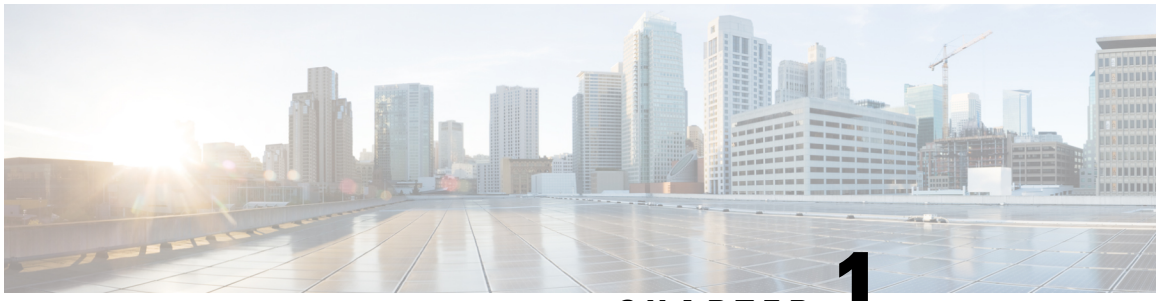
Release Notes for Cisco Hosted Collaboration Solution for Contact Center Solution, Release 11.6(1)

First Published: 2017-08-24

Last Modified: 2021-07-30

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

CONTENTS



CHAPTER 1

Introduction

Release Notes for Contact Center Solutions

Release 11.0 introduced release note compilations for each of the contact center solutions. The compilations contain all of the release notes for one solution type and the components that you can use with that contact center. In addition to the release notes in this document, see the release note compilations for the other contact center solutions at the following links:

- *Release Notes for Cisco Packaged Contact Center Enterprise Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html
- *Release Notes for Cisco Hosted Collaboration Solution for Contact Center* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-release-notes-list.html
- *Release Notes for Cisco Unified Contact Center Enterprise Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-release-notes-list.html
- *Release Notes for Cisco Unified Contact Center Express Solution* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-release-notes-list.html

Cisco Security Advisories

The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that relates to Cisco products and networks.

For information on existing security issues, see *Cisco Security Advisories, Responses, and Alerts* at https://tools.cisco.com/security/center/publicationListing.x.

Customer Documentation Updates for This Release

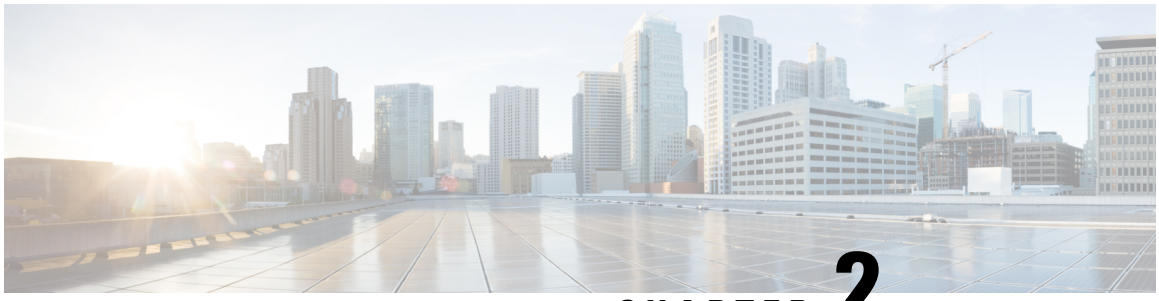
Our Documentation Guides identify the documents that changed for this release:

- **Packaged CCE**—https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-documentation-roadmaps-list.html
- **HCS for Contact Center**—https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-documentation-roadmaps-list.html
- **Unified CCE**—https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-documentation-roadmaps-list.html
- **Unified CCX**—https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-documentation-roadmaps-list.html

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

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

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



CHAPTER 2

Cisco Hosted Collaboration Solution for Contact Center for Contact Center

New Features

VPN-less Access to Finesse Desktop (For Agents and Supervisors)

This feature provides the flexibility for agents and supervisors to access the Finesse desktop from anywhere through the Internet without requiring VPN connectivity to the Enterprise data center. To enable this feature, a reverse-proxy pair must be deployed in the DMZ. For more information on this feature, see the Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1) and Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1).

Media access remains unchanged in reverse-proxy deployments. To connect to the media, agents and supervisors can use Cisco Jabber over MRA or the Mobile Agent capability of Contact Center Enterprise with a PSTN or mobile endpoint.

To use VPN-less access to Finesse desktop feature, you must upgrade Finesse, IdS, and CUIC to Release 12.6(1) ES02. If you are using Unified CCE 12.6(1), you must upgrade Live Data to 12.6(1) ES02. You can access the 12.6(1) ES02 Release and Readme from the following locations:

- Finesse 12.6(1) ES
- CUIC/LD/IdS 12.6(1) ES

Note For Nginx-based reverse-proxy rules, installation, configuration, and security hardening instructions, refer to the Nginx TechNote article. Any reverse-proxy supporting the required criteria (as mentioned in the **Reverse-Proxy Selection Criteria** section of Cisco Unified Contact Center Enterprise Features Guide, Release 12.6(1)) can be used in place of Nginx for supporting this feature.

Outbound Option High Availability

This release includes enhancements to Outbound Option to provide High Availability.

Campaign Manager High Availability

This release supports the Outbound Option High Availability feature that allows the Campaign Managers and the Outbound Option Import on both Loggers to operate in active/standby mode. It ensures replication of the Outbound Option databases on both sides. The dialers automatically connect to the active Campaign Manager.

When the Unified CCE system starts, the Campaign Manager on Logger Side A functions as the active Campaign Manager, while the Campaign Manager on Logger Side B fuctions as the standby Campaign Manager.

The Outbound Option import is synchronized on each Logger side with the Campaign Manager on same Logger side. Therefore, the Outbound Option import and the Campaign Manager on each side work in tandem. Together with two-way replication and dialer high availability, this provides a robust fault tolerant Outbound Option experience with continuous operation even if the active Campaign Manager fails.

For more information, see the *Outbound Option High Availability* section in the Solution Design Guide for Cisco Unified Contact Center Enterprise available at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Two-Way Replication

Outbound Option High Availability supports two-way replication between the Outbound Option database that you create on Logger Side A and the Outbound Option database that you create on Logger Side B. Two-way replication offers a High Availability solution in which a failure on the active side of a server allows continuation of outbound dialing and imports on the standby side. All data is replicated between the two sides using Microsoft SQL Server replication.

Enable the Outbound Option High Availability two-way replication on both Logger sides by using Web Setup.

For more information, see the Outbound Option Guide for Unified Contact Center Enterprise available at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

Platform Updates

This release requires the following prerequisites made to the platform:

- Ensure that you are running Microsoft SQL Server 2014 SP2 (64-bit).
- If your Administration Clients run on Microsoft Windows 7, upgrade to a minimum of Microsoft Windows 7 SP1.

Important Ensure that these prerequisites are in place before upgrading to Release 11.6(1).

Cisco UCS C240 M5 Server Support

Cisco UCS C240 M5SX server is supported for deployment of Release 11.6(1).

License Consumption Report

License Consumption

This release introduces the License Consumption Report. This report uses VRU and dialer port monitoring and utilization statistics.

Use this report to monitor the agent license consumption and other resources such as the VRU-IVR ports and the outbound dialer ports. You can generate this report for specific intervals such as hourly, daily, weekly, monthly or quarterly. This further helps you ensure that you have adequate license allocation to cover the peak or maximum license usage during the license agreement period.

The License Consumption report displays the following for a specific interval:

- Total Agents, Enterprise Agents, and ICM Agents logged in
- Maximum VRU ports utilized
- Maximum Dialer ports utilized

Note The VRU and Dialer port, and ICM Agent data will not be available until the Routers, Loggers and PGs are upgraded.

In this release, the Cisco Unified Intelligence Center (CUIC) reports are updated to present the license consumption data from the updated Database tables.

Spikes in license consumption could occur in events such as shift changes when agents of the outgoing shift have not logged out while the agents of the incoming shift have logged in. The Spike Suppression feature included in the License Consumption report allows you to suppress the steep spikes using the standard 95 percentile algorithm. This makes it convenient to view the report while ignoring the spikes.

The changes made in the Database Schema tables provide the License Consumption report updates. For more information, see the Database Schema Changes topic.

Download and import the License consumption report (Templates_CCE_11.6.1_LC_11.6.1.zip file) from Cisco.com.

Note While importing the report, do the following:

- In the Data Source for ReportDefinition field, select **`UCCE Historical`**
- In the Data Source for ValueList field, select **`CUIC`**.

For more information, see the Cisco Unified Contact Center Enterprise Reporting User GuideCisco Unified Contact Center Enterprise Reporting User Guide.

CLID Masking Feature at Unified ICM/CCE Level

The CLID masking option allows you to mask the original CLID / Automatic Number Identification (ANI) of the caller from appearing on the agent desktops and getting stored in the Unified CCE or Unified ICM database. You can set up masking to either remove digits or replace digits with another character. The feature traditionally was only available in NAM/CICM deployments or ICM to ICM deployments using the INCRP NIC.

Cisco Unified CCE, Release 11.6(1) introduces the CLID masking feature at the enterprise level. It is possible to configure the masking option that needs to be applied, on a per routing client basis using a configuration parameter. For more details, see the tool help in the System Information tool and the NIC Explorer tool in the Configuration Manager tool.

Updated Features

Increased PG Agent Capacity for Mobile Agents

Added on May 14th, 2021

The mobile agent capacity on the PG has increased as follows:

- 2000 with nailed-up connections (1:1)
- 1500 with nailed-up connections if the average handle time is less than 3 minutes, or if agent greeting or whisper announcement features are used with the mobile agent (1.3:1)
- 1500 with call-by-call connections (1.3:1)

For more details, see the *PG Agent Capacity with Mobile Agents* section in the *Sizing and Operating Conditions for Reference Designs* chapter at *Solution Design Guide for Cisco Hosted Collaboration Solution for Contact Center* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-implementation-design-guides-list.html

TLS Versions Support

This release supports Transport Layer Security (TLS) v1.2 and uses it as the default option. The older versions of TLS/SSL are disabled by the Installer.

Note In case there are third party applications installed on CCE VMs that are impacted when the older versions of TLS/SSL are disabled, re-enable the required TLS/SSL versions. For more information, see Microsoft documentation about enabling TLS/SSL provided by Secure Channel (Schannel security support provider) authentication protocol suite.

Similarly, third party applications must use TLS v1.2 while creating connections to CCE VMs or CCE database.

Note For Microsoft Windows 7 client systems, install the Microsoft Windows Update KB3080079 to ensure that the remote desktop connection over TLS v1.1 or 1.2 is supported.

TLS Options for Cisco Unified CCE and Other Components

Configure TLS v1.2 on all the components and Unified CCE. Internet Script Editor (ISE), and other web applications require TLS v1.2 for HTTPS connections.

Note TLS v1.2 is installed by default on all Cisco VOS based deployments.

For Live Data, CUIC, and Cisco IdS to interoperate with older versions of Unified CCE, run the **set tls client min-version** command on these components to set the minimum TLS version to v1.0 or v1.1 as required.

See the individual component sections for more details on upgrade considerations and default behavior of TLS v1.2 in that component.

Component	Default Option
Cisco Unified CCE	TLS v1.2
Cisco Unified Intelligence Center	TLS v1.2
Cisco Finesse	TLS v1.2
Cisco CVP and VVB	TLS v1.2
Cisco SocialMiner	TLS v1.2
Enterprise Chat and Email	TLS v1.2
Cisco Unified Contact Center Domain Manager	TLS v1.2

Use the Transport Layer Security CLI commands to view or change the TLS minimum version for inbound or outbound connections. For product-specific TLS configuration, see *Configuration Guide for Cisco Hosted Collaboration Solution for Contact Center* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

ISE Client Requires Manual Upgrade because of TLS v1.2

This release supports only TLS v1.2 between the Internet Script Editor server and ISE clients. ISE client versions before Release 11.6(1) cannot properly establish a TLS v1.2 connection with the server. This prevents an automatic upgrade of the ISE client to the current release.

You can manually upgrade the ISE client installer by entering the following URL in your browser:

`https://<DistributorHost/addr>/install/upgradescripteditor.htm`

This URL reaches the upgrade web page for the ISE client. You can then upgrade the ISE client normally.

Feature Updates for Outbound Option

Dialer High Availability

With the Campaign Manager High Availability, all the active dialers connect to the active Campaign Manager. During a Campaign Manager fail-over, the dialers try to connect to the last known active Campaign Manager during the configurable interval (EMTClientTimeoutToFailover), after which the standby Campaign Manager becomes active and the dialers connect to the newly active Campaign Manager.

EMTClientTimeoutToFailover is the interval at which the active Campaign Manager sends the failover message to the router if the Dialer or BAImport do not connect with the Campaign Manager.

Note Upgrade the Peripheral Gateway to Release 11.6(1) to utilize the Outbound Option High Availability feature. This upgrade is mandatory to enable the Dialers to connect to the Campaign Managers on side A and side B.

For more information, refer to the Solution Design Guide for Cisco Unified Contact Center Enterprise at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Outbound Option Records Handling

When dialer initiates a call for a customer record, the Campaign Manager moves the CallStatus of the customer record to an intermediate Dialed state in the DialingList table. This new state allows the active Campaign Manager to ensure that the customer records for calls that were disconnected due to a failure or fail-over are not dialed again.

Do Not Call Cache Update

To support Outbound Option High Availability and replication between Logger Side A and Logger Side B, Do Not Call data now resides in a Do_Not_Call database table. Previously, the Do Not Call data was stored in the DoNotCall.restore file on Logger Side A. The DoNotCall.restore file is a text file that contains a comma-delimited list of phone numbers and extensions (if extensions exist).

When you upgrade to the current release and enable Outbound Option (whether or not you enable High Availability), the Do_Not_Call table is initially empty, as it is newly created on each Logger side. Populate the Do_Not_Call table on Side A and Side B by importing the DoNotCall.restore file, just as you would perform any other import of customer contact information. You do this only once, when you perform an upgrade.

See the Outbound Option Guide for Unified Contact Center Enterprise guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

NALENND™ (Region Prefix and Member Data) Database Updates

This release includes new NALENND™ (North American Local Exchange NPA NXX Database) updates for Outbound Option.

Other Notes

The following considerations are important for Outbound Option:

- Outbound Option high availability has specific requirements for the disk size where the outbound database resides, for CCE deployments.
- Optional Outbound High Availability has specific requirements for the *SQL Server Agent* account configuration.

For more information about the specific requirements, see the Outbound Option Guide for Unified Contact Center Enterprise guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html.

Reports

Agent State Trace Historical Report

This release includes an enhancement to the Agent State Trace Historical report. If the Agent State is Ready or Not Ready, the Precision Queue/Skill Group field displays the ALL SG/ALL PG value.

ALL SG/ALL PG value indicates that the agent is associated to several skill groups (SGs) within a PG and has picked one of the SGs for a call.

New Languages Supported in Reports

New Languages

All the stock reports are available in the following new languages:

- Bulgarian
- Catalan
- Czech
- Croatian
- Hungarian
- Slovak
- Slovenian
- Serbian
- Romanian

Live Data Reports

This release provides three new Live Data reports for agent and supervisor call and state logs. See the updates in the Cisco Finesse section for the *View Recent Call History*, *View Recent State History*, and *View My History* updates.

See the *Cisco Unified Contact Center Enterprise Reporting User Guide* for more details about the *Recent Call History* and *Recent State History* reports.

Java Version Update

This release supports Java JRE version 1.8 (32-bit) Update 121.

The Unified CCE installation process installs Java JRE version 1.8 (32-bit) Update 121. Previous versions of Java may be removed, if necessary, after ensuring that Java JRE version 1.8 (32-bit) Update 121 is installed on the server.

For more information, see the *Compatibility Matrix for Cisco HCS for Contact Center 11.6(1)* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html. You can also apply newer Java security updates.

Database Schema Changes

Unified CCE Database Schema Changes

This release introduces minor database schema changes. Therefore, do not use the Enhanced Data Migration Tool for this release. The Unified CCE, Release 11.6(1) installation performs the database migration.

The release includes changes to these tables:

Table	Changes
NALENND™ (Region Prefix and Member Data) Database Updates	Added new NALENND™ (North American Local Exchange NPA NXX Database) updates for Outbound Option.
Configuration_Limit	Added several new values for the ConfigLimitName field. Removed the notes on actual values for the configuration limits. The *Solution Design Guide* is the primary source for that information.
Congestion_Control	Added the new deployment type.
Dialer_Interval	Added description for the FutureUseInt3 field.
Dialer_Real_Time	Added description for the FutureUseInt3 field.
System_Capacity_Interval	Added descriptions for FutureUseInt1 and FutureUseInt2 fields.
System_Capacity_Real_Time	Added description for the FutureUse2 field.

SSO Federation

This release adds support to the following customer IdPs to be federated to the Hosted AD FS 2012 R2 IdP:

Microsoft AD FS (Active Directory Federation Services)	2.0, 2.1, and 3.0
PingFederate	8.2.2.0

OpenAM	10.0.1
Shiboleth	3.3.0
F5	13.0

Documentation is provided only for Microsoft AD FS. For all other customer IdPs, hosting partners must refer to Microsoft and third-party vendor IdP documentation, to create and test Federation trust.

Cisco Unified Contact Center Enterprise, Release 11.6(1) supports SAML v2.0.

Cisco Unified Contact Center Domain Manager 11.6(1) requires Microsoft AD FS 2012 R2.

This release supports an increased number of agents of 12000 SSO users from 4000 SSO users. This release also removes the restrictions imposed by the global deployment model.

In SSO implemented in a single domain environment, this release supports Cisco IdS for Integrated Microsoft Windows Authentication.

For more information, see the *Cisco Hosted Collaboration Solution for Contact Center Configuration Guide, Release 11.6(1)*.

ESXi Release 6.5 Support

This release supports VMware vSphere Hypervisor (ESXi) 6.5.

Cisco Unified CCE supports only the VMFS 5 file system.

For more information, see Virtualization for Hosted Collaboration for Contact Center at: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html

Important Notes

Upgrade to Release 11.6(1)

You can upgrade to Cisco Unified CCE, Release 11.6(1) from Release 11.0(1), 11.0(2) or 11.5(1) directly. To upgrade from a release earlier than Release 11.0(1), upgrade to Release 11.0(1) and then upgrade to Release 11.6(1). If there are later 11.x Maintenance Releases installed, uninstall these maintenance releases before installing Release 11.6(1). You can determine which maintenance releases you have applied, in the Programs and Features list in Control Panel.

Before upgrading or uninstalling Release 11.6(1), close all the open Microsoft Windows Event Viewer instances. This will prevent an installation failure with an error that the following DLLs are locked:

- icrcat.dll
- icrmsgs.dll
- snmpeventcats.dll
- snmpeventmsgs.dll

If the failure occurs, close the Event Viewer and retry the installation or uninstallation.

If the failure persists, restart the Microsoft Windows Event Log service.

COP Files Installation

Before upgrading a standalone deployment of Unified CCE (Release 10.5 or Release 11.0) or Packaged CCE with CUIC to a Release 11.6(1) co-resident `UCCE: 2000 Agents` deployment (CUIC with Live Data and IdS), install the required COP files. See the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide for more information about the installation of the COP files.

Upgrade Utilities

The EDMT, RegUtil, User Migration Tool, and DB Estimator upgrade utilities do not apply in this release. Use the Release 11.0(1) version of the EDMT, RegUtil, User Migration Tool, and DB Estimator upgrade utilities to upgrade to Release 11.0(1), as needed.

For the upgrade utilities, see https://software.cisco.com/download/type.html?mdfid=268439622

Live Data Deployments

In this release, Live Data supports only 12 Agent Peripheral Gateways (PGs). Deployment upgrades from Release 11.0(2) to Release 11.6(1) with more than 12 Agent PGs (UCM PGs and TDM PGs) are only supported if you are not using Live Data.

Microsoft Windows Patches and Updates

An upgrade to Release 11.6(1) requires the latest Microsoft Windows Server 2012 R2 and Microsoft SQL Server 2014 KB patches and Service Packs.

If you applied a Microsoft Windows update since March 2014, the Microsoft Windows Update KB2919355 (Hotfix) should be installed. To determine if this Microsoft Windows Hotfix is installed, from your Control Panel go to **Programs** > **Programs and Features**. Click **View installed updates**.

Make sure that Microsoft Windows Update is not running when you install the Release 11.6(1) patch.

Note On the Microsoft Windows 7 based administration client systems, install Microsoft Windows Update KB3080079 to ensure that the remote desktop connection over TLS v1.1 or 1.2 is supported.

Download and install the necessary Microsoft Patch updates to ensure that the ransomware Wannacry does not affect the Cisco Unified Contact Center deployment.

Upgrade Live Data

Upgrade Live Data and the AW database together. If you restart Live Data after you upgrade the AW database to Release 11.6(1) but before you upgrade Live Data, the Live Data upgrade switch partition step fails. If necessary, resolve this issue by temporarily removing the AW database configuration from Live Data. For the procedure to remove the AW database configuration from Live Data, see CSCvf20136.

Agent Service Logon

For the two-way Outbound Option database replication, it is necessary to create a Microsoft SQL Server user and assign that user the sysadmin privilege. Also, MSSQLSERVERAGENT user must be assigned to the

SQL Server Agent process. If the service is running under a different account, then you must change the account.

Change the Agent service logon using the Microsoft SQL Server Configuration Manager. Do not change it directly using the Services Control Panel application. Ensure that the logon account is included in a SQLSERVERAGENT group on the machine.

Supervisor Sign-on When SSO is Disabled

The login name of a supervisor who is not enabled for single sign-on requires either one of these formats:

- User Principal Name (UPN); for example, user@domain.com
- Security Accounts Manager (SAM); for example, DOMAIN\USER

Note After upgrading to Release 11.6(1), change the supervisor login usernames to comply with the Email ID format (user@domain.com) to ensure that the User List tool functionality does not fail. Alternatively, see the defect CSCvf27253 to apply the necessary updates.

You can change the login name for multiple supervisors at once using the Bulk Edit Person tool.

For supervisors with SSO not enabled, Cisco Unified CCE supports SAM Account Name and User Principal Name format for supervisor login name configuration. However, Cisco Finesse supports only User Principal Name (UPN). Therefore, use only UPN login format for configuring EA (Enterprise Agent) Supervisor login name. As the alternative to using the UPN login format, the supervisors can use the numeric IDs of their peripheral.

Direct Attached Storage (DAS) for Cisco UCS C240 M4 TRC Server

The Cisco Unified Contact Center Enterprise Installation and Upgrade Guide now provides details for mapping Virtual Machines to data stores for the `UCCE: 2000 Agents` deployment for the Cisco UCS C240 M4 Server hardware. This aligns with the Cisco Packaged CCE Virtual Machines mapping.

Check the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide for specific information for product upgrades that may require specific Virtual Machines to datastore placement that may be different from your current design. Check your servers array design and controller settings to ensure that they align with the documented requirements.

For more details about Cisco UCS C240 M4 Server RAID configurations, see https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M4/install/C240M4/raid.html.

Sub-Customer Capacity for Small Contact Centers on UCS TRC Blades

In previous releases, the SCC 100 Agent dedicated sub-customer option supported 10 sub-customers on each blade pair. In Release 11.6, Finesse requires more CPU resources. This reduces the capacity to 6 sub-customers on each blade pair.

Plan your server resources accordingly when upgrading to this release.

Deprecated Features

There is no new development for Deprecated features. These features may be scheduled to be removed in a future release. Plan to transition to the designated replacement feature. If you are implementing a new deployment, use the replacement technology rather than the deprecated feature.

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

Deprecated Feature	Announced in Release	Replacement	Notes
MIB Objects: • cccaDistAwWebViewEnabled • cccaDistAwWebViewServerName • cccaSupportToolsURL • cccaDialerCallAttemptsPerSec	11.6(1)	None	None
SHA-1 certificate	11.5(1)	SHA-256	For more information on SHA-256 compliance, see https://communities.cisco.com/docs/DOC-64548
Generic PG	11.5(1)	Agent, VRU, and MR PGs	None
ECSPIM	11.5(1)	TAESPIM	Avaya SEI/CVLAN protocol was deprecated by vendor.
"Sprawler" deployment	10.0(1)	A Packaged CCE deployment	A "Sprawler" was a Progger with an Administration & Data Server on a single box. It was used for lab deployments.

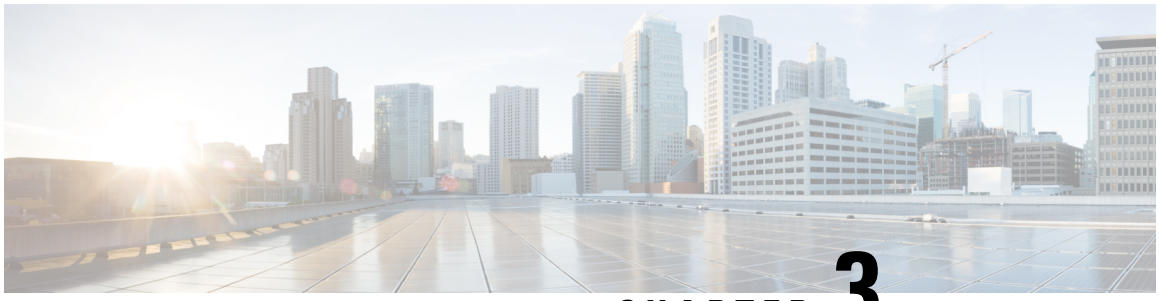
Removed and Unsupported Features

Feature	Effective from Release	Replacement	Notes
HCS for CC 500 Agent Deployment Model	11.6(1)	HCS for CC 2000 Agent Deployment Model	The 2000 agent deployment model for HCS for CC has a subset deployment for 500 agent capacity allowing for reduced hardware footprint. For more information about 2000 Agent Deployment Model and the migration procedures, see *Cisco HCS for Contact Center Installing and Upgrading Guide* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html and *Solution Design Guide for Cisco HCS for Contact Center* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/tsd-products-support-series-home.html
AAS for Symposium (SEI Interface)	11.5(1)		
CTI OS Agent Desktop **Note** CTI OS Agent Desktop is supported for TDM and System PG only.	11.5(1)	Cisco Finesse.	
CTI OS Supervisor Desktop **Note** CTI OS Supervisor Desktop is supported for System PG only.	11.5(1)	Cisco Finesse	
CTI OS-Based Silent Monitoring **Note** CTI OS-Based Silent Monitoring is supported for System PG only.	11.5(1)		
Cisco Agent Desktop (CAD)	11.0(1)	Cisco Finesse	
Cisco Supervisor Desktop	11.0(1)	Cisco Finesse	

Feature	Effective from Release	Replacement	Notes
Cisco Media Blender	11.5(1)	For Unified WIM & EIM, use the Script Editor to configure dialed number prefixes and filters for Agent Request.	
Database Partitioning	9.0(1)	This feature is discontinued.	
H.323 protocol support	11.5(1)	SIP protocol	
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 **Note** The Half Hour database tables available in the database are not populated because these tables are not supported.	11.5(1)	Interval database tables	
On-Demand Licensing Model for Unified CCE	11.5(1)	Cisco Hosted Collaboration Solution (HCS) for Contact Center	
Jabber Guest	11.6(1)	Cisco Remote Expert Mobile for Android	
Support for Secure Socket Layer (SSL) 2.0 and 3.0	11.5(1)	Transport Layer Security (TLS)	
Unified Intelligent Contact Management Hosted (ICMH) and Unified Contact Center Hosted (Unified CCH)	11.5(1)	Cisco Hosted Collaboration Solution (HCS) for Contact Center	
Unified WIM & EIM	11.5(1)	Enterprise Chat and Email	
Remote Silent Monitor	11.6(1)	None	

Third Party Software Impacts

See the *Compatibilty Matrix for Cisco HCS for Contact Center* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html for information on third-party software.



CHAPTER 3

Cisco Unified Customer Voice Portal

New Features

Security Enhancements

Unified CVP has the following new security capabilities:

- SIP over TLS for securing call control over the IVR and agent call legs.
- Log masking of sensitive user DTMF input on Unified CVP Call Studio applications.
- TLSv1.2 enforced for secure communications across solution components.
- Unified CVP Call Studio supports sFTP-based transfer of recorded files.
- The Web Service element of Unified CVP Call Studio supports strong ciphers.

Enforce Maximum Number of Calls

This feature allows administrators to configure maximum number of calls that Unified CVP can handle. This is configurable from OAMP.

vCUBE support

The solution is certified with the virtual Cisco Unified Border Element (vCUBE), enabling a broader range of deployment options and making it possible for businesses to deploy the CVP with less router hardware.

Standalone Application Builder (SAB)

The Standalone Application Builder utility has been restored. This utility allows the deployment of an application through the command-line interface.

Updated Features

Call Studio Enhancements

Unified CVP Call Studio has the following enhancements:

- Install the Unified CVP Call Studio on the Microsoft Windows 10 desktop operating system now.
- Easier addition of comments to Unified CVP Call Studio elements and tooltip display of comments.
- Supports the autopopulation of the subflow parameter and the return parameter of a subflow in the Subflow Call elements to avoid errors.
- Supports the display of spatial coordinates for elements in the script editor.
- Faster loading of the decision element in large Unified CVP Call Studio applications.

Context Service Serviceability Enhancements

Context Service (CS) serviceability improvements make it easier to track and ensure the flow of customer context information into and out of Unified CVP. These improvements include:

- Access to Context Service is validated during registration and de-registration for an enhanced user experience.
- Context Service access status is displayed on the management console, allowing administrators a view of service availability from all component hosts.
- Context Service activity statistics are available and refreshed every 30 minutes, allowing improved performance debugging.

Important Notes

None.

Deprecated Features

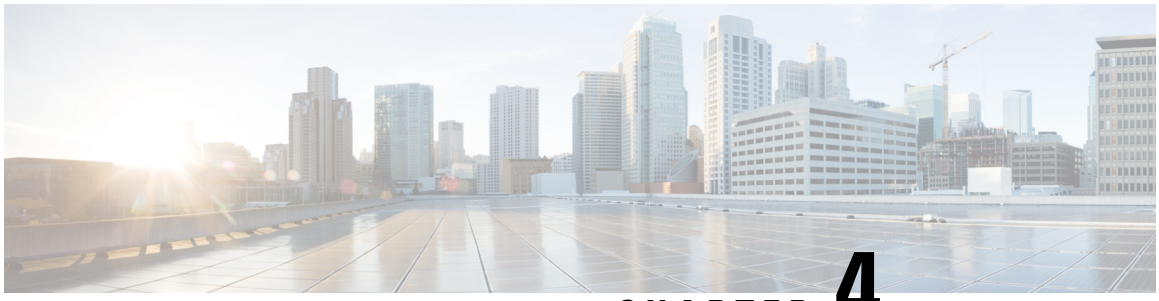
The Key PressMarkup Language (KPML) feature for Cisco unified Customer Voice Portal is deprecated from Release 10.5(1).

Removed and Unsupported Features

None.

Third-Party Software Impact

See the Unified CCE Compatibility related information located at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for information on third-party software.



CHAPTER 4

Cisco Virtualized Voice Browser

New Features

Security Enhancements

Cisco Virtual Voice Browser (VVB) has the following new security capabilities:

- SIP over TLS for securing call control over the IVR and agent call segments.
- SRTP media support over Cisco VVB to secure the IVR voice media stream.

Note Customers in countries that have local government regulations about using software that allows SRTP voice communication, can alternately use the export unrestricted image of Cisco VVB that does not support SRTP. See the *CCBU Ordering Guide* for more details on ordering options available for the Cisco VVB software.

Support for Cisco VVB on Cisco Integrated Service Routers 4000 Series

Cisco VVB can now be installed on the Kernel-based Virtual Machine (KVM) that is available natively on the Cisco Integrated Service Routers 4000 Series. This allows a small-to-medium-sized edge deployment to use the VVB natively on the router hardware by removing the need to host an add-on UCS E module.

Support for Non-Reference VRU

Cisco VVB now supports the Type 2, 3, 7, and 8 VRU non-reference call flow models.

Optimized Hard Disk Size for OVA

Cisco VVB OVA hard disk size is reduced from 2x146 GB to 1x146 GB. Upgrade from 11.5.1 to 11.6.1 is supported for profiles having 1x146 GB disk size OVA.

Change Hostname or IP Address

You can now change the hostname or IP address of Cisco VVB post installation. This feature allows you to clone Cisco VVB instead of installing it afresh for each new deployment.

CLI-based HTTP Timeout Configuration

This release introduces a new CLI command to configure the HTTP timeout. This configuration allows Cisco VVB to wait for a user-specified time interval to receive a response from the HTTP server.

Support for G.729 Codec

Cisco VVB now supports the G.729 codec with a sampling rate of 8kb/s for the IVR call segment.

Note The G.729 codec does not support the ASR-TTS service.

Fetchaudio

This feature uses the *fetchaudio* attribute for enhancing user experience when there may be noticeable delays during the next document retrieval. This feature can be used to play background music or a series of announcements while the document is being retrieved.

Updated Features

Performance Improvement

With this release, Cisco VVB has been scaled up to support a maximum of 20 calls per second.

Important Notes

None.

Deprecated Features

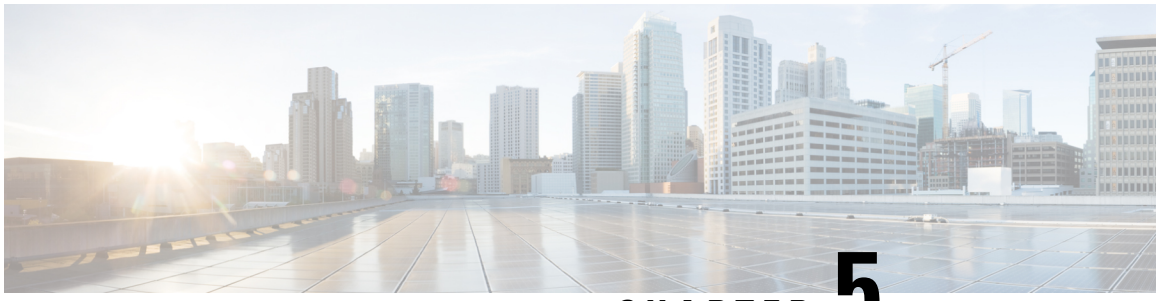
None.

Removed and Unsupported Features

None.

Third-Party Software Impact

See the Unified CCE Compatibility related information located at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for information on third-party software.



CHAPTER 5

Cisco Finesse

New Features

View Recent Call History

Supervisors can now view the recent call history of an agent on an assigned team from the Team Performance gadget. Select the team of the agent, click on the agent from the list. You can view call details like start time of the call, duration, type etc.

You cannot select any other agent or choose another team while the recent call history of the selected agent is being loaded. However, you may change an agent's state or monitor an agent's call during this time-frame.

View Recent State History

Supervisors can now view the recent state history of an agent on an assigned team from the Team Performance gadget. Select the team of the agent, click on the agent from the list. You can view agent state details like start time of the call, agent state, reason, and duration of the call.

You cannot select any other agent or choose another team while the recent state history of the selected agent is being loaded. However, you may change an agent's state or monitor an agent's call during this time-frame.

Make Call from Ready State

Agents and Supervisors can make calls from Ready State.

Gadget Multi-host Specification

Finesse desktop layout.xml provides an additional attribute to specify alternate hosts from which gadgets can be loaded. This is to ensure that the Finesse desktop is fully functional even if the primary servers on which the gadgets are hosted are unavailable.

View My History

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

Initiate a Call back from the My History Report

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

Separate System and Custom Reason Codes in Cisco Finesse Administrator

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

Pre-defined Attributes of the System Reason Codes

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

Queue Details in Call Variables and Workflow

Administrators can configure queue details with the following variables in the call variable layout and workflow. The agents can view queue details in the call variable layout and view a browser pop up:

- queueNumber
- queueName

Filtering of Logged Out Agents

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

Install or Upgrade with Call History and State History Gadgets

To use Recent Call History and Recent State History gadgets, Unified CCE, Cisco Finesse, CUIC, and Live Data need to upgrade to 11.6 (1) version. In the case of fresh install, all components need to be installed and configured for 11.6(1) version.

Queue Statistics enabled by Default

The Queue Statistics gadget is enabled by default as part of Cisco Finesse new installation for Unified CCE. When performing a system upgrade from Cisco Finesse 11.5(1), the desktop custom layout needs to be modified by the administrator for the Queue Statistics gadget to be displayed on the Agent and Supervisor desktop.

Secondary Call ID in Dialog API

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

Updated Features

Enable Trace Logs

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

- utils finesse trace enable
- utils finesse trace disable
- utils finesse trace status

Audit Logs Track Admin User Operations

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

- Timestamp
- User id of the administrator
- Method of operation (PUT, POST, DELETE)
- URL
- Payload

Configuration of viewID in Dynamic Live Data Gadgets

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

Reason Code Conflicts during Upgrade

Configurable Toaster Notifications

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

Context Service Serviceability

Context Service Serviceability Improvements

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

- Context Service SDK version used in Finesse
- Context Service registration status
- Ping Latency of the CS services

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

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

Context Service SDK Re-initialization

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

Cisco Finesse Backward Compatibility

Cisco Finesse 11.6(1) supports TLSv 1.2. For Cisco Finesse 11.6(1) to be backward compatible with earlier Unified CCE versions, TLSv 1.0 and 1.1 protocols must be enabled. Run the following CLI command:

set tls client min-version

This command allows you to set the minimum TLS version to 1.0 or 1.1 in the client that can be used for outbound SSL connections. Restart the system for the changes to take effect.

Note When you update the TLS minimum version from TLSv1.2 to TLSv1.1 or TLSv1.0, restart Cisco Finesse.

In a multi-node Cisco Finesse deployment, run this CLI command on all the nodes of the cluster starting from the publisher. Restart all the nodes after executing the CLI command.

Important Notes

None.

Deprecated Features

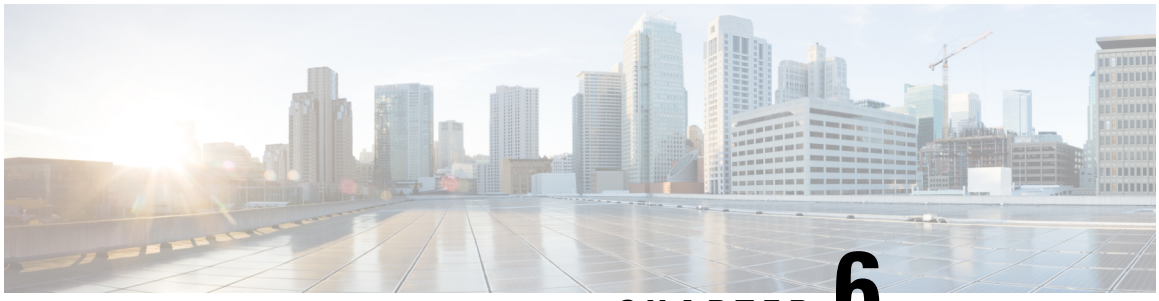
None

Removed and Unsupported Features

None

Third-Party Software Impacts

None



CHAPTER 6

Cisco Unified Intelligence Center

New Features

Dashboards

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

- Create, edit, and manage Dashboards
- Add reports, web pages (URLs), web widgets, and notes to a Dashboard
- Dashboard permalinks
- Mark a Dashboard as favorite and view the personal list of favorites

Chart Configuration

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

- Three step chart creation (Chart Information, Add Data Fields, Preview and Format)
- New chart types; Numeric, Donut
- Create chart view directly from an executed report

Grid View Enhancements

This release provides the following grid view features:

- Improved Threshold selection
- Enabled Group Expansion at a per view level

Updated Features

TLS v1.2 Support

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

Important Notes

Post Installation or Upgradation Tasks

After installation or upgradation of the Cisco Unified Intelligence Center release 11.6, ensure to perform the following actions in OAMP:

Procedure

Step 1 Disable the Unified CCE User Integration. (Uncheck the **Enable UCCE User Integration** check box in **OAMP** > **Cluster Configuration** > **UCCE User Integration**.)

Step 2 Install the latest Cisco Options Package (COP) file for Unified Intelligence Center 11.6 release.

Step 3 Enable the Unified CCE User Integration.

Upgrade Considerations

Dashboard Widgets

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

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

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

Unsupported Widgets

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

- Schedule Report widgets
- URL widgets containing Dashboard permalinks (Nested Dashboards)

Migration Limitations

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

- Schedule Report widgets.
- URL widgets containing Dashboard permalinks (Nested Dashboards).
- Widgets that were placed beyond the new Dashboard canvas size.

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

- Inaccurate widgets (inaccurate database records)

  Example: Report widgets with missing Report Views.

Note For the Schedule Report widgets and Nested Dashboard widgets that are not migrated, the Cisco Unified Intelligence Center server logs do not capture the logs.

For all other widgets, Cisco Unified Intelligence Center server logs captures the log information with the corresponding Dashboard and widget name.

CLI Commands - Switch to TCP/IP

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

- utils cuic cluster show
- utils cuic cluster refresh
- utils cuic cluster mode

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

Screen Resolution Support

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

User Integration to Import Supervisors

After upgrading to Cisco Unified Intelligence Center 11.6, from the Administration Console, perform the User Integration operation (Cluster Configuration > UCCE User Integration) manually to import the Supervisors with the required roles. This setting is required to view gadgets in the Cisco Finesse Desktop for Supervisors.

For more information on User Integration, see *Unified CCE User Integration Configuration* section in the *Administration Console User Guide for Cisco Unified Intelligence Center* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

CUIC Backward Compatibility

Cisco Unified Intelligence Center 11.6(1) supports TLS 1.2. For Cisco Unified Intelligence Center 11.6(1) to be backward compatible with earlier versions, run the CLI command **set tls client min-version**.

This command allows you to set the minimum TLS version to 1.0 or 1.1 in the client that can be used for outbound SSL connections. Restart the system for the changes to take effect.

Note

- When you upgrade the TLS minimum version from TLSv1.0 to TLSv1.1 or TLSv1.2, reinstall the Cisco Unified Real-Time Monitoring Tool.
- In a multi-node CUIC deployment, run this CLI command on all the nodes of the cluster starting from the publisher. Restart all the nodes after executing the CLI command.

Command Syntax
set tls client min-version<*1.0*|*1.1*>

Deprecated Features

None

Removed and Unsupported Features

Dashboards

The Dashboards drawer from the legacy interface is disabled.

Dashboards - Slideshow

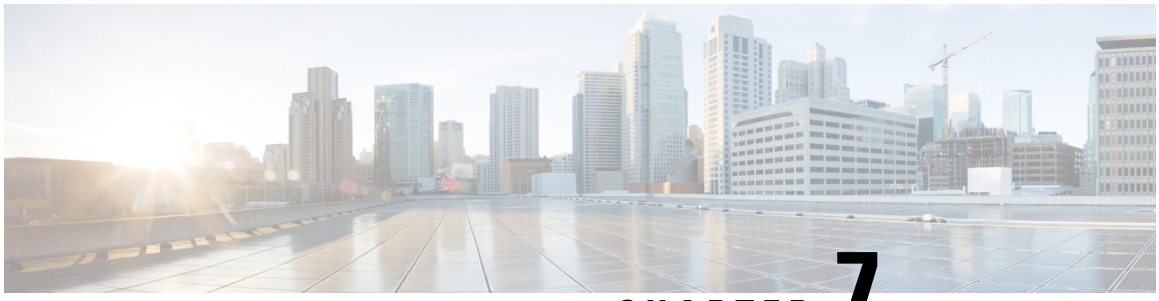
The Dashboard slideshow feature that was used to move through items on the dashboard is removed.

Scheduled Reports on Dashboards

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

Third-Party Software Impacts

None



CHAPTER 7

Cisco Enterprise Chat and Email

New Features

Attachments to Email, Chat and Knowledge Base Articles

You must be an administrator to configure this feature.

As an administrator, you can specify the file types that can be attached to emails, chat messages, and articles in the knowledge base. You can choose to allow or block specific file types by creating a white list or black list. Additionally, for Chat, you can enable attachments, and specify maximum size for each attachment. Lastly, you can control the attachments for chat using queues and limit file sharing to chats received through specific queues.

Customers and agents can now send files to each other during a chat. The customers and agents can use the paper clip attachment button to browse to a file and attach it. Customers can also drag and drop files into the chat text editor.

Agent Not Ready Codes

This release supports the Not Ready reason codes in the Administration Console. This allows you as an Administrator, to configure the deployments to require a reason from agents for not being available to handle activities, such as breaks, meetings, meals, or training.

When you enable this setting, it displays a popup to agents when they mark themselves not available for any of the channels for which they had previously marked themselves as available.

Localization of Custom Attributes

You can localize the custom attribute names created from the Tools Console, using the user interface. In the cases where the custom attributes use enumerated values, you can localize the enumerated values also.

Customer Facing API for Chat

This release provides new Chat Web Services APIs to hide or show the chat on the web sites, based on the availability and capacity of agents to handle new chats.

REST Based Adapters

Enterprise Chat and Email supports new REST based Data Adapters. These data adapters provide capabilities to fetch information by executing RESTful Web Services exposed by third party applications.

Encrypted Logs

This release supports encrypting all the logs. To enable encryption, update the Encrypt Logs setting at the partition level in the System partition, as a system administrator.

By default, the logs are not encrypted by the application. To decrypt the logs, use the logs_decryption_utility, available in the Utilities folder on the services server.

SDK Support for Chat

This release provides JavaScript based SDK support for Chat, Callback, and Delayed Callback.

Factory Reset of Custom Attributes

This Release provides the Factory Reset option for the Context Service feature. You can, as an administrator, reset the configuration files of the service to the original state and remove all the updates that have been installed by the service automatically. The configuration files are updated again to the latest version when you restart the Context Service.

Updated Features

TLS V1.2 Support

Enterprise Chat and Email supports TLS v1.2. As an Administrator, you can now configure email aliases with TLS authentication from the Administration Console.

You can also configure the partition setting or the Default SMTP server setting to use TLS, SSL or Plain text.

Enhanced Chat Management

This release adds the following chat enhancements:

- A new chat template set called Aqua that enables the website visitors to conduct chat interactions with the agents using a docked chat window within the same browser window that they are currently viewing.

  The chat window remains in place while the customer moves from page to page. This feature offers seamless escalation from virtual assistant to chat agent.

- Alternative engagement options to contact the business (such as **Send an email**, **Visit the FAQ** page) can now be displayed to chat customers while they are waiting for agent to join the chat. Once an agent joins the chat, the options are removed from the chat window. You can display these options as soon as the customer starts the chat, or after a delay.

- Sharing files during chat as attachments.

- SAML v2 authentication for chat login helps you configure the chat entry points to transfer customer context information from the company website to ECE. This allows customers (who are already recognized on the company website to use a SSO-enabled entry point) to chat with an agent without the need to provide repetitive information.

  This feature is available for auto-login configuration only.

Callback and Delayed Callback Enhancements

In this release, you need not configure the voice MRD in the Import Wizard.

This release provides a queue for the voice MRD. Configure this queue with a script selector to use it to process the Callback and Delayed Callback activities.

Enhanced SMTP Settings

This release adds the following enhancements to the SMTP settings:

- Default SMTP server settings is a new setting available at the partition level. Administrators can configure the server from this one setting. The following settings are available through this new setting.
  - Default SMTP Server
  - Default SMTP Protocol
  - SMTP Flag
  - Default SMTP User Name
  - Default SMTP Password
- The Maximum Email Size for Dispatcher (MB) setting has been adjusted to allow the minimum value of the setting to be as low as 1.
- This release supports displaying 24-hour date/time format in the application. Configure this feature in the Date and time format setting at the department and user level.
- A new setting **Allow Activity Transfer to Agents Who Are Not Logged In** is now available to allow users to transfer activities to other agents who are not logged in to work on activities.
- The setting **Allow activity transfer to agents who are not available** has been split into two settings: **Allow chat transfer to agents who are not available** and **Allow email transfer to agents who are not available** to allow separate control for email and chat activities.

Exception Queue for Additional Emails

Emails that the Retriever does not parse, are now routed to the Default exception queue.

The following settings are no longer required and have been removed:

- Action on exception emails.
- Exception mail redirection from address.
- Exception mail redirection to address.

Important Notes

None.

Deprecated Features

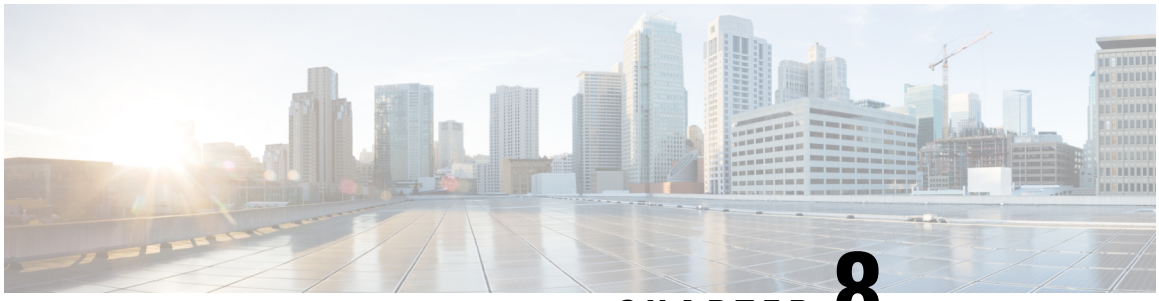
None.

Removed and Unsupported Features

None.

Third-Party Software Impact

See the Unified CCE Compatibility related information located at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for information on third-party software.



CHAPTER 8

Cisco Remote Expert Mobile

New Features

Application Partitioning

Cisco Remote Expert Mobile now supports application partitioning. This feature enables you to pause and resume the co-browse session.

Horizontal Scroll Buttons

This feature provides sideways scroll buttons to change the area viewed in the window, when the co-browse area extends beyond the viewable window.

IE/Edge Touch Support

Cisco Remote Expert Mobile supports the desktop version of Opera.

Note Cisco Remote Expert Mobile does not support the mobile version of Opera.

Opera Browser Support

Cisco Remote Expert Mobile supports touch gestures in Internet Explorer and Edge browsers.

Zoom Feature

The Agent Consoles now have a zoom feature to enable them to magnify their view of the customer's desktop.

Consumer Shadow Pointer

The mouse pointer on the customer's screen is now displayed on the Agent Console during co-browse.

Disabling Agent Features

You can now disable the Specific Expert Assist features in the Exper Assist Configuration.

Audio-Only Calls

Applications can now make audio-only or video-only calls by setting the appropriate flags when making the call.

Updated Features

Android Device Support

Cisco Remote Mobile Expert now supports Android 7.0.

Cisco Remote Mobile Expert also supports the revised Android 6.0 permissions feature. Android changed its permissions setup to enable you to grant permissions to applications while the application is running. For more details, see the Android documentation at the following URL: https://developer.android.com/training/permissions/requesting.html

Consumer-side Logging

You can disable the consumer-side logging.

This allows you to manage the logs that are collected and control the published logs more effectively.

Important Notes

Safari 10.1 Support

The Safari 10.1 WebSockets implementation has a limit on how much data can be sent in a single frame. This is a known issue https://bugs.webkit.org/show_bug.cgi?id=170463 with Safari 10.1. This link contains a patch for the browser.

CLI

After upgrading to Remote Expert Mobile, Release 11.6 from Release 11.5, you need to disable startup tasks in the CLI:

- Load the file `/opt/cisco/cli/Configuration.properties` into a text editor.
- The file has a standard format for a configuration file. Find the *run.startup.tasks* property and either set it to false or comment it out by adding a hash sign (#) at the start of the line.
- Save the file.

You must do this on each node.

Unauthorized URLs

A malicious Agent can push an unauthorized URL to a customer using the Agent Console. This requires the Agent to be logged into their account in the Agent Console. Only authorized Agents can perform such operations outside the scope of normal usage.

Finesse Gadget and Console

The following caveats for the Finesse Gadget and Console apply to this release:

- The mouse pointer image does not show in the Finesse Console.
- On Safari/iOS, video does not resume after hold.
- There is no video after a call is transferred.

Remote Expert Mobile Client SDK

This release includes the following updates:

iOS

- Supports only iOS version 7 or later.
- When CSDK is used for Voice and Video, a red banner displays at the top of the device's screen when the application is put into the background. This is an iOS feature, and cannot be controlled by the application. It permits the user to tap the banner to return to the application.

Plug-ins

- Supports VP8 and H.264 video.
- To configure this, see Cisco Remote Expert Mobile—Install and Config Guide > Configuring IE and Safari Plug-Ins:

Browser	Last Released Version	Minimum Acceptable Version
Internet Explorer	3.2.2	3.2.2

Browser	Last Released Version	Minimum Acceptable Version
Safari	3.2.2	3.2.2

Deprecated Features

None.

Removed and Unsupported Features

Other Features Removed

Feature	Effective from Release	Replacement
Instant Messaging and Presence (IM&P)	Cisco Unified Contact Center Enterprise, Release 11.5(1)	None.

Third-Party Software Impact

See the Unified CCE Compatibility related information located at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for information on third-party software.

Patching the OS

See the *Guidelines for Updating Security Patches* section in the *Cisco Remote Expert Mobile Design Guide*.

Supported iOS

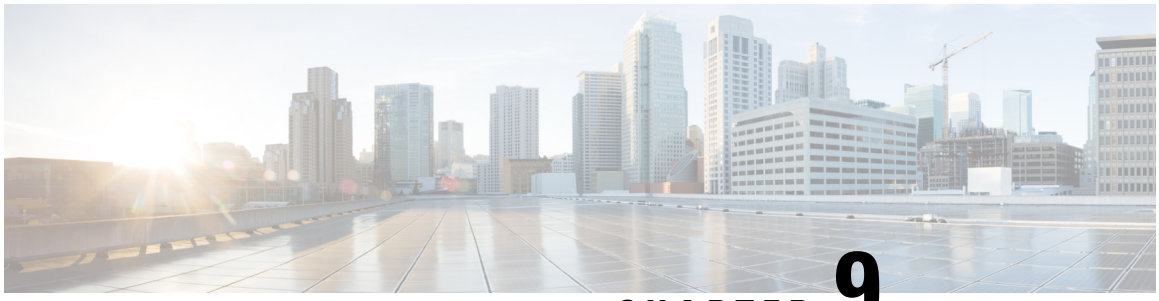
Only iOS version 7 or later are supported.

Supported Web Browsers

The Cisco Remote Expert Mobile Design Guide provides the details of the supported browsers:

- Versions of browsers late than the ones stated in the Cisco Remote Expert Mobile Design Guide may not be compatible.
- Some versions of Internet Explorer are not supported for consumers.
- Web browsers are not supported on iOS or Android.

- Opera v.42 is compatible with REM, but the `isBrowserSupported` function returns `false` for all the versions of Opera. Do not call the `isBrowserSupported` function unless it is verified that the browser is not Opera.



CHAPTER 9

Cisco SocialMiner

The standalone SocialMiner features such as Facebook page, Twitter, RSS Feeds, Standalone single session chat, associated features like filters and notifications have been removed from release 12.0. However, you can still use SocialMiner interface to encrypt MR.

New Features

AUDIT Log Support for all Config changes

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

CORS Support

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

Updated Features

TLS v1.2 Support

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

Important Notes

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

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

Deprecated Features

None

Removed and Unsupported Features

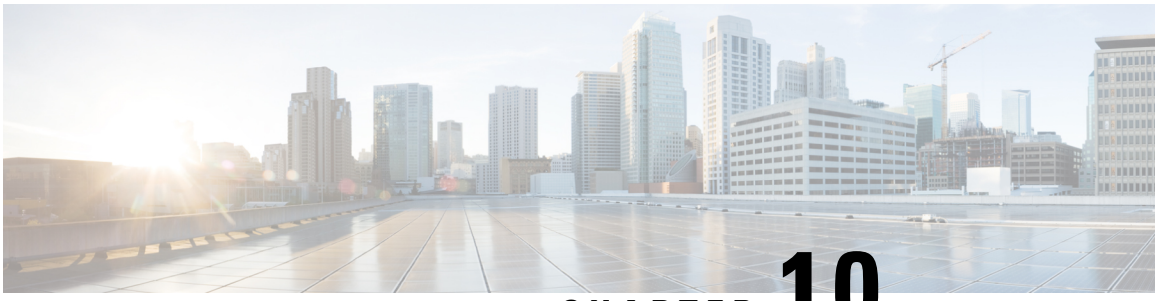
Ability to Browse and Download Logs via HTTP

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

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

Third-Party Software Impacts

None



CHAPTER 10

Cisco Unified Contact Center Domain Manager

New Features

Updated Features

TLS Versions Support

This release supports Transport Layer Security (TLS) v1.2 and uses it as the default option. The older versions of TLS/SSL are disabled by the Installer.

Note In case there are third party applications installed on CCE VMs that are impacted when the older versions of TLS/SSL are disabled, re-enable the required TLS/SSL versions. For more information, see Microsoft documentation about enabling TLS/SSL provided by Secure Channel (Schannel security support provider) authentication protocol suite.

Similarly, third party applications must use TLS v1.2 while creating connections to CCE VMs or CCE database.

Note For Microsoft Windows 7 client systems, install the Microsoft Windows Update KB3080079 to ensure that the remote desktop connection over TLS v1.1 or 1.2 is supported.

TLS Options for Cisco Unified CCE and Other Components

Configure TLS v1.2 on all the components and Unified CCE. Internet Script Editor (ISE), and other web applications require TLS v1.2 for HTTPS connections.

Note TLS v1.2 is installed by default on all Cisco VOS based deployments.

For Live Data, CUIC, and Cisco IdS to interoperate with older versions of Unified CCE, run the **set tls client min-version** command on these components to set the minimum TLS version to v1.0 or v1.1 as required.

See the individual component sections for more details on upgrade considerations and default behavior of TLS v1.2 in that component.

Component	Default Option
Cisco Unified CCE	TLS v1.2
Cisco Unified Intelligence Center	TLS v1.2
Cisco Finesse	TLS v1.2
Cisco CVP and VVB	TLS v1.2
Cisco SocialMiner	TLS v1.2
Enterprise Chat and Email	TLS v1.2
Cisco Unified Contact Center Domain Manager	TLS v1.2

Use the Transport Layer Security CLI commands to view or change the TLS minimum version for inbound or outbound connections. For product-specific TLS configuration, see *Configuration Guide for Cisco Hosted Collaboration Solution for Contact Center* at http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Skill Group Routing

When you create a new skill group in any of the following ways, a new route will be automatically associated to that skill group:

- Resource Management Gadget User Interface
- Resource Management Web Services
- Bulk Upload

To enter a name for the route (instead of the auto-generated name), use the **Route** tab, before you save the skill group.

Browse Domain Accounts

Users with Global Roles can browse through domain accounts. To browse through other supervisor or user accounts, check the **Browse Domain Accounts** checkbox in the **Global Roles** window.

Agent Supervisor Fields

From this release, an agent can have only one supervisor. When you create an Agent record for a person who already has a Supervisor assigned, the **Supervisor** checkbox is disabled. When SSO is disabled, the agent must enter their domain login name to login.

Deprecated Features

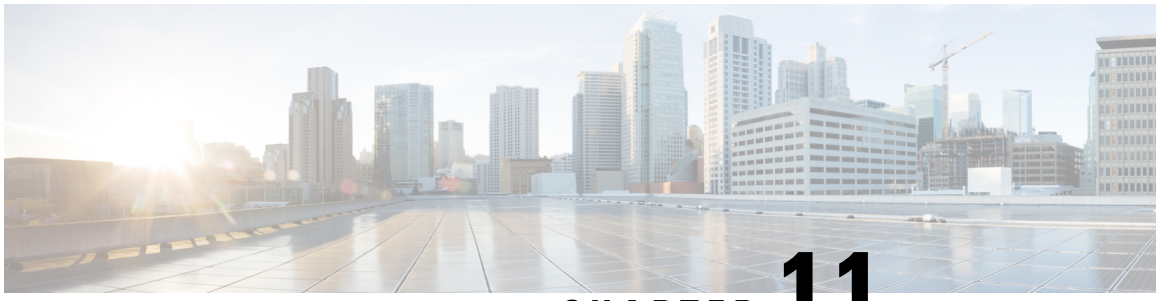
There are no deprecated features for this release.

Removed and Unsupported Features

There are no removed and unsupported features for this release.

Third-Party Software Impacts

There are no third-party software impacts for this release.



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 11.6(1)

Use the following links to the Bug Search Tool to view a list of Severity 3 or higher caveats for each product or component for the current release. You can filter the result by setting the filter values in the tool.

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

Cisco Packaged Contact Center Enterprise

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284360381&rls=11.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Hosted Collaboration Solution for Contact Center

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=284526699&rls=11.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Unified Contact Center Enterprise

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=268439622&rls=11.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Unified Intelligence Center

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

Cisco Unified Customer Voice Portal

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=270563413&rls=11.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Finesse

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

Cisco SocialMiner

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

Cisco Unified Contact Center Management Portal

https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=280810493&rls=11.6(1)&sb=anfr&svr=3nH&bt=custV

Cisco Enterprise Chat and Email

You can search for the following caveats in the Bug Search Tool:

- CSCvf49821 A dialog box displaying "Please select an item" appears after clicking F4 for the Case_ID of a closed case selected.
- CSCvf19519 ECE 11.5 uninstaller is not working for fully distributed ECE Release 11.5 with Microsoft Windows authentication setup.

Cisco Unified Workforce Optimization Workforce Management

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

Cisco Unified Workforce Optimization Quality Management

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