Release Notes for Unified Contact Center Express Solution Release 11.0(1)

First Published: 2015-08-27

CONTENTS

Introduction

• Release Notes for Contact Center Solutions, on page 1

Release Notes for Contact Center Solutions

For Release 11.0, we are introducing 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. Follow these links to find the release note compilations:

• *Release Notes for Cisco Packaged Contact Center Enterprise Solution Release 11.0(1)* at
http://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html

• *Release Notes for Cisco Unified Contact Center Enterprise Solution Release 11.0(1)* 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 Release 11.0(1)* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-release-notes-list.html

• *Release Notes for Cisco Hosted Collaboration Solution for Contact Center Release 11.0(1)* at
http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-release-notes-list.html.

CHAPTER 2

Cisco Unified Contact Center Express

New and Updated Features

New Features

Email Enhancement

This feature allows the agent to discard email. Appropriate historical reports have been enhanced to provide information regarding number of discarded emails.

Finesse IP Phone Agent

As CAD is deactivated in release 11.0(1), Finesse IP Phone Agent provides a replacement for CAD IP Phone Agent (IPPA).

Outbound Enhancement

This feature allows outbound campaigns to have duplicate contact entries so that contacts can be called multiple times within the same day.

Standalone Unified Intelligence Center

This feature allows the Unified Intelligence Center to be installed on a standalone server that is connected to Unified CCX to provide support for multiple data sources and custom reporting.

Unified Intelligence Center Reporting Enhancements

This feature introduces enhancements to Live Data Gadgets and Historical Reports to improve the user experience.

Post Call Treatment

Post Call Treatment allows Unified Contact Center Express (UCCX) to provide treatment to an ICD call once the agent ends the call from the Finesse Desktop.

Post Call Treatment can be used for use cases such as transferring the call to a survey for customer feedback.

Updated Features

The following sections describe updated features pertinent to Unified CCX Release 11.0(1).

Purge Enhancement

This feature enhances the existing feature of purging the database. The administrator can now set the purge duration for a scheduled purge in Unified CCX Administration in addition to the purge start time. The enhancement also allows the administrator to configure to initiate an automatic purge when the extent size exceeds the set limits.

Deprecated Features

Cisco Agent Desktop

In Unified CCX 11.0(1), Cisco Agent Desktop and all its components such as Cisco Supervisor Desktop, Cisco Agent Desktop reporting, on demand recording, remote monitoring, Cisco Agent Desktop Chat, Cisco Agent Desktop Email features are blocked and customers are advised to use Finesse Agent Desktop and its suite of products.

When you upgrade to Unified CCX 11.0(1) or when you do a fresh install of Unified CCX 11.0(1) version, you will notice that:

- You will not be able to download CAD from Unified CCX.

- All CAD references in Unified CCX App admin have been removed.

- The Finesse IP Phone Agent (FIPPA) must now be used in place of CAD's IP Phone Agent (IPPA) and is available as part of standard, enhanced and premium licenses. While FIPPA is the functional equivalent of IPPA, the supported phones have changed. For more information , see the *Compatibility Matrix for Unified CCX*, located at: http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCX to ensure you deploy FIPPA with a supported phone model.

- CAD specific email reports have been removed. However, the data is retained and can be accessed using CAD email stock reports from the CDN (Cisco Developer Network).

- Recordings, configurations, and workflow cannot be migrated to Cisco Finesse.

Important Notes

Encryption of Self-Signed Certificates

Automatically generated self-signed certificates currently use SHA-1 encryption, which is deprecated.

Instead, use the platform administration tools to create self-signed certificates with SHA256 encryption. You can access the tools by selecting **OS Administration** > **Security** > **Certificate Management**.

Note After the self-signed certificates are generated using the SHA256 encryption, the Cisco Unified Intelligence Center Live Data fails with the following error:

```
Team Data & Queue Data for supervisor;Agent Statistics and Agent State Log for
agent): There were issues rendering this gadget.
javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated
```

To resolve this issue, restart the server.

Connectivity Issues When VOS Firewall Disabled

The firewall on a VOS server uses port forwarding. If you disable the firewall, some applications can lose connectivity because they use port forwarding. The Cisco Unified Intelligence Center OAMP page and any other web application that connects to Cisco Tomcat on port 8443 fail when the firewall is down. The Cisco Unified Real-Time Monitoring Tool (RTMT) client displays the following error:

```
RTMT application cannot communicate with specified node/cluster. Please verify
the host IP
address is correct and the network connection is up, and try again.
```

Unsupported and Supported 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 and Supported 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 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 *Compatibility Matrix for Unified CCX*, located at: http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCX.

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.

• Shared non-IPCC extensions with any other Directory Number, irrespective of the configured partition.

• 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" or "Redirect" step from scripts 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 "MeetMe" 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.

• 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

- MeetMe

- Park

- Pickup

Unsupported and Supported Configurations for Agent Phones

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.

- Configuring a Cisco Unified IP Phone with Secure Real-Time Protocol (SRTP) for use in recording with MediaSense.

- 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 lines on the first four buttons on the phone 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.

- Video is not supported if you are using Cisco Jabber for Windows as agent phone.

- 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.

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 *Compatibility Matrix for Unified CCX*, located at:

http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCX

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.

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 11.0, 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 11.0(1).

Third-Party Software Impacts

For information on third-party software, see the Compatibility Matrix for Cisco Unified Contact Center Express available at http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCX.

CHAPTER **3**

Cisco Unfied Intelligence Center

New and Updated Features

New Features

The following sections describe new features that are pertinent to Unified Intelligence Center Release 11.0(1).

Unified Intelligence Center Gadget Improvements

A toolbar is added to the reporting gadget. The toolbar includes options to select views, view thresholds only, play and pause of live data updates, help, and maximize toolbar.

The gadget toolbar allows you to select multiple report views (up to five views), which is configured in the Cisco Finesse administration page.

Support for New Russian Time Zone

Unified Intelligence Center supports the two new Russian time zone : **Asia/Chita** and **Asia/Srednekolymsk**. The new time zones are included as part of Unified Intelligence Center.

Language Pack COP

From this release Unified Intelligence Center's default locale is English (U.S). You can enable all supported locales in Unified Intelligence Center by installing the language pack on all nodes in a cluster. The language pack is available as a Cisco Optional Package (COP), which can be downloaded from Cisco.comhttps://software.cisco.com/download/type.html?mdfid=282163829&catid=null.

Note   Canadian French is removed from the language COP for this release.

> **Note** Customers installing or upgrading to Unified Intelligence Center 11.0(1) must apply the language COP on all nodes in a cluster.

Updated Features

There are no updated features for Cisco Unified Intelligence Center Release 11.0(1).

Browser Support

In this release Unified Intelligence Center supported browser versions are as follows:

	Internet Explorer 10 Native Mode	Internet Explorer 11 Native Mode	Internet Explorer 10 Compatibility Mode	Internet Explorer 11 Compatibility Mode	Firefox 38 Extended Supported Releases (ESRs) and higher ESRs
Cisco Unified Intelligence Center	No	No	Yes	Yes	Yes
Cisco Unified Intelligence Center (Live Data Gadgets)	Yes	Yes	Yes	Yes	Yes

Deprecated Features

There are no deprecated features for Cisco Unified Intelligence Center Release 11.0(1).

Important Notes

VMware Tools Refresh

The VMware tools command **utils vmtools upgrade** is replaced with **utils vmtools refresh**.

To know more about the command syntax, see Command Line Interface in the *Administration Console User Guide for Cisco Unified Intelligence Center*.

Encryption of Self-Signed Certificates

Automatically generated self-signed certificates currently use SHA-1 encryption, which is deprecated.

Instead, use the platform administration tools to create self-signed certificates with SHA256 encryption. You can access the tools by selecting **OS Administration** > **Security** > **Certificate Management**.

Load Balance

A Unified Intelligence Center deployment with an optional Cisco Application Control Engine (ACE) load balancer is not supported. System administrators now have the server load balancing option when Unified

Intelligence Center experiences heavy reporting load. For more information see, the *Administration Console User Guide for Cisco Unified Intelligence Center*.

Recovery Disk

The server recovery instructions are explained in the *Installation and Upgrade Guide for Cisco Unified Intelligence Center* under the chapter *Frequently Asked Questions*. The instructions provide are not updated and a document defect is opened https://tools.cisco.com/bugsearch/bug/CSCuv67000 to address this.

Unsupported and Removed Features

There are no unsupported or removed features for Cisco Unified Intelligence Center Release 11.0(1).

Third-Party Software Impacts

There are no third-party software impacts on Cisco Unified Intelligence Center Release 11.0(1).

Third-Party Software Impacts

Cisco Finesse

New and Updated Features

New Features

Sign In URL Now Requires FQDN

To sign in to the Finesse administration console or the Finesse agent desktop, enter the fully qualified domain name (FQDN) of the Finesse server in the URL. If you enter the server IP address or hostname, Finesse redirects your browser to the server FQDN.

Multiple Call Variables Layouts

In previous releases, Finesse only supported one default Call Variables Layout. With Release 11.0(1), the Call Variables Layout gadget allows you to define up to 200 unique Call Variables Layouts (one default layout and 199 custom layouts) to display on the Finesse agent desktop. As part of this functionality:

• You can use a workflow to specify the Call Variables Layout that an agent sees when they receive a call.

• For a new Release 11.0(1) installation, Finesse provides a default layout.

• For upgrades from an earlier release, Finesse migrates the previously configured default layout and assigns it the default name and description.

Finesse IP Phone Agent

With Finesse IP Phone Agent (IPPA), agents can access Finesse capabilities on their Cisco IP Phone as an alternative to accessing Finesse through the browser. Finesse IPPA does not provide the full set of Finesse features that are supported using the browser, but it does allow agents and supervisors to receive and manage Finesse calls if they lose or do not have access to a PC.

Note Supervisors can sign in to Finesse on their IP Phones and perform all agent tasks, but supervisor tasks such as monitor, barge, and intercept are not supported. To perform supervisor tasks, supervisors must sign in to the Finesse desktop.

In Release 11.0(1), Finesse IPPA supports the following functionality:

- Sign in/sign out

- Pending state

- Wrap-up reasons

- Optional wrap-up

- Not Ready reasons

- State change using reason codes

- One Button Sign In

Account Locked After Five Failed Sign In Attempts

If an administrator tries to sign in to the Finesse administrator console (or diagnostic portal) with the wrong password five times in a row, Finesse blocks access to that user account for a period up to 30 minutes. For security reasons, Finesse does not alert the user that their account is locked. They must wait 30 minutes and try again.

Similarly, if agents or supervisors sign in to the desktop five times in a row with the wrong password, Finesse blocks access to that user account. However, in this case, the lockout period is only 5 minutes. This restriction also applies when agents and supervisors sign in using Finesse IP Phone Agent (IPPA).

Note When an agent or supervisor account is locked, subsequent attempts to sign in, even with correct credentials, reset the lockout period to 5 minutes again. For example, if a locked user tries to sign in again after only 4 minutes, the lockout period is reset and the user must wait another 5 minutes. This reset does not apply to the administrator account.

To view whether a user account is locked, enter the following CLI command:

file get activelog desktop recurs compress

Then extract the zipped output, and search the catalina.out logs (opt/cisco/desktop/finesse/logs/catalina.out) for the following message referring to the locked username:

```
An attempt was made to authenticate the locked user "<username>"
```

Accessibility

The Finesse desktop supports features that improve accessibility for low-vision and vision-impaired users.

![Note pencil icon]

Note Finesse supports these features only with Internet Explorer 11.0 and only on the agent desktop, not the supervisor desktop or administration console.

Gadget Loading Indicator

Finesse now provides a gadget loading indicator that displays a loading message while a gadget is initially loading in Finesse. If you are a developer creating a gadget, include this functionality in your gadget to provide a consistent user experience within Finesse.

X-Frame-Options Support

As a security enhancement, Finesse Release 11.0(1) supports x-frame-options (XFO) HTTP header in the Finesse HTTP messages.

Updated Features

Increased Phone Books and Contacts

Finesse Release 11.0(1) increases the maximum number of team phone books from 50 to 300 and total contacts in all phone books from 1500 to 50,000. See the following table for details.

Table 1: Maximum Numbers of Phone Books and Contacts

Item	Maximum	Notes
Total contacts in all phone books	50,000	Increased from 1500.
Team phone books	300	Increased from 50.
Global phone books	10	Unchanged.
Displayed contacts per agent	1500	Unchanged. These contacts are retrieved first from the global phone books and then from the team phone books.
Contacts per phone book	1500	Unchanged.

Increased Team Wrap-Up Reasons

Finesse Release 11.0(1) increases the maximum number of team wrap-up reasons from 100 to 1500. However, you can still assign no more than 100 team wrap-up reasons to an individual team. The maximum number of global wrap-up reasons remains unchanged at 100.

All ASCII Characters Now Supported When Making a Call

Finesse now supports the use of any ASCII character when you make a call. Finesse no longer converts letters typed into the dial pad into numbers, nor does it remove non-numeric characters (including parentheses and hyphens) from phone numbers.

Dialog Notification API Populates requestId

In the Dialog Notification API, the requestId tag is now populated when a user makes a request. (For an incoming call, the requestId tag is empty.)

Deprecated Features

This release has no deprecated features.

Important Notes

Cisco Finesse Installation

In a Unified CCX deployment, Finesse is installed coresident with Unified CCX, as part of the Unified CCX installer. For more information about installing Finesse with Unified CCX, see the *Cisco Unified Contact Center Express Installation Guide* at http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1846/prod_installation_guides_list.html.

Load Balancing for Finesse

With Finesse, the use of a load balancer after sign-in is neither required nor supported. For information about Finesse support of a load balancer before sign-in or with the Finesse APIs, see the *Cisco Unified Contact Center Express Design Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-implementation-design-guides-list.html .

Encryption of Self-signed Certificates

Encryption of Self-Signed Certificates

Automatically generated self-signed certificates currently use SHA-1 encryption, which is deprecated.

Instead, use the platform administration tools to create self-signed certificates with SHA256 encryption. You can access the tools by selecting **OS Administration** > **Security** > **Certificate Management**.

One Finesse Desktop or Finesse IPPA Session Per Agent

Finesse has the following agent session limitations:

- Finesse can support a mix of agents in which some agents use Finesse IPPA and other agents use the Finesse desktop (license permitting).

- Agents cannot sign in to both the Finesse desktop and Finesse IPPA at the same time.

- Agents can sign in to only one instance of either the Finesse desktop or Finesse IP Phone Agent (IPPA) at one time.

　• When agents are signed in to the Finesse desktop or Finesse IPPA, they can also sign in to a third-party application using the Finesse API at the same time. (This setup is considered a custom development. Like other Finesse customizations, the customer or partner is responsible for proper development and testing of this custom setup.)

Wrap-Up and Transfer

An agent cannot enter wrap-up data following a completed transfer because the call is not only cleared, but also completely ended. If an agent wants to enter wrap-up data for a transferred call, that agent must select a wrap-up reason while the call is in progress.

Note　If an agent is configured for wrap-up, that agent may still enter Wrap-Up state after transferring the call. However, the wrap-up timer does not appear on the Finesse desktop after the call is transferred.

Browser URL Button for Workflow Actions and Internet Explorer 11.0

The context menu for the Browser URL button on the Manage Workflow Actions gadget is disabled in Internet Explorer 11.0. An administrator must use keyboard shortcuts for Select All, Cut, Copy, and Paste for this particular field.

Cisco Jabber for Windows

Finesse supports Cisco Jabber for Windows as a contact center voice endpoint. Finesse supports the following Jabber functionality:

　• Voice only (Video is not supported)

　• Built-In Bridge (for silent monitoring)

　• IM and Presence

Note　Agents cannot use Jabber to transfer or conference calls. Agents must use the Finesse desktop for transfer and conference.

You must change the default configuration for Jabber as follows:

　• Change Maximum number of calls from 6 to 2.

　• Change Busy trigger from 2 to 1.

Hardware and Software Requirements

For Finesse compatibility requirements, including supported phones and browsers, see the Compatibility Matrix for Unified CCX.

Finesse Client Requirements

The minimum supported screen resolution for Finesse clients is 1024 x 768.

☞

Important   Requirements, such as processor speed and RAM, for clients that access the Finesse desktop can vary. Desktops that receive events for more than one agent (such as a supervisor desktop running Team Performance and Queue Statistics gadgets or an agent desktop running Live Data reports that contain information about other agents or skill groups) require more processing power than desktops that receive events for a single agent.

Factors that determine how much power is required for the client include, but are not limited to, the following:

- Contact center traffic

- Additional integrated gadgets in the desktop (such as Live Data reports or third-party gadgets)

- Other applications that run on the client and share resources with the Finesse desktop

Hardware

Click here for information about the system hardware requirements for Unified Communications servers. For virtualization information for Cisco Finesse, go to http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_Finesse.

Load and Capacity

Finesse is qualified to support up to 360 desktop or Finesse IPPA agents and 40 supervisors (for a total of 400 users). Finesse IPPA agents can also access the Finesse desktop (but not both at the same time) without affecting the total number of supported users, license permitting. Unified CCX supports HTTPS only.

Related Documentation

For information about Finesse deployments with Unified Contact Center Express (Unified CCX), see the Unified CCX documentation on Cisco.com:

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

Developer information is available from the Finesse page on the Cisco Developer Network (requires sign in with Cisco.com user ID and password):

https://developer.cisco.com/site/finesse/

Cisco DevNet provides API documentation (*Cisco Finesse Web Services Developer Guide*), a blog, and forums.

Troubleshooting tips for Cisco Finesse are available on DocWiki at:

http://docwiki.cisco.com/wiki/Troubleshooting_Cisco_Finesse

Removed and Unsupported Features

This release has no removed or unsupported features.

Third-Party Software Impacts

This release has no third-party software impacts.

Cisco MediaSense

New and Updated Features

New Features

In-Browser Playback

In addition to Java media player, you can play back an audio recording using the HTML5 playback feature of the browser. While using in-browser playback, you do not need to download the recording. To enable in-browser player, configure the settings in the **Search and Play Configuration** window of **Cisco MediaSense Administration**. In MediaSense Search and Play, an in-browser player appears at the bottom of the recording selected for playback and displays its progress.

For more information, see the "In-Browser Playback" section of the *Cisco MediaSense User Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/products-user-guide-list.html.

Finesse AgentInfo Gadget

Finesse AgentInfo gadget is present on the Finesse Agent desktop to convey agent information from Finesse to MediaSense. When an agent signs in to the desktop, the gadget automatically signs in to MediaSense server and provides agent information. The agent information includes login ID, login extension, first name, and last name. It also keeps a track of the agent signs in and out time.

For more information, see the "Finesse AgentInfo Gadget" section in the *Cisco MediaSense User Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/products-user-guide-list.html.

Agent Information in MediaSense Search and Play

In **MediaSense Search and Play**, you can search for recordings based on agent information and view agent information in the search results. The agent information includes login ID, login name, first name, and last name. To customize the display of agent information parameters in Search and Play, select or deselect the parameters in the **Search and Play Configuration** window of **Cisco MediaSense Administration**.

For more information, see the "Search for, Play, or Download a Recorded Call" and "Search and Play Configuration" sections of the *Cisco MediaSense User Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/products-user-guide-list.html.

Unified Communications Manager Line Display Name in MediaSense Search and Play

In **MediaSense Search and Play**, enter Unified Communications Manager Line Display name in the **Line Name** text box to search for a recording. You can also view the Unified Communications Manager Line Display Name as *Line Name* if it is configured in Unified Communications Manager.

To enable *Line Name* as search option and view it in the search results, check the **Show Line Display Name** check box in **Search and Play Configuration** window in **MediaSense Administration**. For more information, see "Search and Play Configuration" section of the *Cisco MediaSense User Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/products-user-guide-list.html.

Call Association for Network-Based Recording and Unified Border Element Dial Peer Recording

MediaSense groups strongly associated calls which have at least one common xRefCi value in case of sessions recorded through Unified Communications Manager, and at least one common CCID value in case of sessions recorded through Unified Border Element. MediaSense 11.0(1) supports call association for Unified Communications Manager network-based recordings and Unified Border Element dial peer recordings.

Search on Archived Recordings

You can search archived recordings in *MediaSense Search and Play* using the Archive Calls tab. Use the Session ID, participant ID, and date range to search the archived recordings. To enable archived recordings search, check the **Enable Search on Archived Recordings** check box in the **MediaSense Archive Configuration** window of **Cisco MediaSense Administration**.

For more information, see the "Archival" section of the *Cisco MediaSense User Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/products-user-guide-list.html.

Updated Features

There are no updated features for MediaSense 11.0(1).

Deprecated Features

Cisco Finesse

MediaSense 11.0(1) supports Finesse 11.0; earlier versions are not supported any longer.

Cisco Unified Communications Manager AXL Authentication 8.x

MediaSense 11.0(1) no longer supports Cisco Unified Communications Manager AXL Authentication 8.x.

Important Notes

There are no important notes for MediaSense 11.0(1).

Removed and Unsupported Features

There are no removed and unsupported features for MediaSense 11.0(1).

Third-Party Software Impacts

For information on third-party software, see the *Compatibility Matrix for Cisco MediaSense* available at http://docwiki.cisco.com/wiki/Cisco_MediaSense_Compatibility_Matrix.

CHAPTER 6

Cisco SocialMiner

New and Updated Features

New Features

The following sections describe new features for Cisco SocialMiner Release 11.0(1).

Discard an Email Message

SocialMiner Release 11.0(1) provides this feature for Unified Contact Center Express (Unified CCX).

This feature allows email support agents to discard spam and trivial email messages that do not qualify a response.

This feature requires SocialMiner integration with Unified CCX and is delivered through Cisco Finesse. For more information about discarding email message, see the section *Discard an Email Message* in *Cisco Finesse Agent and Supervisor Desktop User Guide for Cisco Unified Contact Center Express, Release 11.0(1)* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-user-guide-list.html.

Account Locked After Five Failed Sign In Attempts

If an administrator tries to sign in to the SocialMiner administration console with the wrong credentials five times in a row, SocialMiner blocks access to that user account for a period up to 30 minutes.

For security reasons, SocialMiner does not alert the user that the account is locked. The administrator must wait for 30 minutes and try again.

This feature also applies to all authenticated REST APIs of SocialMiner.

Updated Features

There are no updated features for SocialMiner 11.0(1).

Deprecated Features

This release has no deprecated features.

Important Notes

SocialMiner OVA Template

Use the OVA template **Cisco_SocialMiner_v11.0_VMv8.ova** for the fresh installation of SocialMiner Release 11.0(1).

You can obtain the Virtual Server Template (OVA) file needed to create a Virtual Machine from https://software.cisco.com/download/type.html?mdfid=283613136&flowid=73189 .

The Cisco SocialMiner 11.0(1) Virtual Server Template (OVA) defines a virtual machine configuration that is supported in the SocialMiner 11.0(1) release. This OVA contains all supported virtual machine configurations of this release.

Upgrade to SocialMiner 11.0(1)

For upgrades from SocialMiner 10.x to SocialMiner 11.x, apply the corresponding COP file from the Command Line Interface (CLI) and modify the SocialMiner Virtual Machine's operating system version, total video memory, and network adapter type parameters before beginning the upgrade process.

Note If you are on version 10.x, perform upgrade directly to 11.0(1).

If you are on a version lower than 10.0(1), upgrade to 10.x and then upgrade to 11.0(1).

For information about SocialMiner Upgrade, see the section *Upgrade SocialMiner* in *SocialMiner Installation and Upgrade Guide, Release 11.0(1)* at http://www.cisco.com/c/en/us/support/customer-collaboration/socialminer/tsd-products-support-series-home.html.

Removed and Unsupported Features

From this release, Cisco Security Agent (CSA) is removed.

Third-Party Software Impacts

This release has no third-party software impacts.

Cisco Unified Workforce Optimization Workforce Management

New and Updated Features

New Features

- Support for Cisco Unified Contact Center Express 11.0

- Support for Microsoft SQL Server 2014

- Support for dynamic scheduling

- Support for multiskill scheduling

- Support for mentoring requests

- Support for scheduling incentives

- Interface localized in Danish, Dutch, English, French, German, Italian, Portuguese (Brazilian), Spanish (European) and Swedish

- Help localized in Danish, Dutch, English, French, German, Spanish (European), and Portuguese (Brazilian)

- Support for high availability for the Workforce Optimization interface

- Support for non-ACD agents in synced systems.

Updated Features

This section details the updated features in this release:

- Advanced bundle features of Vacation Planning and Strategic Planning now available to all WFM customers.

- Support for high availability for the WFO interface.

- Support for non-ACD agents in synced systems.

- Addition of the Balanced Schedule option when running a schedule.

- Block scheduling (MSAQ) is now always on.

- Improvements in how service level percentage rollups are calculated.

Deprecated Features

This release has no deprecated features.

Important Notes

This section details the installation related notes. For step-by-step installation and upgrade instructions, see the *Cisco Workforce Management Installation Guide*.

Recalculating Actual Service Level after Upgrade

The actual service level for the period before WFM 10.5(1) SR3 or newer was installed will not be correct unless the data for that period is recaptured. Data acquired after the date of the upgrade will display the correct actual service date.

See "Historical Data" in the Workforce Management User Guide and "Historical Data Capture" in the Workforce Management Data Import Reference Guide for more information on how to capture your historical data.

Removed and Unsupported Features

This release has no removed and unsupported features. This section lists the limitations and restrictions in this release.

Limitations and Restrictions

The following sections identify limitations of the product, and any workarounds that exist to deal with issues.

PC validation incorrectly indicates that Google Chrome is an invalid browser

The Validate my PC configuration feature will return a result of Bad for the browser type and version if a WFM user's desktop uses the Google Chrome browser, even though Chrome is a supported browser. The user can ignore this incorrect result and log into WFM normally.

Schedule exceptions are not assigned to agents after schedule interval trade

If an exception is added to an agent's schedule after that schedule is run (**Schedule** > **Edit Schedule**), and then that exception interval in that agent's schedule is copied to other agents' schedules to give them the same

exception (**Intraday** > **Schedule Trade**), the exception will appear in all agents' schedules. However, it will appear only in the original agent's list of exceptions (**Agents** > **Agent Detail** > **Exceptions** tab).

To work around this issue, select the "**This service queue allows block scheduling**" check box on the **Service Queue** page and run the schedule again.

Third-Party Software Impacts

This release has no third-party software impacts.

Cisco Unified Workforce Quality Management

New and Updated Features

New Features

The following is a summary of the new features added to the 11.0 release.

- Merged the Desktop Requirements Guide, Desktop Applications Deployment Guide, and Firewall Configuration Guide into the Installation Guide.

- Added support for Network Based Recording using the Cisco Unified CM Recording functionality from either an IP phone (BIB) or gateway. Network Based Recording supports Cisco CUBE Recording via SIP and Cisco MediaSense.

- Added information on hard disk drive (HDD) partitioning.

- Added information on configuring a customer relationship management (CRM) system.

- Added information on integrating SNMP.

- Added the Kerberos Authentication check box to the Enterprise Settings window. When enabled, a user must enter the AD credentials to access Recording controls.

- Added support for cloud based recording storage for Quality Management.

- Added support for two stage upload.

- Added support for Unified CCX version 11.0, Unified CM 11.0(1a), and MediaSense11.0.

- Added support for configuring the default time format at a global level. You can now choose between the 24 hour and the 12 hour time format in Interface Settings under Recordings > Interface Configuration.

- Added support for importing and exporting an inclusion/exclusion list to the Inclusion List under System Configuration.

- Added support for the Contact Basic Search API. The Contact Basic Search API returns details about an in progress or most recently completed call. See the API Programmer Guide for more information.

- Added localized PDFs for the User Guide in Chinese (Simplified and Traditional), Danish, Dutch, French, German, Korean, Portuguese (Brazil), and Spanish (European).

Updated Features

The following is a summary of the new features added to the 11.0 release.

- Desktop Configuration Administration has been renamed Recording Columns and now appears under Recordings > Interface Configuration.

- Export Recordings Administration has been renamed to Export Permissions and now appears under Recordings > Interface Configuration > Interface Settings.

- The roles and scope for the system reports in the Reporting application have changed as follows:

System Report	Old Roles	New Roles
Recording Access By User	Manager Archive User	System Administrator Telephony Administrator Archive User Manager
Recording Access By Contact	Manager Archive User	System Administrator Telephony Administrator Archive User Manager
User Recording Status	Supervisor	System Administrator Telephony Administrator Archive User Manager
System Status	Manager	System Administrator Telephony Administrator
Audit Trail	Not applicable	System Administrator

- Improved the scrubber on the Media Player.

- Updated the instructions for installing desktop applications. See "Installing Desktop Applications" in the Installation Guide.

- Updated the localized strings to the Cisco Workforce Optimization interface in Danish, Dutch, German, French, Italian, Portuguese (Brazil), Spanish (European), and Swedish

• Updated the localized help for Quality Management version 10.5(1) in Danish, Dutch, French German, Portuguese (Brazil), and Spanish (European).

• Included the localized help for Quality Management version 10.0 in Italian and Swedish. For the latest description of Quality Management 11.0 features see the English version of the Application Guide.

Deprecated Features

This release has no deprecated features.

Important Notes

Installation Notes

✏️

Note   Over the top upgrades from version 10.5 and earlier to 11.0 are not supported. All such upgrades must be manual. This means that the old version of Recording and Quality Management (but not your Recording and Quality Management database) must be uninstalled before the new version is installed. Over the top upgrades from 11.0 to newer versions of 11.0 are supported.

If you are upgrading from 10.5(1) SR4, note that the installation instructions has changed for web server redundancy. A Configure High Availability tool has been added to System Configuration (PostInstall.exe). See "Web Server Redundancy" in the Installation Guide for more information.

If you upgrading from 10.5(1) or earlier and you modified the recordingcontrols.properties file (for example, to limit the buttons that users can see) for Recording Controls, you must update the recordingcontrols.properties file after you install 11.0. The recordingcontrols.properties file has been updated to support new features.

Possible errors that might occur when you install 11.0(1) are as follows:

• If you upgraded from an 8.x system to 10.5 before 11.0, you will need to adjust the database entries after installing 10.5(1). To adjust the data base entries run the following command against the SQMDB in SQL:

```
update ServerPropertiesset
setting=100
where id='serverMaxConcurrentRecordings' and set=100
```

• If you notice that the associated call IDs are blank on some calls and that causes recording playback to fail, run the following SQL script in Microsoft SQL Server Management Studio:

```
UPDATE ccr SET associatedCallId=POWER(CAST(2 AS BIGINT),48) |
POWER(CAST(2 AS BIGINT),32) *
FLOOR(DATEDIFF(DAY,'1970-01-01',startTime) / 7) | icmCallId FROM ccr
WHERE associatedCallId=''
```

• If a "script missing" message appears when you install the SR, the Patches.xml file is corrupt. To work around this problem, delete the Patches.xml file in the webapps/TUP/<product> folder, and then run a repair on the base release from Add or Remove Programs. The repair on the SR will be initiated automatically.

For step-by-step installation and upgrade instructions, see the Installation Guide.

Multi-line Devices and Network Recording Service

- Multi-line devices must use the same Network Recording service for each extension

When configuring extensions on a single device for network recording, any extensions that are enabled for network recording must use the same Network Recording service. Quality Management Administrator associates a device with a recording service, so it cannot assign an individual extension with a separate recording service.

Restarting the Network Recording Service and Poor Quality

- Restarting the Network Recording service while performing network recording might cause poor quality audio

Calls that are active when the Network Recording service is stopped and are still active when the service is restarted might result in recordings that have poor-sounding audio.

To work around this problem, do not restart the Network Recording service while calls are active. Symptoms will persist until all the calls that were active when the Network Recording service was stopped have been disconnected.

"Stop running script" Message

The "stop running script" message appears when there are more than five widgets in your dashboard when using Microsoft Internet Explorer 8 or 9. If you use more than five widgets, the page becomes slow and unresponsive.

To work around this problem, upgrade to Microsoft Internet Explorer 10 or 11.

"script missing" Message When Installing an SR

The "script missing" message might appear when you install Quality Management. The message appears when the install attempts to modify a corrupted Patches.xml file.

To work around this problem, delete the Patches.xml file in the webapps/TUP/<product> folder, and then run a repair on the base release from Add or Remove Programs. The repair on the SR will be initiated automatically.

Long Fields Clear When Selecting Language

When you complete the fields on the Workforce Optimization Login page and then choose a language from the Language drop-down list, the login fields are cleared. To work around this issue, choose a language before you complete the remaining login fields.

Contact ID Search

- A search by Contact ID should ignore all other filters

Search Recordings only ignores the values for Specific Date and Date Range when you specify a Contact ID. If you include values for other search fields, the Contact ID you are looking for might not appear in the search results.

To work around this problem, use the Contact ID field alone or only with the Date Range and Specific Date fields that will be ignored. If you use one of the other filters the specified values need to match the data in the record for the search to be successful.

Last Call Attribution

- A call is attributed to the last user who logged into a phone configured for Hot Desking and MediaSense Recording

In this scenario, a Hot Desking agent receives a call. While the first Hot Desking agent is on the call, a second Hot Desking agent logs in to the same phone using an API tool. When the call ends, the Record server assigns the call to the second Hot Desking agent. There is no workaround for this issue.

Screen Recording Playback Memory Error

The generic memory error icon appears when you try to play back a recording that includes a screen recording.

When the generic memory error icon appears in the Screen window and the screen recording will not play back.

Adobe Flash Player displays the generic memory error icon when running in a very low memory environment. It indicates that the web browser does not have much memory available. For more information on the generic memory icon, go to: http://blogs.adobe.com/dekesmith/2012/06/07/what-is-the-gray-circle-with-an-exclamation-mark-or-ba

To work around this issue, close the web browser, then reopen the web browser and try again.

Supervisor or Manager Dashboard Access

- When a supervisor or manager accesses the Dashboard an error message appears

When you first access the Dashboard, the following error message appears:`The <range> is not valid`

Note that the value for each band changed from a range of numbers to a single integer in 11.0.

To resolve this issue, delete the existing Best Performers Widget and then create a new one. Or change the Band values in the widget from a range of numbers to a single integer.

Live Screen Monitoring Screen Flash

- The client PC flashes when Live Screen Monitoring is initiated

When you initiate Live Screen Monitoring, the client PC will flash black for a few seconds before establishing the connection.

To disable the flash:

1. Click Start, type services.msc in the search field, and then press Enter.

2. From the Services window, double-click Desktop Window Manager Session Manager.

3. Choose Disabled from the Startup type drop-down list and then click Apply. You will need to restart your client PC.

4. **Optional:** Disable the Desktop Windows Manager Session Manager if you do not want to restart your client PC.

Team Scores All Data Report Displays Non-configured Users

• The Team Scores All Data report displays non-configured users

When generating a report, the Agent field displays two instances of the same user. In the database, these are actually different users with the same name, only one user is configured and should be shown. There is no workaround for this issue.

Record Option Fails

• Record option in Recording Controls fails to tag and record the call

When issuing a Record option in Recording Controls, the API fails to record the call and mark the call as "agent tagged". There is no workaround for this issue.

Windows Aero Theme Not Supported

Live screen monitoring is based off the Microsoft Windows Desktop Sharing API. This same API is used by Microsoft Windows Remote Assistance. One limitation of the Microsoft Windows Desktop Sharing API is that it does not support the Windows Aero theme for the PC being monitored during the time when another PC is connected to and viewing that PC. Every time a user begins to live screen monitor your PC, Windows must automatically switch your PC to the Windows Basic theme. Once the live screen monitor session on your PC ends, Windows will automatically switch your PC back to the Windows Aero theme. Based on customer feedback, we changed the behavior in 10.5(1) SR5 so it would only switch to the Windows Basic theme once at the start of the Desktop Recording service. The Windows Basic theme will remain until the Desktop Recording service is stopped.

If this is not the desired behavior, choose one of the following work arounds:

• Configure your PC to always use the Windows Basic theme. Then when the QM Desktop Recording service starts it does not have to change to that theme since it is already in place.

• Disable the live screen monitoring feature in Monitoring and Recording Administrator by clearing the Enabled check box under Live Screen Monitor in the Interface Settings window under Recordings. This will disable live screen monitoring for all users. When live screen monitoring is disabled, it will not switch to the Windows Basic theme.

Live Screen Monitoring and Windows Remote Assistance

• Unable to connect to the PC using Windows Remote Assistance if Live Screen Monitoring is enabled

Cisco uses Windows Remote Assistance to provide the live screen monitoring session. You are only allowed to have a single incoming session per PC, so while the Live Monitoring service is in use, any attempts to connect to the PC will be denied. To workaround this issue, disable Live Monitoring or change it to only start the service when a Live Monitoring session is requested. If you are using the Windows Aero theme, every time a Live Monitoring session is requested, the agent's screen will change from Aero to Basic causing a screen flash.

Related Documents

- Cisco Unified Workforce Optimization Recording and Quality Management User Guide
- Cisco Unified Workforce Optimization Recording and Quality Management Quick Start Guide
- Cisco Unified Workforce Optimization Recording and Quality Management Administrator Guide
- Cisco Unified Workforce Optimization Recording and Quality Management Installation Guide
- Cisco Unified Workforce Optimization Recording and Quality Management API Programmer Guide
- Cisco Unified Workforce Optimization Recording and Quality Management Design Guide
- Cisco Unified Workforce Optimization Recording and Quality Management Integration Guide for CAD and Finesse
- Cisco Unified Workforce Optimization Error Code Dictionary
- Cisco Unified Workforce Optimization Recording and Quality Management Troubleshooting Guide

Removed and Unsupported Features

This release has no removed or unsupported features.

Third-party Software Impacts

This release has no third-party software impacts.

Caveats

- Caveat Queries by Product, on page 41

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 11.0

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=11.0(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=11.0(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco Finesse

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=283613135&rls=11.0(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco MediaSense

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=283613140&rls=11.0(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco Social Miner

https://tools.cisco.com/bugsearch/
search?kw=*&pf=prdNm&pfVal=283613136&rls=11.0(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=11.0(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=11.0(1)&sb=anfr&svr=4nH&srtBy=byRel&bt=custV