Release Notes for Cisco Hosted Collaboration Solutions for Contact Center, Release 11.0(1)

First Published: 2016-01-25

Last Modified: 2016-12-14

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

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

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

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

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

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

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

CONTENTS

CHAPTER 1

Introduction

These release notes describe new features and changes for Release 11.0(1) of and its solution components.

Change History

Date	Product Releases
July 05, 2016	11.0(2) EIM and WIM content has been updated
January 25, 2016	11.0(1) release notes for Cisco Hosted Collaboration Solutions for Contact Center
December 2, 2015	11.0(2) release notes for Cisco Unified CCE and Cisco Packaged CCE
September 10, 2015	Initial 11.0(1) release notes for all products.

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 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.

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 http://tools.cisco.com/security/center/publicationListing.x

CHAPTER 2

Cisco HCS for Contact Center

Change History

Release	Updates
Sept 15, 2017	Added notes on SQL Server Service accounts, calculating bucket intervals for abandoned calls, Tomcat version upgrade, and security policies for hardening contact center servers.
11.0(1)	Initial release

New Features

Live Data

Release 11.0(1) introduces Live Data reporting system for Cisco HCS for Contact Center. Unified Intelligence Center supports Live Data on the report viewer and on the Finesse desktop as gadgets.

Live Data Reporting System is a data reporting framework that processes real-time events with fast refresh rates and high availability. The Live Data Reporting System continuously pushes real-time updates to Unified Intelligence Center reporting clients as the event occur.

The Real Time and Historical Data flows are used to support existing stock and custom reports through the Administrative Workstation (AW) database.

The following four new reports use Live Data services:

- Agent
- Agent Skill Group
- Precision Queue
- Skill Group

Cisco Unified Intelligence Center Live Data report uses STOCK data source called Streaming data source in this release.

Cisco Virtualized Voice Browser

Release 11.0(1) introduces new optional component for Cisco HCS for CC, Cisco Virtualized Voice Browser. Cisco Virtualized Voice Browser (Cisco VVB) provides a platform for interpreting Voice XML documents.

When a new call arrives at the contact center, the VVB allocates a VXML port that represents the VoIP endpoint. Cisco VVB sends HTTP requests to Cisco Unified Customer Voice Portal (Unified CVP) VXML server. In response to HTTP request, the Unified CVP VXML server executes the request and sends dynamically generated VXML document.

Finesse IP Phone Agent

Finesse IP Phone Agent (IPPA) helps to access Finesse features on Cisco IP phones as an alternative to accessing Finesse through browser. Finesse IPPA supports less features than the Finesse desktop in the browser, but it does allow you to receive and manage calls if they are lost or do not have access to a desktop.

Precision Queue Enablement in a Hybrid Deployment

System administrators can enable precision queues for routing and queuing to Unified Communications Manager agents in a Unified CCE hybrid deployment.

Precision routing is available for the following deployment types:

- ICM Router/Logger
- ICM Rogger
- UCCE 4000 Agents Rogger
- UCCE 8000 Agents Router/Logger
- UCCE 12000 Agents Router/Logger

You cannot assign precision queue attributes to agents on a third-party Automatic Call Distributor (ACD). Precision queues support only Contact Center Enterprise agents.

Failover Enhancements

Outstanding dialogs terminate in the router during failure scenarios for Type 10 Voice Response Unit (VRU) peripherals. This process ensures that the system does not attempt to use and reserve agent resources without the ability to deliver a call. Outstanding Cisco Unified Customer Voice Portal (Unified CVP) Call Control and VRU Voice XML (VXML) dialogs terminate in the router in the following failure scenarios:

- Network connection loss between the VRU Peripheral Interface Manager (PIM) and Unified CVP
- Network connection loss between the VRU Peripheral Gateway (PG) and router
- Failure of the VRU PG
- Failure of the VRU PIM

For transient Device Management Protocol (DMP) failures that do not result in active VRU PIM failure, the router does not terminate the CVP call control dialogs. These dialogs can then be routed as soon as the DMP path gets established again.

Outstanding Media Routing NEW_TASK MR request dialogs terminate in the router in the following failure scenarios:

- Network connection loss between the MR PG and the router
- Network connection loss between the MR PIM and the application
- Failure of the MR PG
- Failure of the MR PIM

Endpoints for Agents and Callers

This release includes support for the following endpoints:

- 7821, 7841, 7861
- 8811, 8841, 8851, 8861, 8845, 8865

The 8845 and 8865 have video capability.

For the latest information on supported endpoints, check the *Unified CCE Solution Compatibility Matrix* at http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCE.

SQL Server Service Accounts

This release supports Network Service and Virtual account for SQL Server and SQL Server Agent Services. A privilege, Perform Volume Maintenance Tasks, is added to SQL service account if it is running with Network service or Virtual account.

The installer adds a warning message to the installer logs if that SQL server runs with other service accounts.

Updated Features

Shared Components Sub-Customer for Small Contact Center Deployment

In Release 11.0(1) small contact center deployment model uses shared contact center core components with two options based on the placement of peripheral components. Dedicated sub-customer Unified CM and peripheral gateways deployment supports up to 500 agents. In shared unified CM and peripheral gateway deployments the sub-customers can deploy on shared infrastructure within the contact center core.

There are two options that the sub-customer can choose according to the infrastructure.

- **Dedicated components sub-customer** - Dedicated Cisco Unified CM, Peripheral Gateway and Finesse sized for either 100 or 500 agents.
- **Shared components sub-customer** - Shared Cisco Unified CM, Peripheral Gateway and Finesse support up to 2000 agents across 100 department enabled sub-customers.

Note Context Service does not support small contact center deployment model.

Unified CCDM

HCS for CC Release 11.0(1) supports Unified CCDM 11.0(1) , this has enhanced user interface and new features that includes Gadgets and Apps feature and Multi-AD Support.

- Gadgets and apps features support multiple gadgets simultaneously, where you can view/edit the gadgets and Apps are used to save gadgets.
- Using Multi-AD Support you can have active directory for each sub customer.

CTI Server Message Protocol Version 19 Updates

The CTI Server Message Protocol Version 19 has the following added or updated messages:

- AGENT_STATE_EVENT
- AGENT_TEAM_CONFIG_EVENT
- CLIENT_SESSION_OPENED_EVENT
- CLIENT_SESSION_CLOSED_EVENT
- CONFIG_REQUEST_KEY_EVENT
- CONFIG_KEY_EVENT
- CONFIG_REQUEST_EVENT
- CONFIG_BEGIN_EVENT

- CONFIG_SERVICE_EVENT
- CONFIG_SKILL_GROUP_EVENT
- CONFIG_AGENT_EVENT
- CONFIG_DEVICE_EVENT
- CONFIG_CALL_TYPE_EVENT
- CONFIG_END_EVENT
- EMERGENCY_CALL_REQ
- EMERGENCY_CALL_CONF
- EMERGENCY_CALL_EVENT
- OPEN_CONF
- QUERY_AGENT_STATE_CONF
- RTP_STARTED_EVENT
- RTP_STOPPED_EVENT
- START_RECORDING_REQ
- START_RECORDING _CONF
- STOP_RECORDING_REQ
- STOP_RECORDING_CONF

New Security Policies for Hardening Contact Center Enterprise Servers

This release has new security policies for hardening Windows 2012 R2 Servers that run contact center enterprise solutions. For more information on these group policy settings, see the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

Tomcat Version Update

This release bundles a new version of Tomcat (7.0.62) to host CCE web applications.

Fixed Inconsistency in Calculating Bucket Interval Between Answered and Abandoned Calls

This release changes the calculation of bucket interval to make it consistent among answered and abandoned calls.

Starting in this release, Self Service time is not included in the bucket interval calculation for abandoned calls. The time is calculated only from the time the call is queued. This process is similar to the answered calls bucket interval calculation.

Deprecated Feature

No more engineering development will occur for these features. Deprecated features are scheduled for removal in a future release. Plan to transition to the designated replacement feature. If you are implementing a new deployment, use the replacement technology rather than the deprecated feature.

Please review applicable notes for details about exceptions or other qualifiers.

Deprecated Feature	Announced In Release	Replacement	Notes
"Half Hour" database tables: • Agent_Half_Hour • Agent_Skill_Group_Half_Hour • Call_Type_Half_Hour • Call_Type_SG_Half_Hour • Peripheral_Half_Hour • Service_Half_Hour • Skill_Group_Half_Hour	11.0(1)	Interval database tables	Start migrating any custom reports that use the half hour tables to the corresponding interval table.
CTI OS Agent Desktop	11.0(1)	Cisco Finesse	Deprecated for Unified CCE, Packaged CCE, and Cisco HCS for Contact Center. For the foreseeable future, support continues for Avaya (ACM and Aura), Aspect, and System PG.
CTI OS Supervisor Desktop	11.0(1)	Cisco Finesse	
CTI OS-Based Silent Monitoring	11.0(1)		
Cisco Agent Desktop	11.0(1)	Cisco Finesse	**Important** Cisco Agent Desktop 10.0(2) is the last version that Unified CCE will support.
Cisco Media Blender	11.0(1)	For Unified WIM and EIM, use the Script Editor to configure dialed number prefixes and filters for Agent Request.	
AAS for Symposium (SEI Interface)	11.0(1)		Interface retired by vendor.

Deprecated Feature	Announced In Release	Replacement	Notes
H.323 protocol support for Mobile Agent	11.0(1)	SIP protocol	
On-Demand Licensing Model for Unified CCE	10.0(1)	Cisco Hosted Collaboration Solution (HCS) for Contact Center	
CTI OS /LOAD Configuration Parameter	10.0(1)	CTI OS now sets the agent to NOT READY on CTI disconnect (whether desktop or server). The supervisor can force agents to sign out. You can also implement an inactivity timer that forces a sign-out in the agent desk settings configuration. **Note** This parameter was sometimes used in Unified CCE to force agents to sign out on CTI failures.	
Unified Intelligent Contact Management Hosted (ICMH) and Unified Contact Center Hosted (Unified CCH)	10.0(1)	Cisco Hosted Collaboration Solution (HCS) for Contact Center	

Important Notes

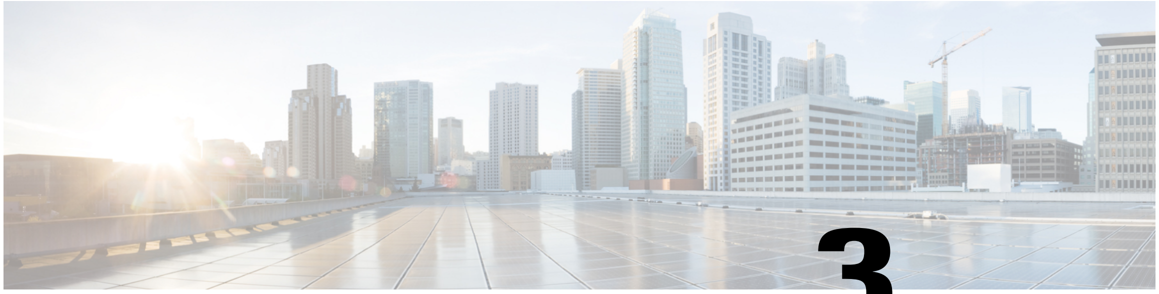
This release has no important notes.

Removed and Unsupported Features

This release has no removed or unsupported features.

Third Party Software Impacts

For more information about third-party software, see the http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Cisco_HCS_for_Contact_Center_11.0(1)



CHAPTER 3

Cisco Unified Customer Voice Portal

Change History

Release	Updates
11.0(1)	Initial release

New Features

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

Unified Call Studio

Set Value Element

In Release 11.0(1), Cisco Unified Call Studio includes a new element called the **Set Value** element which supports basic mathematical operations, and string operations using JavaScript. The Set Value Element allows you to define and assign values to local variables.

Rest_Client Element

Beginning with Unified CVP Release 11.0(1), the Integration element folder includes a new action element called the **Rest_Client**. The Rest_Client element uses REST APIs to send GET, CREATE, DELETE, and UPDATE requests to the application server.

Unified CVP Utility for Java Scripts

Beginning with Unified CVP Release 11.0(1), Cisco Unified Call Studio includes the following utilities:

- XPath Expression—This utility allows you to use XPath expressions in JavaScript to return values from the XML.
- JSONPath Expression—This utility allows you to use JSONPath expressions in JavaScript to return values from the JSON(JavaScript Object Notation).
- Date Validation—This utility allows you to validate the date in JavaScripts on local variables.
- Time Validation—This utility allows you to validate the time in JavaScripts on local variables.

For more information about new features and elements for Unified Call Studio, see *Element Specifications for Cisco Unified CVP VXML Server and Cisco Unified Call Studio* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html.

Call Stack History View

This is a new view in Cisco Unified Call Studio. The information that previously appeared in the **Variables** view now appears in a new view called the **Call Stack History** view. The **Call Stack History** view displays information about the variables that are associated with the stack frame that you selected in the **Debug** view. Click an element in the **Editor** view to view the corresponding data variables in the **Call Stack History** view. In addition, Java objects can be expanded to show the fields. The data variables that are displayed in the **Call Stack History** view can be edited.

Updated Features

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

Platform Updates

In Release 11.0(1), Unified CVP requires Microsoft Windows 2012 R2 Standard Edition. For more information, see the *Compatibility Matrix for Unified CVP DocWiki* at http://docwiki.cisco.com/wiki/Unified_CVP_Software_Compatibility_Matrix_for_11.0%28x%29.

Platform Common Ground Upgrade

Unified CVP 11.0(1) allows in-place operating system upgrades to Microsoft Windows 2012 R2 Standard Edition followed by upgrade of Unified CVP from previous releases. For more information, see the *Installation* *and Upgrade Guide for Cisco Unified Customer Voice Portal* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

ESXi Release 5.5 Support

Support for ESXi Release 5.5 is now available.

VMware Requirement

In Release 11.0(1), Unified CVP requires VMware version 9 Compatible with ESXi 5.1 and later. For more information about upgrading the VMware hardware version, see the Upgrade the Existing Unified CVP Virtual Machine section in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

IBM Informix Support

IBM Informix database server 12.10 FC3 is installed as part of the Reporting Server 11.0(1).

Deprecated Features

No more engineering development will occur for these features. Plan to transition to the designated replacement feature. If you are implementing a new deployment, use the replacement technology rather than the deprecated feature. Deprecated features are scheduled for removal in a future release.

Deprecated Feature	Announced In Release	Replacement	Notes
Unified Intelligent Contact Management Hosted (Unified ICMH) and Unified Contact Center Hosted (Unified CCH)	10.0(1)	Cisco Hosted Collaboration Solution (HCS) for Contact Center	

Important Notes

There are no important notes for this release.

Removed and Unsupported Features

The following feature is no longer available.

Feature	Effective from Release	Replacement
Key Press Markup Language	11.0(1)	No replacement is available.

Third-Party Software Impacts

For more information about third-party software, see the http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Cisco_HCS_for_Contact_Center_11.0(1).

CHAPTER 4

Cisco Finesse

Change History

Release	Updates
11.0(1)	Initial release

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 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.

Outbound Option Direct Preview Calls

Finesse Release 11.0(1) supports Outbound Option Direct Preview calls. When a Direct Preview call arrives on the Finesse desktop, the agent can do one of the following:

- Accept the call—If the agent accepts the call, the call is placed from the agent's phone. If the agent does not reach the customer, the agent can reclassify the call using one of the following options:
  - Voice
  - Answering Machine
  - Fax/Modem
  - Invalid Number

  Note The Busy classification is not supported.

- Decline the call—If the agent declines the call, the agent can either reject the contact and return it to the campaign or close the contact and remove it from the campaign.

Log Collection Using Cisco Unified Real-Time Monitoring Tool

Finesse supports the Unified Real-Time Monitoring Tool (RTMT) for log collection. Finesse supports RTMT only for log collection; other RTMT features are not supported. For more information, see the *Cisco Finesse Administration Guide* (at http://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html), and the *Managed Service Guide for Cisco Unified Communications Manager* (at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html).

SQL User Authentication

Finesse now supports connections to the AW database (AWDB) using SQL authentication as an alternative to Windows authentication. Users must have at minimum read access to the database.

IPv6

Cisco Finesse supports IPv6 using dual stack (IPv4 and IPv6). By default, only IPv4 is enabled at installation. You can enable IPv6 after installation using either Cisco Unified Communications Operating System Administration or the CLI. For details, see the *Cisco Finesse Installation and Upgrade Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

To sign in using IPv6, you must include the HTTP or HTTPS port number in the URL.

Finesse Interface	IPv6 HTTPS URL	IPv6 HTTP URL
Administration Console	https://<*FQDN*>:8445/cfadmin	http://<*FQDN*>:8082/cfadmin
Agent Desktop	https://<*FQDN*>:8445/desktop	http://<*FQDN*>:8082/desktop

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.

Item	Maximum	Notes
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.)

Cisco Finesse Tomcat

The Cisco Tomcat service on Finesse has been renamed to Cisco Finesse Tomcat. As a result, CLI commands that referred to Cisco Tomcat now refer to Cisco Finesse Tomcat, for example: **utils service start Cisco Finesse Tomcat**.

Port Utilization for Cisco Finesse Tomcat and Third-Party (External) Web Server

Cisco Finesse Tomcat HTTP port is changed from 8080 to 8082, and the HTTPS port is changed from 8443 to 8445. The same port usage updates also apply to the third-party (external) web server.

SystemInfo Object Support for peripheralId

The Finesse SystemInfo object now displays the peripheralId value of the peripheral to which Finesse is connected.

Aligned Partitions Support

Finesse 11.0 now supports aligned partitions, but only with a fresh installation.

If you perform an upgrade from a previous release, the platform detects the unaligned partitions and displays the following error:

```
ERROR-UNSUPPORTED: Partitions unaligned
```

Cluster Settings Gadget Now Supports Hostname Only

To specify the secondary Finesse Server in the Cluster Settings gadget, you can now enter only the hostname of the secondary server. The gadget no longer supports IP address entries.

Localization of Wrap Up Reasons, Call Variables, and ECC Variables

Call Context data (Wrap Up Reasons, call variables, and ECC variables) is Unicode enabled and independent of the desktop locale.

The following restrictions apply to Call Context data with localized characters.

Variable	Limit
Wrap-Up Reasons	Limited to 40 bytes of UTF-8 data.
Call Variables 1-10	Limited to 40 bytes of UTF-8 data. **Note** If Finesse sends a set call data request that exceeds 40 bytes of data, the request fails.
ECC Variables	

If any of the limits in this table are exceeded, the variable data is truncated. This is more likely with localized characters that occupy more than one byte in size (for example, characters with an accent require two bytes to store one character and Asian characters require three or four bytes).

Deprecated Features

This release has no deprecated features.

Important Notes

Cisco Finesse Installation

Cisco Finesse is installed on a virtual machine (VM) and runs on the Cisco Unified Voice Operating System platform, similar to Cisco Unified Communications Manager. This platform does not support navigation into, or manipulation of, the file system.

To install Finesse, you must first obtain the Finesse installer and the Cisco Finesse Open Virtual Archive (OVA) file. You can obtain the Cisco Virtual Server (OVA) files needed to create a Virtual Machine from http://www.cisco.com/cisco/software/type.html?mdfid=283613135&flowid=30701.

Important DNS client configuration is mandatory for Cisco Finesse. During the installation, you must select Yes on the DNS Client Configuration screen and specify the DNS client information. If you fail to complete this step, after the installation is complete, agents will not be able to sign in to the desktop. You will need to reinstall Finesse.

You can find detailed installation instructions in the *Cisco Finesse Installation and Upgrade Guide* at http://www.cisco.com/en/US/products/ps11324/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.

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.)

Conference Limitations

An agent or supervisor who signs in to the Finesse desktop while on an active conference with other devices (which are not associated with another agent or supervisor) may experience unpredictable behavior with the desktop because of incorrect call notifications. These limitations also encompass failover scenarios where failover occurs while an agent or supervisor is participating in a conference call. When failover occurs and the agent is redirected to the alternate Finesse server, that agent may see unpredictable behavior on the desktop. Examples include (but are not limited to):

- The desktop does not reflect all participants in the conference call.
- The desktop does not reflect that the signed-in agent is in an active call.
- Finesse receives inconsistent call notifications.

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.

Retrieve Button on Finesse Triggers Conference with BiB on EX90

An agent is using the Finesse desktop and EX90. The agent places a call on hold and makes a consultation call to another agent. When the agent clicks the Retrieve button on the Finesse desktop to go back to the original call, the action triggers the Built-In Bridge (BiB) on the EX90. To prevent this, the agent can click the Hold button to place the consultation call on hold and then click Retrieve to go back to the original call.

Cisco Jabber for Windows

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

- 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.

Related Documentation

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.

CHAPTER 5

Cisco Unified Intelligence Center

Change History

Release	Updates
11.0(1)	Initial release

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.

Unified Intelligence Center Live Data for Unified Contact Center Enterprise

Release 11.0(1) introduces Live Data reporting for Unified Contact Center Enterprise (Unified CCE). Unified Intelligence Center supports Live Data on the report viewer and on the Finesse desktop as gadgets.

The following four new reports use Live Data services:

- **Agent**
- **Agent Skill Group**
- **Precision Queue**
- **Skill Group**

Cisco Unified Intelligence Center Live Data report uses STOCK data source called Streaming data source in this release.

In a Packaged CCE deployment, this datasource is preconfigured as part of install.

To configure streaming datasource in a Unified CCE deployment, refer to *Live Data Services Registration* section in Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, Release 11.0(1) http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

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.

IPv6

Unified Intelligence Center supports IPv6 using dual stack (IPv4 and IPv6). By default, IPv4 only is enabled at installation. You can enable IPv6 after installation using the CLI or from Cisco Unified Intelligence Operating

System Administration page. For more information, see the *Administration Console User Guide for Cisco Unified Intelligence Center, Release 11.0(1)*.

Upgrade to 11.0(1)

For upgrades from Unified Intelligence Center 10.x to Unified Intelligence Center 11.x, apply the Cisco Options Package (COP) patch file `ciscocuic.refresh_upgrade_v1.3.cop.sgn` before beginning the upgrade process.

Note To perform an upgrade of Unified Intelligence Center to 11.x, you must first upgrade to 10.x from the previous versions and then upgrade to 11.x. For more information on refresh upgrade, see *Installation and Upgrade Guide for Cisco Unified Intelligence Center 11.0(1)*.

Updated Features

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

Grid Enhancements

In this release, Cisco Unified Intelligence Center provides you with new grid features on the report viewer for historical reports. In the reporting grid you can perform dynamic field selection, resize columns, sorting, expand, and collapse of grouped data. For more information on the new grid, see *Cisco Unified Intelligence Center User Guide, Release 11.0(1)* and to customize the reports on the new grid, see *Cisco Unified Intelligence Center Report Customization Guide 11.0(1)*.

Stock Report Templates

When you perform an upgrade of Unified Intelligence Center to 11.0(1), use the latest Unified Intelligence Center stock template file **Templates_CUIC_11.0_AS_11.0.zip**. The latest stock report template file is available here https://software.cisco.com/download/type.html?mdfid=282163829&catid=null

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).

CHAPTER 6

Cisco MediaSense

Change History

Release	Updates
11.0(1)	Initial release

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 7

Cisco Remote Silent Monitoring

Change History

Release	Updates
11.0(1)	Initial release

New Features

The following sections describe new features for Cisco Remote Silent Monitoring, Release 11.0(1).

Platform Upgrade to Windows 2012 R2 Standard Edition

RSM 11.0(1) requires Windows 2012 R2 Standard Edition. The Windows OS requirements and the VMware requirements are as follows:

- VMWare ESXi 5.5
- Two virtual CPU cores with 2.13-GHz Reservation
- 4-GB virtual RAM

- One 75 GB virtual Disk
- One virtual NIC with both IPv4 and IPv6 enabled
- Windows 2012 R2 Standard Edition

Note Support for Windows 2008 R2 is deprecated with the RSM 11.0(1) version.

Support for IPv6 Endpoints

In addition to IPv4 only endpoints, RSM 11.0 also supports IPv6 only or dual stack (IPv4 and IPv6) endpoints.

Precision Queue (PQ) Based Monitoring in RSM APIs

Updated Features

There are no updated features for Cisco Remote Silent Monitoring, Release 11.0(1).

Deprecated Features

There are no deprecated features for Cisco Remote Silent Monitoring, Release 11.0(1).

Important Notes

The following sections are important notes for Cisco Remote Silent Monitoring, Release 11.0(1).

Anti-Virus Software Requirements

RSM requires the use of one of the following Cisco-approved anti-virus software:

- Trend Micro ServerProtect 5.7
- McAfee VirusScan Enterprise 8.7i
- Symantec Endpoint Protection 11.0

Refer to Chapter 2, "Cisco Hardware and Software Requirements", of the *Cisco Remote Silent Monitoring Installation and Administration Guide* for BOM information.

RSM CVP Comprehensive Call Flow Script Support

RSM 9.1(1) and above uses RTSP in CVP call flow script. You can set up the RSM CVP Script using RTSP in either Standalone or Comprehensive mode. The Comprehensive Call Flow setup using UCCE/ICM requires an IOS version that resolves a media loop issue in VXML Gateway. (Refer to related defect, CSCul89581.)

Maximum Configured Agents with CTI OS Integration

For Unified CCE, RSM can support a Java CIL-based, CTI OS integration with up to 8,000 configured agents on each PG. If the number of configured agents on a PG exceeds 8,000, the RSM VLengine service fails to stay connected with the CTI OS Server. To overcome this CTI OS limitation, use a Unified CCE CTI integration in RSM 10.0(1).

Cannot Monitor Agent Greeting or Whisper Announcement

RSM does not support monitoring the Agent Greeting or Whisper announcement portion of a call. RSM can establish a monitoring (BIB) call only after receiving a Call Established event, which comes after the initial Agent Greeting and Whisper announcements.

Cannot Monitor Simphones from Supervisor Desktop

Currently, you cannot monitor RSM simulated supervisor phones (that is, simphones) from a Cisco Supervisor Desktop (CSD). The simphones are purposefully added to the Communications Manager platform with their BIB (built-in-bridge) disabled.

Fail-Over Redundancy and Load Balancing with CVP

Currently, RSM does not support load balancing and clustering if CVP is used as a VRU.

For this purpose, load balancing means the association of multiple RSM servers so that the incoming request load is distributed among them. By contrast, fail-over redundancy means the association of RSM servers so that if one fails, the others act in its place.

Mobile Agent Not Supported

RSM uses the Unified Communications Manager (Unified CM) monitoring mechanism, which currently does not support Cisco Mobile Agent monitoring. Therefore, RSM does not support monitoring Mobile Agents.

Multiple Unified CM Clusters Must Use Same Version

If you configure a single RSM server to use Unified CM multiple clusters, each cluster’s constituent servers must run the same version of Unified CM. Because of JTAPI libraries between versions, attaching to multiple clusters running different versions of Unified CM is not supported.

Supported IP Phones with Unified CCE

Agents must use a third-generation or later Unified CCE-supported IP phone with RSM. (Unified CCE does not support Personal Communicator.) Supported phones include: 7906G, 7911G, 7921G (Aug 08 upd), 7925G, 7931G, 7941G-GE, 7942G, 7945G, 7961G-GE, 7962G, 7965G, 7970G, 7971G-GE, 7975G, 6900, and IP Communicator 7.0(1) and later.

Unsupported phones include: 7910, 7912, 7940, and 7960.

All new phones are supported. For phone support information, see the Unified CCE Solution Compatibility Matrix at http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCE.

Cannot Monitor Encrypted Calls

RSM does not allow for the monitoring of encrypted calls.

Transfers and Alternate Call Monitoring

Transfers and alternate calls require manual intervention to continue monitoring. RSM does not do this switch automatically. When an agent starts a consult call, RSM stops monitoring the customer call, which is now on hold, and starts monitoring the consult call, if desired. When the agent transfers the call to another agent, the RSM monitoring session is terminated.

Agent Monitoring When Not Talking or on Hold

If the agent puts a call on hold while a supervisor is monitoring, the monitoring session is kept alive during the hold period. If the supervisor exits out of the monitoring session by pressing * or 1 for information or instructions, then they cannot resume monitoring. This situation is due to BIB functionality, where you can only establish a monitoring call when the agent is in a talking state. You can only monitor an agent with RSM when they are talking on a call. You cannot monitor the agent while on hold or not on a call. Calls on hold before the supervisor begins a monitoring session are not included for monitoring. The VLEngine filters these calls from being monitored by any of the IVR options (for instance, agentid, skill group, newest call, random call, or list of talking agents).

Monitoring Sessions for Each Agent

If a dialed-in supervisor attempts to monitor an agent who is at the monitoring call limit, the request is denied. An audio prompt feedback from the system states that the agent cannot be monitored. Unified CM provides for one active monitoring session for each agent. The agent's phone can handle only one active monitoring session and one active recording session at any given time. If a third-party recorder is recording the agent's conversations, a supervisor can still monitor the agent through the supervisor desktop or RSM. However, if a RSM-based supervisor and a supervisor desktop-based supervisor both try to monitor the agent simultaneously, the request fails. RSM sets up only one monitoring session through Unified CM for an agent, even if two or more RSM users request to monitor the agent's call at the same time. In this case, RSM forks the stream to cover all RSM users, so that more than two RSM-based supervisors can monitor the same agent. However, if there are multiple RSM servers in the environment that monitor the same agent, each server makes a separate monitoring call to that agent.

Bandwidth Requirements

The agent IP phone must have sufficient bandwidth available to the RSM server for the monitoring voice stream and the regular voice streams for the call. This requirement is important for employees who work remotely and in small branches on limited bandwidth. Regular Call Admission Control (CAC) and bandwidth calculations are applicable for monitoring calls.

G.711 a-law, G.711 mu-law, and G.729 are the supported codecs for monitoring calls between agent IP phone and RSM server (phonesim). Use the Cisco TAC Voice Bandwidth Codec Calculator for extra bandwidth capacity planning at http://tools.cisco.com/support/vbc/jsp/codec_calc1.jsp.

VLEngine and Email Alerts

Currently, the VLEngine service does not support the sending of email alerts in error situations.

Cannot Monitor Calls Before VLEngine Service Starts

RSM does not support monitoring calls that are established before the RSM VLEngine service starts. RSM can only monitor calls that start after the VLEngine starts up.

Removed and Unsupported Features

There are no removed or unsupported features for Cisco Remote Silent Monitoring, Release 11.0(1).

Third-Party Software Impacts

There are no third-party software impacts for Cisco Remote Silent Monitoring, Release 11.0(1).

CHAPTER 8

Cisco Unified Web and E-Mail Interaction Manager

Change History

Change	See	Date
Updated Upgrades to Relase 11.0(1) to add 9.0(2) ES9	Upgrades to Release 11.0(1), on page 43	December 22, 2016
Updated Server Requirements	Updated Server Requirements, on page 44	June 1, 2016
Updated User Desktop Requirements	Updated User Desktop Requirements, on page 44	

New and Updated Features

New Features

Deployment and Configuration

Integrate with Unified CCE from the Administration Console

Administrators can now integrate Unified EIM and WIM with Unified CCE from the Administration Console. Administrators can also import and map Unified CCE objects from the Administration Console. All business object management is now done through the user interface. (In previous releases, these tasks were done using the UI Configuration Wizard, which required access to a server.)

Be aware that once you enable integration, configure an application instance, select an Agent PG, and save, you change the deployment from a nonintegrated system to an integrated one. This operation is not reversible (that is, you cannot revert to the nonintegrated system).

Configure Dynamic Messages for Integrated Chats from the Administration Console

A Dynamic Run Application Script Request (DRASR) allows you to display wait messages with dynamic text (such as expected wait time) to customers while Unified EIM and WIM and Unified CCE integrated systems process chat and call requests. You can use ECC variables and call variables to display the dynamic content.

Partition administrators can configure these wait messages from the DRASR node in the Administration Console.

New Settings in the Administration Console

Partition administrators can now configure the following new settings from the Administration Console:

- Proactive monitoring refresh interval (seconds)
- Chat watchdog interval (seconds)
- Reason code for Agent Not Ready
- Alert agent when non-interruptible activity is assigned
- Maximum wait time for login response from UCCE (seconds)
- Enable eGain-picks-the-agent routing
- Enable chat queueing
- Starvation time for activities
- Media class names
- Agent availability settings after completion of call

For details about each setting, see the *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Administration Console* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-email-interaction-manager/products-maintenance-guides-list.html.

Updated Features

Agent Experience

Changes to Pick, Pull, and Transfer

Integrated agents can now:

- Transfer more than one email activity to another integrated user or queue at one time
- Transfer emails to agents who have not made themselves available to receive work
- Pick more than one email activity from another integrated user or queue at one time
- Pick email activities that are queued in Unified CCE
- Pick email activities from another integrated user who is not logged in to the application

Deployment and Configuration

Refreshed Templates for CallBack

A modern, completely redesigned template set, named Rainbow, is available out-of-the-box for call back.

Improved Routing for Chat

Auto-pushed back chats are now placed at the top of the External Agent Assignment Service (EAAS) queue. (In previous releases, integrated chat activities that were auto-pushed back to the queue were placed at the queue's end.)

Platform

Upgrades to Release 11.0(1)

The Unified EIM & WIM Release 9 installation must be on one of the following versions for you to be able to upgrade to Unified EIM & WIM 11.0(1):

- 9.0(1): ES1 to ES3
- 9.0(2): ES1 to ES8
- 9.0(2): ES9

Note To upgrade from ES9 you must have the latest media from Cisco.

Please contact your Cisco representative for additional information.

Updated Server Requirements

This release requires newer versions of the following software to deploy Unified WIM and EIM:

- Wildfly 8.2.0
- JDK 1.8, Update 65 (64 bit)

For instructions about installing these requirements, see the *Cisco Unified Web and E-Mail Interaction Manager Upgrade Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-email-interaction-manager/products-installation-guides-list.html.

Updated User Desktop Requirements

Unified WIM and EIM Release 11.0(2) requires one of the following versions of Internet Explorer:

- Internet Explorer 11 (Compatibility Mode)
- Internet Explorer 10 (Compatibility Mode)

No other browser or version is supported.

Deprecated Features

This release has no deprecated features.

Important Notes

This release has no important notes.

Removed and Unsupported Features

This release has no removed and unsupported features.

Third-Party Software Impacts

There are no third-party software impacts for Unified WIM and EIM Release 11.0(2).

CHAPTER 9

Cisco Virtualized Voice Browser

Introduction

Cisco Virtualized Voice Browser (VVB) is designed to facilitate concurrent multimedia communication processing.

The Cisco VVB provides following features:

- Facilitates self-service options such as access to check account information or user-directed call routing, by processing user commands through touchtone input or speech-recognition technologies
- Allows customers to retrieve the required information through voice commands without interacting with an agent, to navigate to the correct department, or to get help from an agent
- Provides multilingual support for Cisco VVB server prompts, for automated speech recognition (ASR) and text-to-speech (TTS) capabilities
- Provides more comprehensive and effective customer service by efficiently handling call traffic with self-service or fast transfer to the correct agent the first time.

This document describes new features and limitations for Cisco VVB Release 11.0(1).

Feature Set

Cisco VVB Administration Console

This administration console is used to manage and configure Cisco VVB.

Prompts Management

This console stores prerecorded prompts such as custom prompts on Cisco VVB.

Application Management

This management console helps to create applications and assign triggers to invoke the application when the specific dialed number (DN) is dialed.

Media Handling

Cisco VVB supports G.711 U-Law and A-Law codec for prompts and supports in-band Dual Tone Multi-Frequency (DTMF) detection using RFC 2833.

Language

The current version only supports English language.

SIP Support

Cisco VVB supports Session Initiation Protocol (SIP) for call signaling.

HTTPS Support

Cisco VVB supports HTTPS secure connection.

CCB Support

Cisco VVB supports Courtesy Call Back (CCB) feature as implemented in Unified CVP.

Template-Based Configuration Support

Cisco VVB supports template-based configuration from Unified CVP Operations Console using pre-defined template.

VXML compliance

For the complete list of supported VXML tags and attributes, see *Developers Guide for Cisco VVB*.

CVP Compliance

Cisco VVB is fully compliant with VXML that is generated by the Cisco Unified Call Studio application running on Unified CVP Server. For more information on Call Studio elements, see *Element Specifications for Cisco Unified CVP VXML Server and Cisco Unified Call Studio.*

ASR/TTS Server Compliance

Cisco VVB uses Media Resource Control Protocol (MRCP) to communicate with speech servers to enable Text-To-Speech (TTS)/Automated-Speech-Recognition (ASR) functionality. Cisco VVB currently supports MRCPv1.

CVP Call Flows

- Standalone—The VXML Server (standalone) functional deployment model provides organizations with a standalone IVR solution for automated self-service.

- Comprehensive—The Comprehensive functional deployment model provides organizations with a method to route and transfer calls across a VoIP network to offer IVR services, and to queue calls before they are routed to a selected agent. Cisco VVB supports the Unified Call Studio application and the Unified CVP microapp in comprehensive calls.

Serviceability

- Real-Time Reporting Tool (RTR)—This tool helps to generate reports that provide detailed information about the status of your Cisco VVB system.
- Real-Time Monitoring Tool (RTMT)—This tool helps to monitor system performance, device status, device discovery, CTI applications, and voice-messaging ports. RTMT can connect directly to devices via HTTPS to troubleshoot system problems.

Administrator CLI Support

Cisco VVB supports command line interface for administration. You can use administrative credentials to access admin CLI and perform operations like set, show etc. for status and statistics.

Primary / Secondary VXML Server Support

Cisco VVB supports primary and secondary VXML server for standalone flows.

Whisper Agent and Agent Greeting / Agent Recording Support

Cisco VVB supports agent recording, whisper agent, and agent greeting feature.

UCS-E Single wide and double wide blade support on 4451 router

Cisco VVB is supported on Cisco UCS-E blades (both single and double wide variants). A customer should have 4 CPU and 8 GB RAM to deploy the VVB OVA template. By default, UCS-E blades comes with 8 GB RAM in which 1.5 GB is used by ESX platform. So the customer should add additional 8 GB RAM in the bladed to deploy VVB.

OVA Specifications

Capacity	vCPU	vRAM	vDisk	vNIC
600 ports	4 (each 900 MHz)	8 GB	2 x 146 GB	1

Updated Features

There are no updated features in this release.

Limitations and Restrictions

This section describes important limitation, restriction, and workaround that apply to this release.

The following features are not supported:

- MRCPv2
- RTSP streaming
- VXML 2.1

Third-Party Software Impacts

For more information about third-party software, see the Cisco Hosted Collaboration Solution for Contact Center Compatibility Matrix DocWiki

CHAPTER 10

Unified Contact Center Domain Manager

New Features

IPV6 Support

Release 11.0(1) for Unified CCDM uses IPv6 addressing to handle web traffic. System infrastructure and domain controller must be configured to handle IPv6 addressing.

Web Services Support

Unified CCDM 11.0(1) provides the following Web Service APIs to be used by third party client applications.

- Resource Management Web Service APIs - that allows client applications to invoke provisioning operations on the underlying equipment and to create system resources.
- Subscriptions APIs - that allows client applications to receive notifications when specified Unified CCE items change state.

For more information about the web services, see *Web Services Reference for Cisco Unified Contact Center Domain Manager.*

Unified CCE, Unified CM and Unified CVP Support

Unified CCDM 11.0(1) supports the following new versions of Cisco Unified Communications products.

- Unified CCE 10.0, 10.5 and 11.0
- Unified CM 10.0, 10.5 and 11.0
- Unified CVP 10.0, 10.5 and 11.0

Updated Features

Improvements to Resource Manager Gadget

In release 11.0(1) the method to enable ISE for a user has changed. To enable ISE for a user, perform the following:

- To edit a user, check the ISE enabled check box. The ISE password field appears.
- Enter the ISE password.

ISE will now be enabled for the user. The ISE Password field will not appear if the system is in SSO mode.

Enhancements to Installation and Configuration

CCDM 11.0(1) release has changes to trust relationships.

- A two way trust relationship is required between Unified CCE and CCDM.
- A two way trust relationship is required between the customer domain and where the CCDM server is configured.

Deprecated Features

This release has no deprecated features.

Important Notes

Windows 2012 and SQL Server 2014

This release of CCDM requires Windows 2012 R2 and SQL Server 2014, 64-Bit, Service Pack 1. Before installing Unified CCDM 11.0, the servers must be completely rebuilt. In-situ upgrades are not supported. For more information, see the http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

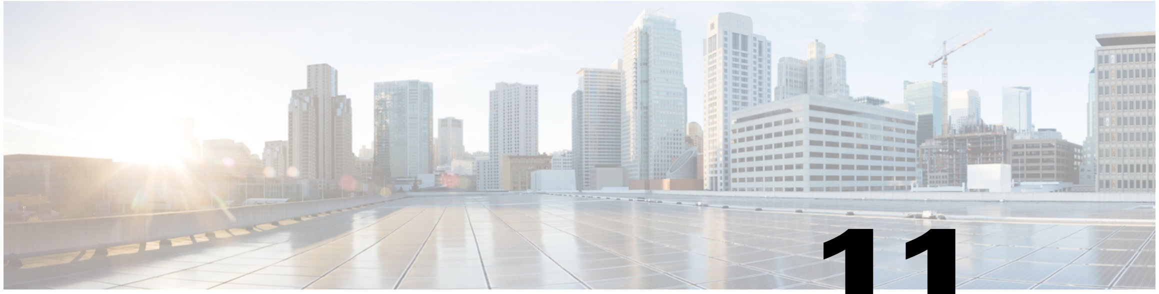
ICE Error

When you open ICE for the first time after an upgrade from CCDM 10.5 or earlier, you may see the following error message for one or more types like **Type Mappings Missing**.

To fix these type of errors, open **ICE**, select the **Cluster Configuration** tool. Start the **Setup UCCDM Servers** wizard and click **Next** repeatedly to work through the steps in the wizard without changing any of the settings. When the wizard completes, the errors will be cleared, save the changes.

Removed and Unsupported Features

This release has no removed or unsupported features.



CHAPTER 11

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 11.0

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 Hosted Collaboration Solution for Contact Center

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284526699&rls=11.0%281%29&sb=anfr&svr=3nH&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 Unified Customer Voice Portal

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=270563413&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 Remote Silent Monitoring

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=272901421&rls=11.0(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco Unified Web and E-Mail Interaction Manager

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=280970910&rls=11.0(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV

Cisco Virtualized Voice Browser

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=286290211&rls=11.0%281%29&sb=anfr&bt=emCstV

Cisco Unified Contact Center Domain Manager

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=280810493&rls=11.0(1)&sb=anfr&svr=3nH&srtBy=byRel&bt=custV