensure the web address: https://<uccx-ip>:8553 is correct. Refresh the page and it would get redirected to the login page of the Identity Provider.

- Cisco Unified CCX Editor application must be run as an Administrator. The Windows User launching the application must be a part of the Windows Administrator Group.

- During an upgrade of Unified CCX from version 11.0(1) or any earlier version to 11.6(1), the Chat Web Form must be regenerated and redeployed on the website.

Removed and Unsupported Features

Unsupported Languages for Chat Transcript Download

The default language of the chat transcript PDF is English for customers whose languages (locales) are not supported by SocialMiner. The chat transcript PDF supports all languages that SocialMiner supports except for the following:

- Chinese Simplified (zh_CN)

- Chinese Traditional (zh_TW)

- Japanese (ja_JP)

- Korean (ko_KR)

If you type in any of the unsupported languages, the PDF will have a blank line in place of the line that is in the unsupported language.

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 http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html.

- For multicountry 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.

Supported Features and Configurations for Progressive and Predictive Agent Outbound

- CUBE is supported with the SIP Outbound Dialer and CPA . For more information , see the Unified CCX Compatibility related information located at:

  http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

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:

  http://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 "CSCul43754".

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).

- Expansion servers, except for Automatic Speech Recognition (ASR), Text-To-Speech (TTS), SocialMiner, and MediaSense, which must be separate, dedicated servers.

- 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 in a queue.

- 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.

- 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.)

- 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, then 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 http://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:
http://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:

http://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:

http://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).

Removed Features

The link to the Troubleshooting Tips from the Cisco Unified CCX Administration web page from the **Help** menu has been removed from this release.

Third Party Software Impacts

See the Unified CCX Compatibility related information located at:
http://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.

C H A P T E R **3**

Cisco Unified Intelligence Center

New Features

Dashboards

This release provides an improved user experience for Cisco Unified Intelligence Center Dashboard creation. The following are the feature enhancements:

• Create, edit, and manage Dashboards

• Add reports, web pages (URLs), web widgets, and notes to a Dashboard

• Dashboard permalinks

• Mark a Dashboard as favorite and view the personal list of favorites

Chart Configuration

This release provides a simplified user experience Cisco Unified Intelligence Center chart creation. The following are the feature enhancements:

• Three step chart creation (Chart Information, Add Data Fields, Preview and Format)

• New chart types; Numeric, Donut

• Create chart view directly from an executed report

Grid View Enhancements

This release provides the following grid view features:

- Improved Threshold selection

- Enabled Group Expansion at a per view level

Updated Features

TLS v1.2 Support

This release supports Transport Layer Security (TLS) version 1.2 as the default version for both incoming and outgoing SSL connections.

Important Notes

Upgrade Considerations

Dashboard Widgets

Cisco Unified Intelligence Center 11.6 supports a maximum of ten widgets per Dashboard. Hence, for Dashboards with more than ten widgets in versions before 11.6, ensure to split those Dashboards with a maximum of ten widgets each before upgrade.

Example: Consider a Dashboard with 15 widgets in Unified Intelligence Center versions before 11.6. Before upgrading to version 11.6, use the **Save As** feature to clone the Dashboard and manage the widgets up to ten per Dashboard.

⚠️

Warning   Migrating Dashboards with more than ten widgets to version 11.6 allows you to only run the Dashboards. You cannot modify and save these Dashboards unless you retain only a maximum of ten widgets per Dashboard.

Unsupported Widgets

The Cisco Unified Intelligence Center 11.6 interface for Dashboards does not support the following widgets:

- Schedule Report widgets

- URL widgets containing Dashboard permalinks (Nested Dashboards)

Migration Limitations

The following widgets if added to the Dashboard before Cisco Unified Intelligence Center 11.6 are not migrated.

- Schedule Report widgets.

- URL widgets containing Dashboard permalinks (Nested Dashboards).

• Widgets that were placed beyond the new Dashboard canvas size.

| **Note** | Post upgrade to Cisco Unified Intelligence Center 11.6, the positions of the widgets placed in the legacy dashboard interface are retained. However, in few cases the position and size of the widgets are modified to fit inside the new dashboard interface. |

• Inaccurate widgets (inaccurate database records)

Example: Report widgets with missing Report Views.

| **Note** | For the Schedule Report widgets and Nested Dashboard widgets that are not migrated, the Cisco Unified Intelligence Center server logs do not capture the logs. |
| | For all other widgets, Cisco Unified Intelligence Center server logs captures the log information with the corresponding Dashboard and widget name. |

CLI Commands - Switch to TCP/IP

This release provides the capability to cluster Cisco Unified Intelligence Center nodes using TCP/IP instead of the default discovery mechanism using Multicast. Use the following CLI commands to switch to TCP/IP only if the customer's network does not support Multicasting:

• utils cuic cluster show

• utils cuic cluster refresh

• utils cuic cluster mode

| **Note** | The default mechanism to cluster Cisco Unified Intelligence Center nodes remains to be Multicast. |

Screen Resolution Support

Supported screen resolution for Cisco Unified Intelligence Center 11.6: 1366 x 768 or higher.

Deprecated Features

None

Removed and Unsupported Features

Dashboards

The Dashboards drawer from the legacy interface is disabled.

Dashboards - Slideshow

The Dashboard slideshow feature that was used to move through items on the dashboard is removed.

Scheduled Reports on Dashboards

You can no longer add scheduled reports on Dashboards. If there are existing Dashboards with scheduled report widgets in versions prior to 11.6, those widgets (not the Dashboards) will be dropped on upgrade to 11.6.

Third-Party Software Impacts

None

Cisco Finesse

New Features

Make Call from Ready State

Agents and Supervisors can make calls from Ready State.

View My History

As an Agent or Supervisor, you can view your call history by clicking on the 'My History' tab. You can view call details like start time of the call, duration, type etc.

Initiate a Call back from the My History Report

As an agent or supervisor, you can initiate a call back by clicking the Make Call icon for a selected row in the Agent Call History report from the My History tab.

Separate System and Custom Reason Codes in Cisco Finesse Administrator

The Finesse Administrator can differentiate between system reason codes and custom reason codes in the Not Ready and Sign Out Reason code gadgets. The Type column can be sorted to display both reason codes (System or Custom) in the Finesse Admin Console. System reason code "labels" can be edited and saved but the global attribute and "code" cannot be edited. Admin cannot create or update a new Reason Code that conflicts with a predefined Reason Code already present in the system.

Pre-defined Attributes of the System Reason Codes

In the Not Ready system reason codes and Sign Out system reason codes, only the reason code label can be edited and saved. The Global attribute and system code cannot be modified. In case the system reason code label is modified and you wish to revert back to the default label, see *Pre-Defined System reason Codes* listed in the *Cisco Finesse Administration Guide*. The first letter of the system reason code is capitalized.

Queue Statistics for Finesse IPPA

The following queue statistics information is now displayed on the Finesse IPPA home screen:

- Current call state.

- Number of calls waiting across assigned queues.

- Longest Queue time across assigned queues.

- Last refreshed time of the Queue Statistics data (auto update happens every 15 seconds).

Filtering of Logged Out Agents

By default, in the Team performance gadget, supervisors will not be able to view logged out agents. To view both logged in and logged out agents, click the **Include logged out agents** checkbox.

Secondary Call ID in Dialog API

Secondary call ID is added in the additional element of the primary dialog API for consult, transfer and conference calls scenarios.

Updated Features

Enable Trace Logs

Use the admin privilege level CLI command to enable and disable trace logging for Finesse IPPA. Use any one of the following commands to toggle trace logs for Cisco Finesse.

- utils finesse trace enable

- utils finesse trace disable

- utils finesse trace status

Audit Logs Track Admin User Operations

Generate audit logs to track all admin operations (including Finesse admin UI and REST client operations). The log includes the following parameters:

- Timestamp

- User id of the administrator

- Method of operation (PUT, POST, DELETE)

- URL

- Payload

Configuration of viewID in Dynamic Live Data Gadgets

Dynamic Live Data gadgets (identified by the "type=dynamic" URL parameter) in the supervisor desktop layout can have only a single viewID URL param configured. This enables you to view call history and state history on the desktop correctly.

Monitor Manual Outbound Call

Supervisor can silent monitor when an agent makes an outbound call in the Not-Ready state from the ACD line.

Reason Code Conflicts during Upgrade

When upgrading from a previous Unified CCX version to 11.6(1), you can manage reason code conflicts so that reports reflect accurate reason codes after upgrade.

When performing a system upgrade in a Unified CCX deployment, if the predefined system reason codes already exist in the system as custom reason codes, they need to be modified with new values to avoid conflict post upgrade.

Configurable Toaster Notifications

Toaster notifications are enabled by default after a fresh installation of Cisco Finesse. Use CLI commands to disable, enable and check the status of the toaster notifications. You can set the duration (timeout in seconds) of the toaster notification.

Context Service Serviceability

Context Service Serviceability Improvements

Cisco Finesse, if registered, logs the following information in Fusion Management Connector

- Context Service SDK version used in Finesse

- Context Service registration status

- Ping Latency of the CS services

The Finesse Authorization logs are available in the `/opt/cisco/ccbu/logs/fusion-mgmt-connector` and `/opt/cisco/desktop/logs/finesseauth` directories respectively.

Additionally, Cisco Finesse polls the CS JMX counters and, if registered, it logs the resulting information, at intervals, in the Finesse Authorization log available in the `/opt/cisco/desktop/logs/finesse-auth` directory.

Context Service SDK Re-initialization

Cisco Finesse support a new REST API, called CS re-init API, to re-initialize the Context Service SDK without re-starting Tomcat.

Important Notes

None.

Deprecated Features

None

Removed and Unsupported Features

None

Third-Party Software Impacts

None

CHAPTER 5

Cisco MediaSense

CHAPTER 6

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

AUDIT Log Support for all Config changes

Cisco SocialMiner, Release 11.6(1) provides audit log capabilities for all its administrative operations.

CORS Support

The Cross Origin Resource Sharing support has been included in SocialMiner 11.6(1) for all public REST APIs including chat APIs.

Updated Features

TLS v1.2 Support

Cisco SocialMiner, Release 11.6(1) supports TLS v1.2 as the default protocol for secure incoming connections as a server and for secure outgoing connections as a client. However, support for earlier TLS versions can be configured. For more information, see the *Cisco SocialMiner User Guide*.

Important Notes

SocialMiner Installation displays "Installing Cisco SocialMiner component" freezing the screen momentarily

While the SocialMiner installation is in progress, the message `Installing Cisco SocialMiner component` causes the screen to freeze. Do not abort the process. Wait for the installation to complete, although it might appear that the system has frozen momentarily.

Deprecated Features

None

Removed and Unsupported Features

Ability to Browse and Download Logs via HTTP

Effective with Cisco SocialMiner, Release 11.6(1), the ability for administrators to browse system logs from browsers (using the System Logs -> Log Directory option in SocialMiner Administration interface) has been removed.

Standard mechanisms of accessing and downloading system logs are available through Real-Time Monitoring Tool (RTMT) and through the application CLI commands. For more information on RTMT, see the *Cisco SocialMiner User Guide*, available at, http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/products-user-guide-list.html.

Third-Party Software Impacts

None

CHAPTER 7

Cisco Unified Workforce Optimization Workforce Management

New Features

The following is a summary of the new features added to this release:

- Added mobile device support for agents. Agents can now access My Schedule and Messaging on smart phones and tablets.

Updated Features

The following is a summary of the updated features added to this release:

- Added the ability to select the preferred method of generating variable schedules for agents who have assigned exceptions. You can opt to avoid assigned exceptions in order to maximize coverage, or include assigned exceptions (which might be for required events like team meetings) but that might result in insufficient coverage.

Deprecated Features

None.

Important Notes

None.

Removed and Unsupported Features

None.

Third Party Software Impacts

None.

CHAPTER 8

Cisco Unified Workforce Advanced Quality Management

New Features

None.

Updated Features

The following is a summary of the updated features added to the 11.6(1) release.

- Added a field to the Workflow Administration window that allows after call work recording to stop when a new call begins.

Deprecated Features

None.

Third Party Software Impacts

None.

Removed and Unsupported Features

None.

Third Party Software Impacts

None.

CHAPTER 9

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://www.cisco.com/cisco/psn/bssprt/bss. 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 11.6(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 focus the result set by setting more filters in the tool.

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

Cisco Unified Contact Center Express

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=270569179&rls=11.6(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco Unified Intelligence Center

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=282163829&rls=11.6(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco Finesse

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=283613135&rls=11.6(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco SocialMiner

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=283613136&rls=11.6(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco Unified Workforce Optimization Workforce Management

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=286288929&rls=11.6(1)&sb=anfr&svr=4nH&srtBy=byRel&bt=custV

Cisco Unified Workforce Optimization Quality Management

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=286288919&rls=11.6(1)&sb=anfr&svr=4nH&srtBy=byRel&bt=custV