UCCX 11.6 Pre-Release Communication

Contents

Introduction

This document describes the UCCX 11.6 Pre-Release communication.

> **Note**: The Unified Contact Center Express (UCCX) 11.6 release is a very important release with important updates to critical features and serviceability updates that will help partners and customers. This pre-release communication provides an overview of critical updates and important information that helps to plan a quick, smooth upgrade to UCCX 11.6.

Background Information

UCCX 11.6 has a number of features aimed to enhance the product feature set and productivity of agents, supervisors and administrators. Major updates have gone in the email, chat functionality while updates to the Cisco Unified Intelligence Center (CUIC) reporting and Finesse Desktop

updates greatly enhance the experience of the contact center users. Important serviceability updates such as the Context Service Dashboard have been added too while updates have been made to the system to provide benefits such as reduced time taken for upgrades

A summary of the new features (refer to the release notes for a detailed list):

Cisco Finesse	UCCX Email	UCCX Chat	CUIC a Report
• Direct Transfer • Agent States based on secondary line • Display Reason Code labels by default • Enhanced Finesse Failover • Recent Call History and Agent State reports • Queue Statistics for FIPPA • Ability to make call from READY state • Ability to monitor Outbound call on ACD line • Supervisor Historical Reports • System Generated Reason Codes as labels for agents and ability to modify System Generated Reason Code labels	• Email cc/bcc/forward • Reply and Reply-all • Email Signature • GMAIL support • Wrap-up reasons • Multichannel Agent Summary Report	• Group Chat • Wrap up reasons • Chat Scheduler to have open and close hours • Typing Indicator • Multichannel Agent Summary Report	• New Dash s • New Chart view updat • Wrap reaso repor chat a email • Multic el Ag Sumr Repo
Scripting Enhancements	**Outbound Campaign Enhancements**	**SSO**	**Othe**
• Header and Proxy support for Make REST call • Get Reporting Statistic step to allow for agents to be counted based on Not Ready Reason Code • New Create JSON Document step • New JSON Document Data step • Context Service based IVR scripts added as templates • TLS 1.2 support	• Ability to save the explicitly stated order of fields in the contact list imported. • Automatic import of contact lists thorugh SFTP or HTTP server	• Integrated Windows Authentication • Qualification of 4 new IDPs and generic SAML 2.0 support	• ESXi suppo • TLS updat • Impro Upgra times • Supp Hype

Prepare for UCCX 11.6 Upgrade

UCCX 11.6 supports direct upgrades from these paths:

10.x	11.0	11.5
10.5(1)SU1	11.0(1)	11.5(1)
10.6(1)	11.0(1)SU1	11.5(1)SU1
10.6(1)SU1		
10.6(1)SU2		

Any Engineering Specials (ES) applied on the above versions does not affect the upgrade path,

the upgrade can be performed from any of the above versions irrespective of which ES is installed on the system. If there is a software release after the publication date of this document, check the UCCX Software Compatibility Matrix to verify the availability of an upgrade path.

SocialMiner Upgrade and Microsoft Exchange

The UCCX interacts with SocialMiner for all email and chat functionality. The 11.6 upgrade should be planned to ensure that both the UCCX and the SocialMiner servers are upgraded to 11.6 in the same maintenance window. In UCCX 11.6, the email and chat features have undergone major updates. Using these features of UCCX 11.6, with SocialMiner still on 11.5, has unexpected results and errors/warnings are displayed.

The recommended sequence for upgrade is to upgrade the SocialMiner server and the UCCX server(s) in the same maintenance window.

UCCX 11.6 solution supports **Microsoft Exchange Server 2013 and 2016 - Enterprise and Standard Edition** for the UCCX Email functionality. If you use **Microsoft Exchange Server 2013**, ensure to install Cumulative Update 15 for Exchange Server 2013 (KB3197044) so that TLS 1.2 is supported by Exchange. Without this patch, the communication between SocialMiner and **Microsoft Exchange Server 2013** fails and email routing fails. If you already have a **Microsoft Exchange Server 2013** server setup with UCCX, ensure to install this patch before it goes into production with UCCX 11.6.

This is not needed for **Microsoft Exchange Server 2016.**

> **Note**: If you do not wish to use TLS 1.2 for connections to Exchange, the minimum server TLS version can be set to 1.0 on the SocialMiner server (see details in the TLS section below). If there is a TLS mismatch between Exchange and SocialMiner, all email feeds will fail.

TLS 1.2 Support for UCCX

In UCCX 11.6, the default is TLS 1.2 for connections when UCCX acts as either a client or a server in the connection. Customers, who upgrade to UCCX 11.6 and have third party applications that interact with UCCX and uses TLS are to be aware of this change.

UCCX 11.6 also provides the ability to update the minimum TLS version for both client and server connections:

- set tls client min-version <1.1 or 1.0>
- set tls server min-version <1.1 or 1.0>

Example: set tls server min-version 1.2

The command has to be run on both the nodes if this is a high availability system. One the command is run, the system has to be restarted using the **utils system restart** command.

The minimum TLS version being supported can also be verified by running the commands:

- **show tls client min-version**
- **show tls server min-version**

> **Note**: If the minimum version is set to 1.0, that means the connection will support 1.0, 1.1 and 1.2.

Impact to RTMT and Script Editor

Due to the security standards to have TLS 1.2, and this being the standard, all UCCX plugins such as RTMT and Script Editor are re-installed so that they can continue to work with UCCX 11.6. Post the upgrade to UCCX:

1. Download and re-install RTMT on all machines that previously had RTMT. Older versions of RTMT are unable to establish connection with UCCX.
2. Download and re-install the UCCX Script Editor on all machines that previously had UCCX Script Editor.

Support for ESXi 6.5

To start from UCCX 11.6, ESXi 6.5 is supported. Due to performance issues with VMFS 6 and ongoing investigations from VMWare, ESXi 6.5 is supported with VMFS 5 only.

	ESXi 6.5 Support	VMFS version with ESXi 6.5	Comments
BE6K	Yes	VMFS 5	Dependency on other applications prevent use of V 6
non-BE6k	Yes	VMFS 5 and VMFS 6	Upgrade of ESXi and VMFS might require migratior the VMs

Ensure that you use the latest OVA template published for 11.6.

> **Note**: Support for VMFS 6 can be updated in the future for previous releases. Refer to the UCCX Virtualization wiki for the latest update.

Reduced Time for Upgrade

In UCCX 11.6, updates have been done to reduce the total time taken for a complete upgrade exercise. As part of the switch-version process, a number of scripts run sequentially to migrate data for individual applications such as Finesse, CUIC and historical data. In UCCX 11.6, the design is updated to have the scripts run in parallel and thereby reduce the time taken for switch-version significantly.

While the actual time for switch-version cannot be displayed due to the size of the customer database, internal testing has shown about 30% time reduction in the switch-version process.

Single ISO for Upgrades and Fresh-Install

In UCCX 11.6, there is only 1 ISO released that is posted on Cisco.com and this ISO can be used for either an upgrade or a fresh install. The ISO follows the regular naming convention of **UCSInstall_UCCX _11.6.XXXXX-XX.sgn.iso**

This ISO is provided with both boot options, so serves as a bootable image as well.

Desktop and Browser Updates

Realtime Reporting Tool

The Real Time Reporting Tool is no longer fully browser based, but uses the Java Applet that requires to be downloaded on the PC to be accessed. With security updates introduced in most browsers regarding Java security, it is necessary to introduce the UCCX Real Time Reporting (RTR) tool as a Java Applet that is downloaded during the first time install.

Updated behaviour in 11.6:

1. RTR is now also available to be downloaded as a plugin, navigate to **Tools > Plugins** page. It continues to exist in the **Tools > RealTime reporting** page.
2. Upon accessing RTR for the first time from a given PC post upgrade to UCCX 11.6, a Java applet is downloaded from the UCCX server. The user ust have the rights to allow for the download and open the same.

   Note: This needs to be done in every PC that wishes to access RTR after the upgrade. Once the RTR applet is downloaded, any user who has access to the PC can open the same.

Recommended Java version for using RTR is **Java 8**. If the user has Java 7, the user must enable TLS 1.2 in the Java Control Panel.

Compatibility Mode for Browsers

If you are using Internet Explorer (IE), Finesse desktop does not support Compatibility mode. Changes are done to show a warning to an agent if compatibility mode is enabled. The only scenario where the compatibility mode is required is for the accesses of old-UI for CUIC which contains features such as Security drawer, Scheduler and so on.

Single Sign On (SSO)

UCCX now supports Integrated windows authentication. Refer to the UCCX Release Notes and related documents for more details.

Support for New Identity Providers

In UCCX 11.6, a number of new Identity Providers (IDP) are qualified and added for support:

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

UCCX 11.6 also works with any IDP that works with SAML v2.0. As long as the IDP confirms to the SAML v2.0 standard and is able to cater to the UCCX (IdS) configuration, the IDP can be used for UCCX SSO even if it is not part of the above list.

Finesse Failover Enhancements

To start from UCCX 11.6, the failover behavior is enhanced to ensure agent productivity during a Finesse failover without doing a full system failover. It is important to understand the same so that agents are made aware of the changes in behavior.

Overview of change in behavior.

Scenario	UCCX HA Behaviour	Finesse Service on Node1	Finesse Service on Node2	Finesse Client Behaviour
CCX Engine Failure on Node1	CCX Engine on SideB becomes master	Finesse goes Out Of Service and returns to IN_SERVICE as soon as it connects to the new master engine.	Finesse goes Out Of Service and returns to IN_SERVICE as soon as it connects to the new master engine.	Agent sees the red disconnection bar, and automatically re-logins into the Finesse side that comes to IN_SERVICE first. It can be either Node1 or Node2.
CCX Engine Failure on Node2	CCX Engine on SideA continues master	Finesse continues to be IN_SERVICE	Finesse goes Out Of Service and returns to IN_SERVICE as soon as it connects to the master engine.	Agents connected to Node1 continues to be logged in. Agents connected to Node2 are temporarily disconnected and gets connects to the Finesse Service on the node that is IN_SERVICE.
Finesse Service OOS on Node1	Engine mastership is not affected	OUT_OF_SERVICE	Finesse on Node2 continues to be IN_SERVICE	Any agents connected to Node1 are temporarily disconnected and gets connected to Finesse on Node2. Agents connected to Node2 will not be impacted.
Finesse Service OOS on	Engine mastership is not	Finesse on Node1 will continue to be IN_SERVICE	OUT_OF_SERVICE	Any agents connected to Node2 are

Node2	affected			temporarily disconnected and gets connected to Finesse on Node2. Agents connected to Node1 will not be impacted.
CCX Notification Service Failure on Node1	Engine mastership is not affected	OUT_OF_SERVICE	Finesse on Node2 will continue to be IN_SERVICE	Any agents connected to Node1 are temporarily disconnected and gets connected to Finesse on Node2. Agents connected to Node2 are not impacted.
CCX Notification Service Failure on Node2	Engine mastership is not affected	Finesse on Node1 continues to be IN_SERVICE	OUT_OF_SERVICE	Any agents connected to Node2 are temporarily disconnected and gets connected to Finesse on Node2. Agents connected to Node1 are not impacted.
Island Mode	Both HA nodes become Master	Finesse on Node1 continues to be IN_SERVICE and will be connected to Engine on Node1.	Finesse goes Out Of Service and will return to IN_SERVICE as soon as it connects to the engine on Node2 which is also the master.	Agents connected to Node1 continues to be logged in. Agents connected to Node2 are temporarily disconnected and gets connected to the Finesse Service on the second node.

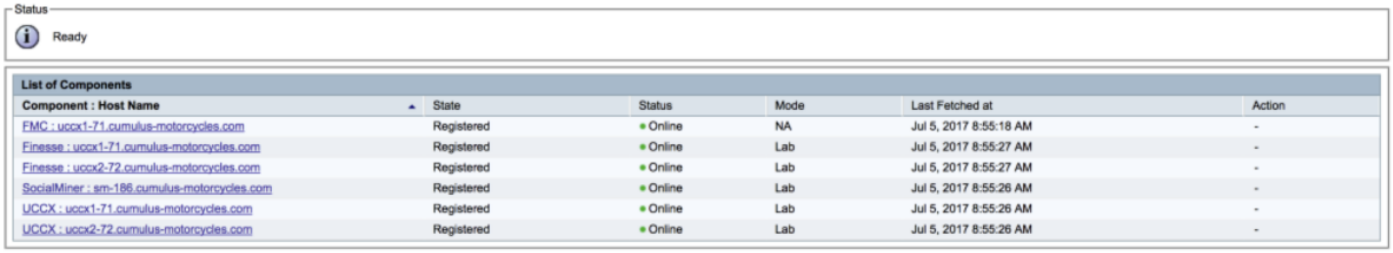
Important Considerations

1. UCCX does not support load balancing of agent login. All agents should login to only the Master Node. The enhancement in behavior is for failover support only.
2. It is not supported to have the same agent login to both the nodes at the same time. This can lead to inconsistencies in the agent experience.
3. In the event of multiple failovers leading to agents connected to both the nodes, all agents should be moved to the master node at the earliest. It need not be done immediately, but the administrator can plan for this based on the maintenance windows available.

Serviceability enhancements

Context Service Dashboard and alerts

In UCCX 11.6, there is a dashboard provided to verify the status of all components registered to Context Service. The dashboard can be accessed on the **UCCX Serviceability** page, as you navigate to **Tools > Context Service Status** page.



Component : Host Name	State	Status	Mode	Last Fetched at	Action
FMC : uccx1-71.cumulus-motorcycles.com	Registered	Online	NA	Jul 5, 2017 8:55:18 AM	-
Finesse : uccx1-71.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:27 AM	-
Finesse : uccx2-72.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:27 AM	-
SocialMiner : sm-186.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:26 AM	-
UCCX : uccx1-71.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:26 AM	-
UCCX : uccx2-72.cumulus-motorcycles.com	Registered	Online	Lab	Jul 5, 2017 8:55:26 AM	-

These are a few statuses to interpreted:

Registered	Connectivity Status	Status Displayed
YES	200	• **ONLINE**
YES	NON-200	• **ONLINE**
YES	N/A	• **OFFLINE**
NO	200	• **OFFLINE**
NO	NON-200	• **OFFLINE**
N/A	N/A	• **STOPPED**
N/A	N/A	• **UNKNOWN***

*When the CS dashboard is unable to retrieve status due to errors or timeouts.

This information can be exported in a JSON/text format too.

In addition to the dashboard, an RTMT alert isadded as well:
ContextServiceStepsExecutionIssue

This is triggered when:

1. Context Service steps in the script timeout due to connectivity issues with the Context Service cloud.
2. Context Service steps fail due to an error in the Context Service cloud.

Know Before you Upgrade

Reporting User Password Consistency and Impact to LiveData

Starting from UCCX 11.6, both LiveData and Historical Reports use the Reporting User password for setting up the Datasource. If the passwords do not match between the nodes, reporting is impacted.

Before you upgrade, ensure the password is consistent between both the nodes. You can verify through these steps:

1. Navigate to **Tools > Password Management**.
2. Click on **Check Consistency**.
3. If no errors, you are good. If there is consistency mismatch (especially with the reporting user), update the password on both the nodes.

Reporting Users Unable to Access CUIC Reports after Upgrade to UCCX 11.6

The Cisco Unified Intelligent Center (CUIC) allows access to reports based on the permissions assigned to the user accessing. Based on the permission level, the user is provided access to either the agent reports or the supervisor reports or the complete report set to the reporting administrator.

These permissions are synced from the Unified Contact Center Express (UCCX) based on the role assigned to the user on the UCCX. The user can be specifically made a CUIC administrator by running the command **utils cuic user make-admin CCX\<username>**

During the upgrade process, the permissions between the UCCX and the CUIC applications gets re-synced and therefore the elevated CUIC administrator rights given to the user get overwritten. The user, therefore, sees only those reports that his original role allows.

To provide access to the reports that the user had before the upgrade:

1. Run **utils cuic user make-admin CCX\<username>** on both the UCCX nodes.

2. Restart the CUIC Reporting Service on both the UCCX nodes.

Increased Attachment Size Limit for Emails and Exchange Considerations

In UCCX 11.6, the limits on the size of attachments is updated to these:

- Max number of attachments by an agent : 10

- Max size of total attachmennts by an agent : 20MB

- Max size of single attachment by an agent : 10MB

While the UCCX solution allows the increased attachment size, the **Message Size Limit** is

updated on the Exchange (mail server) so that the attachments are not blocked. The limit might be applied based on enterprise wide IT policy. If the Exchange server blocks the message, the agent sees the error: "Unable to reply to customer's email. Click Send to retry or requeue. If problem persists, contact you system administrator."

Calculate the Message Limit Size

Message size = Size of email include attachments + Base64 encoding

Base64 encoding = ~33% of the size of the message

Suggested formula is **Message size = 1.5*Size of email include attachments**

Example: If the size of the message is 9MB (include attachments), the message size to be set as limit should be (9*1.5) = 14MB.

Given that UCCX 11.6 allows attachment size upto 20MB, the message size limit to be set is **1.5*20MB=30MB** if you have to take advantage of this increased limit on the UCCX solution side.

The limit can be set on the Exchange server by running the command:

Set-TransportConfig -ExternalDsnMaxMessageAttachSize 30 MB -InternalDsnMaxMessageAttachSize 30MB -MaxReceiveSize 30MB -MaxSendSize 30MB

Important Upgrade Considerations

- Clear the cache of all agent machines after the upgrade. If not, issues related to state changes and real time data on the desktop can be seen.
- Finesse Desktop custom layout is not auto-migrated. Ensure to factor this in and have the layout correctly configured post the upgrade.
- Update VM settings to match the latest OVA template for UCCX 11.6. If you are doing a fresh install, use the OVA template.
- If you perform the upgrade during production hours, perform the upgrade on the non-master node to avoid any potential disruptions.
- In UCCX 11.6, the Platform Tomcat can get restarted during the upgrade. This has no impact on the users, but can generate an RTMT alert. This can be ignored.
- Post the upgrade, re-install all instances of RTMT and Script Editor.
- Ensure all supervisors and administrators using the Real Time Reporting Tool have the plugin installed post the upgrade.
- If you have any TLS integrations, review the TLS support and verify you are setup with the right versions.

- Review the browser requirements and make changes as necessary.
- Familiarize yourself with the new Finesse Failover enhancements and discuss with agents about this updated behaviour.

Obtain Documentation and Submit a Service Request

For information on how to obtain documentation, use the Cisco Bug Search Tool (BST), submit a service request, and gather additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original

on-line version should be referred to for latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

©2016 Cisco Systems, Inc. All rights reserved.