



Communicator for Desktop

UC-One for Desktop

Configuration Guide

Communicator Release 22.9.37

UC-One SaaS Release 3.9.37

Document Version 1

Copyright Notice

Copyright© 2022 Cisco Systems, Inc. All rights reserved.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

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.

Document Revision History

Release	Version	Reason for Change	Date
9	1	Branded document with BroadSoft template.	December 10, 2011
9	1	Edited document.	December 10, 2011
9	1	Made minor modifications. Edited and published document.	December 20, 2011
9.0.1	2	Updated logging parameters in section 10.18 Logging .	January 18, 2012
9.0.1	2	Edited and published document.	February 16, 2012
9.1.0	1	Added section 2 Changes for Configuration Files . Removed and modified some deprecated information.	March 28, 2012
9.1.0	1	Corrected cross-references in two places. Added details about installing and uninstalling for OS X. Described the telephone-event payload type configuration change.	March 30, 2012
9.1.0	1	Edited changes and published document.	April 2, 2012
9.1.0	2	Edited document based on feedback. Removed Linux references. Removed references to RCS, RCSe, RCS2, SMS, MMS, and OMA.	April 10, 2012
9.1.0	2	Edited changes and published document.	April 13, 2012
9.2.0	1	Edited changes for Release 9.2.0.	June 21, 2012
9.2.0	1	Edited changes and published document.	June 29, 2012
9.2.0	2	Re-introduced voice mail details after accidental deletion in previous version of this document.	July 5, 2012
9.2.0	2	Edited changes and published document.	July 5, 2012
9.2.2	1	Fixed errors in proxy discovery example. Added details about banner support. Added information about Real-Time Transport Protocol (RTP) port range configurations. Fixed error in proxy discovery example. Fixed incorrect reference to %SBC_PORT% in preferred-port; it now refers to correct variable, %SOURCE_PORT%.	July 26, 2012
9.2.2	1	Edited changes and published document.	July 26, 2012
9.2.2	2	Removed outdated information.	August 27, 2012
9.2.2	2	Edited changes and published document.	August 29, 2012
9.3.0	1	Added details related to the client version update for Release 9.3.0: file transfer, Xsi-version, call diversion inhibitor, help URL, and directory listing. Added details related to support for multiple configuration versions in one configuration file. Added information related to new codec-configurations. Added "Xsi-Only" package.	September 27, 2012

Release	Version	Reason for Change	Date
9.3.0	1	Edited changes and published document.	September 27, 2012
9.3.2	1	Corrected details about %XSI_VERSION% values and added information about %XSI_NAMESPACE%. Corrected error in configuration file example regarding toggling call-info subscriptions. Introduced a new tag variable to control the XMPP protocol (%ENABLE_XMPP%). Added new variable to define <i>tcp-threshold</i> size (%TCP_SIZE_THRESHOLD%). Fixed missing reference to %ENABLE_MEDIA_SHARE% in the example configuration file.	October 15, 2012
9.3.2	1	Edited changes and published document.	November 2, 2012
10.0.0	1	Updated document for Release 10.0.0.	December 21, 2012
10.0.0	1	Edited changes and published document.	December 27, 2012
10.0.1	1	Updated document for Release 10.0.1.	January 30, 2013
10.0.1	1	Edited changes and published document.	February 6, 2013
10.0.1	2	Added <i>preferred-port</i> text and removed some unsupported text.	February 8, 2013
10.0.1	2	Edited changes and published document.	February 8, 2013
10.0.2	1	Added new configuration items.	March 19, 2013
10.0.2	1	Edited changes and published document.	March 26, 2013
10.0.3	1	Added information about configuration parameters and Domain Name System (DNS) configuration.	May 3, 2013
10.0.3	1	Edited changes and published document.	May 13, 2013
10.0.4	1	Added information on DNS proxy discovery, Secure Sockets Layer (SSL) certificates, and video optimization.	June 11, 2013
10.0.4	1	Edited changes and published document.	June 28, 2013
10.1	1	Added configuration parameters for <i>My Room</i> , Xsi-Events, call transfer, contact card, and Lightweight Directory Access Protocol (LDAP).	August 19, 2013
10.1	1	Edited changes and published document.	August 30, 2013
10.1	2	Added information about the Secure Real-time Transport Protocol (SRTP).	September 4, 2013
10.1	2	Edited changes and published document.	September 5, 2013
10.1	3	Made small correction and republished document.	September 11, 2013
10.1	4	Added flow-through provisioning parameters.	September 12, 2013
10.1	4	Edited changes and published document.	September 13, 2013
10.1	5	Added Login dialog section.	October 1, 2013

Release	Version	Reason for Change	Date
10.1	5	Edited changes and published document.	October 9, 2013
10.1.2	1	Added SRTP information, changed document-numbering scheme, and removed unused diagnostics logging option.	October 14, 2013
10.1.2	1	Edited changes.	October 31, 2013
10.1.2	1	Reviewed editing changes.	October 31, 2013
10.1.2	1	Edited changes and published document.	November 1, 2013
20.0.0	1	Updated document for Release 20.0.0, added Device Management (DM) tags, and updated configuration parameters. Described new features: Security Classification, Attended Transfer, Call Pull, Call Park/Retrieve, Call and Chat Recording, SRTP enhancements, file transfer encryption, logging enhancements, video enhancements, Xtended Services Interface (Xsi) failover, XMPP failover, and connectors.	November 25, 2013
20.0.0	1	Edited changes and published document.	December 18, 2013
20.0.0	2	Changed numbering scheme to 20.0.0 and made minor edits.	December 19, 2013
20.0.0	2	Edited changes and published document.	December 23, 2013
20.0.0	3	Added IM_SECURITY_LEVEL DM tag and modified the template to include tag information with the configuration example.	January 7, 2014
20.0.0	3	Edited changes and published document.	January 10, 2014
20.0.0	4	Corrected local generation of <i>Busy – In Call</i> example.	January 13, 2014
20.0.0	4	Edited changes and published document.	January 15, 2014
20.0.0	5	Removed future configuration options from the parameter lists and added additional information about the call transfer option.	January 17, 2014
20.0.0	5	Edited changes and published document.	January 17, 2014
20.0.1	1	Added a new configuration parameter for Sharing Server (USS), edited <i>ini-file</i> examples, modified location publishing section, added a new parameter for XMPP certificate handling, and modified N-way video, added reference to the <i>UC-One Solution Guide</i> for SIP failover and version check.	January 20, 2014
20.0.1	1	Edited changes and published document.	February 6, 2014
20.0.1	2	Added text to conference auto-provisioning, changed text about N-way video, as behavior has been changed, and added text to Transport Layer Security (TLS) certificates. Added text to section 10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence .	February 10, 2014
20.0.1	2	Edited changes and published document.	February 10, 2014
20.0.1	3	Made changes to section 6 Installation .	February 11, 2014
20.0.1	3	Edited changes and published document.	February 13, 2014
20.0.1	4	Added section 10.16.8 XMPP SRV Support and Certificate Validation .	February 18, 2014

Release	Version	Reason for Change	Date
20.0.1	4	Edited changes and published document.	February 25, 2014
20.0.2	1	Modified text for <i>Busy – In call</i> and Shared Call Appearance (SCA) section, silent installation, HTTP proxy authentication and server settings, removed unused parameters and their text, added text about SSL certificates, re-ordered sections, and added text to SIP proxy discovery and version control failover.	March 17, 2014
20.0.2	1	Updated reference to the Cisco BroadWorks Sharing Server. Edited changes and published document.	March 31, 2014
20.1.0	1	Added information about new configuration parameters and the new features: forced logout, Echo service, integrated call window, configurable left pane order, silent dialing into Meet-Me Conference, flexible contact card configuration, and add-in enhancements. Made changes to file transfer text about size limits, ad hoc room size, and Sharing Server (USS) failover. Added a new tag for call-info subscription.	April 22, 2014
20.1.0	1	Edited changes and published document.	April 29, 2014
20.1.0	2	Added information about DM tag %BWE164-x% into federated calling, added note about forced logout, added a section about disabling Xsi search, and added two new DM tags for <i>rport</i> and contact card.	May 2, 2014
20.1.0	2	Edited changes and published document.	May 26, 2014
20.1.1	1	Added DM tag %USE_PROXY_DISCOVERY%. Modified text for SIP proxy discovery. Added information about bandwidth consumption. Made minor change in the <i>displayname-order</i> node and added section 10.19.4 <i>Display Name for Contacts</i> . Added /ALLUSERS switch to installation from the command line.	June 17, 2014
20.1.1	1	Edited changes and published document.	June 20, 2014
20.1.1	2	Corrected the tag-name for Meet-Me direct-dial value.	July 14, 2014
20.1.1	2	Edited changes and published document.	July 16, 2014
20.1.1	3	Modified file locations chapter, added DM tag for Real-Time Control Protocol (RTCP) XR local group, updated the DM tag for Call Pull, updated the contact card sync DM tag in section 10.19.2 <i>Flexible Contact Card Field Configuration</i> , added voice mail section, and added DM tag tables.	August 1, 2014
20.1.1	3	Reformatted section <i>1 Summary of Changes</i> . Edited changes and published document.	August 7, 2014
20.2.0	1	Updated config example in Federated Calling in XMPP Deployments section, added more details to file transfer encryption, added new configuration parameters, and added Cisco BroadWorks requirements for Meet-Me.	August 15, 2014
20.2.0	1	Edited changes and published document.	September 26, 2014
20.2.0	2	Updated Cisco BroadWorks requirements for Meet-Me Moderator Controls.	October 1, 2014
20.2.0	2	Edited changes and published document.	October 2, 2014

Release	Version	Reason for Change	Date
20.2.0	3	Edited Cisco BroadWorks requirements for Meet-Me Moderator Controls and added more text about TCP and UDP keepalives.	October 15, 2014
20.2.0	3	Edited changes and published document.	November 6, 2014
21.0.0	1	Added text about new features: Team Telephony, new media framework, Executive-Assistant, new search options, TLS1.2, Video Server, guest client, Emergency Call Service Address verification, DNS Time to Live (TTL), and minimize Communicator option. Modified sections 1 through 9 based on review. Changed format of the document, modified text for full directory, and used new template with new corporate identity.	November 19, 2014
21.0.0	1	Rebranded document and updated the BroadSoft legal notice. Edited changes and published document.	December 21, 2014
21.0.0	2	Removed <i>Appendix B</i> , which is moved to the <i>UC-One Solution Guide</i> .	December 22, 2014
21.0.0	2	Edited changes and published document.	December 30, 2014
21.0.0	3	Modified text about BroadSoft Media Engine (BME) logging and made minor editorial changes. Added reference to Cisco BroadWorks specifications in the call recording section.	January 5, 2015
21.0.0	3	Edited changes and published document.	January 8, 2015
21.0.0	4	Added Video Server (UVS) configuration details and Microsoft Installer (MSI) information as well as location configuration information.	January 30, 2015
21.0.0	4	Edited changes and published document.	February 5, 2015
21.1.0	1	Added new features: Microsoft Lync Integration, web button, terminating Xsi call control, XMPP security enhancements, and Emergency Call Service Address Change (ECACS) menu. Added more details to the TLS certificate section, incoming call display name matching as well as N-way video parameters (in Video Server case). Added Team Telephony userid limitations, new Xsi parameter for ad hoc conferences, and DM tag for RTP Maximum Transmission Unit (MTU). Removed %USS_MAX_PARTICIPANTS%. Added Message Waiting Indicator (MWI) text and DM tags as well as text about disabling SIP. Added idle detection description and tags as well as text about Call History. Added text about SIP refresh and timers and SIP vs Tel Uniform Resource Identifier (URI) dialing. Added text about configurable left pane and Outlook search local cache.	March 9, 2015
21.1.0	1	Edited changes and published document.	April 1, 2015
21.1.0	2	Added a note about share joining and no fallback in XMPP failover, SIP port allocation, and Sharing Server (USS) certificates. Modified text for <i>P-Associated-URI</i> and file transfer as well as share parameter usage. Added a note to section 10.16.3 SSL/TLS Certificates .	April 7, 2015
21.1.0	2	Edited changes and published document.	April 15, 2015

Release	Version	Reason for Change	Date
21.2.0	1	Added a note about contact card sync without XMPP, SIP URI validation, and enhanced text for SUBSCRIBE retry interval. Added note about SIP/TLS with dynamic proxy discovery, dynamic proxy discovery text update, and new features: Skype for Business (S4B), Visual Voice Mail, share passing, Call Center Agent, presence rules. Removed Windows Vista. Corrected voice mail disabling configuration and MWI configuration. Added a note to web button limitations. Added text to SRTP section. Edited uninstallation text and OpenLDAP auth details. Added version control details and sticky 302 support.	May 4, 2015
21.2.0	1	Edited changes and published document.	June 29, 2015
21.2.0	2	Added a note about non-SCA deployments.	July 2, 2015
21.2.0	2	Added Acronyms and Abbreviations . Edited changes and published document.	July 8, 2015
21.2.1	1	Modified picture for TLS certificates. Modified DM table for Dynamic Video Bit Rate Adaptation (DVBA). Updated call transfer default value and example.	July 27, 2015
21.2.1	1	Edited changes and published document.	July 29, 2015
21.3.0	1	Added text to dynamic SIP proxy discovery and DVBA configuration, corrected LDAP example, added a note to S4B section about Xsi-Only configuration, added Team Telephony, and added new features.	December 14, 2015
21.3.0	1	Edited changes and published document.	December 18, 2015
21.3.3	1	Added new features and a made editorial changes.	March 22, 2016
21.3.3	1	Edited changes and published document.	March 30, 2016
21.4.0	1	Added new features and a made editorial changes.	April 5, 2016
21.4.0	1	Edited changes and published document.	April 25, 2016
21.5.0	1	Updated document for Release 21.5.0.	July 13, 2016
21.5.0	1	Edited changes and published document.	July 21, 2016
21.5.2	1	Updated document for Release 21.5.2. Added one parameter and tag to section <i>2.2 Changes for Configuration Files for Release 21.5.2</i> (which was subsequently removed).	November 3, 2016
21.5.2	1	Edited changes and published document.	November 8, 2016
21.6.0	1	Added new and changed features.	November 21, 2016
21.6.0	1	Edited changes and published document.	December 20, 2016
21.6.0	2	Added a note about Cisco BroadWorks aliases.	December 23, 2016
21.6.0	2	Edited changes and published document.	December 27, 2016
21.6.1	1	Added new parameter and notes.	January 2, 2017
21.6.1	1	Edited changes and published document.	January 12, 2017

Release	Version	Reason for Change	Date
21.6.2	1	Added notes.	February 16, 2017
21.6.2	1	Edited changes and published document.	February 16, 2017
22.0.0.	1	Added new features for Release 22.0.0.	March 22, 2017
22.0.0	1	Edited changes and published document.	March 30, 2017
22.0.1	1	Added LDAP configuration and notes.	April 18, 2017
22.0.1	1	Edited changes and published document.	May 19, 2017
22.1.0	1	Added new features and notes for Release 22.1.0.	June 8, 2017
22.1.0	1	Edited changes and published document.	June 27, 2017
22.2.0	1	Added new functionality and notes.	August 2, 2017
22.2.0	1	Added RTCP MUX. Added note about E.164 flag.	September 27, 2017
22.2.0	1	Edited changes and published document.	September 29, 2017
22.2.1	1	Added notes.	October 5, 2017
22.2.1	1	Edited changes and published document.	November 14, 2017
22.3.0	1	Added notes and new features.	November 16, 2017
22.3.0	1	Edited changes and published document.	December 22, 2017
22.3.1	1	Made minor changes.	December 29, 2017
22.3.1	1	Edited changes and published document.	January 30, 2017
C 22.3.1 S 3.3.0	1	Added UC-One Software as a Service (SaaS) information.	February 1, 2018
C 22.3.1 S 3.3.0	1	Edited changes and published document.	February 19, 2018
C 22.4.0 S 3.4.0	1	Made additional edits.	March 7, 2018
C 22.4.0 S 3.4.0	1	Edited changes and published document.	March 27, 2018
C 22.4.0 S 3.4.0	2	Made textual edits.	April 12, 2018
C 22.4.0 S 3.4.0	2	Edited changes and published document.	April 23, 2018
C 22.4.2 S 3.4.0	1	Added new features and made edits.	May 18, 2018
C 22.4.2 S 3.4.0	1	Edited changes and published document.	May 25, 2018
C 22.5.0 S 3.5.0	1	Added new features and made editorial changes.	June 5, 2018

Release	Version	Reason for Change	Date
C 22.5.0 S 3.5.0	1	Edited changes and published document.	June 26, 2018
C 22.5.2 S 3.5.1	1	Added additional configuration details introduced in Release 22.5.2 for Lightweight Directory Access Protocol (LDAP)-configurability. Clarified command line options usage for installer.	July 18, 2018
C 22.5.2 S 3.5.1	1	Edited changes and published document.	July 19, 2018
C 22.5.3 S 3.5.3	1	Added new features and made editorial changes.	July 31, 2018
C 22.5.3 S 3.5.3	1	Edited changes and published document.	August 30, 2018
C 22.6.0 S 3.6.0	1	Added new features and made editorial changes.	September 3, 2018
C 22.6.0 S 3.6.0	1	Edited changes and published document.	October 11, 2018
C 22.6.1 S 3.6.1	1	Added new features and made editorial changes.	October 15, 2018
C 22.6.1 S 3.6.1	1	Edited changes and published document.	October 25, 2018
C 22.7.0 S 3.7.0	1	Added new features and made editorial changes.	November 13, 2018
C 22.7.0 S 3.7.0	1	Edited changes and published document.	January 8, 2019
C 22.7.5 S 3.7.5	1	Added updates and made editorial changes.	July 2, 2019
C 22.7.5 S 3.7.5	1	Edited changes and published document.	July 4, 2019
C 22.7.5 S 3.7.5	2	Added another configuration parameter.	July 5, 2019
C 22.7.5 S 3.7.5	2	Edited changes and published document.	July 9, 2019
C 22.7.6 S 3.7.5	1	Added updated configurations.	August 12, 2019
C 22.7.6 S 3.7.5	1	Edited changes and published document.	August 14, 2019
C 22.7.6 S 3.7.5	2	Added a note.	September 9, 2019
C 22.7.6 S 3.7.5	2	Edited changes and published document.	September 13, 2019
C 22.9.1 S 3.9.0	1	Added notes and new features.	August 16, 2019

Release	Version	Reason for Change	Date
C 22.9.1 S 3.9.0	1	Edited changes and published document.	September 30, 2019
C 22.9.2 S 3.9.0	1	Corrected version number.	October 29, 2019
C 22.9.2 S 3.9.0	1	Edited changes and published document.	October 29, 2019
C 22.9.2 S 3.9.1	1	Added notes.	November 26, 2019
C 22.9.2 S 3.9.1	1	Edited changes and published document.	November 28, 2019
C 22.9.6 S 3.9.6	1	Added notes.	January 22, 2020
C 22.9.6 S 3.9.6	1	Edited changes and published document.	January 29, 2020
C 22.9.6 S 3.9.6	2	Added notes.	January 30, 2020
C 22.9.6 S 3.9.6	2	Edited changes and published document.	January 31, 2020
C 22.9.8 S 3.9.8	1	Updated document for Communicator Release 22.9.8 and UC-One SaaS Release 3.9.8.	February 21, 2020
C 22.9.8 S 3.9.8	1	Edited changes and published document.	February 25, 2020
C 22.9.10 S 3.9.10 W 3.0	1	Updated document for Communicator Release 22.9.10, UC-One SaaS Release 3.9.10, and Webex with BroadWorks Calling 3.0.	April 14, 2020
C 22.9.10 S 3.9.10 W 3.0	1	Edited changes and published document.	April 16, 2020
C 22.9.12 S 3.9.12 W 3.0	1	Updated document for Communicator Release 22.9.12, UC-One SaaS Release 3.9.12, and Webex with BroadWorks Calling 3.0.	May 13, 2020
C 22.9.12 S 3.9.12 W June 20	1	Added section <i>12 Webex for BroadWorks</i> (which was subsequently removed). Added <i>Appendix C: Webex for BroadWorks DM Tag Provisioning Script</i> (which was subsequently removed).	June 3, 2020
C 22.9.12 S 3.9.12 W June 20	1	Added parameters and notes.	June 22, 2020
C 22.9.12 S 3.9.12 W June 20	1	Edited changes and published document.	June 29, 2020

Release	Version	Reason for Change	Date
C 22.9.12 S 3.9.12 W July 20	1	Added parameters and notes.	August 3, 2020
C 22.9.12 S 3.9.12 W July 20	1	Edited changes and published document.	August 4, 2020
C 22.9.14 S 3.9.12 W July 20	1	Added parameters and notes.	August 6, 2020
C 22.9.14 S 3.9.12 W July 20	1	Edited changes and published document.	August 10, 2020
C 22.9.14 S 3.9.12 W Aug 20	1	Added Webex parameters and notes.	August 26, 2020
C 22.9.14 S 3.9.12 W Aug 20	1	Edited changes and published document.	August 27, 2020
C 22.9.16 S 3.9.16 W Sept 20	1	Added Webex parameters and notes.	September 14, 2020
C 22.9.16 S 3.9.16 W Sept 20	1	Edited changes and published document.	September 14, 2020
C 22.9.16 S 3.9.16 W Sept 20	2	Added notes.	September 17, 2020
C 22.9.16 S 3.9.16 W Sept 20	2	Edited changes and published document.	September 18, 2020
C 22.9.16 S 3.9.16 W Sept 20	3	Added notes.	September 22, 2020
C 22.9.16 S 3.9.16 W Sept 20	3	Edited changes and published document.	September 28, 2020
C 22.9.18 S 3.9.18	1	Removed Webex parameters and notes, and added new features.	November 1, 2020
C 22.9.18 S 3.9.18	1	Edited changes and published document.	November 6, 2020
C 22.9.20 S 3.9.20	1	Added new features.	December 9, 2020
C 22.9.20 S 3.9.20	1	Edited changes and published document.	December 17, 2020

Release	Version	Reason for Change	Date
C 22.9.21 S 3.9.21	1	Added internal SSL certificate notification information.	March 4, 2021
C 22.9.21 S 3.9.21	1	Updated copyright notice. Edited changes and published document.	March 5, 2021
C 22.9.22 S 3.9.22	1	Added note about token expiry.	May 24, 2021
C 22.9.22 S 3.9.22	1	Edited changes and published document.	May 27, 2021
C 22.9.24 S 3.9.24	1	Added new configuration for token expiry.	July 15, 2021
C 22.9.24 S 3.9.24	1	Edited changes and published document.	July 19, 2021
C 22.9.30 S 3.9.30	1	Corrected automatic update interval tag.	November 18, 2021
C 22.9.30 S 3.9.30	1	Edited changes and published document.	November 19, 2021
C 22.9.37 S 3.9.37	1	Added new configuration for contact dir request caching.	October 7, 2022

Table of Contents

1	Summary of Changes	22
1.1	Changes for Communicator Release 22.9.37, UC-One SaaS Release 3.9.37	22
1.2	Changes for Communicator Release 22.9.30, UC-One SaaS Release 3.9.30	22
1.3	Changes for Communicator Release 22.9.24, UC-One SaaS Release 3.9.24	22
1.4	Changes for Communicator Release 22.9.22, UC-One SaaS Release 3.9.22	22
1.5	Changes for Communicator Release 22.9.21, UC-One SaaS Release 3.9.21	22
1.6	Changes for Communicator Release 22.9.20, UC-One SaaS Release 3.9.20	22
1.7	Changes for Communicator Release 22.9.18, UC-One SaaS Release 3.9.18	22
1.8	Changes for Communicator Release 22.9.16, UC-One SaaS Release 3.9.16, Webex for BroadWorks Release September 20.....	22
1.9	Changes for Communicator Release 22.9.14, UC-One SaaS Release 3.9.12, Webex for BroadWorks Release August 20	23
1.10	Changes for Communicator Release 22.9.14, UC-One SaaS Release 3.9.12, Webex for BroadWorks Release July 20.....	23
1.11	Changes for Communicator Release 22.9.12, UC-One SaaS Release 3.9.12, Webex for BroadWorks Release July 20.....	23
1.12	Changes for Communicator Release 22.9.12, UC-One SaaS Release 3.9.12, Webex for BroadWorks Release June 20	23
1.13	Changes for Communicator Release 22.9.10, UC-One SaaS Release 3.9.10	24
1.14	Changes for Communicator Release 22.9.8, UC-One SaaS Release 3.9.8.....	24
1.15	Changes for Communicator Release 22.9.6, UC-One SaaS Release 3.9.6.....	24
1.16	Changes for Communicator Release 22.9.2, UC-One SaaS Release 3.9.1.....	25
1.17	Changes for Communicator Release 22.9.2, UC-One SaaS Release 3.9.0.....	25
1.18	Changes for Communicator Release 22.9.1, UC-One SaaS Release 3.9.0.....	25
1.19	Changes for Communicator Release 22.7.6, UC-One SaaS Release 3.7.5.....	25
1.20	Changes for Communicator Release 22.7.5, UC-One SaaS Release 3.7.5.....	25
1.21	Changes for Communicator Release 22.7.0, UC-One SaaS Release 3.7.0.....	26
1.22	Changes for Communicator Release 22.6.1, UC-One SaaS Release 3.6.1.....	26
1.23	Changes for Communicator Release 22.6.0, UC-One SaaS Release 3.6.0.....	26
1.24	Changes for Communicator Release 22.5.3, UC-One SaaS Release 3.5.3.....	27
1.25	Changes for Communicator Release 22.5.2, UC-One SaaS Release 3.5.1.....	27
1.26	Changes for Communicator Release 22.5.0, UC-One SaaS Release 3.5.0.....	27
1.27	Changes for Communicator Release 22.4.2, UC-One SaaS Release 3.4.0.....	28
1.28	Changes for Communicator Release 22.4.0, UC-One SaaS Release 3.4.0.....	28
1.29	Changes for Communicator Release 22.3.1, UC-One SaaS Release 3.3.0.....	28
1.30	Changes for Release 22.3.1	29
1.31	Changes for Release 22.3.0	29
1.32	Changes for Release 22.2.1	29
1.33	Changes for Release 22.2.0	29
1.34	Changes for Release 22.1.0	30
1.35	Changes for Release 22.0.1	30

1.36	Changes for Release 22.0.0	30
2	Changes for Configuration Files.....	32
2.1	Changes for Configuration Files for Release 3.9.37/22.9.37	32
2.2	Changes for Configuration Files for Release 3.9.21/22.9.21	32
2.3	Changes for Configuration Files for Release 3.9.20/22.9.20	32
2.4	Changes for Configuration Files for Release 3.9.18/22.9.18	33
2.5	Changes for Configuration Files for Release 3.9.16/22.9.16/Webex September 20	33
2.6	Changes for Configuration Files for Release 3.9.12/22.9.14/Webex August 20	34
2.7	Changes for Configuration Files for Release 3.9.12/22.9.12/ Webex July 20	34
2.8	Changes for Configuration Files for Release 3.9.12/22.9.12/ Webex June 20	34
2.9	Changes for Configuration Files for Release 3.9.8/22.9.8	35
2.10	Changes for Configuration Files for Release 3.9.6/22.9.6	35
2.11	Changes for Configuration Files for Release 3.9.0/22.9.1	36
2.12	Changes for Configuration Files for Release 22.7.6	37
2.13	Changes for Configuration Files for Release 22.7.0	39
2.14	Changes for Configuration Files for Release 22.6.1	39
2.15	Changes for Configuration Files for Release 22.6.0	40
2.16	Changes for Configuration Files for Release 22.5.3	40
2.17	Changes for Configuration Files for Release 22.5.0	41
2.18	Changes for Configuration Files for Release 22.4.2	42
2.19	Changes for Configuration Files for Release 22.4.0	43
2.20	Changes for Configuration Files for Release 22.3.1	43
2.21	Changes for Configuration Files for Release 22.3.0	43
2.22	Changes for Configuration Files for Release 22.2.0	44
2.23	Changes for Configuration Files for Release 22.1.0	45
2.24	Changes for Configuration Files for Release 22.0.1	45
2.25	Changes for Configuration Files for Release 22.0.0	46
3	Device Management Tags	48
3.1	Communicator Device Type – System Default Tags	48
3.2	Communicator Device Type – Custom Tags.....	49
3.3	Communicator Device Type – Cisco BroadWorks System Tags.....	66
4	Introduction to Configuration	68
5	File Locations	69
6	Installation	71
6.1	Installation Options.....	72
6.2	Install on Windows	74
6.3	Install on OS X	74
6.4	Administration Rights	74
6.5	Uninstall	74
6.6	Limitations.....	74
7	Account-Specific Files	75

7.1	comms_encrypted.db	75
7.2	user_local_data_encrypted.db.....	75
7.3	vCard Cache	77
7.4	Web Cache.....	77
8	Client-Specific Files	78
8.1	Server Settings – config.xml.....	78
8.1.1	Backward Compatibility	78
8.2	Credentials_encrypted.db	79
8.3	HTTP Proxy Settings – proxy_settings.ini	79
8.4	User Interface Settings – application_setting.ini	79
8.5	Connectors_encrypted.db	80
8.6	Logging Definitions – LogConfig.xml	81
9	UC-One SaaS	82
9.1	General	82
10	UC-One Collaborate Config.xml Examples.....	85
10.1	SIP and Calling	85
10.1.1	Change Basic SIP Server Settings.....	85
10.1.2	Codec Configuration for Client.....	88
10.1.3	Force TCP or UDP Usage and Keepalives.....	89
10.1.4	Dynamic SIP Proxy Discovery	91
10.1.5	Enable SIP Audio and Video Calls	95
10.1.6	SIP Failover.....	96
10.1.7	SIP Port Selection and Preferred-port Usage.....	100
10.1.8	SIP rport Management for NAT Traversal	101
10.1.9	Use P-Associated-URIs in REGISTER	102
10.1.10	Enable Shared Call Appearance and Automatic Busy – In Call Presence.....	103
10.1.11	N-way Conferencing URI.....	105
10.1.12	Display Name Matching for Incoming and Outgoing Calls and Call History and Diversion Information	105
10.1.13	Undesired CallerID Suppression for Display Name	107
10.1.14	Call History Display Name Override	108
10.1.15	Call and Chat Recording	108
10.1.16	Call Pull.....	109
10.1.17	Call Park and Retrieve.....	110
10.1.18	Selection of SIP Response for Busy Signal	110
10.1.19	Exclude SIP Error Codes in Failover	110
10.1.20	Transfer Call.....	111
10.1.21	Forced Logout.....	112
10.1.22	Echo Service (Test Call).....	113
10.1.23	Select Outband or Inband DTMF.....	114
10.1.24	Federated Calling in XMPP Deployments.....	114
10.1.25	Voice Mail Number and Message Waiting Indicator	115

10.1.26	N-Way and My Room Video Calls	116
10.1.27	Reduce Use of Call Hold in Conferencing.....	117
10.1.28	Maximum Conference Parties (N-Way Calling).....	118
10.1.29	My Room, N-Way, and N-Way Owner Participant List	119
10.1.30	Meet-Me Moderator Controls and Participant List	120
10.1.31	Video Server.....	121
10.1.32	Team Telephony	122
10.1.33	Executive-Assistant.....	124
10.1.34	SIP SUBSCRIBE and REGISTER Refresh and SUBSCRIBE Retry	125
10.1.35	Configure SIP URI or Tel URI in Outgoing Calls	126
10.1.36	SIP URI Validation	126
10.1.37	SIP UPDATE Support	127
10.1.38	Remote Control Event Package	128
10.1.39	SIP Auto-Answer.....	129
10.1.40	Web Pop.....	129
10.1.41	Auto-Show Dial Pad.....	130
10.1.42	SIP P-Early Media (PEM) Header	131
10.2	Real-Time Protocol	132
10.2.1	Real-Time Control Protocol Extended Report	132
10.2.2	Real-Time Transport Protocol Port Range.....	132
10.2.3	Real-Time Transport Protocol Packet Maximum Transmission Unit	133
10.2.4	RTCP MUX	134
10.2.5	BroadSoft Media Engine (from Cisco).....	134
10.2.6	Dynamic Video Bit Rate Adaptation	135
10.2.7	Comfort Noise (CN) for Early Media.....	136
10.3	Extensible Messaging and Presence Protocol	137
10.3.1	Use Extensible Messaging and Presence Protocol	137
10.3.2	XMPP Service Discovery	139
10.3.3	XMPP Failover	141
10.3.4	Publish Location.....	143
10.3.5	File Transfer	143
10.3.6	Chat.....	145
10.3.7	Group Chat.....	145
10.3.8	Presence and Automated Presence	146
10.3.9	Offline Presence Control	146
10.3.10	Idle Detection	147
10.3.11	Presence Rules.....	148
10.3.12	Presence on Demand.....	149
10.3.13	vCard Download Options	150
10.4	Messaging HTTP API.....	151
10.4.1	Messaging HTTP API Service Discovery.....	151
10.4.2	Message History and Badge Sync	152

10.4.3	IM Retention Policy	154
10.4.4	Connect Messaging Support.....	155
10.4.5	Aggregated Presence.....	156
10.5	Use Cisco BroadWorks Xtended Services Interface Features.....	157
10.5.1	Xtended Service Interface Basic Configuration – URL and Version	157
10.5.2	Xsi Service Discovery	160
10.5.3	Sticky Xsi 302 Response Support	160
10.5.4	Xtended Service Interface Failover.....	161
10.5.5	Xsi-Event Channel	163
10.5.6	Click To Dial	165
10.5.7	Xtended Services Interface Mid-Call Controls	165
10.5.8	Terminating Xsi Call Control.....	166
10.5.9	Incoming Call Notifications in Xsi-Only Mode	167
10.5.10	Call Settings and Call Settings Toolbar	168
10.5.11	Enterprise Directory Listing	171
10.5.12	Xsi Directory Search, Enable or Disable	172
10.5.13	Enhanced Search Options	173
10.5.14	Enable Xsi Ad Hoc Conference Calls.....	175
10.5.15	Visual Voice Mail.....	175
10.5.16	Call Center Agent Login	177
10.5.17	Call History – Basic Call Logs	178
10.5.18	Call History – Enhanced Call Logs	178
10.5.19	Single Sign-On.....	179
10.5.20	Personal Assistant and Nordic Presence.....	180
10.6	Share	183
10.6.1	Desktop Sharing (Sharing Server and Web Collaboration)	183
10.6.2	Share Service Discovery	186
10.6.3	Sharing Server (USS) Failover	186
10.6.4	Share Passing.....	186
10.7	DNS	187
10.7.1	DNS TTL Management	187
10.8	Provisioning.....	188
10.8.1	Flow-Through Provisioning	188
10.8.2	Meet-Me Conference Bridge Auto-Provisioning and Silent Dialing.....	189
10.9	My Room	194
10.9.1	Enable My Room	194
10.9.2	Guest Client.....	195
10.10	Search	197
10.10.1	Contact Search	197
10.10.2	LDAP Search	198
10.11	Outlook Integration.....	204
10.12	Outlook – Plugin.....	205

10.13 UC-One Hub Integration.....	207
10.14 Google Analytics	209
10.15 Communicator Packages and Device Management.....	210
10.15.1 Packages.....	210
10.15.2 Xsi-Only Deployments Without SCA	211
10.15.3 Partial Match Enhancements for Device Type Selection	211
10.15.4 Forced DM Configuration File Update.....	212
10.16 Security	213
10.16.1 Pinned SSL Certificate in Client	213
10.16.2 Installer Certificates.....	213
10.16.3 SSL/TLS Certificates	214
10.16.4 SIP Over TLS and Secure Real-time Transport Protocol	217
10.16.5 SIP TLS Certificate Validation	220
10.16.6 Xtended Service Interface TLS Certificate Validation	222
10.16.7 Messaging API SRV Support and Certificate Validation	223
10.16.8 XMPP SRV Support and Certificate Validation	224
10.16.9 Sharing Server (USS) Certificate Validation	227
10.16.10 LDAP Certificate Validation	227
10.16.11 Change Password	228
10.16.12 Cisco BroadWorks MAC Field and Specific Configuration File Name	230
10.16.13 XMPP Security Enhancement for Unauthorized File Types	230
10.16.14 XMPP Security Enhancement for Preventing Clickable Links.....	230
10.16.15 HTTP Proxy Support	231
10.16.16 3GPP SIP Headers for SRTP	233
10.16.17 SRTP Re-keying Configurability	233
10.16.18 PIV URL.....	234
10.17 Emergency Calling.....	234
10.17.1 Banner Support.....	234
10.17.2 Disable Emergency Calls	235
10.17.3 Login Dialog.....	236
10.17.4 Emergency Call Address Change Service.....	237
10.18 Logging	239
10.18.1 Release 20.0.0 Enhancements.....	239
10.18.2 Standard HID Logging	240
10.18.3 Preferences User Interface for Logging	240
10.18.4 Outlook Add-in Logging	241
10.18.5 Disable Logging	241
10.19 User Interface.....	241
10.19.1 Configurable Left Pane Order	241
10.19.2 Flexible Contact Card Field Configuration and Synchronization	243
10.19.3 Integrated Call Window	247
10.19.4 Display Name for Contacts	247

10.19.5	Select Service Name Over First Name in Directory Search	248
10.19.6	Active Communications Extra Buttons	249
10.19.7	Minimize After Login	250
10.19.8	Auto-Close S4B PSTN Call Window	250
10.19.9	Configurable Web Button and Web Tab View	251
10.19.10	Pass Parameters and Encoding Web Button URLs.....	256
10.19.11	Hide My Room Email Invitation BTBC Link.....	259
10.19.12	Configurable History Tab Order	260
10.19.13	Enable Main Window Communications Buttons	261
10.19.14	Hide Communications Window Notifications and Tones	261
10.19.15	Communications Window UI Control via API.....	263
10.19.16	Hide Voice Mail Settings.....	264
10.19.17	Control Number of Rings for Call Forwarding	265
10.19.18	Hide Spell Checker Settings	266
10.20	UC-One Add-in for Microsoft Skype for Business (S4B).....	266
10.21	API for Third-Party Applications.....	269
10.22	Help URL	270
10.23	IPv6.....	270
10.24	BTBC URL Scheme	270
11	Video Optimization	271
11.1	Default Video Parameter Values	271
11.2	Video Parameter Selection Algorithm	272
11.2.1	General	272
11.2.2	SIP/SDP Signaling.....	272
11.3	Video Bit Rate Selection.....	273
11.4	Video Frame Rate Selection	274
11.5	Optimization Examples.....	274
11.6	Symmetric Versus Asymmetric Video	275
12	Typical Bandwidth Consumption Scenarios.....	276
13	Version Control and Automatic Upgrade.....	277
14	Appendix A: TLS Ciphers and OpenSSL	284
15	Appendix B: UC-One Communicator DM Tag Provisioning Script.....	286
	Acronyms and Abbreviations.....	291

Table of Figures

Figure 1 Communicator Device Management Tag Sets	48
Figure 2 SIP Port Selection and Rport Not Enabled.....	101
Figure 3 Desktop Share Credentials.....	189
Figure 4 Conference Bridge Settings.....	190
Figure 5 Meet-Me Conference Default Settings	192
Figure 6 SNI and TLS Certificate Validation.....	215
Figure 7 TLS Certificate Verification	217
Figure 8 SIP Certificate Validation with Less Safe Branding Option	220
Figure 9 SIP Certificate Validation with Safer Certificate Validation (Default).....	221
Figure 10 SIP Certificate Validation and Configuration Options	221
Figure 11 Xsi Certificate Validation – Non-Branded	222
Figure 12 Xsi Certificate Validation – Branded	223
Figure 13 Messaging HTTP API Certificate Validation.....	224
Figure 14 XMPP Certificate Validation	225
Figure 15 Sharing Server (USS) Certificate Validation.....	227
Figure 16 LDAP Certificate Validation	228

1 Summary of Changes

This section describes the changes to this document for each release and document version.

1.1 Changes for Communicator Release 22.9.37, UC-One SaaS Release 3.9.37

This version of the document includes the following change:

- Added new configuration parameter for directory contact request caching.

1.2 Changes for Communicator Release 22.9.30, UC-One SaaS Release 3.9.30

This version of the document includes the following change:

- Corrected automatic update interval tag.

1.3 Changes for Communicator Release 22.9.24, UC-One SaaS Release 3.9.24

This version of the document includes the following change:

- Added new configuration parameter for token expiry notification.

1.4 Changes for Communicator Release 22.9.22, UC-One SaaS Release 3.9.22

This version of the document includes the following change:

- Added note about token expiry.

1.5 Changes for Communicator Release 22.9.21, UC-One SaaS Release 3.9.21

This version of the document includes the following change:

- Added internally used SSL certificate expiry warning pop-up configurations.

1.6 Changes for Communicator Release 22.9.20, UC-One SaaS Release 3.9.20

This version of the document includes the following change:

- Added new UC-One to Webex migration configuration parameter.

1.7 Changes for Communicator Release 22.9.18, UC-One SaaS Release 3.9.18

This version of the document includes the following changes:

- Made editorial changes and removed Webex section.
- Added new Presence on Demand (PoD) limit configuration parameter.
- Added cipher list for CiscoSSL.
- Added text for SIP certificate management.

1.8 Changes for Communicator Release 22.9.16, UC-One SaaS Release 3.9.16, Webex for BroadWorks Release September 20

Release 22.9.16, Release 3.9.16, Release September 20, Document Version 3

This version of the document includes the following changes:

- Made editorial changes.

- Removed EFT-only features:
 - Call Settings Web View
 - Call Center integration

Release 22.9.16, Release 3.9.16, Release September 20, Document Version 2

This version of the document includes the following changes:

- Made editorial changes.
- Added a note about audio codecs.

Release 22.9.16, Release 3.9.16, Release September 20, Document Version 1

This version of the document includes the following changes:

- Added SIP failover enhancement.
- Added offline presence enhancement.
- Added the following new Webex features:
 - Call pickup
 - Call Center queues
 - Call Settings Web View
- Added a note about ad hoc conference calls without XMPP.

1.9 Changes for Communicator Release 22.9.14, UC-One SaaS Release 3.9.12, Webex for BroadWorks Release August 20

This version of the document includes the following change:

- Added Call Auto Recovery in the Webex section.

1.10 Changes for Communicator Release 22.9.14, UC-One SaaS Release 3.9.12, Webex for BroadWorks Release July 20

This version of the document includes the following changes:

- Added a note about localhost DNS entry for SSO.
- Removed VP9 codec from Webex section.
- Removed WME section.

1.11 Changes for Communicator Release 22.9.12, UC-One SaaS Release 3.9.12, Webex for BroadWorks Release July 20

This version of the document includes the following changes:

- Added a note about SIP SUBSCRIBE 503 response.
- Added Webex configuration parameters.

1.12 Changes for Communicator Release 22.9.12, UC-One SaaS Release 3.9.12, Webex for BroadWorks Release June 20

This version of the document includes the following changes:

- Added section *12 Webex for BroadWorks* (which was subsequently removed).

- Added *Appendix C: Webex for BroadWorks DM Tag Provisioning Script* (which was subsequently removed).
- Corrected MSI installation parameters.
- Added section for Comfort Noise.
- Added vad parameters for SIP.
- Added a note on contact synchronization at login.
- Added a note on SIP failover.
- Added a note on forced DM configuration update.
- Added a note on Single Sign-On (SSO).
- Added a note on XMPP exponential back-off timer for HTTP messaging.

1.13 Changes for Communicator Release 22.9.10, UC-One SaaS Release 3.9.10

This version of the document includes the following changes:

- Added a note to active communications button parameters.
- Moderated My Room note added.

1.14 Changes for Communicator Release 22.9.8, UC-One SaaS Release 3.9.8

This version of the document includes the following changes:

- Modified MSI installer command line examples and added notes.
- Added Xsi exponential back-off timer note.
- Added note for Server Name Indication (SNI) in Sharing Server (USS).
- Added SIP failover enhancement for TCP connection loss.
- Added a new parameter for My Room email invitation.

1.15 Changes for Communicator Release 22.9.6, UC-One SaaS Release 3.9.6

Release 22.9.6, Release 3.9.6, Document Version 2

This version of the document includes the following change:

- Added a note for %HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMINS%.

Release 22.9.6, Release 3.9.6, Document Version 1

This version of the document includes the following changes:

- Added a note about SSO and Save Login.
- Added a note about installer languages.
- Added a note about Outlook Plugin.
- Added new features:
 - Team Telephony window sorting order
 - Automatic upgrade preferences hiding
- Added missing configuration parameter for display name translations enhancement.
- Added missing configuration parameter for LDAP sorting.

- Added missing parameter for local Busy – In Call for aggregated presence.
- Upgraded OpenSSL version.

1.16 Changes for Communicator Release 22.9.2, UC-One SaaS Release 3.9.1

This version of the document includes the following changes:

- Added a note about SIP/TLS.
- Added a note about My Room participant list.
- Added a note about Connect Messaging support.
- Added a note about Visual Voice Mail.
- Added a note about contacts' display name.

1.17 Changes for Communicator Release 22.9.2, UC-One SaaS Release 3.9.0

This version of the document includes the following change:

- Incremented the Collaborate version number to match revised release plan.

1.18 Changes for Communicator Release 22.9.1, UC-One SaaS Release 3.9.0

This version of the document includes the following changes:

- Added new configuration for SIP and XMPP failover enhancement.
- Updated UC-One SaaS configuration table with new configuration parameter split.
- Added a note about internal search wild cards.
- Added a note about file extensions case insensitivity in file transfer.
- Added a new feature:
 - New installer

1.19 Changes for Communicator Release 22.7.6, UC-One SaaS Release 3.7.5

Release 22.7.6, Release 3.7.5, Document Version 2

This version of the document includes the following change:

- Added clarifications to Connect messaging support.

Release 22.7.6, Release 3.7.5, Document Version 1

This version of the document includes the following changes:

- Added new configuration for minimum rings in Personal Assistant.
- Added new configuration for Connect messaging modes.

1.20 Changes for Communicator Release 22.7.5, UC-One SaaS Release 3.7.5

Release 22.7.5, Release 3.7.5, Document Version 2

This version of the document includes the following change:

- Added section [10.1.19 Exclude SIP Error Codes in Failover](#).

Release 22.7.5, Release 3.7.5, Document Version 1

This version of the document includes the following changes:

- Modified text in the installer section for remote installations and desktop short cut as well as auto-run.
- Added clarification of room owner participant list with Xsi-Events.
- Added a note about voice mail.
- Added a note about URL schemes.
- Added a note about do-not-hold parameter recommended default value.
- Added a note about case-sensitive codec names.
- Added enhancements:
 - Service name display enhancement
 - New configuration parameter that allows customers to configure whether Personal Assistant (PA) or Lync takes precedence

1.21 Changes for Communicator Release 22.7.0, UC-One SaaS Release 3.7.0

This version of the document includes the following changes:

- Modified text in ECACS section for the removed parameter.
- Added a note about SSO login.
- Added a note about Video Server (UVS) and participant lists.
- Added a note about maximum number of rings.
- Added a note about safer certificate validation branding option being the default.
- Added note about utilized Xsi search fields.
- Removed old Linux tags from appendix.
- Added new features:
 - New configuration parameter for call hold handling in ad hoc conferencing.
 - Hiding silent alert in Personal Assistant preferences.
 - New configuration parameter for selecting service name or display name in search results.

1.22 Changes for Communicator Release 22.6.1, UC-One SaaS Release 3.6.1

This version of the document includes the following changes:

- Added a note about contact card fields not being editable in automatic mode.
- Added a note about presence without chat packages not supporting share or My Room.
- Configuration file changes as follows:
 - ECACS format parameter removed
 - Hide automatic upgrade user interface (UI) for non-admins
 - New parameter for Copy Guest Link

1.23 Changes for Communicator Release 22.6.0, UC-One SaaS Release 3.6.0

This version of the document includes the following changes:

- Added a note about Personal Assistant requiring aggregated presence.
- Corrected erroneous DM tag for automatic upgrade.
- Added a note about DNS NAPTR records for SIP proxy discovery.
- Added the following new features with configuration or deployment impact:
 - New deployment package, presence without chat
 - Call window auto-close for S4B integration
 - Control the number of rings for Call Forwarding (CF) to Voice Mail
 - Guest client enhancement for enabling auto-acceptance

1.24 Changes for Communicator Release 22.5.3, UC-One SaaS Release 3.5.3

This version of the document includes the following changes:

- Added a note about version control channels.
- Added Federal Information Processing Standards (FIPS) ciphers to Appendix and updated SIP/TLS cipher list.
- Removed security classification.
- Edited and modified Xtended Services Interface (Xsi), SIP, Extensible Messaging and Presence Protocol (XMPP), and Sharing Server (USS) failover sections.
- Added a note about required API-provider parameters for USB headsets.
- Added the following new features:
 - P-Early Media (PEM) support
 - vCard caching enhancement
 - Hiding spell checker

1.25 Changes for Communicator Release 22.5.2, UC-One SaaS Release 3.5.1

NOTE: Changes are not applicable to any currently available UC-One SaaS Release.

This version of the document includes the following changes:

- Added two new attributes to control wild-card character usage in specific LDAP search-locations.
- Clarified the usage of command line options with installer.

1.26 Changes for Communicator Release 22.5.0, UC-One SaaS Release 3.5.0

This version of the document includes the following changes:

- Added a note about Extensible Messaging and Presence Protocol (XMPP) failover.
- Added the following new features:
 - Personal Assistant
 - Four web buttons
 - Additional Personal Identity Verification (PIV) URI in Xtended Services Interface (Xsi) settings

- Call History sync
- Forced DM file update
- Added a note about logging.

1.27 Changes for Communicator Release 22.4.2, UC-One SaaS Release 3.4.0

This version of the document includes the following changes:

- Added two new configuration parameters for vCard fetching (XMPP).
- Added a note to Google analytics section.

1.28 Changes for Communicator Release 22.4.0, UC-One SaaS Release 3.4.0

Release 22.4.0, Release 3.4.0, Document Version 2

This version of the document includes the following changes:

- Added text for installed configuration files.
- Added a section for *connectors_encrypted.db* file.
- Added a section on *vcards_encrypted.db*.
- Added Call History note for sync and local Call History.
- Added new parameter values for hiding voice mail settings.

Release 22.4.0, Release 3.4.0, Document Version 1

This version of the document includes the following changes:

- Added note for Multi-part search enhancement.
- Added note about moderated My Room.
- Added note for UseXmppCredentials to share authentication configuration section.
- Added section about IPv6.
- Added note about Callto and Tel URL schemes.
- Added section about Single Sign-On (SSO).
- Added note about Outlook Add-in administrator rights.
- Added note about Connect messaging enhancements.

1.29 Changes for Communicator Release 22.3.1, UC-One SaaS Release 3.3.0

This version of the document includes the following changes:

- Added a section on UC-One SaaS configuration.
- Added a note about IM retention.
- Added BTBC URL scheme details.
- Added section for Call History display name modification.
- Added new SIP proxy discovery parameters.
- Updated the OpenSSL version.
- Updated roaming path for Windows configuration file location.

1.30 Changes for Release 22.3.1

This version of the document includes the following changes:

- Added a note about IM retention parameter values.
- Added BTBC URL scheme details.
- Added new configuration parameter to hide voice mail settings.
- Updated roaming path for Windows configuration file location.
- Updated the OpenSSL version.

1.31 Changes for Release 22.3.0

This version of the document includes the following changes:

- Added a network display name explanation to display name matching.
- Added a note about Outlook Add-in DNS provisioning.
- Added a note about UC-One SDK DLL Application Programming Interface (API) version deprecation.
- Added new section about HTTP messaging API certificate validation.
- Added the following new features:
 - IM retention policy
 - Automatic upgrade
 - Outlook Add-in presence source
 - Single installer for Outlook Add-in and S4B integration

1.32 Changes for Release 22.2.1

This version of the document includes the following changes:

- Added *X-Broadworks* header explanation to display name matching.
- Added a note about Xsi failover and SRV-record to IP address mapping.
- Added a note about SIP *Retry-after* header usage in SIP failover section.
- Added a section about SIP auto-answer.
- Support for Web Collaboration using an external browser window.

1.33 Changes for Release 22.2.0

This version of the document includes the following changes:

- Made editorial corrections.
- Stated that Visual Voice Mail (audio) is officially supported.
- Added note for Microsoft Installer (MSI).
- Added UCaaS style auto-configuration based on assigned services:
 - Executive-Assistant
 - Team Telephony
 - Visual Voice Mail

- Call Center Agent
- Added LDAP certificate section.
- Added note about incoming call display name for the related calling number.
- Added the following new features:
 - Google Analytics
 - Web tab view
 - Real-Time Control Protocol (RTCP) MUX

1.34 Changes for Release 22.1.0

This version of the document includes the following changes:

- Added note about RTCP being mandatory in the BME.
- Made S4B integration changes.
- Added note about branding option for Transport Layer Security (TLS) certificate validation.
- Added note about XMPP failover.
- Added note to SIP failover.

1.35 Changes for Release 22.0.1

This version of the document includes the following changes:

- Added LDAP credentials configurability.
- Added a note to sync-from parameter.
- Added more explanation to the API parameter.
- Added notes about SIP NOTIFY configurability.
- Corrected SRTP re-keying tag.
- Added an Outlook Add-in example for MSI installation.
- Added a note about RTCP FB fallback.
- Added a note about recommended parameter values for S4B integration.

1.36 Changes for Release 22.0.0

This version of the document includes the following changes:

- Added the following new features:
 - UC-One Hub integration
 - Auto-showing of dial pad
 - Communications Window user interface (UI) control via API
 - Hiding Communications window notifications and tones
- Removed old document version information (see the *Document Revision History* section for changes prior to this release).
- Removed Chrome.
- Removed HTTP API configuration.

- Added new installation option for Outlook Add-in.
- Added a note about Xtended Services Platform (Xsp) login token with Sharing Server (USS).

2 Changes for Configuration Files

2.1 Changes for Configuration Files for Release 3.9.37/22.9.37

UC-One → Webex migration

```
<services>
  <contacts>
    <contact-cache
cacheInterval="%CONTACT_CACHE_TIME_INTERVAL_MINUTES%" />
    </contacts>
</services>
```

The following DM tags were added on the UC-One side:

- %CONTACT_CACHE_TIME_INTERVAL_MINUTES%

Where the default value is 1440 (24 * 60)

2.2 Changes for Configuration Files for Release 3.9.21/22.9.21

UC-One → Webex migration

```
<config>
<services>
<internal-cert-expiry-notification enabled="true"
warn-before-days= "90"
warn-frequency-days = "7"/>
```

The following DM tags were added on the UC-One side:

- %INTERNAL_CERT_EXPIRY_NOTIFICATION%
- %INTERNAL_CERT_EXPIRY_WARN_BEFORE_DAYS%
- %INTERNAL_CERT_EXPIRY_WARN_FREQUENCY_DAYS%

2.3 Changes for Configuration Files for Release 3.9.20/22.9.20

UC-One → Webex migration

```
<config>
<services>
<version-control enabled="true">
<migration-upgrade enabled="true" mandatory="false" migration-
link="https://test.com">
```

The following DM tags were added on the UC-One side:

- %ENABLE_MIGRATION_DESKTOP%
- %MANDATORY_MIGRATION_DESKTOP%
- %MIGRATION_LINK_DESKTOP%

2.4 Changes for Configuration Files for Release 3.9.18/22.9.18

Presence on Demand Maximum Limit

```
<config>
  <services>

  <presence-on-demand enabled="true">

    <poll-interval seconds="300" /> <!--interval in seconds-->

    <maximum-limit>%PRESENCE_ON_DEMAND_MAXIMUM_LIMIT%</maximum-limit>

  </presence-on-demand>

</services>
```

The following DM tag was added on the UC-One side:

- %PRESENCE_ON_DEMAND_MAXIMUM_LIMIT%

2.5 Changes for Configuration Files for Release 3.9.16/22.9.16/Webex September 20

DNS TTL Minimum Value

```
<config>
  <protocols>
    <sip>
      <proxy address="domain.com" port="5060"/>
      <proxy-discovery enabled="true">
        <dns-ttl-minimum-value>%DNS_TTL_MINIMUM_VALUE%</dns-ttl-
minimum-value>
```

Offline Presence Enhancement

```
<config>
  <services>
    <presence enabled="%ENABLE_PRESENCE%"> <!--true/false-->
      <manual-offline-set enabled="%DISABLE_OFFLINE_PRESENCE%">
```

The following DM tags were added on the UC-One side:

- %DNS_TTL_MINIMUM_VALUE%
- %DISABLE_OFFLINE_PRESENCE%

The following changes were added on the Webex side:

- Added <call-pickup> under <calls>.

```
<config>
<services><calls>
<call-pickup blind="%ENABLE_CALL_PICKUP_BLIND_WXT%"
directed="%ENABLE_CALL_PICKUP_DIRECTED_WXT%"/>
```

- Added <web-call-settings> under <services>.

```
<config>
<services>
<web-call-settings>
  <url>%WEB_CALL_SETTINGS_URL_WXT%</url>
</web-call-settings>
```

The following %TAG%s were added:

- %ENABLE_CALL_PICKUP_BLIND_WXT%
- %ENABLE_CALL_PICKUP_DIRECTED_WXT%
- %WEB_CALL_SETTINGS_URL_WXT%

The following %TAG% was deprecated:

- %SETTINGS_PORTAL_URL_WXT%

2.6 Changes for Configuration Files for Release 3.9.12/22.9.14/Webex August 20

Call Auto Recovery

```
<config>
<services><calls>
<auto-recovery enabled="%ENABLE_CALLS_AUTO_RECOVERY_WXT%"/>
```

The following DM tag was added on the Webex side:

- %ENABLE_CALLS_AUTO_RECOVERY_WXT%

2.7 Changes for Configuration Files for Release 3.9.12/22.9.12/ Webex July 20

Comfort Noise for NAT/Firewall Opening

```
<config>
  <protocols>
    <xsi>
      <paths>
        <root>%XSI_ROOT_WXT%/root>
        <actions>%XSI_ACTIONS_PATH_WXT%/actions>
        <events>%XSI_EVENTS_PATH_WXT%/events>
      </paths>
```

The following DM tags were added on the Webex side:

- %XSI_ROOT_WXT%
- %XSI_ACTIONS_PATH_WXT%
- %XSI_EVENTS_PATH_WXT%

2.8 Changes for Configuration Files for Release 3.9.12/22.9.12/ Webex June 20

Comfort Noise for NAT/Firewall Opening

```
<config version="20">
  <services>
    <calls>
      <audio>
        <send-on-inactive enabled="%ENABLE_SEND_ON_INACTIVE%"/>
```

The following DM tags were added on the UC-One side:

- %ENABLE_SEND_ON_INACTIVE%
- %BLF_UTILISE_SERVER_SORTING_ORDER%

2.9 Changes for Configuration Files for Release 3.9.8/22.9.8

Hide My Room Email Invitation

```
<config version="20">
  <services>
    <rooms enable d="true">
      <myroom enabled="true">
        <guest-client-support enabled="true">
          <guest-client-url>https://xsp.domain.com/cgc</guest-
client-url>
          <guest-client-domain>kowabunga-
guest.broadsoft.com</guest-client-domain>
          <auto-accept-all>>false</auto-accept-all>
        </guest-client-support>
        <include-btbc-link-to-email-
invitation>%ENABLE_BTBC_LINK_INVITATION%</</include-btbc-link-to-email-
invitation>
        <include-btbc-link-to-copy-guest-
link>%ENABLE_BTBC_LINK_TO_COPY_GUEST_LINK%</include-btbc-link-to-copy-
guest-link>
        <include-email-invitation-
menu>%ENABLE_EMAIL_INVITATION_MENU%</include-email-invitation-menu>
      </myroom>
    </rooms>
  </services>
</config>
```

The following DM tag was added:

- %ENABLE_EMAIL_INVITATION_MENU%

2.10 Changes for Configuration Files for Release 3.9.6/22.9.6

Automatic Upgrade Preferences Hiding

```
<config version="20">
  <services>
    <automatic-upgrade enabled="true" auto-hide-for-non-admin="%
HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMIN%" hide-
settings="%HIDE_AUTOMATIC_UPGRADE_SETTINGS%" />
  </services>
</config>
```

Hide Automatic Upgrade UI for Non-admins

```
<config version="20">
  <services>
    <automatic-upgrade enabled="%ENABLE_AUTOMATIC_UPGRADE_DESKTOP%" auto-
hide-for-non-admin="%HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMIN%" hide-
settings="%HIDE_AUTOMATIC_UPGRADE_SETTINGS%" />
  </services>
</config>
```

Display Name Customized List

```
<config version="20">
  <services>
    <call-history enabled="true"> <!-- To enable/disable call
history, if Xsi is disabled, falls back to local call history -->
      <name-overrides>
        <private>Private</private>
        <unavailable>Unavailable</unavailable>
        <customized-list>Anonymous, Anonymous
Unavailable, Public</customized-list>
      </name-overrides>
    </call-history>
  </services>
</config>
```

Team Telephony Window Sorting Order

```

<config version="20">
  <services>
    <contacts>

      <busy-lamp-field
enabled="%ENABLE_BUSY_LAMP_FIELD_DESKTOP%">

        <allow-
pickup>%ENABLE_BLF_DIRECT_PICKUP_DESKTOP%/allow-pickup>

        <display-
caller>%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%/display-caller>

<utilise-server-sorting-order>%ENABLE_BLF_SERVER_SORTING_ORDER%/utilise-
server-sorting-order>%

      </busy-lamp-field>

```

Enable LDAP Sorting

```

<config version="20">
  <protocols>
    <ldap>

.....
<sorting enabled="%ENABLE_LDAP_SORTING
">
<sort-control enabled="%ENABLE_LDAP_SORT_CONTROL%"> </sort-control>
</sorting>

```

Local Busy In Call with Aggregated Presence

```

<config version="20">
  <services>
    <presence>
      <server-presence-aggregation
enabled="%ENABLE_SERVER_PRESENCE_AGGREGATION_DESKTOP%" enable-local-busy-
in-call="%ENABLE_LOCAL_BUSY_IN_CALL_DESKTOP%" />

```

The following DM tags were added:

- %HIDE_AUTOMATIC_UPGRADE_SETTINGS%
- %HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMINS%
- %ENABLE_BLF_SERVER_SORTING_ORDER%
- %ENABLE_LDAP_SORTING%
- %ENABLE_LDAP_SORT_CONTROL%
- %ENABLE_LOCAL_BUSY_IN_CALL_DESKTOP%

2.11 Changes for Configuration Files for Release 3.9.0/22.9.1

Exponential back-off timer

```

<config version="20">
  <protocols>
    <sip>

```

```

        connection-retry-
parameter>%CONNECTION_RETRY_PARAMETER_DESKTOP%/connection-retry-
parameter>
        <xmpp>
        <connection-retry-
parameter>%CONNECTION_RETRY_PARAMETER_DESKTOP%/connection-retry-
parameter>

```

The following DM tag was added:

- %CONNECTION_RETRY_PARAMETER_DESKTOP%

2.12 Changes for Configuration Files for Release 22.7.6

Minimum number of rings in Personal Assistant

```

<config version="20">
  <services>
    <services>
      <supplementary-services enabled="%ENABLE_XSI_SRV_MANAGEMENT%"
toolbar="%ENABLE_TOOLBAR%" toolbar-call-
settings="%ACCESS_CALL_SETTINGS%">
        <xsi> <!-- Any service can be individually
enabled/disabled, xdm services not supported in BTBC. xdm xsi -->
          <number-of-rings-range
min="%NUMBER_OF_RINGS_RANGE_MIN_VALUE_DESKTOP%"
max="%NUMBER_OF_RINGS_RANGE_MAX_VALUE_DESKTOP%" />
        ....
      </supplementary-services>
    </services>
  </services>
</voice-mail>

```

Connect Messaging modes

```

<config version="20">
  <services>
    <group_messaging enabled=" %ENABLE_GROUP_MESSAGING_DESKTOP%"
use-collaborate-style-participant-
management="%USE_COLLABORATE_STYLE_PARTICIPANT_MANAGEMENT%" />
  </services>
</config>

```

Exclude Error Codes in Failover

```

<config>
  <protocols>
    <sip>
      <session>
        <failover-excluded-invite-errors>
          <entry>%FAILOVER_EXCLUDED_INVITE_ERRORS%/</entry>
          <entry>604</entry>
        </failover-excluded-invite-errors>
      </session>
    </sip>
  </protocols>
</config>

```

Personal Assistant

```

<config version="20">
  <services>
    <lync-integration
enabled="%ENABLE_LYNC_INTEGRATION%">
      <pa-presence-precedes-lync-
presence>%PA_PRESENCE_PRECEDES_LYNC_PRESENCE%/</pa-presence-precedes-lync-
presence>
      <s4b-windowing-model enabled="true" />
    </lync-integration>
  </services>
</config>

```

The following DM tags were added:

- %FAILOVER_EXCLUDED_INVITE_ERRORS%
- %PA_PRESENCE_PRECEDES_LYNC_PRESENCE%
- %NUMBER_OF_RINGS_RANGE_MIN_VALUE_DESKTOP%
- %NUMBER_OF_RINGS_RANGE_MAX_VALUE_DESKTOP%
- %USE_COLLABORATE_STYLE_PARTICIPANT_MANAGEMENT%

The following DM tag was removed:

- %NUMBER_OF_RINGS_RANGE_DESKTOP%

2.13 Changes for Configuration Files for Release 22.7.0

Reducing the Number of Call Hold in Conferencing

```
<config version="20">
    <services>
        <calls>
            <conference>
                .....
                <do-not-hold-conference-before-
                refers>%ENABLE_DO-NOT-HOLD-CONFERENCE-BEFORE-REFER%</do-not-hold-
                conference-before-refers>
            </conference>
        </calls>
    </services>
</config>
```

Hiding Personal Assistant Silent Alert in Preferences

```
<config version="20">
<services>
  <presence>
    <personal-assistant enabled="%DESKTOP_PERSONAL_ASSISTANT_ENABLED%">
      <silent-alert show="%ENABLE_SILENT_ALERT_SHOW%" />
    </personal-assistant/>
  </presence>
</services>
</config>
```

Selecting Service Name over Display Name

```
<config version="20">
  <services>
    <contacts>
      <use-service-name
      enabled="%ENABLE_SERVICE_NAME_IN_SEARCH%"/>
    </contacts>
  </services>
</config>
```

The following DM tags were added:

- %ENABLE_SERVICE_NAME_IN_SEARCH%
- %ENABLE_SILENT_ALERT_SHOW%
- %ENABLE_DO-NOT-HOLD-CONFERENCE-BEFORE-REFER%

The following DM tag was removed:

- %USE_NEW_URL_FORMAT%

2.14 Changes for Configuration Files for Release 22.6.1

Hide Automatic Upgrade UI for Non-admins

```
<config version="20">
<services>
  <automatic-upgrade enabled="%ENABLE_AUTOMATIC_UPGRADE_DESKTOP%" auto-
  hide-for-non-admin="%HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMINS%" />
</services>
</config>
```

Hide BTBC Link in Copy Guest Link

```
<config version="20">
  <services>
    <rooms enable d="true">
      <myroom enabled="true">
        <guest-client-support enabled="true">
          <guest-client-url>https://xsp.domain.com/cgc</guest-client-
url>
          <guest-client-domain>kowabunga-guest.broadsoft.com</guest-
client-domain>
          <auto-accept-all>>false</auto-accept-all>
        </guest-client-support>
        <include-btbc-link-to-email-
invitation>%ENABLE_BTBC_LINK_INVITATION%</include-btbc-link-to-email-
invitation>
        <include-btbc-link-to-copy-guest-
link>%ENABLE_BTBC_LINK_TO_COPY_GUEST_LINK%</include-btbc-link-to-copy-
guest-link>
      </myroom>
    </rooms>
  </services>
</config>
```

The following DM tags were added:

- %HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMINIS%
- %ENABLE_BTBC_LINK_TO_COPY_GUEST_LINK%

2.15 Changes for Configuration Files for Release 22.6.0

The following parameters were added in Release 22.6.0.

Auto-Close S4B Window

```
<config version="20">
  <services>
    <lync-integration>
      <s4b-windowing-model enabled="%ENABLE_S4B_WINDOWING_MODEL_DESKTOP%">
    </s4b-windowing-model>
  </services>
</config>
```

Control number of rings for Call Forwarding (CF) to Voice Mail

```
<config version="20">
  <services>
    <supplementary-services enabled="true" toolbar="true" toolbar-call-
settings="true">
      <number-of-rings-range max="%NUMBER-OF-RINGS-RANGE-DESKTOP%" />
    </supplementary-services>
  </services>
</config>
```

The following new DM tags were added:

- %ENABLE_S4B_WINDOWING_MODEL_DESKTOP%
- %NUMBER_OF_RINGS_RANGE_DESKTOP%

2.16 Changes for Configuration Files for Release 22.5.3

The following parameters were added in Release 22.5.3.

PEM support

```
<config version="20">
  <protocols>
    <sip>
      <support-p-early-media>%ENABLE_PEM_SUPPORT_DESKTOP%</support-p-
early-media>
    </sip>
  </protocols>
</config>
```


vCard download enhancement

```
<config version="20">
  <protocols>
    <xmpp>
      <vcard>
        <batch-size>%VCARD-BATCH-SIZE%/batch-size>
        <batch-timeout>%VCARD-BATCH-TIMEOUT%<batch-timeout>
          <batch-failed-timeout-per-item>%VCARD-BATCH-
            FAILED-TIMEOUT%/batch-failed-timeout-per-item>
        </vcard>
      </xmpp>
    </protocols>
  </config>
```

Hide spell checker

```
<config version="20">
  <services>
    <spell-checker enabled="%ENABLE_SPELL_CHECK_DESKTOP%" />
  </services>
</config>
```

The following DM tags were added:

- %ENABLE_SPELL_CHECK_DESKTOP%
- %VCARD-BATCH-FAILED-TIMEOUT%
- %ENABLE_PEM_SUPPORT_DESKTOP%

2.17 Changes for Configuration Files for Release 22.5.0

The following parameters were added in Release 22.5.0.

Forced DM file update

```
<config version="20">
  <services>
    <auto-reconfigure enabled="%ENABLE_AUTOMATIC_RECONFIGURE_DESKTOP%"
  />
</config>
```

Personal Assistant

```
<config version="20">
  <services>
    <presence>
      <personal-assistant
        enabled="%DESKTOP_PERSONAL_ASSISTANT_ENABLED%" />
    </presence>
  </services>
</config>
```

PIV URL

```
<config version="20">
  <protocols>
    <xsi>
      <paths root="%XSI_ROOT%" piv-enabled-
        root="%PIV_XSI_ROOT%">
    </xsi>
  </protocols>
</config>
```

Additional Web Buttons (old configs still work)

```
<web-button-2 enabled="%DESKTOP_WEBBUTTON_2_ENABLED%"
  type="%DESKTOP_WEBBUTTON_2_TYPE%"
  target="%DESKTOP_WEBBUTTON_2_TARGET%"
  url="%DESKTOP_WEBBUTTON_2_URL%">
  <tooltip language="%DESKTOP_WEBBUTTON_2_TOOLTIP_LANGUAGE-
1%">%DESKTOP_WEBBUTTON_2_TOOLTIP-1%</tooltip>
</web-button-2>
```

```

        <web-button-3 enabled="%DESKTOP_WEBBUTTON_3_ENABLED%"
            type="%DESKTOP_WEBBUTTON_3_TYPE%"
            target="%DESKTOP_WEBBUTTON_3_TARGET%"
            url="%DESKTOP_WEBBUTTON_3_URL%">
            <tooltip language="%DESKTOP_WEBBUTTON_3_TOOLTIP_LANGUAGE-
1%">%DESKTOP_WEBBUTTON_3_TOOLTIP-1%</tooltip>
        </web-button-3>
        <web-button-4 enabled="%DESKTOP_WEBBUTTON_4_ENABLED%"
            type="%DESKTOP_WEBBUTTON_4_TYPE%"
            target="%DESKTOP_WEBBUTTON_4_TARGET%"
            url="%DESKTOP_WEBBUTTON_4_URL%">
            <tooltip language="%DESKTOP_WEBBUTTON_4_TOOLTIP_LANGUAGE-
1%">%DESKTOP_WEBBUTTON_4_TOOLTIP-1%</tooltip>
        </web-button-4>

```

The following DM tags were added:

- %DESKTOP_PERSONAL_ASSISTANT_ENABLED%
- %ENABLE_AUTOMATIC_RECONFIGURE_DESKTOP
- %PIV_XSI_ROOT%
- %DESKTOP_WEBBUTTON_2_ENABLED%
- %DESKTOP_WEBBUTTON_2_TYPE%
- %DESKTOP_WEBBUTTON_2_TARGET%
- %DESKTOP_WEBBUTTON_2_URL%
- %DESKTOP_WEBBUTTON_2_TOOLTIP_LANGUAGE-1%
- %DESKTOP_WEBBUTTON_2_TOOLTIP-1%
- %DESKTOP_WEBBUTTON_3_ENABLED%
- %DESKTOP_WEBBUTTON_3_TYPE%
- %DESKTOP_WEBBUTTON_3_TARGET%
- %DESKTOP_WEBBUTTON_3_URL%
- %DESKTOP_WEBBUTTON_3_TOOLTIP_LANGUAGE-1%
- %DESKTOP_WEBBUTTON_3_TOOLTIP-1%
- %DESKTOP_WEBBUTTON_4_ENABLED%
- %DESKTOP_WEBBUTTON_4_TYPE%
- %DESKTOP_WEBBUTTON_4_TARGET%
- %DESKTOP_WEBBUTTON_4_URL%
- %DESKTOP_WEBBUTTON_4_TOOLTIP_LANGUAGE-1%
- %DESKTOP_WEBBUTTON_4_TOOLTIP-1%

2.18 Changes for Configuration Files for Release 22.4.2

The following parameter was added in Release 22.4.2.

vCard Download Options

```

<config version="20">
  <protocols>
    ...

```

```

<xmpp>
...
  <vcard>
    <batch-size>%VCARD-BATCH-SIZE%/</batch-size>
    <batch-timeout>%VCARD-BATCH-TIMEOUT%</batch-timeout>
  </vcard>

```

2.19 Changes for Configuration Files for Release 22.4.0

Hide voice mail settings has different possible values, but the same DM tag.

Hide Voice Mail Settings

```

<config version="20">
  <services>
    <voice-mail enabled="false"
settings="%VOICEMAIL_SETTINGS_ENABLED%" visual-voicemail="true">
...
</voice-mail>

```

2.20 Changes for Configuration Files for Release 22.3.1

Hide Voice Mail Settings

```

<config version="20">
  <services>
    <voice-mail enabled="false"
settings="%VOICEMAIL_SETTINGS_ENABLED%" visual-voicemail="true">
...
</voice-mail>

```

2.21 Changes for Configuration Files for Release 22.3.0

Outlook Presence Source

```

<config version="20">
  <services>
    <outlook-presence-source name="%OUTLOOK_PRESENCE_SOURCE%"/>

```

IM Retention Policy

```

<config version="20">
  <chat>
    <message-retention-time-
days>%CHAT_MESSAGE_RETENTION_TIME_DAYS_DESKTOP%/</message-retention-time-
days>

```

Automatic Upgrade

```

<config>
  <services>
    <version-control enabled="%ENABLE_VERSION_CONTROL_DESKTOP%"
<url>http://%BWDEVICEACCESSFQDN%:80/%BWDMSCONTEXT%/%BWDEVICEACCESSURI%ver
sion_check.xml</url>
    <automatic-upgrade enabled="%ENABLE_AUTOMATIC_UPGRADE_DESKTOP%"/>
  <Upgrade>

```

```

    <Interval>%AUTOMATIC_UPGRADE_INTERVAL_MINUTES%</Interval>
  <Windows>
    <Must>%MUST_VERSION_WINDOWS%</Must>
    <Recommended>%RECOMMENDED_VERSION_WINDOWS%</Recommended>
    <Download
hash="%URL_HASH_WINDOWS%">%DOWNLOAD_URL_WINDOWS%</Download>
    <alpha
      version="%ALPHA_VERSION_WINDOWS%"
hash="%ALPHA_HASH_WINDOWS%">%ALPHA_URL_WINDOWS%</alpha>
    <beta
      version="%BETA_VERSION_WINDOWS%"
hash="%BETA_HASH_WINDOWS%">%BETA_URL_WINDOWS%</beta>
  </Windows>
  <OSX>
    <Must>%MUST_VERSION_OSX%</Must>
    <Recommended>%RECOMMENDED_VERSION_OSX%</Recommended>
    <Download hash="%URL_HASH_OSX%">%DOWNLOAD_URL_OSX%</Download>
    <alpha
version="%ALPHA_VERSION_OSX%"
hash="%ALPHA_HASH_OSX%">%ALPHA_URL_OSX%</alpha>
    <beta
version="%BETA_VERSION_OSX%"
hash="%BETA_HASH_OSX%">%BETA_URL_OSX%</beta>
  </OSX>

  </Upgrade>
</version-control>

```

2.22 Changes for Configuration Files for Release 22.2.0

The following configuration parameters were added.

RTCP MUX

```

<config version="20">
  protocols
    <rtp>
      <mux enabled="%ENABLE_RTCP_MUX%" />

```

Google Analytics

```

<services>
  <analytics enabled="%ENABLE_ANALYTICS_DESKTOP%" />

```

Web Tab View

A new supported value for attribute *target* was added (tab).

The following DM tags were introduced:

- %ENABLE_RTCP_MUX%
- %ENABLE_AUTOMATIC_UPGRADE_DESKTOP%
- %AUTOMATIC_UPGRADE_INTERVAL_MINUTES%
- %URL_HASH_WINDOWS%
- %ALPHA_VERSION_WINDOWS%
- %ALPHA_HASH_WINDOWS%
- %ALPHA_URL_WINDOWS%

- %BETA_VERSION_WINDOWS%
- %BETA_HASH_WINDOWS%
- %BETA_URL_WINDOWS%
- %URL_HASH_OSX%
- %ALPHA_VERSION_OSX%
- %ALPHA_HASH_OSX%
- %ALPHA_URL_OSX%
- %BETA_VERSION_OSX%
- %BETA_HASH_OSX%
- %BETA_URL_OSX%
- %ENABLE_ANALYTICS_DESKTOP%

2.23 Changes for Configuration Files for Release 22.1.0

The following configuration parameters were removed.

S4B Integration

```
<config version="20">
  <services>
  ...
  <force-call-intercept-presences>
    <entry>None</entry>
    <entry>Offline</entry>
    <entry>DoNotDisturb</entry>
    <entry>AutomaticAway</entry>
  </force-call-intercept-presences>
```

2.24 Changes for Configuration Files for Release 22.0.1

The following configuration parameters were added.

LDAP Credentials

The following example provides information on enabling an LDAP search.

```
<config version="20">
  <protocols>
  ...
    <ldap>
      ...
      <credentials>
        <username>user@domain.com</username>
        <password>1pqotr fuhwep fiböjwpobj</password>
      </credentials>
```

The following DM tags were introduced:

- %LDAP_USERNAME%
- %LDAP_PASSWORD%

2.25 Changes for Configuration Files for Release 22.0.0

The following configuration parameters were added.

UC-One Hub

```
<services>
  <uchub
    enabled="%ENABLE_HUB%"
    login_url="%HUB_LOGIN_URL%"
    <hub-button
      enabled="%ENABLE_HUB_BUTTON%"
      url="%HUB_BUTTON_URL%" />
    <hub-banner
      enabled="%ENABLE_HUB_BANNER%"
      url="%HUB_BANNER_URL%"
      height="%HUB_BANNER_HEIGHT%" />
    <contextual-gadget
      enabled="%ENABLE_CONTEXTUAL_GADGET%"
      url="%CONTEXTUAL_GADGET_URL%" />
    <hub-analytics
      enabled="%ENABLE_HUB_ANALYTICS%"
      serviceproviderid="%HUB_ANALYTICS_SERVICE_PROVIDERID%"
      resellerid="%HUB_ANALYTICS_RESELLERID%"
      companyid="%HUB_ANALYTICS_COMPANYID%" />
  </uchub>
```

Auto-Show Dial Pad

```
<config version="20">
  <services>
    <calls>
      <auto-show-dial-pad mode="%AUTO_SHOW_DIAL_PAD%" />
    </calls>
  </services>
</config>
```

Communications Window UI Control via API

```
<config version="20">
  <services>
    <use-communication-window type="%COMMUNICATION_WINDOW_TRIGGER%" />
  </services>
</config>
```

Hide Communications Window Notifications and Tones

```
<config version="20">
  <services>
    <hide-communication-notifications
      mode="%HIDE_NOTIFICATIONS_MODE_DESKTOP%" />
    <mute-communication-alerts mode="%MUTE_ALERTS_MODE_DESKTOP%" />
  </services>
</config>
```

The following DM tags were added:

- %AUTO-SHOW-DIAL-PAD%
- %LEFT_PANE_CHAT_HISTORY_Q%
- %ENABLE_HUB%
- %HUB_LOGIN_URL%
- %ENABLE_HUB_BUTTON%
- %HUB_BUTTON_URL%

- %ENABLE_HUB_BANNER%
- %HUB_BANNER_URL%
- %HUB_BANNER_HEIGHT%
- %ENABLE_CONTEXTUAL_GADGET%
- %CONTEXTUAL_GADGET_URL%
- %ENABLE_HUB_ANALYTICS%
- %HUB_ANALYTICS_SERVICE_PROVIDERID%
- %HUB_ANALYTICS_RESELLERID%
- %HUB_ANALYTICS_COMPANYID%
- %COMMUNICATION_WINDOW_TRIGGER%
- %HIDE_NOTIFICATIONS_MODE_DESKTOP%
- %MUTE_ALERTS_MODE_DESKTOP%

The following DM tag was removed:

- %ENABLE_WEB_API%

3 Device Management Tags

Communicator uses the *Device Management Tag Sets* shown in the following figure. The *System Default* and custom *BroadTouch_Tags* sets are required to provision specific device/client settings. Note the system administrator must configure these tags through the *System* → *Resources* → *Device Management Tag Sets* option.

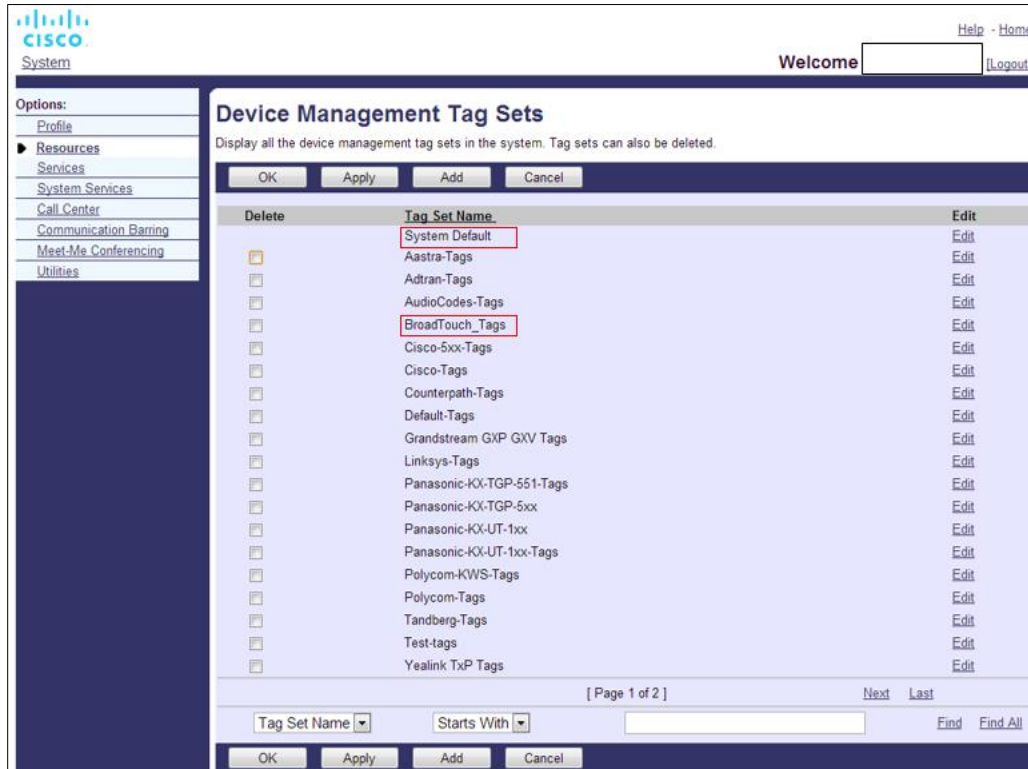


Figure 1 Communicator Device Management Tag Sets

3.1 Communicator Device Type – System Default Tags

As the system administrator, you can access the *System Default* tags through *System* → *Resources* → *Device Management Tag Sets* option. The following *System Default* tags must be provisioned.

Tag	Value
%SBC_ADDRESS%	This should be configured as the fully qualified domain name (FQDN) or IP address of the SBC deployed in the network. For more information on recommended usage, see section 10.1.1 Change Basic SIP Server Settings . Example: sbc.yourdomain.com
%SBC_PORT%	If the <i>SBC_ADDRESS</i> is an IP address, then this parameter should be set to the SBC port. If the <i>SBC_ADDRESS</i> is an FQDN, then it can be left unset. Example: 5060

3.2 Communicator Device Type – Custom Tags

A new custom tag set must be created for the Communicator client and associated with the client's device type. This tag set provides flexibility in managing the client's network or service connectivity settings as well as feature activation controls.

This custom tag set is provisioned by the system administrator through the *System* → *Resources* → *Device Management Tag Sets* option. The administrator must add a new tag set called *BroadTouch_Tags*, create each individual tag, and set its value as shown in the following table. The *References Section* column in the following table provides detailed descriptions for each tag behind a link. The *License* column lists the required licenses for the feature. The *Feature* column groups most frequently used sub-items of that feature together. Note as well that for some features, default or system tags are required (for example, for SIP and XMPP).

The SCA license is not mandatory for any feature to work, although it is typically used. For more information on SCA versus primary line provisioning, see the *UC-One Solution Guide*.

Feature	Tag	License*	Reference Section
Xsi with Mid-Call Controls	%ENABLE_XSI_CALLS%	1, 2, or 3	For more information, see sections 10.15 Communicator Packages and Device Management and 10.5.6 Click To Dial .
	%ENABLE_XSI_EVENT_CHANNEL%		For more information, see section 10.5.5 Xsi-Event Channel .
	%CHANNEL_NOT_PERSISTENT%		
	%CHANNEL_HEARTBEAT%		
	%ENABLE_XSI_MIDCALL_CONTROLS%		For more information, see section 10.5.7 Xtended Services Interface Mid-Call Controls .
	%DESKTOP_ENABLE_XSI_CONFERENCE%		For more information, see section 10.5.14 Enable Xsi Ad Hoc Conference Calls .
	%XSI_NAMESPACE%		For more information see section 10.5.1 Xtended Service Interface Basic Configuration – URL and Version .
	%XSI_ROOT%		
Call Settings Toolbar	%ENABLE_XSI_SRV_MANAGEMENT%	1, 2, or 3	For more information, see section 10.5.10 Call Settings and Call Settings Toolbar .
	%ENABLE_TOOLBAR%		
	%ACCESS_CALL_SETTINGS%		
Number of Rings for CF to Voice Mail	%NUMBER_OF_RINGS-RANGE_MIN_VALUE_DESKTOP%	1, 2, or 3	For more information, see section 10.19.17 Control Number of Rings for Call Forwarding .
	%NUMBER_OF_RINGS-RANGE_MAX_VALUE_DESKTOP%		

Feature	Tag	License*	Reference Section
Enhanced Call Logs	%ENABLE_ENHANCED_CALL_HISTORY_DESKTOP%	1, 2, or 3	For more information, see section 10.5.18 Call History – Enhanced Call Logs .
Terminating Xsi Call Control	%ENABLE_TERMINATING_XSI_CALLS%	1, 2, or 3	For more information, see section 10.5.8 Terminating Xsi Call Control .
Incoming Call Xsi Notifications	%ENABLE_XSI_REMOTE_ANSWER_DESKTOP%	1, 2, or 3	For more information see section 10.5.9 Incoming Call Notifications in Xsi-Only Mode .
Call Center Login	%ENABLE_CALL_CENTER_DESKTOP%	1, 2, or 3	For more information, see section 10.5.16 Call Center Agent Login .
Remote Control Event Package	%ENABLE_REMOTE_CONTROL_EVENTS_DESKTOP%	1, 2, or 3	For more information, see section 10.1.38 Remote Control Event Package .
Web Button	%DESKTOP_WEBBUTTON_ENABLED%	1, 2, or 3	For more information, see section 10.19.9 Configurable Web Button and Web Tab View .
	%DESKTOP_WEBBUTTON_TYPE%		
	%DESKTOP_WEBBUTTON_TARGET%		
	%DESKTOP_WEBBUTTON_URL%		
	%DESKTOP_WEBBUTTON_TOOLTIP_LANGUAGE-1%		
	%DESKTOP_WEBBUTTON_TOOLTIP-1%		
	%DESKTOP_WEBBUTTON_2_ENABLED%		
	%DESKTOP_WEBBUTTON_2_TYPE%		
	%DESKTOP_WEBBUTTON_2_TARGET%		
	%DESKTOP_WEBBUTTON_2_URL%		
	%DESKTOP_WEBBUTTON_2_TOOLTIP_LANGUAGE-1%		
	%DESKTOP_WEBBUTTON_2_TOOLTIP-1%		
	%DESKTOP_WEBBUTTON_3_ENABLED%		
	%DESKTOP_WEBBUTTON_3_TYPE%		
%DESKTOP_WEBBUTTON_3_TARGET%			
%DESKTOP_WEBBUTTON_3_URL%			

Feature	Tag	License*	Reference Section
	%DESKTOP_WEBBUTTON_3_TOOLTIP_LANGUAGE-1%		
	%DESKTOP_WEBBUTTON_3_TOOLTIP-1%		
	%DESKTOP_WEBBUTTON_4_ENABLED%		
	%DESKTOP_WEBBUTTON_4_TYPE%		
	%DESKTOP_WEBBUTTON_4_TARGET%		
	%DESKTOP_WEBBUTTON_4_URL%		
	%DESKTOP_WEBBUTTON_4_TOOLTIP_LANGUAGE-1%		
	%DESKTOP_WEBBUTTON_4_TOOLTIP-1%		
Web Pop	%ENABLE_WEB_POP_DESKTOP%	1, 2, or 3	For more information, see section 10.1.40 Web Pop .
	%WEB_POP_ALLOW_EDIT_DESKTOP%		
	%WEB_POP_URL_DESKTOP%		
SIP Audio Calling with Supplementary Services	%USE_PROXY_DISCOVERY%	2 or 3 (Call Park also works in Xsi-Only mode)	For more information, see section 10.1.4 Dynamic SIP Proxy Discovery .
	%DOMAIN_OVERRIDE%		For more information, see section 10.1.1 Change Basic SIP Server Settings .
	%SOURCE_PORT%		For more information, see section 10.1.3 Force TCP or UDP Usage and Keepalives .
	%TCP_SIZE_THRESHOLD%		For more information, see sections 10.15 Communicator Packages and Device Management and 10.1.5 Enable SIP Audio and Video Calls .
	%ENABLE_AUDIOCALLS%		For more information, see section 10.1.20 Transfer Call .
	%ENABLE_TRANSFER_CALLS%		
	%TRANSFER_CALL_TYPE%		
	%MAX_CONF_PARTIES%		For more information, see section 10.1.28 Maximum Conference Parties (N-Way Calling) .
	%ENABLE_CALL_PARK_DESKTOP%		For more information, see section 10.1.17 Call Park and Retrieve . This also works with Xsi-Only mode.
%ENABLE_CALL_PULL_DESKTOP%	For more information, see section 10.1.16 Call Pull .		

Feature	Tag	License*	Reference Section
	%DNS_TTL_MINIMUM_V ALUE%		For more information, see section 10.1.6.2 Failover Triggering and Failover Time .
	%CONNECTION_RETRY _PARAMETER_DESKTO P%		For more information, see section 10.1.6.2 Failover Triggering and Failover Time .
SIP Ad hoc Conferencing	%ENABLE_DO-NOT- HOLD-CONFERENCE- BEFORE-REFER%	2 or 3	For more information, see section 10.1.27 Reduce Use of Call Hold in Conferencing .
	%MAX_CONF_PARTIES %		For more information, see section 10.1.28 Maximum Conference Parties (N-Way Calling) .
	%ENABLE_NWAY_VIDE O%		For more information, see section 10.1.26 N-Way and My Room Video Calls .
	%ENABLE_NWAY_PART ICIPANT_LIST_DESKTO P%		For more information, see section 10.1.29 My Room, N-Way, and N-Way Owner Participant List .
Rport for NAT Traversal	%USE_RPORT_IP%	2 or 3	For more information, see section 10.1.8 SIP rport Management for NAT Traversal .
Alternative Identities in REGISTER	%USE_ALTERNATIVE_I DENTITIES	2 or 3	For more information, see section 10.1.9 Use P-Associated-URIs in REGISTER .
SIP Rejection Code Selection	%REJECT_WITH_486_D ESKTOP%	2 or 3	For more information, see section 10.1.18 Selection of SIP Response for Busy Signal .
Exclude SIP Error codes in Failover	%FAILOVER_EXCLUDED _INVITE_ERRORS%	2 or 3	For more information, see section 10.1.19 Exclude SIP Error Codes in Failover .
SIP Video Calling	%ENABLE_VIDEOCALLS %	3 typically also 6 or 7 and 8	For more information, see sections 10.15 Communicator Packages and Device Management and 10.1.5 Enable SIP Audio and Video Calls .
	%ENABLE_NWAY_VIDE O%		For more information, see section 10.1.26 N-Way and My Room Video Calls .
PEM Support	%ENABLE_PEM_SUPPO RT_DESKTOP%	1, 2, or 3	For more information, see section 10.1.42 SIP P-Early Media (PEM) Header .
UVS	%CONFERENCE_TYPE %	2 or 3 and 7 and/or 8	For more information, see section 10.1.31 Video Server . For allowing ad hoc Video Server (UVS) calls in Xsi-Only mode, the Video Server (UVS) license must be assigned.
Voice Mail Number and MWI	%DESKTOP_MWI_ENAB LE%	1, 2, or 3	For more information, see section 10.1.25 Voice Mail Number and Message Waiting Indicator .
	%DESKTOP_MWI_MODE %		

Feature	Tag	License*	Reference Section
Visual Voice Mail	%ENABLE_VISUAL_VOICEMAIL%	1, 2, or 3	For more information, see section 10.5.15 Visual Voice Mail .
	%TIMELINE_CHAT_Q%		
	%TIMELINE_CALLS_Q%		
	%TIMELINE_VOICEMAIL_Q%		
Hiding Voice Mail Settings	%VOICEMAIL_SETTING_S_ENABLED%	1, 2, or 3	For more information, see section 10.19.16 Hide Voice Mail Settings .
Executive Assistant	%ENABLE_EXECUTIVE_ASSISTANT_DESKTOP%	1, 2, or 3	For more information, see section 10.1.33 Executive-Assistant .
Team Telephony	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	1, 2, or 3	For more information, see section 10.1.32 Team Telephony .
	%ENABLE_BLF_DIRECT_PICKUP_DESKTOP%		
	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%		
	%ENABLE_BLF_SERVER_SORTING_ORDER%		
Forced Logout	%ENABLE_FORCED_LOGOUT%	2 or 3	For more information, see section 10.1.21 Forced Logout .
	%FORCED_LOGOUT_API%		
Call and Chat Recording	%ENABLE_CALL_RECORDING_DESKTOP%	1, 2, or 3 for calls, 4 for chat	For more information, see section 10.1.15 Call and Chat Recording .
	%ENABLE_CHAT_RECORDING_DESKTOP%		
Emergency Calls	%ENABLE_EMERGENCY_CALLING%	1, 2, or 3	For more information, see section 10.17.2 Disable Emergency Calls .
	%ENABLE_EMERGENCY_CALL_NOTIFICATION%		
	%EMERGENCY_NUMBER_LIST%		
Login Dialog	%ENABLE_LOGIN_INFORMATIONAL_DIALOG%	2 or 3	For more information, see section 10.17.3 Login Dialog .
	%DECLINE_BUTTON_ACTION%		
	%DECLINE_BUTTON_URL%		
ECACS	%ENABLE_EXT_SERVICE_VERIFICATION%	2 or 3	For more information, see section 10.17.4 Emergency Call Address Change .
	%EXT_SERVICE_VERIFICATION_URL%		

Feature	Tag	License*	Reference Section
	%SHOW_EXT_VERIFICATION_MENU		
	%USE_SESSION_EXT_SERVICE_VERIFICATION%		
Echo Service	%ENABLE_TEST_SERVICES_DESKTOP%	2 or 3	For more information, see section 10.1.22 Echo Service (Test Call) .
	%ENABLE_TEST_CALLS_DESKTOP%		
	%TEST_NUMBER_LANGUAGE_DESKTOP-1%		
	%TEST_NUMBER_DESKTOP-1%		
	%TEST_NUMBER_LANGUAGE_DESKTOP-2%		
	%TEST_NUMBER_DESKTOP-2%		
SIP UPDATE	%ENABLE_SIP_UPDATE_SUPPORT_DESKTOP%	2 or 3	For more information, see section 10.1.37 SIP UPDATE Support .
Active Communications Extra Buttons	%ACTIVE_COMMS_ENABLE_TRANSFER_BUTTON%	1, 2, or 3	For more information, see section 10.19.6 Active Communications Extra Buttons .
	%ACTIVE_COMMS_ENABLE_CONFERENCE_BUTTON%		
	%ACTIVE_COMMS_ENABLE_CALL_PARK_BUTTON%		
Minimize After Login	%MINIMIZE_AFTER_LOGIN%	1, 2, or 3	For more information, see section 10.19.7 Minimize After Login .
Banner	%ENABLE_BANNER%	1, 2, or 3	For more information, see section 10.17.1 Banner Support .
	%BANNER_URL%		
	%BANNER_HEIGHT%		
Configurable Left Pane Order	%LEFT_PANE_DEFAULT%	1, 2, or 3	For more information, see section 10.19.1 Configurable Left Pane Order .
	%LEFT_PANE_CONTACTS_Q%		
	%LEFT_PANE_ROOMS_Q%		
	%LEFT_PANE_HISTORY_Q%		

Feature	Tag	License*	Reference Section
	%LEFT_PANE_CHAT_HI STORY_Q%		
	%LEFT_PANE_DIALPAD _Q%		
	%LEFT_PANE_DIRECTO RY_Q%		
	%LEFT_PANE_WEB_BU TTON_Q%		
	%LEFT_PANE_WEB_BU TTON_2_Q%		
	%LEFT_PANE_WEB_BU TTON_3_Q%		
	%LEFT_PANE_WEB_BU TTON_4_Q%		
Integrated Call Window	%SHOW_COMM_WINDO W%	1, 2, or 3	false For more information, see section 10.19.3 Integrated Call Window .
Main Window Communications Buttons	%ENABLE_BOTTOM_BA R%	1, 2, or 3	For more information, see section 10.19.13 Enable Main Window Communications Buttons .
Xsi Search and Contact Sync	%ENABLE_XSI_SEARCH %	1, 2, or 3	For more information, see section 10.5.12 Xsi Directory Search, Enable or Disable .
	%CONTACT_SOURCE_S YNC%		For more information, see section 10.19.2 Flexible Contact Card Field Configuration and Synchronization .
	%SHOW_TITLE%		
	%SHOW_DEPARTMENT %		
	%SHOW_HIRAGANAFIR STNAME%		
	%SHOW_HIRAGANALAS TNAME%		
	%SHOW_REGION%		
	%SHOW_LOCATION%		
	%SHOW_YAHOOID%		
	%SHOW_PAGER%		
	%SHOW_GROUPID%		
	%SHOW_BWUSERID%		
	%ALLOW_EDIT_TITLE%		
	%ALLOW_EDIT_DEPART MNT%		
%ALLOW_EDIT_HIRAGA NAFIRSTNAME%			

Feature	Tag	License*	Reference Section
	%ALLOW_EDIT_HIRAGANALASTNAME%		
	%ALLOW_EDIT_REGION%		
	%ALLOW_EDIT_LOCATION%		
	%ALLOW_EDIT_YAHOOID%		
	%ALLOW_EDIT_PAGER%		
	%ALLOW_EDIT_GROUPID%		
Enhanced Search Options	%ENABLE_CONTACTS_ENTERPRISE_SEARCH_DESKTOP%	1, 2, or 3	For more information, see section 10.5.13 Enhanced Search Options .
	%ENABLE_CONTACTS_ENTERPRISE_COMMON_SEARCH_DESKTOP%		
	%ENABLE_CONTACTS_PERSONAL_SEARCH_DESKTOP%		
	%ENABLE_CONTACTS_GROUP_COMMON_SEARCH_DESKTOP%		
Enterprise Directory Listing	%ENABLE_SHOW_ALL_DIRECTORY%	1, 2, or 3	For more information, see section 10.5.11 Enterprise Directory Listing .
Selecting service name over display name	%ENABLE_SERVICE_NAME_IN_SEARCH%"/>	1, 2, or 3	For more information, see section 10.19.5 Select Service Name Over First Name .
Personal Assistant	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	1, 2, or 3 and 4	For more information, see section 10.5.20 Personal Assistant and Nordic Presence .
	%ENABLE_SILENT_ALERT_SHOW%		
LDAP Search	%ENABLE_LDAP_SEARCH%	1, 2, or 3	For more information, see section 10.10.2 LDAP Search .
	%ENABLE_TLS%		
	%LDAP_SERVER_URI%		
	%LDAP_SERVER_PORT%		
	%LDAP_BASE_OBJECT%		
	%LDAP_PROTOCOL_VERSION%		
	%LDAP_AUTHENTICATION%		
	%LDAP_DOMAIN%		

Feature	Tag	License*	Reference Section
	%LDAP_USERNAME%		
	%LDAP_PASSWORD%		
	%ENABLE_LDAP_SORTING%		
	%ENABLE_LDAP_SORT_CONTROL%		
Outlook integration	%ENABLE_OUTLOOK_CALENDAR_PRESENCE%	1, 2, or 3	For more information, see section 10.11 Outlook Integration .
	%ENABLE_OUTLOOK_SEARCH%		
Outlook Add-in Presence Source	%OUTLOOK_PRESENCE_SOURCE%	1, 2, or 3	For more information, see section 10.12 Outlook – Plugin .
XMPP Presence and Chat	%ENABLE_XMPP%	1, 2, or 3 and 4	For more information, see sections 10.15 Communicator Packages and Device Management and 10.3.1 Use Extensible Messaging and Presence Protocol .
	%ENABLE_PRESENCE%		For more information, see section 10.3.7 Group Chat .
	%ENABLE_LOCATION%		For more information, see section 10.3.4 Publish Location .
	%ENABLE_CHAT%		For more information, see section 10.3.6 Chat .
	%ENABLE_OFFLINE_INDICATION%		
	%ENABLE_GROUP_CHAT%		For more information, see section 10.3.7 Group Chat .
	%XMPP_SSL_ENABLE%		For more information, see section 10.3 Extensible Messaging and Presence Protocol .
	%XMPP_SRV_ENABLED%		
	%USE_FOR_SSL_VERIFICATION%		
	%USE_AS_BACKUP_RECORD%		
	%VCARD-BATCH-SIZE%		For more information on vCard download options, see section 10.3.13 vCard Download Options .
	%VCARD-BATCH-TIMEOUT%		
	%VCARD-BATCH-FAILED-TIMEOUT%		
	Idle Detection		%ENABLE_IDLE_DETECTION%
%IDLE_DETECTION_TIMEOUT%			
%ENABLE_PRESENCE_AWAY%			

Feature	Tag	License*	Reference Section
Message History and Badge Sync	%UMS_HTTP_SRV_SERVICE_NAME_DESKTOP%	1, 2, or 3 and 4 and 9	For more information, see section 10.4.2 Message History and Badge Sync .
	%UMS_SRV_ADDRESS_DESKTOP%		
	%ENABLE_MESSAGE_SYNC_DESKTOP%		
	%UMS_USE_SSL%		
	%MESSAGE_SYNC_FETCH_PATH_DESKTOP%		
	%MESSAGE_SYNC_POST_PATH_DESKTOP%		
IM Retention Policy	%CHAT_MESSAGE_RETENTION_TIME_DAYS_DESKTOP%	1, 2, or 3 and 4 and 9	For more information, see section 10.4.3 IM Retention Policy .
Connect Messaging	%ENABLE_GROUP_MESSAGING_DESKTOP%	1, 2, or 3 and 4 and 9	For more information, see section 10.4.4 Connect Messaging Support .
	%USE_COLLABORATE_STYLE_PARTICIPANT_MANAGEMENT%		
Presence Aggregation	%ENABLE_SERVER_PRESENCE_AGGREGATION_DESKTOP%	1, 2, or 3 and 4 and 9	For more information, see section 10.4.5 Aggregated Presence .
	%ENABLE_LOCAL_BUSINESS_IN_CALL_DESKTOP%		
Presence Rules	%ENABLE_PRESENCE_RULES_DESKTOP%	1, 2, or 3 and 4	For more information, see section 10.3.11 Presence Rules .
Presence on Demand	%ENABLE_PRESENCE_ON_DEMAND_DESKTOP%	1, 2, or 3 and 4	For more information, see section 10.3.12 Presence on Demand .
	%PRESENCE_ON_DEMAND_POLL_INTERVAL_DESKTOP%		
	%PRESENCE_ON_DEMAND_MAXIMUM_LIMIT%		
Preventing Clickable Links	%CHAT_PREVENT_CLICKABLE_LINKS%	1, 2, or 3 and 4	For more information, see section 10.16.14 XMPP Security Enhancement for Preventing Clickable Links .
Migration to other apps (Webex)	%ENABLE_MIGRATION_DESKTOP%	1, 2, or 3 and 4	For more information, see section 13 Version Control and Automatic Upgrade .
	%MANDATORY_MIGRATION_DESKTOP%		
	%MIGRATION_LINK_DESKTOP%		
	%INTERNAL_CERT_EXPIRY_NOTIFICATION%	1, 2, or 3 and 4	

Feature	Tag	License*	Reference Section	
Internal SSL certificate notification	%INTERNAL_CERT_EXPIRY_WARN_BEFORE_DAYS%		For more information, see section 10.16.1 Pinned SSL Certificate in Client .	
	%INTERNAL_CERT_EXPIRY_WARN_FREQUENCY_DAYS%			
File Transfer	%ENABLE_MEDIA_SHARE%	1, 2, or 3 and 4	For more information, see section 10.3.5 File Transfer .	
	%ENABLE_FILE_TRANSFER%			
	%FT_MAX_IN%			
	%FT_MAX_OUT%			
	%FT_REQUIRE_ENCRYPTION%			
File Transfer Extension Limit	%ENABLE_FILE_TRANSFER_FILE_EXTENSION_LIMIT%	1, 2, or 3 and 4	For more information, see section 10.16.13 XMPP Security Enhancement for Unauthorized File Types .	
My Room and Moderator Controls	%ENABLE_ROOMS%	1, 2, or 3 and 4 Typically, also 6 or 7 and/or 8	For more information, see section 10.9.1 Enable My Room .	
	%ENABLE_MYROOM%			
	%ROOMS_HISTORY_SIZE%		For more information, see section 10.8.2 Meet-Me Conference Bridge Auto-Provisioning .	
	%AUTODETECT_CONFERENCE%			
	%BRIDGE_ID%			
	%CONFERENCE_TITLE%			
	%DIRECT_DIAL%		For more information, see section 10.1.30 Meet-Me Moderator Controls and Participant List .	
	%ENABLE_MEETME_MODERATOR_CONTROLS%			
	%ENABLE_BTBC_LINK_INVITATION%			For more information, see section 10.19.11 Hide My Room Email Invitation BTBC Link .
	%ENABLE_BTBC_LINK_TO_COPY_GUEST_LINK%			
%ENABLE_EMAIL_INVITATION_MENU%				
Share	%ENABLE_WEBCOLLAB%	1, 2, or 3 and 4 and 10	For more information, see section 10.6.1 Desktop Sharing (Sharing Server and Web Collaboration) .	
	%WEBCOLLAB_BASEDOMAIN%			
	%WEBCOLLAB_SUBDOMAIN%			
	%WEBCOLLAB_USE_XMPP_CREDENTIALS%			

Feature	Tag	License*	Reference Section
	%SHARE_TYPE%		
	%USS_ADDRESS%		
	%ENABLE_PARTICIPANT_SHARE%		
Guest Client	%GUEST_CLIENT_ENABLE%	1, 2, or 3 and 4 and 10	For more information, see section 10.9.2 Guest Client .
	%GUEST_CLIENT_URL%		
	%GUEST_CLIENT_DOMAIN%		
	%GUEST_CLIENT_AUTO_ACCEPT%		
RTP	%RTP_AUDIO_PORT_RANGE_START%	2 or 3	For more information, see section 10.2.2 Real-Time Transport Protocol Port Range .
	%RTP_AUDIO_PORT_RANGE_END%		
	%RTP_VIDEO_PORT_RANGE_START%		
	%RTP_VIDEO_PORT_RANGE_END%		
	%RTP_VIDEO_MTU%		For more information, see section 10.2.3 Real-Time Transport Protocol Packet Maximum Transmission Unit .
BroadSoft Media Engine	%MEDIA_HANDLER%	2 or 3	For more information, see section 10.2.5 BroadSoft Media Engine .
RTCP MUX	%ENABLE_RTCP_MUX%	2 or 3	For more information, see section 10.2.4 RTCP MUX .
Comfort noise	%ENABLE_SEND_ON_INACTIVE%>	2 or 3	For more information, see section 10.2.7 Comfort Noise (CN) for Early Media .
DVBA	%ENABLE_DVBA%	2 or 3	For more information, see section 10.2.6 Dynamic Video Bit Rate Adaptation .
RTCP XR	%RTCP_XR_AUDIO_ENABLE%	2 or 3	For more information, see section 10.2.1 Real-Time Control Protocol Extended Report .
	%RTCP_XR_SERVICE_URI%		
	%RTCP_XR_LOCALGROUP_DESKTOP%		
SIP/TLS and SRTP	%USE_SRTP%	2 or 3	For more information, see section 10.16.4 SIP Over TLS and Secure Real-time Transport Protocol .
	%SRTP_PREFERENCE%		
	%USE_TLS%		
3GPP SIP Headers for SRTP	%USE_MEDIASEC_DESKTOP%	2 or 3	For more information, see section 10.16.16 3GPP SIP Headers for SRTP .

Feature	Tag	License*	Reference Section
SRTP Re-Keying	%ENABLE_RE-KEYING_DESKTOP%	2 or 3	For more information, see section 10.16.17 SRTP Re-keying Configurability .
PIV URL	%PIV_XSI_ROOT%	1, 2, or 3	For more information, see section 10.16.18 Sharing Server (USS) Certificate Validation .
API	%ENABLE_API_PROVIDER%	1, 2, or 3	For more information, see section 10.21 API for Third-Party Applications .
	%ENABLE_WEB_API%		
	%ALLOW_CONNECTORS%		
DNS TTL Management	%SIP_REFRESH_ON_TTL%	1, 2, or 3	For more information, see section 10.7.1 DNS TTL Management .
	%XMPP_REFRESH_ON_TTL%		
S4B Integration	%ENABLE_LYNC_INTEGRATION%	1, 2, or 3	For more information, see section 10.20 UC-One Add-in for Microsoft Skype for Business (S4B) .
	%AUTO-SHOW-DIAL-PAD%		
	%ENABLE_S4B_WINDOW_MODEL_DESKTOP%		
	%PA_PRESENCE_PRECEDES_LYNC_PRESENCE%		
Change Password	%ENABLE_PASSWORD_UPDATE%	1, 2, or 3	For more information, see section 10.16.11 Change Password .
	%PASSWORD_UPDATE_WARN_BEFORE_DAYS%		
Version Control	%ENABLE_VERSION_CONTROL_DESKTOP%	1, 2, or 3	For more information, see section 13 Version Control and Automatic Upgrade .
	%MUST_VERSION_WINDOWS%		
	%RECOMMENDED_VERSION_WINDOWS%		
	%DOWNLOAD_URL_WINDOWS%		
	%MUST_VERSION_OSX%		
	%RECOMMENDED_VERSION_OSX%		
	%DOWNLOAD_URL_OSX%		

Feature	Tag	License*	Reference Section
Automatic Upgrade	%ENABLE_AUTOMATIC_UPGRADE_DESKTOP%	1, 2, or 3	For more information, see section 13 Version Control and Automatic Upgrade .
	%HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMINS%		
	%HIDE_AUTOMATIC_UPGRADE_SETTINGS%		
	%AUTOMATIC_UPGRADE_INTERVAL_MINUTES%		
	%URL_HASH_WINDOWS%		
	%ALPHA_VERSION_WINDOWS%		
	%ALPHA_HASH_WINDOWS%		
	%ALPHA_URL_WINDOWS%		
	%BETA_VERSION_WINDOWS%		
	%BETA_HASH_WINDOWS%		
	%BETA_URL_WINDOWS%		
	%URL_HASH_OSX%		
	%ALPHA_VERSION_OSX%		
	%ALPHA_HASH_OSX%		
	%ALPHA_URL_OSX%		
	%BETA_VERSION_OSX%		
%BETA_HASH_OSX%			
%BETA_URL_OSX%			
Google Analytics	%ENABLE_ANALYTICS_DESKTOP%	1, 2, or 3	For more information, see section 10.14 Google Analytics .
UC-One Hub	%ENABLE_HUB%	1, 2, or 3	For more information, see section 10.13 UC-One Hub Integration .
	%HUB_LOGIN_URL%		
	%ENABLE_HUB_BUTTON%		
	%HUB_BUTTON_URL%		
	%ENABLE_HUB_BANNER%		
	%HUB_BANNER_URL%		

Feature	Tag	License*	Reference Section
	%HUB_BANNER_HEIGHT%		
	%ENABLE_CONTEXTUAL_GADGET%		
	%CONTEXTUAL_GADGET_URL%		
	%ENABLE_HUB_ANALYTICS%		
	%HUB_ANALYTICS_SERVICE_PROVIDERID%		
	%HUB_ANALYTICS_RESellerID%		
Hiding Spell Checker Settings	%ENABLE_SPELL_CHECK_DESKTOP%	1, 2, or 3	For more information, see section 10.19.18 <i>Hide Spell Checker</i> Settings.
Hiding Communications Window Notifications and Tones	%HIDE_NOTIFICATIONS_MODE_DESKTOP%	1, 2, or 3	For more information, see section 10.19.14 <i>Hide Communications Window Notifications and Tones</i> .
	%MUTE_ALERTS_MODE_DESKTOP%		
Communications Window UI Control via API	%COMMUNICATION_WINDOW_TRIGGER%	1, 2, or 3	For more information, see section 10.19.15 <i>Communications Window UI Control via API</i> .
Forced DM file update	%ENABLE_AUTOMATIC_RECONFIGURE_DESKTOP%" />	1, 2, or 3	For more information, see section 10.15.4 <i>Forced DM Configuration File Update</i> .
Connection retry parameter	%CONNECTION_RETRY_PARAMETER_DESKTOP%	1, 2, or 3	For more information, see sections 10.1.6 <i>SIP Failover</i> and 10.3.3 <i>XMPP Failover</i> .
Contact dir search	%CONTACT_CACHE_TIME_INTERVAL_MINUTES%	1, 2, or 3	This value decides how frequently contact cache can be updated on demand, default value is 1440 (24 Hours, 24 hrs before same contact search request will not be sent to xsi server.)

NOTE: Tag values are case-sensitive and must be set as shown.

The following table lists the license mappings used in the previous table.

License	Reference
BroadTouch Business Communicator Desktop	1
BroadTouch Business Communicator Desktop – Audio	2
BroadTouch Business Communicator Desktop – Video	3
Integrated IM&P	4

License	Reference
Shared Call Appearance	5
Meet-Me Conferencing	6
Collaborate – Audio	7
Collaborate – Video	8
Collaborate – Messaging	9
Collaborate – Sharing	10

To offer a potential way to only specify a subset of all the custom DM tags, each of the following lists defines a set of features whose matching custom DM tags can be selected from the previous table while leaving other tags undefined to get their default values.

Note that in addition to the custom tags, Cisco BroadWorks system tags and System Default tags must also be used. The default configuration template can be used as a good starting point, which typically should not require major changes. If the deployment requires features on top of the following lists, those tags must be defined.

Additionally, if the deployment deviates from these feature lists, the configuration must be changed.

Example basic full feature set without additional UI components contains the following features:

- Xsi with mid-call controls (HTTPS paths recommended)
 - Ad hoc conference calls
 - Xsi-Event channel (on-demand mode recommended by default unless features that require permanent event channel are used)
 - Basic Call Settings UI
- Xtended Services Interface (Xsi) search with basic UI (no toolbar)
- SIP/TLS audio calling with Supplementary Services (recommended with TCP transport):
 - Call transfer
 - Conference
 - Call Park
 - Call pull
- XMPP/TLS chat and presence:
 - Location
 - Busy-In Call presence
- Encrypted file transfer
- Voice mail:
 - MWI
 - Visual Voice Mail
- Video calling:
 - N-way video

- Video Server (UVS) conferencing
- Share:
 - Sharing Server (USS)
 - Participant share
- My Room:
 - Moderator Controls
 - Direct Dial
 - Auto-provisioning for the bridge
- Version control
- Google Analytics

The Voice over IP (VoIP) Only feature set contains the following features:

- Xtended Services Interface with mid-call controls
 - Ad hoc conference calls
 - Xtended Services Interface event channel (on-demand mode recommended by default)
 - Basic Call Settings UI
- Xtended Services Interface search with basic UI (no toolbar)
- SIP/TLS audio calling with Supplementary Services (recommended with TCP transport):
 - Call transfer
 - Conference
 - Call Park
 - Call pull
- Voice Mail:
 - MWI
 - Visual Voice Mail
- Video Server (UVS) audio conferencing
- Version control
- Google Analytics

Assistant–Enterprise (AE) replacement feature set contains the following features:

- Xtended Services Interface with mid-call controls:
 - Ad hoc conference calls
 - *Xsi-event* channel (permanent mode required, for example, for terminating Xsi call control):
 - Basic Call Settings UI
 - Terminating Xtended Services Interface Call Control

- Incoming Call Xtended Services Interface Notification in Xtended Services Interface-Only Mode
- Xtended Services Interface search with basic UI and enhancements:
 - Toolbar
 - Search for additional directories (Personal, group common, and enterprise common)
- LDAP search
- Outlook integration
- Web button
- Banner
- SIP/TLS audio calling with Supplementary Services (recommended with TCP transport):
 - Call transfer
 - Conference
 - Call Park
 - Call pull
- Voice mail:
 - MWI
 - Visual Voice Mail
- Version control
- Google Analytics

3.3 Communicator Device Type – Cisco BroadWorks System Tags

In addition to the default system tags and the custom tags that must be defined, there are also existing Cisco BroadWorks system tags that are typically used and are part of the recommended Device Type Archive File (DTAF). These tags are listed in this section.

Tag	Value
%BWNWORK-CONFERENCE-SIPURI-1%	This the server URI used to enable N-way conferencing.
%BWVOICE-PORTAL-NUMBER-1%	This number is used for voice mail. The client dials this number when retrieving voice mail.
%BWLINPORT-1%	SIP username used in SIP signaling, for example, in registration.
%BWAUTHPASSWORD-1%	SIP password used in SIP signaling.
%BWDN-1%	Primary phone number. After login, this is put into the XMPP vCard for automated contact card details provisioning in pre-Release 20.x deployments. For more information, see section 10.1.23 Select Outband or Inband DTMF .
%BWHOST-1%	Typically used as the SIP domain.

Tag	Value
%BWAUTHUSER-1%	SIP username typically used in <i>401</i> and <i>407</i> signaling. Can be different from the default SIP username.
%BW_USER_IMP_ID-1%	This is the XMPP username.
%BW_USER_IMP_PWD-1%	This is the XMPP password.
%BW_IMP_SERVICE_NET_ADDRESS-1%	This is the XMPP server domain.
%BWDEVICEACCESSFQDN%	This is used as part of the version control URI in the version control feature. For more information, see section 13 Version Control and Automatic Upgrade Version Control and .
%BWDMSCONTEXT%	This is used as part of the version control URI in the version control feature. For more information, see section 13 Version Control and Automatic Upgrade Version Control and .
%BWDEVICEACCESSURI%	This is used as part of the version control URI in the version control feature. For more information, see section 13 Version Control and Automatic Upgrade Version Control and .
%BWE164-x%	This is used for SIP protocol settings. For SIP configuration, see section 10.1.1 Change Basic SIP Server Settings . This tag provides a phone number in international format that can also be used for federated calling (see section 10.1.24 Federated Calling in XMPP Deployments). It is recommended that this DM tag be used instead of the previously used %BWDN-x%, but only in Cisco BroadWorks Release 20.0 and later. Note also that the “x” in these tags is replaced by a number, typically “1”.

4 Introduction to Configuration

The section introduces the configuration for the Communicator Desktop client. The *Config.xml* file is common to all platforms; however, there are some files for the Desktop client only.

The Desktop client is configured using several different configuration files. The main configuration file is:

- *Config.xml* – Provides server-specific information, such as the server addresses, ports, and runtime options for the client, for example, the type of presence to be used.

NOTE: This file is retrieved from the network at login and it is not saved locally.

In addition, there are further local configuration files common to all accounts:

- *application_setting.ini* – Mostly lists the configurable UI features that the end user can change for the client using the *Preferences*. For more information, see section [8.4 User Interface Settings – application_setting.ini](#).
- *credentials_encrypted.db* – Contains cached credentials. For more information, see section [8.2 Credentials_encrypted.db](#).
- *proxy_settings.ini* – Contains HTTP proxy settings. For more information, see section [10.16.15 HTTP Proxy Support](#).
- *LogConfig.xml* – Contains logging settings. For more information, see section [10.18 Logging](#).

The configuration files are read by the client after the user logs in. Additionally, there are account-specific files utilized by the client:

- *comms_encrypted.db* – This file stores Chat History for both one-to-one and group chats.
- *user_local_data_encrypted.db* – This file is for local temporary storage for contact list that is also stored in BroadCloud or Messaging Server (UMS) when XMPP is used. In addition, some user settings are stored in this file.
- *web cache* – Files used by the internal web browser when using banner or web button features.
- *connectors_encrypted.db* – This contains settings related to UC-One API users, for example, USB headsets.

Finally, there is a system-wide file for all accounts, which is not local:

- Version control file, located on a remote Web server, is used for version control purposes at login. For more information, see section [13 Version Control and Automatic Upgrade Version Control](#) and .

5 File Locations

The following directories contain client configuration files:

- Installation directory
- Main configuration directory
- Account directory (inside the main configuration directory)

The main configuration file is located in the main configuration directory. Note that the default can vary based on branding. The usual file locations are as follows.

Installation Directory

Operating System	File Path	Files
Windows 7/8/8.1	C:\Program files(x86)\ <company_name>\<application_name>\ In the reference client: C:\Program Files(x86)\BroadSoft\Communicator\	Internal files
OS X	/Applications/<application_name>/Contents /Resources/ Note that the directory here ends with “.app”.	

Main Configuration Directory

The files in the main configuration directory apply to all accounts. The files and the typical locations for these files in the main configuration directory are shown in the following table. Note that roaming path is used by default on Windows starting with Release 22.2.0.

Operating System	File Path	Files
Windows 7/8/8.1	C:\Users\<USERNAME>\AppData\Roaming\ <company_name>\<application_name>\ Or, one of the following: "C:/ProgramData/<APPNAME>," "<APPDIR>", "<APPDIR>/data", "<APPDIR>/data/<APPNAME>" For the reference client: C:\Users\<USERNAME>\AppData\Roaming\ BroadSoft\<Communicator\	application_setting.ini proxy_settings.ini credentials_encrypted.db connectors_encrypted.db LogConfig.xml In each account directory, there are additional user- specific files (see the table that follows).
OS X	/Users/<USERNAME>/Library/Application Support/<company_name>/<application_na me> For the reference client: /Users/<USERNAME>/Library/Application Support/BroadSoft/Communicator	

Account Directory (inside main configuration directory)

In each account directory inside the main configuration directory, there are additional user-specific files as follows.

Operating System	File Path	Files
Windows 7/8/8.1	C:\Users\ <i><USERNAME></i> \AppData\Local\ <i><company_name></i> \<i><application_name>\ For the reference client: C:\Users\ <i><USERNAME></i> \AppData\Local\BroadSoft\ <i><Communicator></i>	<i>comms.db</i> <i>user_local_data_encrypted.db</i> <i>webcache</i> <i>vcards_encrypted.db</i>
OS X	/Users/ <i><USERNAME></i> /Library/Application Support/ <i><company_name></i> / <i><application_name></i> For the reference client: /Users/ <i><USERNAME></i> /Library/Application Support/BroadSoft/ <i>Communicator</i>	

Logs are also saved in the same directory in a folder called “logs” with a new log-related configuration file called *LogConfig.xml*. The logs directory can contain several different log files, including Outlook Add-in log files. For more information, see section 10.18.1 [Release 20.0.0 Enhancements](#).

NOTE: For Mac OS 10.7 and higher, this folder can be accessed using the Finder and *Go → Go to Folder → Menu*.

6 Installation

The Desktop client installation is performed by an installation wizard. The client is installed using WiX framework, which is an open source system to create Windows MSI installers. The installation procedure is simple and does not require the user to select many options. Both OS X and Windows installers are signed with a BroadSoft certificate that the operating system verifies at installation time.

Release 22.3.0 introduced a single installer supporting both S4B integration and Outlook Add-in in the same product. Release 3.9.0/22.9.1 added support for not requiring administrator rights for automatic upgrade. In addition, Windows End-User License Agreement (EULA) is shown at first launch as on Mac OS.

During installation, the user can select the following options after the .msi file is run on Windows:

- Run when system starts (can be changed later in *Preferences*).
- Install Outlook Add-in.
- Install S4B integration.
- Change S4B registry values to enable S4B dial pad.
- Install for all users.
- Create a desktop icon.
- Select destination folder for installation.
- Select the name of the software in the *Program* menu.
- Launch the client after installation.

The installer can support several languages as a branding option. For more information on localization, see the *Communicator Language Guide*. The chosen language is written to the *application_setting.ini* file at installation and when the end user changes the Communicator language.

For a Mac OS installation, the default language is the language of the operating system, used in the native Mac OS installation windows.

After installation, the branded default language (first in the language list in the branding kit) is used unless there is a language already selected in *application_setting.ini* or if the OS language is one of the branded languages. If the OS language is one of the branded languages, it is selected by default. The installer language can also be set using command line argument.

For Windows, the default installer language is the language of the operating system. If the language of the OS cannot be found in the languages branded for the client, English is used as the fallback.

After installation, the branded default language (first one in the language list in the branding kit) is used unless there is a language already selected in *application_setting.ini* or if the OS language is one of the branded languages. If the OS language is one of the branded languages, it is selected by default.

To choose another supported language for the installation, use as the following command line argument:

```
msiexec /i <installer_name> TRANSFORMS=":<language-code>"
```

For example, for Polish:

```
C:/msiexec /i communicator.msi TRANSFORMS=":1045"
```

For more information, see the *UC-One Desktop Language Guide*.

When the installation is upgraded, the language last-used in the Communicator client is automatically chosen. If that language is not available, English is chosen if available; otherwise, the first language available in the installer is used.

6.1 Installation Options

The `/quiet` option for a silent installation is supported. The silent installer can be used, for example, for a mass-install deployment. It uses default installation options; hence, auto-run is enabled, and desktop short cut provided but only if a system account is used. In remote installation deployments where the installer could be running in system account/user context, it is necessary to also use the `ALLUSERS` option that will configure auto-run and desktop shortcuts for all users.

It is not recommended to install several client versions on one machine at the same time since it is not an officially supported configuration. However, it is technically possible to install several versions, for example, for limited testing purposes using different installation paths and application names. Running two clients at the same time is not supported.

An example of a silent installation using the command line interface on Windows is as follows.

```
C:\> msiexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi" /quiet
```

Note that in the previous example, the executable installer name is located in the root directory. Its name is *UCOne.msi* and it is followed by the `/i` and `/quiet` switches. In general, it is recommended that all programs, in particular Outlook, must be exited before installing Communicator with `/quiet`. When using the `/i` switch, the installer path should be specified.

In addition, the `INSTALL_ROOT` msi property for specifying the installation directory is supported (see the following example where a "Test" directory is used for installation).

```
C:\> msiexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi" /quiet  
INSTALL_ROOT="C:\Program Files\Test"
```

For administrator usage, there is also a command line switch to install the client for all users of the desktop device. Some previous versions automatically installed the client for all users but to better support all silent installation use cases, the following switch has been added. Without this switch, installation only takes place for the installing user. Capital letters are used.

```
C:\> msiexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi" ALLUSERS=1
```

Note that Release 22.1.0 and later no longer by default attempts to write the necessary registry key values to enable the dial pad in Lync. Instead, this functionality can be enabled using another command line switch (or using the installer UI).

```
C:\> msiexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi"  
ENABLE_S4BADDIN_WITH_DIALPAD=1
```


When the S4B branding option is enabled, the installer checks that the system has a valid version of the .NET framework installed. The previously used installer flag for Lync/S4B integration is taken back into use starting with Release 22.3.0. See the following for an example.

```
C:\> msixexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi"  
ENABLE_S4BADDIN=1
```

To disable the built-in S4B component, use explicit false value with the parameter.

```
C:\> msixexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi"  
ENABLE_S4BADDIN=0
```

Release 21.3.0 introduced a new command line option to not use the default “Run this program when system starts” option.

```
C:\> msixexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi" NOSTART=1
```

Without this option, the installation uses the “Run this program when system starts” option. If MSI installer is run in admin mode and the default “Run this program when system starts” option is enabled, end users cannot change this setting.

Release 22.0.0 introduced an installation option to enable or disable the Outlook Add-in.

```
C:\> msixexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi"  
ENABLE_OUTLOOK_PRESENCE=1
```

Release 3.9.0/22.9.1 installer also supports the desktop shortcut command line option as follows.

```
C:\> msixexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi"  
DESKTOP_SHORTCUT=1
```

Installer log file can also be specified using standard msixexec procedures.

```
C:\> msixexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi" /lv  
logfile.txt
```

Several options can also be used in the same command with MSI. In addition, extra logging onto a file can be enabled if needed as shown in the following example, using msixexec procedures.

```
msixexec /i "C:\Packages\UC-One.bc-uc.win-3.9.0.12345.msi" /quiet  
INSTALL_ROOT="C:\Program Files (x86)\BroadSoft\UC-One" /l*v  
"C:\Users\bsupdate_installer.log" ENABLE_OUTLOOK_PRESENCE=1  
ENABLE_S4BADDIN=1
```

Some options such as Outlook Add-in or S4B integration must be first enabled in branding.

Installing Release 22.3.0 or newer from the command line will allow using the “ALLUSERS” and “ENABLE_OUTLOOK_PRESENCE” parameters to install for all and add the Outlook Add-in.

An uninstall will by default not delete user profiles and other settings data. An uninstall will by default clear the “connectors” folder so installed custom add-ins will be deleted.

6.2 Install on Windows

Installation on Windows is started by double-clicking on the downloaded *.msi* file. The WiX installation wizard starts and the installation directory as well as some defaults can be chosen as previously depicted.

With mass installations, the procedure is the same, although the installation command is typically given from command line with installation parameters previously explained.

6.3 Install on OS X

Installation on Mac is started by double-clicking on the downloaded *.dmg* file. In the subsequent install dialog box, the application is installed by dragging the application icon to the *Applications* directory.

6.4 Administration Rights

By default, installation only takes place for the user performing the installation. However, in Release 21.0.0, a new check box was added to allow installation for all accounts in the operating system.

Installation can be done without administrator rights, which is typical in enterprise environments. For S4B integration deployments, administrator rights are required, as well as for Outlook Add-in installation.

6.5 Uninstall

Windows “uninstallation” does not require the user to select any options. With Mac, uninstalling is performed by simply dragging the application folder from the *Applications* directory to the trash can.

All files are deleted at uninstallation, except for the following files:

- Windows
 - Registry entries
 - Account files are only deleted when explicitly allowed by the end user on Windows
- OS X
 - No account files are deleted by OS X uninstallation

6.6 Limitations

It is not recommended to install several client instances on the same machine. The only exception would be in test scenarios. Using several clients at the same time on the same machine is not a supported configuration.

7 Account-Specific Files

Cisco BroadWorks Release 22.0 introduced an alias feature that allows using different user IDs for the same user. When using Communicator Desktop, it is recommended to choose which user ID is at provisioning time and always use the same user ID when Communicator is used to avoid user data such as Chat History being scattered across different accounts.

Additionally, even if the alias feature is not used, changing the userid does not migrate existing local message history, settings, and credentials being tied to the new account. Therefore, when using the new user ID, there is no previous local message history, settings, or stored credentials.

7.1 comms_encrypted.db

The *comms_encrypted.db* is an internal encrypted database file that contains the local Chat History for one-to-one and group chats that are presented to the user in the *Main* window (if configured to be visible).

The encryption is done using a 256-bit Advanced Encryption Standard (AES) cipher. As a PRAGMA key used as salt for AES encryption, an id similar to device_lock key is used. The PRAGMA key length is 32.

7.2 user_local_data_encrypted.db

The *user_local_data_encrypted.db* file is used to provide temporary storage for the following:

- Contacts
- User settings cache

Adding contacts to this file renders them in the contact list after the next login. This file is encrypted using AES256 cipher as the *comms_encrypted.db* file.

Example Contacts Data

```
<?xml version="1.0" encoding="UTF-8"?>
<addressbook version="1.0" timestamp="2014-11-03T06:58:49Z"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="contact_store.xsd" schema-version="2">
  <contacts>
    <contact id="1896529">
      <communication
type="sip">sip:+12345678@domain.com</communication>
      <first_name>John</first_name>
      <last_name>Doe</last_name>
      <email>johndoe@domain.com</email>
      <street>Street 1 </street>
      <postal_code>12345</postal_code>
      <city>Somecity</city>
      <country>Somecountry</country>
      <communication type="work_phone">+18765432</communication>
      <communication type="mobile_phone">222-333-
444</communication>
      <communication
type="jid">johndoe@domain.com</communication>
    </contact>
    <contact id="2311039">
      <communication
type="sip">sip:+1223334444@domain.com</communication>
```

```

    <communication
type="jid">testuser32@domain.com</communication>
    </contact>
    <contact id="3626495">
    <communication
type="jid">testuser2@domain.com</communication>
    </contact>
</contacts>

```

Another use case for the *user_local_data_encrypted.db* file is the cache of the account-specific UI settings. Some of these settings can be modified by the end user using the *Preferences* tab at runtime without a need to restart the client. However, the file itself is not to be changed by the end user or the service provider and its contents are listed in the following example file for completeness only.

Example Cache Data

```

[settings]
audio\saveDirectory=/Users/johndoe/Documents/My Recording Files
sounds\defaultRinger=:/sounds/ringing.wav
sounds\incomingMessageEnabled=true
sounds\incomingCallEnabled=true
audio\duringacalldevice=@ByteArray()
audio\recordingdevice=@ByteArray()
audio\withoutacalldevice=@ByteArray()
video\captureresolution=30
video\capturedevice=@ByteArray(FaceTime HD Camera)
video\qualitydetection=true
audio\automaticgaincontrol=false
confirmations\removeContact=true
confirmations\historyRecord=true
outlook_calendar_enabled=true
outlook_search_enabled=true

[presence]
location_publish\manually_published=false
location_publish\last_received_ip_address=194.100.122.196
location_publish\dontAskAgain=false
location_publish\accepted=true

[contactlist]
showProfilePhotos=true
showOfflineContacts=true
showFavoritesGroup=false

[security]
myRoomDialInNumber=+1-112233445566
myRoomPin1=12345678
myRoomHostPin=87654321
myRoomPin2=

[timeline]
filterFlag=0

[mainWindow]
leftpane=contacts

```

7.3 vCard Cache

Starting with Release 22.0, there is an account-specific file containing a local cache of contact list vCards. The file name is *vcards_encrypted.db*. It is encrypted using the same mechanism as *comms_encrypted.db*.

7.4 Web Cache

Starting with Release 21.3.0, cookies are supported in the configurable web button that shows web content. For more information on configurable web button, see section [10.19.9 Configurable Web Button and Web Tab View](#). The saved cookies are stored inside the *WebCache* folder in addition to other web browsing related details. To remove old cookies, the end user must first exit UC-One Communicator, remove the file, and then sign back in. Failing to exit the client recreates the *cookies.dat* file with cookies from memory.

8 Client-Specific Files

8.1 Server Settings – config.xml

Essential runtime options are set in the *config.xml* file, which is downloaded at login. This file contains protocol-level configuration parameters and can be used to disable/enable some features altogether. In addition, the *application_settings.ini* file can be used to disable/enable some features for all accounts.

8.1.1 Backward Compatibility

The configuration XML file can contain configurations for different client versions. The separation between versions is done with the *<extended-configs>* XML-element, which should contain at least one *<version-config>* element. This element should define the client versioning with the attribute called *clientversion*. In Release 20.0.0 and higher, the default templates no longer contain the *extended-configs* section, which makes the configuration file shorter for easier management. However, the *extended-configs* section can still be added when needed.

The *clientversion* attribute in the *version-config* node refers to the first (that is, oldest) version of Communicator that should use that particular configuration node. This is not updated for each release.

Only add new *version-config* nodes when it is necessary to make a configuration file change that would break the functionality of older clients using the same configuration file (see the following example for *extended-configs*).

Example file snippet with extended-configs

```
<?xml version="1.0"?>

<config version="10.0.0"> <!--if no version, 0 is default -->

    <name>BroadSoft Communicator PC Config 10.0</name>

    <services>
    .
    .
    .
</extended-configs>

    <version-config clientversion="20.0.1">

        <name>BroadSoft Communicator PC Config 20.0</name>

        <services>
        .
        .
        .
    </version-config>

    </extended-configs>
</config>
```

Use the official DTAF as an example configuration file, as it is recommended for use in a deployment. Also note that the Release 20.0.2 configuration file is otherwise backward compatible with Release 10, but XMPP does not work when using Release 20.x.x configuration file with Release 10.x.x clients. Using the *extended-configs* mechanism, this can be handled in deployments.

For more information on the Conferencing URI, see section **Error! Reference source not found. Error! Reference source not found.**

8.2 Credentials_encrypted.db

In Release 21.3.0 and later, this database file contains encrypted credentials. *Credentials.dat* is no longer used in Release 21.3.0 and later.

The file contains the SIP, XMPP, LDAP, and Xsi credentials. When the end user chooses to remember login credentials (Xsi), they are stored in this file. User-provided LDAP credentials are also stored after the end user provides them in the *Preferences* window.

The same file contains credentials for all used accounts on the machine. 256-bit AES in CBC mode is used with a PRAGMA key similar to the key used when tying a Cisco BroadWorks MAC field with a specific configuration file (for more information on that feature, see section [10.16.12 Cisco BroadWorks MAC Field and Specific Configuration File Name](#)). The PRAGMA key here is a hardware id with 32-bit length. The SQLCipher library is used using OpenSSL for the actual encryption/decryption.

Release 21.6.1 introduced a branding option for disabling the use of salt in the encryption process to allow copying of this file across machines in, for example, VDI environments. For more information, see the *Communicator for Desktop Branding Guide*.

8.3 HTTP Proxy Settings – proxy_settings.ini

This file only contains the HTTP proxy parameter selection.

Example File (without UI features disabled)

```
[proxy]
proxy_type=1

[proxy_settings]
type=1
httpserver=
httpport=
httpsserver=
httpsport=
```

8.4 User Interface Settings – application_setting.ini

The *application_setting.ini* file can be used to configure user interface features. It applies mostly to user interface features that the end user can modify. The file is not created during installation, but rather after the first successful session (the file stub is then present). It is not supposed to be changed by the end user. The client rewrites parameters in this file at runtime; therefore, caution is recommended if the service provider intends to remotely manage this file.

The changes are only available after the client has been restarted. The *loginusername* parameter in the login node is encrypted using the same key that was previously used for *credentials.dat*.

Example File (using local configuration file)

```
[General]
eulaAccepted=true

[login]
autologin=false
savepassword=true
loginusername="313qpyi/Bhyff1x4vdrzygqv7Md4wCo="
```

```
[defaults]
dm_config_file=/Users/johndoe/Documents/Data 16-03-
2012/Business/BroadSoft/NPI/Config
guides/20.0.0/pc_config_R20_15_01_2014.xml

[settings]
xmpp\resourcehash=50399a3a334df0ccce1e138121b79f9bd6f0bba2
api_provider_enabled=true
api_provider_allow_web_api=true
themes\active=broadsoft
language\active=en
loggingenabled=true
xmpploggingenabled=true
advloggingenabled=true
api_provider_allow_connectors=first-party
api_connection_no_confirmation=false
api_connection_accept_by_default=false

[mainwindowpos]
x=916
y=42

[mainwindowsize]
w=245
h=425

[mediavolume]
volumelevel=97
```

The parameters in the file are categorized as follows:

- *[General]* – This is used if the End-User License Agreement (EULA) has been accepted by the user. At installation, the EULA must be accepted, so this parameter is set to “true”. If it is changed to “false”, then the EULA page is shown at login.
- *[settings]* – In general, this category can be changed at runtime using *Preferences* (however, there are some exceptions, such as XMPP resource hash). The *api_provider* parameters are related to third-party connector applications, such as Outlook adding and USB headsets. The XMPP resource hash is an internal identifier, which should not be altered.
- *[login]* – This category can be changed in the *Login* window and for *autologin* in *Preferences*.
- *[defaults]* – This specifies the local configuration file location (if used).
- *[mainwindowpos]* – This tracks the last-used *Main* window position on the screen.
- *[mainwindowsize]* – This saves the last-used *Main* window size as selected by the end user.
- *[mediavolume]* – This tracks the last-used volume as set by the end user.

8.5 Connectors_encrypted.db

This file contains basic data such as version, URL, and state for each utilized connector (add-in) for the Communicator API. The encryption utilized is similar to *comms_encrypted.db*.

8.6 Logging Definitions – LogConfig.xml

This file contains logging settings, defining which log files are enabled, what are the size limits, how many backup files are created, and with what logging levels used in each file. For more information on logging enhancements, see section 10.18.1 [Release 20.0.0 Enhancements](#).

9 UC-One SaaS

9.1 General

UC-One Software as a Service (SaaS) has a different configuration scheme in comparison to UC-One Collaborate. Configuration parameters are divided into two separate files, one for service provider Cisco BroadWorks VoIP configuration, and another for cloud UC-One SaaS configuration. Additionally, it may be that for some deployments there is no Cisco BroadWorks VoIP configuration, so the UC-One SaaS configuration also works in a stand-alone mode. Most parameters used in Release 22.3.1 and later are not available in the UC-One SaaS model for the service provider to modify.

This section lists configuration parameters that are used in Cisco BroadWorks VoIP side while the Reseller Guide describes the available settings for the service provider. The UC-One SaaS DTAF contains the template for Cisco BroadWorks VoIP, while the reseller portal contains a user interface to change some settings.

The following table lists configuration parameter groups that are part of the service provider Cisco BroadWorks VoIP configuration file. For a complete detailed list, see the UC-One DTAF. The parameters themselves have not changed and are described in other parts of this document. In addition, the DM tags used for these parameters remain the same.

Note that in deployments where the value for `include-btbc-link-to-email-invitation` is “true”, the value for `include-btbc-link-to-copy-guest-link` is also “true”. Additionally, when `include-btbc-link-to-email-invitation` is omitting, its default value “true” is assigned to also `include-btbc-link-to-email-invitation`. Therefore, the `btbc-link` would be enabled by default in both the email invitation and Copy Guest Link (to clipboard) if the whole node is omitting.

My Room uses its own SIP stack without SIP registrations and re-uses the same DNS records that are used for 1-1 calls. 1-1 calls use the same SIP stack as all Collaborate calls. My Room SIP stack always uses TLS entries from DNS when available, regardless of the SIP/TLS configuration parameter value (DM tag `%USE_TLS%`). See section [10.1.4 Dynamic SIP Proxy Discovery](#) for more details on SIP proxy discovery DNS procedures. SRTP mode in My Room is hard-coded to transport so it follows what My Room SIP stack is using.

Only if DNS does not provide TLS entries would UC-One SaaS My Room use TCP or UDP and no SRTP.

Release 3.9.0 introduced a significant change in UC-One SaaS configuration files. Several calling related parameter groups were moved from the SaaS configuration file to the Cisco BroadWorks configuration file to enhance service provider configuration flexibility. See the following table for details.

Parameter Group	Reference Sections
Basic SIP Settings	For more information, see the following sections: 10.1.1 Change Basic SIP Server Settings 10.1.2 Codec Configuration for Client 10.1.3 Force TCP or UDP Usage and Keepalives 10.1.4 Dynamic SIP Proxy Discovery 10.1.5 Enable SIP Audio and Video Calls 10.1.7 SIP Port Selection and Preferred-port Usage 10.1.8 SIP rport Management for NAT Traversal 10.1.9 Use P-Associated-URIs in REGISTER Error! Reference source not found. Error! Reference source not found. 10.1.18 Selection of SIP Response for Busy Signal 10.1.23 Select Outband or Inband DTMF 10.1.25 Voice Mail Number and Message Waiting Indicator
Basic RTP Settings	For more information, see the following sections: 10.2.1 Real-Time Control Protocol Extended Report 10.2.2 Real-Time Transport Protocol Port Range 10.2.3 Real-Time Transport Protocol Packet Maximum Transmission Unit 10.2.4 RTCP MUX 10.2.6 Dynamic Video Bit Rate Adaptation
Emergency Calling	For more information, see the following sections: 10.17.2 Disable Emergency Calls 10.17.4 Emergency Call Address Change Service

Parameter Group	Reference Sections
Calling Related Settings (moved to Cisco BroadWorks configuration file in Release 3.9.0)	For more information, see the following sections: 10.5.10 Call Settings and Call Settings Toolbar 10.1.15 Call and Chat Recording 10.1.18 Selection of SIP Response for Busy Signal 10.1.6 SIP Failover 10.1.29 My Room, N-Way, and N-Way Owner Participant List 10.1.26 N-Way and My Room Video Calls 10.1.42 SIP P-Early Media (PEM) Header 10.1.32 Team Telephony 10.1.20 Transfer Call 10.1.31 Video Server 10.1.27 Reduce Use of Call Hold in Conferencing 10.1.16 Call Pull 10.1.17 Call Park and Retrieve Error! Reference source not found. Error! Reference source not found. 10.1.25 Voice Mail Number and Message Waiting Indicator 10.1.33 Executive-Assistant 10.5.16 Call Center Agent Login 10.1.38 Remote Control Event Package 10.20 UC-One Add-in for Microsoft Skype for Business (S4B) 10.19.8 Auto-Close S4B PSTN Call Window 10.1.41 Auto-Show Dial Pad 10.19.7 Minimize After Login 10.1.5 Enable SIP Audio and Video Calls 10.15 Communicator Packages and Device Management 10.19.6 Active Communications Extra Buttons

10 UC-One Collaborate Config.xml Examples

This section describes deployment settings with the config.xml file. To determine if a setting applies to an older client version, see the appropriate release-specific configuration guide.

10.1 SIP and Calling

10.1.1 Change Basic SIP Server Settings

The client is commonly configured to use a SIP network, which is done by modifying the *config.xml* file. Typically, the following parameters must be changed:

- SIP domain. This is used as the domain part of own SIP URI (own SIP URI is also sometimes called line port) in general in SIP headers and in Xsi calls. The user part of own SIP URI comes from SIP credentials configuration (parameter <username> under <credentials>).
- SIP server URI or IP address of the SIP proxy server if DNS resolving should fail. Note that in order to use TLS, IP addresses cannot be used in the proxy parameter as TLS certificate validation will fail. For more information on the proxy port, see the DM tag %SOURCE_PORT%. Note that DNS TTL management feature described in section [10.7.1 DNS TTL Management](#) cannot be used when an IP address is used in the proxy address parameter. In general, it is not recommended to use an IP address in this field for these reasons.

Other parameters can also be changed to enable various features for calling. However, the previous settings enable basic functionality for the following:

- Registering on the SIP network.
- Making audio or video calls.
- Performing DNS-based proxy discovery, which allows using several proxies.

Once SIP registration is enabled, enabling SIP SUBSCRIBE for MWI and telephony presence must be done via separate configuration parameters. For more information on voice mail and telephony presence, see sections [10.1.25 Voice Mail Number and Message Waiting Indicator](#) and [10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence](#), respectively.

Note that basic SIP configuration is always needed for MWI and client-based Busy-In Call presence status updates even when SIP calls are disabled. MWI and telephony presence rely on SIP NOTIFYs.

To turn off SIP altogether, SIP proxy address is to be left empty and audio and video calls disabled as described in section [10.15 Communicator Packages and Device Management](#).

The setup of the SIP servers follows this basic scheme:

- The proxy address contains the SIP server URI.
- Only one proxy can be defined.
- The DNS proxy discovery provides support for many proxies, which require the proper set up of the DNS.

In addition, SIP timers can be configured if needed (see the following example).

```

<config version="20">>
<protocols>

    <sip>

        <timers>

            <T1>500</T1> <!--the amount of
time, in milliseconds, for a network round trip delay-->
            <T2>4000</T2> <!--the maximum
amount of time, in milliseconds, before retransmitting non-invite
requests and invite responses-->
            <T4>5000</T4> <!--the maximum
amount of time, in milliseconds, for a message to remain in the network--
>

        </timers>
    
```

Separate SIP authentication credentials can be used for 401 and 407 signaling if needed.

The following table and example provide information on the most typical DM tags used for SIP configuration.

Tag	Default if Omitted	Supported Values	Example	Description
%BWLINPORT-1%	Empty	String	<username>johndoe </username>	Typically SIP username. For more information, see section 3.3 Communicator Device Type – Cisco BroadWorks System Tags .
%BWAUTHPASSWORD-1%	Empty	String	<password>secretpa ssword</password>	Typically SIP password. For more information, see section 3.3 Communicator Device Type – Cisco BroadWorks System Tags .
%BWE164-1%	Empty	Phone number	<phone- number>12345678 </phone-number>	Default phone number for the user in international format, also uploaded to the XMPP vCard. For more information, see section 3.3 Communicator Device Type – Cisco BroadWorks System Tags .
%SBC_ADDRESS%	empty	String	<proxy address="sbceexam ple.domain.com"	For more information, see section 3.1 Communicator Device Type – System Default Tags .

Tag	Default if Omitted	Supported Values	Example	Description
%SBC_PORT%	empty	Number	port="5060"	For more information, see section 3.1 Communicator Device Type – System Default Tags .
%BWHOST-1%	empty	String	<domain>exampledomain.com</domain>	Typically used as the SIP domain. For the list of BroadWorks tags, see section 3.3 Communicator Device Type – Cisco BroadWorks System Tags .
%SOURCE_PORT%	empty	Number	<preferred-port>5061</preferred-port>	Typically used for the <i>preferred-port</i> parameter. For more information, see section 10.1.7 SIP Port Selection and Preferred-port Usage .

```

<config version="20">>
<protocols>

    <sip>

        <credentials> <!-- Used to login to SIP to
enable calls -->

                                <username>%BWLINERPORT-
1%</username>

                                <password>%BWAUTHPASSWORD-
1%</password>

                                <phone-number>%BWE164-
1%</phone-number> <!-- Used to get primary phone number from DM to
auto-populate own contact card so that watchers automatically get phone
number for contacts to avoid manual editing of all contacts phone
numbers -->

                                </credentials>
<use-rport-ip>%USE_RPORT_IP%</use-rport-ip> <!-- enable rport feature
for NAT traversal , RFC3581 -->

                                <secure>%USE_TLS%</secure> <!-- if true use
TLS for SIP-->

                                <proxy address="%SBC_ADDRESS%"
port="%SBC_PORT%" /> <!-- SIP outbound proxy, outgoing SIP requests go
to this proxy -->
<domain>%BWHOST-1%</domain> <!-- SIP domain, used e.g. to form SIP URIs
when no domain is given in dial pad and search and dial field, also
adds domain for Xsi calls, authentication realm is taken from this
value-->

```

```

        <preferred-port>%SOURCE_PORT%/preferred-
port> <!-- There have been some usage scenarios where other software
has been running on the same machine with the client, occupying the
default SIP port. To configure the client to use another port for SIP,
the preferred-port parameter can be used. It tries to use the
configured port value specified in the parameter, but if it is taken it
incrementally tries port values above the configured value -->

```

10.1.2 Codec Configuration for Client

Release 21.0.0 introduced a new media framework, which has a different list of codecs.

This segment is still under `<calls>` `<codecs>`, but the list of codecs is different.

The configuration file format is the same in both media frameworks. The preferred usage of codecs can be indicated with the *XML-attribute* "q" value, where a higher q-value has a higher priority. For all codecs that can be dynamically mapped to payload identifiers, the payload ID (or numerical value) can be set by defining *XML-attribute* "pl". Note that the bandwidth parameter is not used in this release.

Voice activity detection (VAD) can also be configured, see the following example.

For the H.264 video codec, the Communicator for Desktop client supports decoding of incoming video stream packetized in Single NAL unit mode or non-interleaved mode, while the outgoing video stream always uses Single NAL unit mode. It is not configurable.

For the list of codecs supported for each media framework, see the *Communicator (Desktop, Mobile, iOS Tablet, and Android Tablet) Product Guide*. The combined list of codecs is also present in the DTAF as all codecs are listed in the configuration file. See the following example for format instructions. Note that the newer (default) media framework may not have all codecs listed in the DTAF. The codec names are case sensitive and need to be as in the following example.

```

<config version="20">
  <services>
    <calls>
      <audio enabled="%ENABLE_AUDIOCALLS%"> <!-- this enables audio
calling -->

                                <codecs>
                                  <!--Attributes:
name =
<codec_mime_type>
                                q =
<codec_preference_1.0_to_0.0>
                                be =
<bandwidth_efficient_true_or_false> missing|false=octet_aligned
                                pl = dynamic
payload number
                                -->
                                <codec name="opus" q="1"
vad="true"/>
                                <codec name="PCMA"
q=".7" vad="true"/>
                                <codec name="PCMU"
q=".8 vad="true"/>

```



```

q=".9" vad="true"/>
q=".5" vad="true"/>
name="telephone-event" pl="101" />
</codecs>
</audio>
<video enabled="%ENABLE_VIDEOCALLS%"> <!-- enables BTBC video calling-->
>
<codecs>
<codec
name="H264" q=".9" pl="109" >
</codec>
</codecs>

```

10.1.3 Force TCP or UDP Usage and Keepalives

Communicator can be configured to use either TCP or UDP for both SIP signaling and RTP media. Note that the client defaults to TCP. Note that without TCP keepalive SIP TCP connections are closed after a period of inactivity.

The following example depicts this configuration node.

```

<config version="20">
  <protocols>
    <sip>
      <transports>
        <tcp-size-threshold>%TCP_SIZE_THRESHOLD%/</tcp-size-threshold>

```

The following tag, in the custom *BroadTouch_Tags* set, controls whether the client uses TCP or UDP.

Tag	Default if Omitted	Supported Values (Bytes)	Example	Description
%TCP_SIZE_THR ESHOLD%	0	0	<tcp-size-threshold>0</tcp-size-threshold>	Forces TCP to be used. The decision to use TCP or UDP for the client is up to the service provider; however, the suggested recommendation is to use TCP with the default value "0".

Tag	Default if Omitted	Supported Values (Bytes)	Example	Description
	0	1 through 99,000	<tcp-size-threshold>10000</tcp-size-threshold>	Forces UDP to be used when the message size is below the value specified here. This defaults to TCP when the message size is greater than the set value. To use UDP, 1500 is the default recommendation.
	0	100000	<tcp-size-threshold>100000</tcp-size-threshold>	Forces UDP to be used.

The same configuration node also has parameters for TCP and UDP keepalive, depicted in the following example. The possible parameters are:

- Enabling TCP keepalive true/false, the default is “false” if the node is missing. Note that when this feature is enabled, TCP keepalives are sent even if UDP transport is being used for SIP.
- Enabling UDP keepalive true/false, the default is “false” if the node is missing. Note that when this feature is enabled, UDP keepalives are sent even if TCP transport is being used for SIP. Additionally, even if TCP is used for SIP, Communicator also accepts traffic over UDP as per *RFC 3261*.
- Timeout specifies the maximum time of inactivity in seconds after which the keepalive message is sent. No value means the keepalive is disabled for the protocol.
- Payload for the keepalive messages, possible values (no value means keepalive is disabled for the protocol):
 - Crlf
 - Null (not to be used)
 - Custom string (not to be used)

```

<config version="20">
  <protocols>
    <sip>
      <transports>
        <tcp-size-threshold>%TCP_SIZE_THRESHOLD%</tcp-size-threshold>

                                <udp>

                                <keepalive
enabled="true"> <!-- when enabled sends UDP keep alive to outbound
proxy, used e.g. to keep NAT/firewall bindings open -->

                                <timeout>20</timeout>

                                <payload>crlf</payload> <!-- The possible values for payload
are: crlf, null or custom text string -->

                                </keepalive>

```

```

                                </udp>

                                <tcp>

                                <keepalive
enabled="false"> <!-- when enabled sends TCP keep alive to outbound
proxy, used e.g. to keep NAT/firewall bindings open -->

                                <timeout>0</timeout>

                                <payload></payload> <!-- The possible values for payload are:
crlf, null or custom text string -->

                                </keepalive>

                                </tcp>

```

The keepalives can be used for NAT traversal purposes to keep NAT bindings open with little extra traffic.

The server IP address and port for keepalives are determined using the normal procedures for SIP proxy discovery. Note that SIP ports and selection of transport protocol obtained via SIP dynamic proxy discovery override any static port or transport configuration. For more information on dynamic proxy discovery, see section [10.1.4 Dynamic SIP Proxy Discovery](#).

10.1.4 Dynamic SIP Proxy Discovery

To enable SIP dynamic proxy discovery functionality, see the following example.

```

<config version="20">
  <protocols>
    <sip>
      <proxy-discovery enabled="%USE_PROXY_DISCOVERY%"
tcp="%USE_TCP_FROM_DNS%" udp="%USE_UDP_FROM_DNS%"
tls="%USE_TLS_FROM_DNS%"> <!--
  if enabled and records found, the default proxy is removed
  -->
      <record-name>%SBC_ADDRESS%</record-name>
      <domain-override>%DOMAIN_OVERRIDE%</domain-override>
    </proxy-discovery>
  </sip>
</protocols>
</config>

```

Release 22.4.0/3.3.0 introduced the capability to control which transport protocols entries from DNS SRV are used when many are available. The selection of transport protocol then takes place using the procedures provided in this section. For certificate management details regarding dynamic SIP proxy discovery, see section [10.16.5 SIP TLS Certificate Validation](#).

The following tags, in the custom *BroadTouch_Tags* set or *BroadWorks* tags, control this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%USE_PROXY_DISCOVERY%	false	true, false	<proxy-discovery enabled="true">	Enables dynamic SIP proxy discovery for audio and video calls. The recommended value is "true".

Tag	Default if Omitted	Supported Values	Example	Description
%SBC_ADDRESSES%	empty	Any valid URL (cannot be an IP address)	record-name> sbc.domain.com </record-name>	This Cisco BroadWorks tag is typically used for the record-name parameter. For more information, see the following section.
%DOMAIN_OVERRIDE%	empty	Any valid URL (cannot be an IP address)	<domain-override> other.domain.com </domain-override>	This custom tag is used for the domain-override. For more information, see the following section.
%USE_TCP_FOR_DNS%	true	true, false	<proxy-discovery enabled="true" tcp=true udp=true tls=true>	If this parameter value is "false", then the DNS SRV results for this transport protocol (TCP) are discarded. If "true", then the results from DNS SRV for this transport protocol (TCP) are used. Depending on the SRV priorities, another transport may still be elected.
%USE_UDP_FOR_DNS%	true	true, false	<proxy-discovery enabled="true" tcp=true udp=true tls=true>	If this parameter value is "false", then the DNS SRV results for this transport protocol (UDP) are discarded. If "true", then the results from DNS SRV for this transport protocol (UDP) are used. Depending on the SRV priorities, another transport may still be elected.
%USE_TLS_FOR_DNS%	true	true, false	<proxy-discovery enabled="true" tcp=true udp=true tls=true>	If this parameter value is "false", then the DNS SRV results for this transport protocol (TLS) are discarded. If "true", then the results from DNS for this transport protocol (TLS) are used. Depending on the SRV priorities, another transport may still be elected.

DNS allows Communicator to get the IP address, port, and transport protocol for the SIP proxy as per *RFC 3263*.

Communicator supports DNS SRV, Naming Authority Pointer (NAPTR) and A-record queries. At login, the 3-step flow is as follows:

- 1) Perform a NAPTR query using the <record-name> field above to obtain the server URIs with the transport protocols if they exist. The value for the <record-name> parameter should be the full domain that DNS is to resolve and cannot be an IP address.

- 2) Resolve items found in the NAPTR query using an SRV-query to obtain the final server URI and port. The domain part used in the SRV-query is taken from the result of the NAPTR query to find the final server URI (and port). The port received from DNS SRV-query is used when the DNS SRV entries are available. Note that the port, only from the configuration file, applies to the static proxy in the configuration file, and not to the URIs resolved using SRV. See the following examples for the usage of the various record names.

If no NAPTR is found, then the client tries an SRV-query with the record-name taken from *<domain>* parameter unless there is *<domain-override>* parameter present in which case *<domain-override>* is used and automatically tries to find separate entries for TCP, UDP, and TLS (*_sip_protocol* [UDP, TCP, or TLS]). Note that the Stream Control Transmission Protocol (SCTP) is not supported. If SRV queries do not yield any results, proxy discovery fails, and the end user is presented with an error indicating that calls are not available. In this case, there is no SIP registration. However, even if all SRV queries fail or if the servers received there do not work, as a fallback, Communicator still checks if the configured static proxy works, only with A-queries to the URI specified in *<proxy address>* in order to see if it yields an IP address that provides a working SIP registration. Port and transport in this last resort case come from *tcp-threshold* and *<secure>* parameters.

- 3) Resolve found URIs using the A-record query. The received final IP addresses are tried in the order in which they are received to get a working connection to the SIP proxy. This order can be defined by the service provider in the DNS. The first SIP proxy URI, with a successful A-record lookup, is selected and is used until it no longer works, or the client logs out. In the A-query step, only one IP address is used at a time even if many are received. However, all SRV entries are resolved until logout or loss of the network.

Important Notes

- 1) If DNS proxy discovery results in transport protocol selection in the SRV step by receiving a working SIP proxy URI for a transport protocol, it overrides the *tcp-threshold* parameter typically used to select UDP or TCP in the configuration file. The same also applies to configuration of SIP/TLS. TCP or UDP is used depending on the priority in DNS.
- 2) Items received via SRV are prioritized over the static proxy in the configuration file. The NAPTR order is not looked at; only SRV priority counts. When SRV results in several items with equal transport protocol, priority, and weight, any one received is selected at random. NAPTR weights are not supported in this release but SRV weights are supported. SRV priority is looked at first, and for items with equal priority, weight is looked at to determine the likelihood in which a certain server is tried next.
- 3) For Release 10.x, the *extended-configs* section must be used in the main XML configuration file; otherwise, the configuration change does not take effect. For Release 20.0.0 and later, the *extended-configs* section has been removed by default.
- 4) The optional *domain-override* parameter allows A-record name other than the one in the SIP domain configuration parameter to be resolved with SRV when NAPTR results are omitted. See the following examples for the usage of the *domain-override* parameter.
- 5) Communicator uses operating system primitives for DNS operations and, typically, DNS responses are cached to honor the TTL of the DNS response.
- 6) The DNS type (service) for NAPTR records must follow *RFC 3263* procedures, otherwise, DNS resolution may fail. For example, it is required to use SIPS+D2T for SIP over TLS.

Example 1: Using DNS proxy discovery without domain-override configuration parameter

The following is an example of a configuration using SIP proxy discovery when only SIP over TCP is used and NAPTR query in step 1 returns results.

```
<config version="20">
  <protocols>
    <sip>
      <proxy address="domain.com" port="5060"/>
      <proxy-discovery enabled="true"> <!-- if enabled and records
found, the default proxy is removed -->
        <record-name>record-domain.com</record-name>
        <domain-override>override-domain.com</domain-override> <!--
if record-name part is different from sip domain, use this -->
      </proxy-discovery>
      <domain>sip-domain.com</domain>
```

This results in the following steps in the protocol level.

```
1. NAPTR query for record-domain.com, answer:
record-domain.com.
28591 IN NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-
domain.com.
2. SRV query for _sip._tcp.test.sip.record-domain.com (received in the
NAPTR query), answer
_sip._tcp.test.sip.record-domain.com. 28635 IN SRV
10 10 5061 test.sipgeo.record-domain.com.
3. A-record query for test.sipgeo.record-domain.com, answer:
test.sipgeo.record-domain.com. 16 IN A 1.2.3.4
```

As a result, the SIP registration takes place over TCP using port 5061 (received in the SRV step) and towards the IP address 1.2.3.4.

Example 2: Using domain-override parameter in configuration file

The following is a second example of a configuration using SIP proxy discovery where the SIP domain is different from the proxy domain, and only SIP over UDP, is used and NAPTR query does not return results.

```
<config version="20">
  <protocols>
    <sip>
      <proxy address="domain.com" port="5060"/>
      <proxy-discovery enabled="true"> <!-- if enabled and records
found, the default proxy is removed -->
        <record-name>record-domain.com</record-name>
        <domain-override>override-domain.com</domain-override> <!--
if record-name domain part is different from sip domain, use this -->
      </proxy-discovery>
      <domain>sip-domain.com</domain>
```

This results in the following steps at the protocol level.

```
1. NAPTR query for record-domain.com, no answer.
2. SRV query for _sip._tcp.override-domain.com (from configuration file),
answer
_sip._tcp.override-domain.com. 28635 IN SRV
10 10 5061 test.override-domain.com.
3. A-record query for test.override-domain.com, answer:
test.sipgeooverride-domain.com. 16 IN A 4.3.2.1
```

As a result, the SIP registration takes place over UDP using port 5061 (received in the SRV step) and towards the IP address 4.3.2.1.

Example 3: Using SRV priorities

The following is another example of a configuration using SIP proxy discovery when only SIP over TCP is used and NAPTR query in step 1 returns results, but several NAPTR and SRV records with different priorities are received. In this case, only SRV priority matters in this release event although several NAPTR records with varying priorities are also received.

```
<config version="20">
  <protocols>
    <sip>
      <proxy address="domain.com" port="5060"/>
      <proxy-discovery enabled="true"> <!-- if enabled and records
found, the default proxy is removed -->
        <record-name>record-domain.com</record-name>
        <domain-override>override-domain.com</domain-override> <!--
if record-name part is different from sip domain, use this -->
      </proxy-discovery>
      <domain>sip-domain.com</domain>
    </sip>
  </protocols>
</config>
```

This results in the following steps at the protocol level.

```
1. NAPTR query for record-domain.com, answer:
record-domain.com.
28591 IN NAPTR 100 10 "S" "SIPS+D2T" "" _sip._tcp.test.sip.record-
domain.com.
28591 IN NAPTR 120 10 "S" "SIPS+D2U" "" _sip._udp.test.sip.record-
domain.com.

2. SRV query for _sip._tcp.test.sip.record-domain.com (received in the
NAPTR query), answer
_sip._tcp.test.sip.record-domain.com. 28635 IN SRV
10 10 5061 test.sipgeo.record-domain.com.

SRV query for _sip._udp.test.sip.record-domain.com (received in the NAPTR
query), answer
_sip._udp.test.sip.record-domain.com. 28635 IN SRV
20 10 5062 test.sipgeo.record-domain.com.

3. A-record query for test.sipgeo.record-domain.com, answer:
test.sipgeo.record-domain.com. 16 IN A 1.2.3.4
```

As a result, the SIP registration takes place over TCP using port 5061 (received in the SRV step) and towards the IP address 1.2.3.4 that would support both UDP and TCP.

10.1.5 Enable SIP Audio and Video Calls

In addition to basic SIP configuration depicted in the previous sections, SIP audio and video calls must be separately enabled using configuration parameters defined in the following example. This is required to support the various configuration packages explained in more detail in section [10.15 Communicator Packages and Device Management](#).

Note that to have fully working video calls, SIP INFO must be enabled on the server side. For more information on required settings, see the *UC-One Solution Guide*.

These parameters dictate whether audio and video call buttons appear in the UI.

```

<config version="20">
  <services>
    <calls>
      <audio enabled="%ENABLE_AUDIOCALLS%">
      .
      .
      .

      <video enabled="%ENABLE_VIDEOCALLS%">
      .
      .
      .
  
```

The following tags, in the custom *BroadTouch_Tags* set, control this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_AUDIOCALLS%	false	true, false	<audio enabled="true">	Set to "true" to enable audio call button in the UI. Set to "false" to disable audio call button in the UI.
%ENABLE_VIDEOCALLS%	false	true, false	<video enabled="true">	Set to "true" to enable video call button in the UI. Set to "false" to disable video call button in the UI.

10.1.6 SIP Failover

10.1.6.1 Configuration and DNS Operations

SIP failover follows Cisco BroadWorks procedures. Server IP addresses needed for failover can be obtained using either SIP proxy discovery described in the previous section or a static outbound proxy that resolves to several IP addresses (see sections 10.1.4 [Dynamic SIP Proxy Discovery](#) and 10.1.1 [Change Basic SIP Server Settings](#)).

Operating system DNS cache is used to avoid unnecessary DNS traffic. There is no hard-coded limit for the maximum number of IP addresses in the list.

10.1.6.2 Failover Triggering and Failover Time

In the case of dynamic SIP proxy discovery, the transport protocol is specified in the list, so it can be that server1 is tried with UDP, then server2 with UDP, then server1 with TCP, and so forth depending on DNS SRV responses. For UDP, SIP T1 timer defines how long a proxy on the list is tried before moving to the next one, typically 32 seconds value is used (64*T1).

For TCP socket setup, a separate hard-coded transport-level timer dictates how long the connection is tried when no connection can be established before failover to the next proxy on the list is triggered. The timeout value is 5 seconds for TCP and 10 seconds for TLS connections.

In failover, the first working server is retained for SIP registrations until it stops working as follows:

- 1) TCP connection terminated by server, no response to a request from server [apart from PUBLISH].

- 2) Definitive error response received from server. Release 22.7.5 introduced a configuration parameter for specifying excluded error codes. For more information, see section [10.1.19 Exclude SIP Error Codes in Failover](#).
- 3) Network connection is lost.
- 4) Log out/log in takes place.

If there is one SIP-request that does not get a response, the failover process is triggered even though other requests have worked. The procedure for each of these cases is depicted in the following list, one IP address is processed at a time. The time to detect that the SIP proxy is not reachable is typically around half a minute but depends on the configuration of SIP timers as per *RFC 3261* for UDP and on the new TCP-level timer introduced in Release 21.4.0 for TCP and TLS. For SIP PUBLISH used for RTCP XR reporting, missing responses to SIP PUBLISH do not trigger failover.

Release 22.9.8 introduced an enhancement where a failing TCP connection is retried once to see if it gets back up if the network interface is otherwise working. If the TCP connection is re-established, failover is not triggered. A registration refresh is performed instead. The motivation for this enhancement is to keep SIP signaling handle for the call so that call control operations such as hold and unhold can be still done in the call.

For case 1 in the previous list, the following SIP error responses from the server to a SIP REGISTER trigger a failover. Release 22.7.5 introduced a configuration parameter for specifying excluded error codes. For more information, see section [10.1.19 Exclude SIP Error Codes in Failover](#).

- 5xx
- 6xx

The following SIP 4xx responses to SIP REGISTER do not cause failover:

- 401 *Unauthorized*
- 403 *Forbidden*
- 404 *Not Found*
- 407 *Proxy Authentication Required*
- 423 *Interval Too Brief*

Furthermore, 4xx error responses to SIP INVITE do not trigger failover, but 5xx and 6xx do. Failback is not currently supported.

Additionally, Release 22.9.12 introduced an enhancement to honor SIP *Retry* header when it receives a 503 response to a SUBSCRIBE.

10.1.6.3 Failover Process

The generic failover process is as follows:

- 1) SIP proxy discovery: Communicator resolves the SIP proxy typically using a DNS NAPTR, SRV, and A-query lookups and receives multiple IP addresses. For SIP proxy discovery details, see section [10.1.4 Dynamic SIP Proxy Discovery](#).
- 2) Communicator starts using the received IP address in priority order and chooses the first one that works. When a failure is detected, Communicator goes back to step 1 SIP proxy discovery. However, if a SIP proxy failed while the network interface remains up, that SIP proxy is tried last even if it would come back as the highest priority proxy from DNS.

Since the different failover subcases have subtle nuances, the specific cases are discussed in more detail below. Release 3.9.0/22.9.1 introduced an exponential back-off timer for the new connection setup round after DNS operation, for cases when the network remains up, but the SIP connection is lost. Details are as follows:

- When a SIP proxy can no longer be used for SIP registration, for any reason (no response to a request except PUBLISH or error response such as 503 with a retry-after header received), a SIP proxy list is regenerated. The client then tries to register to the first one on the list (except if the recently failed proxy is still the highest priority one when network interface is alive). If that fails, the whole list of servers is tried until either a working one is found, or all servers fail. If all SIP proxies fail, an error is shown in the Main window, and the client waits for a configurable number of seconds to minimize Denial of Service (DOS) impacts, regenerates the list of SIP proxies using DNS, and starts the SIP re-registration procedure using the first server on the list as above. See the following bullet point for details on the configurable timer for the exponential back-off.
- When the network is lost, an error is shown in the *Main* window about the lost network and unavailable calls. With TCP, network loss is detected immediately while on UDP, SIP timers provide an exponential retrying mechanism. Once network connectivity is regained, the list of SIP proxies is regenerated normally based on either SIP proxy discovery using DNS (see section 10.1.4 [Dynamic SIP Proxy Discovery](#)) or via static configuration of SIP proxy address (see section 10.1.1 [Change Basic SIP Server Settings](#)). SIP proxies are tried in the order received from DNS. The first working one is retained until it stops working, the network connection is lost, or a logout/login takes place. If all SIP proxies fail, an error is shown in the *Main* window and registration is re-tried after a configurable exponential timer to minimize DOS impacts starting from the first server of a regenerated list of SIP proxies. The exponential timers introduced in Release 3.9.0/22.9.2 follows the following logic and only applies if UC-One loses its SIP connection but the network in general remains up. It is intended to avoid DOS situations when all clients are trying to reconnect. It only applies to the new connection setup round when DNS resolution for servers is complete:
 - A new timer defines the retry delay in seconds, which is denoted as T in the following sub-list.
 - When retrying to connect, UC-One wait time increases according to the Fibonacci series as follows:
 - 1 * T
 - 1 * T
 - 2 * T
 - 3 * T
 - 5 * T
 - 8 * T
 - 13 * T
 - 21 * T
 - 21 * T
 - ...
 - Note that the delay does not grow beyond 21 times the unit delay.

- In addition to the increasing delay, a random factor is applied to prevent spikes of clients attempting to reconnect at the same time. This is implemented by drawing a random number from a uniform distribution between 0.3 and 1.7 and multiplying the delay by that number. A new random number should be drawn on each round.

For example, on round four, if T is 10 seconds, the expected delay time is 30 seconds (3 * T), but the actual wait time can vary between 9 seconds and 51 seconds, after applying the random factor.

- When the DNS TTL feature is enabled, there is a new configuration parameter introduced in Release 22.9.16 that allows to set a minimum value for the DNS TTL of the secondary SIP server. This is intended for deployments where the service provider may not control the DNS TTL of the secondary SIP server in all cases. The problematic case can be a very short TTL value for the secondary while the failed primary is still the top priority server in DNS, causing Communicator to repeatedly unregister from the secondary and trying to re-register back to the primary. For these situations, the new parameter allows the service provider to set a higher value for the DNS TTL for the Communicator failover process so that the primary is not retried every time the DNS TTL of the secondary expires but only after the configured minimum TTL time has elapsed.
- At login, SIP registration is performed using either SIP proxy discovery using DNS or static configuration of the SIP proxy address as in the previous case for network loss.

RTP uses the same port as SIP; therefore, as long as the SIP session with the SIP proxy is alive, consecutive calls would use the same interface, unless the network interface or SIP proxy is lost between two calls and the next SIP session with a proxy ends up using another interface.

If WiFi is used for the call and the WiFi connection drops and an Ethernet connection is used instead, Communicator drops the call and automatically re-registers to the Ethernet connection. There is no support today to automatically recreate the call on the Ethernet side.

When several network interfaces are available, Communicator takes the one that the OS provides (the client asks for a socket and the OS provides it).

SIP Retry-after header in 503 responses is supported for REGISTER only and not for other requests in this release. When present, the corresponding proxy node is blacklisted so it will not be considered during the next proxy discovery during the blacklisting time period.

In Release 21.2 and onwards, ongoing calls should not be killed at failover situations.

For more information about the solution level, see the *UC-One Solution Guide*.

The following is an example configuration of the exponential back-off timer.

```
<config version="20">
  <protocols>
    <sip>
      <connection-retry-
timer>%CONNECTION_RETRY_PARAMETER_DESKTOP%/</connection-retry-timer>
<proxy address="domain.com" port="5060"/>
      <proxy-discovery enabled="true">
        <dns-ttl-minimum-value>%DNS_TTL_MINIMUM
_VALUE%/</dns-ttl-minimum-value>
      ...
    </sip>
  </protocols>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used to control chat for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%CONNECTION_RETRY_PARAMETER_DESKTOP%	10	Positive integer (seconds)	<connection-retry-timer>15</connection-retry-timer>	Set the starting value for the exponential back-off timer. See the section above for details.
%DNS_TTL_MINIMUM_VALUE%	No minimum value set	Positive integer (seconds)	<dns-ttl-minimum-value>600</dns-ttl-minimum-value>	Set minimum DNS TTL value for the DNS TTL feature.

10.1.7 SIP Port Selection and Preferred-port Usage

At login, Communicator gets a socket for incoming and outgoing SIP communications from OS, and the local port for the socket is obtained this way. SIP proxy and port parameters define the target server to which SIP registration is done.

With TCP, Communicator acts as a TCP client concerning this socket. With TCP, Communicator also gets another port for listening to incoming SIP traffic, acting as a TCP server. The TCP connection with local port obtained at login is expected to be re-used for all SIP traffic.

In practice, there are very rarely incoming TCP connections for SIP outside of the connection established by the client already at login as NAT/FW boxes typically block new incoming TCP connections. Therefore, this parameter mostly does not have an impact on Communicator operation.

Since Communicator does not have client-side certificates to authenticate the client to the server, it rejects any incoming TLS connections. Instead, the server is expected to reuse the TLS connection initiated by the client towards the server where the client is authenticated to the server using a username and password while the server is authenticated to the client using a server-side certificate. For more information about TLS certificate handling, see the respective sections for SIP, XMPP, Xsi, and Share as well as the generic TLS section [10.16.3 SSL/TLS Certificates](#).

There have been some cases when another other software has been running on the same machine as the client, occupying the default SIP port. In addition, SIP specification requires clients to have a capability where they can listen to incoming SIP traffic. With TCP, Communicator is acting as a TCP server in that case. To configure the port for listening to incoming SIP traffic, the *preferred-port* parameter can be used. The client tries to use the configured port value specified in the *preferred-port* parameter for the port where it is listening to incoming traffic, but if it is taken, the client incrementally tries port values above the configured value.

For example, if the value of the *preferred-port* is “6000” and that port is taken, the client tries 6001, 6002, 6003, and so on until it finds an unused port. Once an unused port is found, it uses that for its own SIP communication when new TCP connections are opened. The resulting port received for listening to incoming TCP SIP traffic is also placed in the SIP Contact header.

The *rport* parameter is related in the sense that if that is enabled, the IP address and port used in the SIP Contact header are obtained using *rport* functionality. For more information on *rport*, see section [10.1.8 SIP rport Management for NAT Traversal](#).

With UDP, there is no separate port obtained for listening to incoming traffic, but only one socket is obtained from the OS for incoming and outgoing SIP traffic. *Preferred-port* defines the port used in the SIP Contact header. UDP keepalive can be used to manage the UDP socket so that incoming traffic is possible. For more information on keepalives, see section [10.1.3 Force TCP or UDP Usage and Keepalives](#).

The SIP Via header is populated with the local port in both TCP and UDP cases. The following figure shows an example of TCP without rport. With rport enabled, the SIP Contact header would have the IP address from the outer side of the NAT/FW box (in the following example it would be 8.7.6.5).

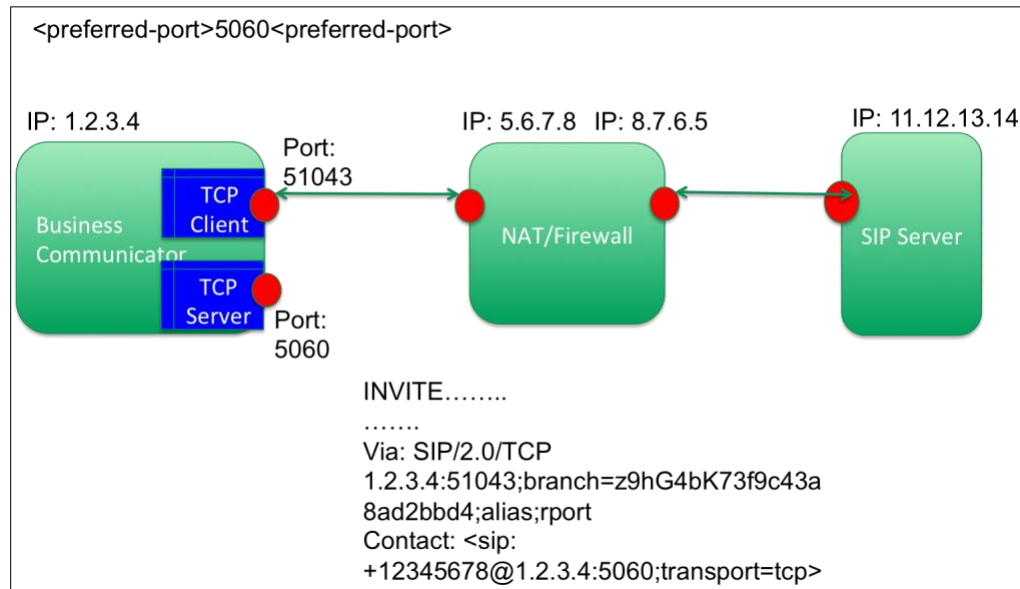


Figure 2 SIP Port Selection and Rport Not Enabled

For the DM tags typically used for this parameter, see section [10.1.1 Change Basic SIP Server Settings](#).

10.1.8 SIP rport Management for NAT Traversal

The client can be configured to use the SIP rport mechanism for NAT traversal. Note that, typically, it cannot be the only solution for NAT traversal and SBC is mainly used for this purpose. For a description of the rport specification, see *RFC 3581*. This feature can be set using the following configuration node.

For more information on SIP port and transport protocol recommendations when SIP Application Layer Gateways (ALGs) are used in the network, see the *UC-One Solution Guide*.

Note that the “rport” string is always present in outgoing SIP requests regardless of configuration. The parameter only affects the usage of IP address and port received from the server in the SIP “received” and “rport” headers. When the feature is enabled, the values from “received” and “rport” headers are used in the SIP Contact header of SIP requests (even when the “received”-header is missing in REGISTER response).

The *Preferred-port* parameter is related in that it otherwise defines the port used in the SIP Contact header. For more information on SIP port allocation, see section [10.1.7 SIP Port Selection and Preferred-port Usage](#).

```
<config version="20">
    <protocols>
        <sip>
            <use-rport-ip>%USE_RPORT_IP%</use-rport-ip>
        </sip>
    </protocols>
<!-- enable rport feature for NAT traversal, RFC3581 -->
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%USE_RPORT_IP%	false	true, false	<use-rport-ip>false</use-rport-ip>	Enables rport for audio and video calls. The default is "false".

10.1.9 Use P-Associated-URIs in REGISTER

The following parameter is used when registering and handling the related *200 OK* response.

If the parameter is set to "false", then the client does not use the *P-Associated-URI* and uses the identity from its own SIP URI instead.

```
<config version="20">
    <protocols>
        <sip>
            <use-alternative-identities>%USE_ALTERNATIVE_IDENTITIES%</use-alternative-identities>
        </sip>
    </protocols>
</config>
```

If the parameter is set to "true", then the client takes its own identity from the last *P-Associated-URI* header for all outgoing SIP requests (INVITE, SUBSCRIBE, CANCEL, INFO, and REFER) from the *200 OK* response in the REGISTER. In addition, these URIs are not shown as contacts in the contact list.

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%USE_ALTERNATIVE_IDENTITIES%	false	true, false	<use-alternative-identities>true</use-alternative-identities>	Enables use of alternative identities in SIP REGISTER. If "true", then the client takes its own identity from the last <i>P-Associated-URI</i> header for outgoing SIP requests. If "false", then its own identity for outgoing SIP requests is taken from its own SIP URI.

For the related parameter for selecting outgoing target SIP URI for calls, see section [10.1.35 Configure SIP URI or Tel URI in Outgoing Calls](#).

10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence

There are several alternatives for setting telephony (*Busy – In Call*) presence:

- Using a presence server
- Using Communicator as an SCA end point
- Using Communicator as a primary end point with alternate locations
- Using Communicator as a primary end point

In conjunction with this, the *SIP Call-Info* event package usage can also be enabled or disabled. When enabled, a SIP SUBSCRIBE for call-info event package is sent. Note however that enabling forced logout or Moderator Controls causes SIP SUBSCRIBE to be sent for the call-info event package regardless of the *bsoft-call-info* parameter value as those features depend on call-info notifications.

When aggregated presence is in use, the presence server option for *Busy – In Call* presence is typically selected, although in Release 22.9.6 and later, local generation of *Busy – In Call* can also be used. For more information on aggregated presence, see section [10.4.5 Aggregated Presence](#).

The following setting depicts the parameters for triggering *Busy – In Call* presence.

```

<config version="20">
<services>
  <dnd enabled="%ENABLE_DND%" />
    <presence>
      <bsoft-call-info enable= "%ENABLE_TELEPHONY_PRESENCE%">
- <!--
  this is SCA, SOME DATA in the future
  -->
    </bsoft-call-info>

```

The following table describes the different recommended configuration parameter values for *dnd* and *bsoft-call-info*.

Case	Value for dnd enabled=	Value for bsoft-call-info enabled=
Presence server is used	false	false
Communicator as SCA endpoint	false	true
Communicator as primary device with alternate locations defined	false	true
Communicator as primary device	true	false

NOTE: In Xsi-Only mode, the only possible mode to have fully working telephone presence is to have *call-info* set to “true”.

10.1.10.1 SCA End Point

When Communicator is an SCA endpoint, call-info subscription is to be used (*bsoft-call-info enabled=true*). In this case, Communicator is configured to rely only on Cisco BroadWorks information for setting *Busy – In Call* presence, using the *SIP Call-Info* event package notifications. The advantage of this approach is that since the server is providing the triggering info, *Busy – In Call* presence is also set when the call is made from other devices.

10.1.10.2 Primary Device

When the Desktop client is the primary device and not an SCA device, the *call-info* subscription is not accepted by Cisco BroadWorks. Therefore, the local configuration of *Busy – In Call* presence is the only option in those deployments.

The *dnd* parameter can also have an opposite value from the *bsoft-call-info* parameter to support telephony presence in deployments where only the Device Management system tag %BWSHAREDLINE-BOOL-1% is used to control the automatic *Busy – In Call* feature. Note that either local triggering or SCA-triggering must be chosen, and both cannot be used at the same time.

```
<config version="20">>
  <services>
    <dnd enabled="not %BWSHAREDLINE-BOOL-1%" />
    <presence enabled="true">
      <xmpp/>

    <subscription>
      <bsoft-call-info enabled="%BWSHAREDLINE-BOOL-1%">
```

Starting with Release 20.0.2, local generation of *Busy – In Call* presence also works for Xsi calls initiated using the client.

10.1.10.3 Primary Device with Alternate Locations

There was a minor change introduced in Cisco BroadWorks Release 20.0 so that the *call-info* subscription is accepted even if the Desktop client is a primary device when at least one of the “alternate location services” is assigned to the user. Alternate location services include BroadWorks Anywhere, BroadWorks Mobility, Executive, Shared Call Appearance, and Flexible Seating. Whenever one of these alternate location services is assigned, the Communicator client should subscribe to *call-info* instead of locally generating the call presence.

10.1.10.4 Presence Server

BroadCloud can support a presence server that handles the setting of automatic *Busy – In Call* presence on behalf of the client. For this, the client-based setting of *Busy – In Call* must be disabled.

The following DM tags, in the custom *BroadTouch_Tags* set, control this capability.

Tag	Default if Omitted	Supported Value	Example	Description
%ENABLE_DND%	false	true, false	<dnd enabled="false" />	Enables local configuration of <i>Busy – In Call</i> presence. See the previous tables for correct usage with other parameters. The default is “false”.
%ENABLE_TELEPHONY_PRESENCE%	false	true, false	<bsoft-call-info enabled="true" >	Enables telephony presence. See the previous tables for correct usage with other parameters. The default is “false”.

10.1.11 N-way Conferencing URI

As of Release 9.3.0, the *service-uri* value for N-way conference has changed (see the following example) and the template provided no longer automatically includes the prefix “sip”. The protocol prefix should now be defined as the value of the %BWNWORK-CONFERENCE-SIPURI-1% variable for Releases before 20.0.0. As of Release 20.0.0, logic has been added so that the client adds the “sip.” prefix, if needed. Removing the Conferencing URI for N-way also disables conferencing menus in the client UI.

The segment in the example was previously the following:

```
<conference><service-uri>sip:%BWNWORK-CONFERENCE-SIPURI-1%</service-uri>
```

It has been changed to the following:

```
<conference><service-uri>%BWNWORK-CONFERENCE-SIPURI-1%</service-uri>
```

10.1.12 Display Name Matching for Incoming and Outgoing Calls and Call History and Diversion Information

A revised logic is employed in Release 21.1.0 and later for finding a display name for an incoming call so that both the display name and phone number are always shown when available. The display name is shown in the first row of the incoming call toaster with a larger font while the phone number is shown in the second line and is always taken from the SIP *From* header. This is not configurable currently. The incoming call may match an existing contact, it can be found in Cisco BroadWorks telephony directory or incoming calls have two or more *P-Asserted-ID* (PAI) or other headers that can be used for showing a display name, for example, one *PAI* header with a SIP URI and another with a Tel URI.

To assist in display name matching, it is recommended to use Cisco BroadWorks E.164 flag. For more information, see the *UC-One Solution Guide*.

The display name used in Call History is retrieved from Cisco BroadWorks. However, if there is a local contact for the number, it overrides the display name from Cisco BroadWorks call logs. “Unavailable” from Cisco BroadWorks is shown together with the received phone number when there is no display name found. However, in Release 21.4.x and later, this can be suppressed. For more information, see section [10.1.13 Undesired CallerID Suppression for Display Name](#). If the local contact data changes, it is also used in Call History.

For outgoing calls, the following process is used for display name:

- 1) Display name is fetched from local contact list if the called number or URI matches a contact card field in the local contact list.
- 2) If there is no local contact for the outgoing call, all enabled directories are searched to find a display name. The first single match is utilized when multiple matches are received based on the following priority order:
 - Enterprise directory
 - Personal directory
 - Group common directory
 - Enterprise common directory
 - Local Outlook directory
 - LDAP directory

- 3) If the directory searches did not yield a successful result, SIP 200 OK headers are looked at to find a network display name.
- 4) If SIP headers did not provide a network display name, the dialed number is shown.

The following general display name-matching rule is used for incoming calls:

- 1) If the call is anonymous, the string *Unknown* is shown as display name. The “Unknown” string can be branded. For more information, see the *Communicator for Desktop Branding Guide*. If the call is from the own number, the caller name is shown as “Unknown”. This happens for instance when a Click To Dial call is made using, for example, the Receptionist client, own number in this case is the one available in the DM configuration file tag <phone-number> inside sip node.
- 2) If the call is not anonymous, then Communicator tries to see if the caller is in the contact list by:
 - Checking *x-broadworks-remote-party-info*
 - Checking the *PAI* header if *x-broadworks-remote-party-info* is not present
 - Checking the *From* header, if *PAI* check is not successful
- 3) If there is no match to a contact based on step 2, a directory search to all enabled directories is done. If the search yields multiple results, the first match is utilized based on the following priority order, with *x-broadworks-remote-party-info* header the Cisco BroadWorks ID is present so that can be used for search:
 - Enterprise directory
 - Personal directory
 - Group common directory
 - Enterprise common directory
 - Local Outlook directory
 - LDAP directory
- 4) If the search does not yield matches, the client checks if a network display name is specified in the first SIP headers listed in the next step (order can be configured). If it finds one, it uses it as the display name.
- 5) If there is no match to a contact and no network display name is found in SIP headers, and the Xsi search does not provide a match, the client takes the display name from the (first) header type that matches the following configuration parameter (user part taken only). The order of these can be altered via configuration.
 - *From* header
 - *P-Asserted-ID* header with a SIP URI
 - *P-Asserted-ID* header with a Tel URI
 - *P-Preferred-ID* (PPI) header with a SIP URI
 - *P-Preferred-ID* header with a Tel URI
- 6) If there is no *PAI* or *PPI* header, the client shows the identity (user part only) based on the *From* header.

The following is an example of a configuration for a priority list of headers to be checked.

```
<config version="20">
    <services>
        <contacts>
            <uri-handling>

                <network-displayname-source-
order>

<entry>FROM</entry>      <!-- SIP URI's displayname is set as it's
in the from header -->

<entry>PAI_SIP_URI</entry>  <!-- SIP URI's displayname is set from P-
Asserted-Id header which contains SIP URI -->

<entry>PAI_TEL_URI</entry>  <!-- SIP URI's displayname is set from P-
Asserted-Id header which contains TEL URI -->

<entry>PPI_SIP_URI</entry>  <!-- SIP URI's displayname is set from P-
Preferred-Id header which contains SIP URI -->

<entry>PPI_TEL_URI</entry>  <!-- SIP URI's displayname is set from P-
Preferred-Id header which contains TEL URI -->

</network-displayname-source-order
</contacts>
</services>
</config>
```

There is no configurability for showing diversion information in the incoming call toaster. Only the diversion header is utilized for this purpose instead of other headers such as *History-Info*.

10.1.13 Undesired CallerID Suppression for Display Name

In display name matching, Communicator tries to make educated guesses as to the CallerID when it does not have complete information for display name matching. For incoming calls from contacts that are not in the contact list, there have been incidents of “Unavailable” received in call logs replacing, for example, SIP network display name in certain parts of the UI. The following configuration parameter allows to specify strings that are not used for display names if any other information exists.

```
<config version="20">
    <services>
        <contacts>
            <caller-id-keywords>
                <entry>Unavailable</entry>
                <entry>Unknown</entry>
            </caller-id-keywords>
        </contacts>
    </services>
</config>
```

The default strings not used for display name matching are:

- Unavailable
- Unknown

Strings in any language can be specified in the same way, one string per entry. If the list omits in configuration file, it defaults to a list with one entry, “Unavailable”.

10.1.14 Call History Display Name Override

Release 21.5 added a new feature where the Call History display name can be overridden by translatable “Unavailable” and “Private” both in call log and Visual Voice Mail. The same strings can be specified in several languages. Release 22.9.2 added support for further strings using the new customized-list parameter. The default values for these are empty (if omitted). The process is as follows:

- 1) Define the strings seen in call logs that need to be modified using the configuration node below. Any string can be used for both “Private” and “Unavailable” nodes. For the customized-list, the supported strings are: “Anonymous”, “Anonymous Unavailable”, and “Public”.
- 2) Use standard localization concepts to define the new values for the client Call History strings “Unavailable”, “Private”, “Anonymous”, “Anonymous Unavailable”, and “Public” and then make a new branded build with that branding. For more information on the exact strings that must be modified, see the section *Call History Name Override on Desktop* in the *UC-One Communicator Language Guide*.
- 3) Use the new branded build.

See the following for general configuration examples.

```

<config version="20">
  <services>
    <call-history enabled="true"> <!-- To enable/disable call
history, if Xsi is disabled, falls back to local call history -->
      <name-overrides>
        <private>Private</private>
        <unavailable>Unavailable</unavailable>
        <customized-list>Anonymous,Anonymous
Unavailable,Public</customized-list>
      </name-overrides>
    </call-history>
  </services>
</config>

```

An example configuration and translation for the whole process to change a call log caller named MysteryCaller to JohnDoe is as follows:

- 1) The following DM configuration change is to be done:
`<unavailable>MysteryCaller</unavailable>`.
- 2) New branded build made with the following localization: Unavailable → JohnDoe. For more information on translation strings, see the *UC-One Communicator Language Guide*.
- 3) Use the new branded build where JohnDoe is shown in Call History for calls that would otherwise be “Unavailable”.

10.1.15 Call and Chat Recording

Call recording controls and indicators as well as the chat recording indicator in the *Communications* window can be enabled using a configuration parameter, shown in the following example. Note that one parameter is required for calls and another one for chat. Xsi is used to retrieve currently utilized call recording mode from Cisco BroadWorks so Xsi is needed. For basic Xsi configuration information, see section [10.5.1 Xtended Service Interface Basic Configuration – URL and Version](#).

- Clients request audio recording when on audio call and audio + video when on video call.
- There is no indication to the user for the selected recording type (audio/video or both), including cases where the server is not able to record video while on video calls.

- There is no user control for the type of recording. This must be done on the Cisco BroadWorks side. For more information on how the different Cisco BroadWorks recording modes affects the user interface, see the *Communicator for Desktop User Guide*.
For more information on the call recording server-side feature, see the *Cisco BroadWorks Call Recording Interface Guide*. Server-side call recording cannot be impacted via client configuration.
- Chat recording UI is an indication only and cannot be used for any changes.

```
<config version="20">
    <services>
        <calls>
            <record
enabled="%ENABLE_CALL_RECORDING_DESKTOP%"/>

        <protocols>
            <xmpp>
                <chat-recording
enabled="%ENABLE_CHAT_RECORD_DESKTOP%"/>
    </services>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set, control this capability.

Tag	Default if Omitted	Supported Value	Example	Description
%ENABLE_CALL_RECORDING_DESKTOP%	false	true, false	<record enabled="true" />	Enables the call recording UI for audio and video calls. The default is "false".
%ENABLE_CHAT_RECORD_DESKTOP%	false	true, false	<chat-recording enabled="true" />	Enables the recording UI for chats. The default is "false".

10.1.16 Call Pull

The Call Pull menu in the *Main* window can be enabled using a single configuration parameter, shown in the following example.

```
<config version="20">
    <services>
        <calls>
            <call-pull
enabled="%ENABLE_CALL_PULL_DESKTOP%"/>
    </services>
</config>
```

The following Device Management tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_CALL_PULL_DESKTOP%	false	true, false	<call-pull enabled="true"/>	Enables Call Pull menus in the <i>Main</i> window. The default is "false".

10.1.17 Call Park and Retrieve

The Call Park/Retrieve menu in the *Main* and *Communications* windows can be enabled using a single configuration parameter, as shown in the following example.

```
<config version="20">
  <services>
    <calls>
      <call-park
enabled="%ENABLE_CALL_PARK_DESKTOP%"/>
    </calls>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_CALL_PARK_DESKTOP%	false	true, false	<call-park enabled="true"/>	Enables Call Park menus in the <i>Communications</i> window. The default is "false".

10.1.18 Selection of SIP Response for Busy Signal

Some deployments require using either SIP *603* or *486* response to indicate *Busy* status when the end user rejects an incoming call. This can be configured using the following configuration parameter.

```
<config version="20">
  <services>
    <calls>
      <reject-with-486>
        %REJECT_WITH_486_DESKTOP%
      </reject-with-486>
    </calls>
  </services>
</config>
```

Setting the parameter to "true" makes the client respond with *486*. The default is "false". When absent from the configuration file, the default value is used.

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%REJECT_WITH_486_DESKTOP%	false	true, false	<reject-with-486>true</reject-with-486>	True=486 is used. False=603 is used.

10.1.19 Exclude SIP Error Codes in Failover

Release 22.7.5 introduced a new configuration parameter to exclude *5xx* or *6xx* SIP error codes in failover. Therefore, the configured error codes do not cause failover and specifying error codes from other number series such as *4xx* is not supported. See the following example configuration (one entry per error code is required, the DM tag can be used for the first one).

```
<config>
  <protocols>
    <sip>
      <session>
        <failover-excluded-invite-errors>
          <entry>%FAILOVER_EXCLUDED_INVITE_ERRORS%</entry>
        </failover-excluded-invite-errors>
      </session>
    </sip>
  </protocols>
</config>
```

```

<entry>604</entry>
</failover-excluded-invite-errors>

```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%FAILOVER_EXCLUDED_INVITE_ERRORS%	empty	Numeric SIP error code value such as 603.	<pre> <failover-excluded-invite-errors> <entry>603</entry> </failover-excluded-invite-errors> </pre>	<p>Included SIP error codes do not trigger SIP failover.</p> <p>Leave empty to disable this feature.</p>

10.1.20 Transfer Call

The Transfer Call configuration node has been enhanced so that it is also used with attended call transfer. See the following example for the custom DM tags and the configuration parameters. This configuration is for SIP calls only.

```

<config>
  <services>
    <calls>
      <transfer-call enabled="%ENABLE_TRANSFER_CALLS%"
type="%TRANSFER_CALL_TYPE%">true</transfer-call>

```

Possible values for the *type* field are:

- “full” – Both attended and blind transfers are enabled.
- “blind” – Only blind transfer is enabled.
- “talk-first” – Only attended transfer is enabled.

NOTE: Transfer Call is not enabled by default. Note that this setting also affects the Xsi call transfer UI.

Creating the following Transfer Call tags in the *BroadTouch_Tags* set provides the ability to customize the Transfer Call option.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_TRANSFER_CALLS%	false	false, true	<pre> <transfer-call enabled="true" type="full">true</transfer-call> </pre>	<p>When set to “true”, call transfer is enabled.</p> <p>When set to “false”, call transfer is disabled.</p>
%TRANSFER_CALL_TYPE%	empty	full, blind, or talk-first (see the previous NOTE)	<pre> type="full"> </pre>	<p>Selects the type of call transfer enabled. If this node is omitted, call transfer is disabled.</p>

10.1.21 Forced Logout

This feature allows Cisco BroadWorks to track online client instances with the same device type (for example, mobile or desktop) and only allow one of them to be online at any one time. When Cisco BroadWorks notifies the client to log out, all connections are terminated, and the client returns to the login window. A pop-up dialog is also shown to the end user.

This feature is needed in some deployments where similar clients can be otherwise online at the same time, causing side effects. One example is a user with a desktop machine at work and at home, where the incoming calls would only be received by one of the clients, depending on which SIP registration is active.

Forced logout is based on SIP, the client sends a SIP SUBSCRIBE to the *call-info* event package with a special *appid-value* in the *From* header, regardless of the *bsoft-call-info* parameter value. When Cisco BroadWorks detects multiple client instances online with the same *appid*, it sends a special SIP NOTIFY to the older client instance, causing it to log out. For example, Desktop clients would have an identical *appid-value* although there is no restriction about the usage of this identifier on the client side. The *appid-value* is configured by the service provider.

Note that in order to use forced logout, the SIP *Call-Info* subscription must be enabled. For more information, see section [10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence](#).

For information about the Cisco BroadWorks patches and releases needed for this feature, see the section on BroadWorks Software Requirements in the *UC-One Solution Guide*.

See the following example for configuration details (SIP is the only supported control protocol in this release).

```
<config version="20">
    <services>
        <forced-logout enabled="%ENABLE_FORCED_LOGOUT%"
control-protocol="SIP" appid="%FORCED_LOGOUT_APPID%" /> <!-- All
applications that appear online with identical appid-value will be forced
to logout once other instance registers -->
```

The following table describes the DM tags for forced logout.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_FORCED_LOGOUT%	false	true, false	<forced-logout enabled="true"	Enables forced logout. The default is "false".
%FORCED_LOGOUT_APPID%	empty	string	appid="123abc"	Appid used on the server side for correlation. This can be any string, for example, "123abc". The current rule for a valid appid is 1*(alphanum).

10.1.22 Echo Service (Test Call)

This feature allows the end user to make a test call to verify voice and video quality using a *Main* window menu option. It is available in different languages and matches the client language. The Echo service asks the user to record a message and plays that message back immediately before hanging up. For Cisco BroadWorks requirements regarding the Echo service, see the solution guide. The example Voice Extensible Markup Language (VXML) script that can be used with the Cisco BroadWorks media server is provided as an appendix in the solution guide.

If there are multiple languages specified in configuration and the client does not find a match to its current language, it takes the first item from the configuration.

```

<config version="20">
    <services>
        <test-services
enabled="%ENABLE_TEST_SERVICES_DESKTOP%"> <!-- Test call menu option -->

            <test-calls enabled="%ENABLE_TEST_CALLS_DESKTOP%">

                <test-number language="%TEST-NUMBER-LANGUAGE-
DESKTOP-1%" number="%TEST-NUMBER-DESKTOP-1%"/>

                <test-number language="%TEST-NUMBER-LANGUAGE-
DESKTOP-2%" number="%TEST-NUMBER-DESKTOP-2%"/>

                <!-- Add test number nodes for additional
languages -->

            </test-call

```

The following table describes the DM tags for the Echo service.

Tag	Default If Omitted	Supported Values	Example	Description
%ENABLE_TEST_SERVICES_DESKTOP%	false	true, false	<test-services enabled="true">	Enables the Echo service feature. The default is "false".
%ENABLE_TEST_CALLS_DESKTOP%	false	true, false	<test-calls enabled="true">	To use the Echo service, both the <i>test-calls</i> and <i>test-service</i> must be enabled in the configuration.
%TEST-NUMBER-LANGUAGE-DESKTOP-1%	en	supported language code	language="en"	This can be any language code that the client supports, for example, "en" for English or "fr" for French. For the list of supported languages, see the <i>Communicator Language Guide</i> .
%TEST-NUMBER-DESKTOP-1%	empty	number	number="1234567"	This can be any number.

Tag	Default If Omitted	Supported Values	Example	Description
%TEST-NUMBER-LANGUAGE-DESKTOP-2%	empty	supported language code	language="fr"	This can be any language code that the client supports, for example, "en" for English or "fr" for French. For the list of supported languages, see the <i>Communicator Language Guide</i> .
%TEST-NUMBER-DESKTOP-2%	empty	number	number="1234567"	This can be any number.

10.1.23 Select Outband or Inband DTMF

Outband Dual-Tone Multi-Frequency (DTMF) is the default as per *RFC 2833*. It is used when:

- `<codec name="telephone-event" pl="101" />` is included in the configuration file
- `<codec name="telephone-event" pl="101" />` negotiation succeeds

Otherwise, the client uses inband DTMF.

10.1.24 Federated Calling in XMPP Deployments

As a part of the login sequence, Communicator receives the number specified in a DM tag and uploads it to its own public XMPP vCard so that it is available to all contacts, for example, for calling. As a result, when user A calls a manually added user B, at least one phone number is available via the vCard for calling regardless if Cisco BroadWorks directory synchronization for contact cards works. This hidden fallback number is not visible in the contact card.

Usually contact card synchronization takes care of providing phone numbers into contact cards. However, when manually adding an XMPP contact using a Jabber Identifier (JID) only from another deployment, the phone numbers from the other deployments are not likely to be directly available in the contact card nor in international format. When deployments are separate, automatic Cisco BroadWorks directory synchronization for contact cards does not work and no other phone numbers are directly available in the contact card.

For this reason, calling a contact with a national, for example, North American number from a European deployment does not work, as these deployments are not aware of each other's numbering schemes (typically across countries).

To force the phone number in the vCard to be in international format, a new DM tag %BWE164-x% must be used instead of the previously used %BWDN-x%. Note also that the "x" in these tags is replaced a number, typically "1". By using this tag, users of the deployment have an internationally dialable phone number in their vCard as the last resort when users from other deployments add them to their contact lists and are calling them.

Note that the %BWE164-x% tag is currently only supported in Cisco BroadWorks Release 20.0 and later. Using this tag in deployments prior to Release 20.0, results in nothing being returned and the vCard phone number being populated with the SIP username and domain (as a fallback solution). Typically, this would look like “sip:%BWLINPORT-1%@@%BWHOST-1%”. This SIP URI typically does not work. However, the %BWE164-x% tag is patched back to Release 17.sp4 to provide a long-term solution. For the list of required Cisco BroadWorks patches, see the *UC-One Solution Guide*.

The following is an example for the configuration.

```
<config version="20">
    <protocols>
        <credentials>
            <sip>
                <phone-number>%BWE164-1%</phone-number>
            </sip>
        </credentials>
    </protocols>
<!-- Used to get primary phone number from DM to auto-populate own
contact card so that watchers automatically get phone number to avoid
manual editing of all contacts phone numbers -->
```

The following table describes the DM tag for federated calling.

Tag	Default if Omitted	Supported Values	Example	Description
%BWE164-x%	empty	Phone number	<phone-number>1234567</phone-number>	Phone number in international format. For more information about Cisco BroadWorks system tags, see section 3.3 Communicator Device Type – Cisco BroadWorks System Tags .

10.1.25 Voice Mail Number and Message Waiting Indicator

The number that Communicator dials when clicking on voice mail in the *Communications History* view in the *Main* window can be configured (see the following example). The call is made with video by default. The server downgrades it to audio if video is not supported. To hide the voice mail button, leave the related voice mail number empty. Note that disabling SIP registration also disables Message Waiting Indicator (MWI) for new voice mails. See the following table for more information on enabling MWI.

To show voice mail message information in the UI, Communicator needs to receive SIP MWI notifications from the server (that is, the voice mail event package). See the following table for subscription options. Note also that MWI is needed for Visual Voice Mail notifications to work.

Note that if SIP subscription to voice mail event package fails, the client keeps retrying when configured to do so. For more information on SIP SUBSCRIBE retry configuration, see section [10.1.34 SIP SUBSCRIBE and REGISTER Refresh and SUBSCRIBE Retry](#).

```
<config version="20">
    <services>
        <mwi
enabled="%DESKTOP_MWI_ENABLE%">%DESKTOP_MWI_MODE%</mwi>
        </mwi>
    </services>
</config>
```

```

        <calls>
            <voice-mail enabled="false" visual-
voicemail="false"> <!-- Will enable voicemail tab, not used in BTBC
10.0 -->

                                <center-number>%BWVOICE-
PORTAL-NUMBER-1%</center-number> <!-- number for MWI, can be used
without enabling voicemail tab -->

        </voice-mail>

```

Enabled attribute for voice-mail is not used anymore and can have either a true or false value. For the related Visual Voice Mail configuration, see section [10.5.15 Visual Voice Mail](#).

The following tags, in the custom *BroadTouch_Tags* set, control this capability.

Tag	Default if Omitted	Supported Value	Example	Description
%BWVOICE-PORTAL-NUMBER-1%	empty	number	1234567	The client calls this number typically specified using an existing Cisco BroadWorks system tag when clicking on voice mail in <i>Communications History</i> .
%DESKTOP_MWI_ENABLED%	false	true, false	<mwi enabled="true">explicit</mwi>	Set to "true" to enable MWI and to "false" to disable MWI.
%DESKTOP_MWI_MODE%	MWI disabled	implicit, explicit	<mwi enabled="true">explicit</mwi>	Set to "explicit" to send SIP SUBSCRIBE for MWI event package when MWI is enabled. Using "implicit" does not send a SIP SUBSCRIBE for MWI event package when MWI is enabled.

10.1.26 N-Way and My Room Video Calls

The Communicator Desktop client configuration supports N-way video calls (see the following example). The same parameter also controls the visibility of the video call button in My Room sessions.

```

<config version="20">
    <services>
        <calls>
            <conference>

                                <service-uri>sip:%BWNETWORK-
CONFERENCE-SIPURI-1%</service-uri> <!-- if this is empty, ad hoc conf
feature is disabled, this parameter is used for BW N-way feature in
BTBC 9.3 and 10.0 -->

```

```

                                <video-
enabled>%ENABLE_NWAY_VIDEO%/></video-enabled> <!-- enables video
conferencing in the UI -->
<call-participants>true</call-participants>
                                <max-nway-participants>
%MAY_CONF_PARTIES%/></max-nway-participants>
                                </conference>

```

The *call-participants* parameter must be set to “true” with Cisco BroadWorks.

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_NWAY_VIDEO%	false	true, false	<video-enabled>true</video-enabled>	Enables N-way video calls in the UI (requires server support). The default is “false”.

When N-way video is set to “false”, the client rejects N-way video offers from the server when received. The same also applies for 1-1 calls that are expanded to multi-party calls. For more information on combinations of configuration parameters for the Video Server, see section [10.1.31 Video Server](#).

10.1.27 Reduce Use of Call Hold in Conferencing

Release 22.7.0 added official support for a new configuration parameter that reduces the number of call hold operations done when creating an ad hoc conference session. This has helped with ad hoc conferencing issues in several deployments. See the following example. This parameter is recommended to be set to “true”.

```

<config version="20">
    <services>
        <calls>
            <conference>
                .....
                <do-not-hold-conference-before-
refers>%ENABLE_DO-NOT-HOLD-CONFERENCE-BEFORE-REFER%/></do-not-hold-
conference-before-refers>
            </conference>
        </calls>
    </services>
</config>

```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE-DO-NOT-HOLD-CONFERENCE-BEFORE-REFER%	false	true, false	<do-not-hold-conference-before-refers>true</do-not-hold-conference-before-refers>	Set to “true” to enables reduced usage of call hold in ad hoc conferencing. Set to “false” to utilize the traditional call hold behavior in ad hoc conferencing.

10.1.28 Maximum Conference Parties (N-Way Calling)

The Cisco BroadWorks system setting (*maxConferenceParties*) is used to set the maximum number of conference parties. For a given call, it indicates the number of active simultaneous parties a user can have or add through the “Add participants” mid-call control option or through the BroadWorks N-way Calling feature.

This information is retrieved from the Application Server using the following command line interface (CLI) command.

```
AS_CLI/SubscriberMgmt/Policy/CallProcessing/Conferencing> get
```

```
Example output:
maxConferenceParties = 6
conferenceURI =
```

Once the value for the *maxConferenceParties* is obtained, (which has a range of 4 through 15), the following Communicator tag should be set accordingly. Note that this feature was introduced in Cisco BroadWorks Release 20.0. This setting is not configurable for XMPP group chat.

The following example shows the parameter.

```
<config>
  <services>
    <calls>
      <conference>
        <service-
uri>sip:conf@server.domain.com</service-
uri>
        <video-enabled>true</video-
enabled> <!-- enables video conferencing in the UI -->
        <call-participants>true</call-
participants>
        <max-nway-participants>
%MAX_CONF_PARTIES%</max-nway-participants>
      </conference>
```

Tag	Default if Omitted	Supported Values	Example	Description
%MAX_CONF_PARTIES%	No client-side limit	Number between 4 and 15 (empty)	<max-nway-participants> 10</max-nway-participants>	Specifies the maximum N-way participant number, enforced by the client, for example, 10. Server side has its own limits. Empty value disables client-side enforcing of N-way participant limit.

10.1.29 My Room, N-Way, and N-Way Owner Participant List

Release 21.4.0 and later supports full participant list for the N-way owner in addition to the participants. This way, non-XMPP participants such as Public Switched Telephone Network (PSTN) callers can be shown in the list as well. The configuration depicted in this section only applies to non-Video Server (UVS) deployments, as in Video Server (UVS), the full owner participant list is done using Xsi-Events. For more information, see section [10.5.5 Xsi-Event Channel](#). Participants always get the participant list via SIP NOTIFY, controlled by the configuration depicted in this section. In My Room, the owner always gets the participant list via Xsi-Events, regardless of Meet-Me or Video Server (UVS) being used while My Room participants also get the participant list information using SIP NOTIFY and the configuration depicted in this section.

This feature is implemented using SIP SUBSCRIBE/NOTIFY and conference event package. The owner’s client learns the URI to send the SIP SUBSCRIBE to via preceding SIP Contact header of the 200 OK message sent in response to the INVITE to the conference URI while for participants the same information is in a preceding call-info NOTIFY.

Ad hoc conference calls may also have an XMPP group chat component when XMPP is enabled and the related ad hoc session XMPP JID is exchanged in SIP signaling, making XMPP mandatory for seeing ad hoc conference call participant info for other than the ad hoc session owner. However, in Release 22.9.16 and later, if the use-collaborate-style-participant-management parameter described in section [10.4.4 Connect Messaging Support](#) is set to “false” for Connect interworking, ad hoc conference calls can show participant info received over SIP even when XMPP is disabled.

This feature requires Cisco BroadWorks patches to work. For more information, see the *UC-One Solution Guide*. The following example depicts the configuration.

```

<config>
  <services>
    <calls>
      <conference>
        <service-
uri>sip:conf@server.domain.com</service-uri>
          <video-enabled>true</video-enabled> <!--
- enables video conferencing in the UI -->
          <call-participants>true</call-
participants>
          <max-nway-participants>
%MAX_CONF_PARTIES%</max-nway-participants>
          <subscribe-conference-
info>%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%</subscribe-conference-
info>
        </conference>

```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%	false	true, false	<subscribe-conference-info>true</subscribe-conference-info>	Set to “true” to enable N-way owner participant list for non-Video Server (UVS) cases. Set to “false” to disable N-way owner participant list.

10.1.30 Meet-Me Moderator Controls and Participant List

Starting with Release 20.2.0, Meet-Me Moderator Controls can be activated in the Communications window UI for My Room. Moderator Controls are also available in ad hoc multi-party sessions, but only when the Video Server (UVS) is enabled. For more information on the Video Server, see section [10.1.31 Video Server](#). Release 22.3.0 added further moderation control to My Room (moderated My Room feature) but this functionality does not come with additional configuration parameters. Instead, Communicator learns server support at login and enables moderated My Room if server support is enabled.

Cisco BroadWorks configuration and provisioning tools must be used for controlling if the bridge is terminated when the owner leaves or if the owner is required to be present when the audio session starts.

The following configuration parameter has been added to the conference-bridge node in the rooms-section.

```
<config version="20">
    <services>
        <rooms enabled="true">
            <conference-bridge autodetect="false"
type="meetme" title="MyRoom" default-bridge="meet-me@domain.com"
moderator-controls="%ENABLE_MEETME_MODERATOR_CONTROLS%" />
        </rooms>
    </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_MEETME_MODERATOR_CONTROLS%	false	true, false	moderator-controls="true"	Enables Moderator Controls in the UI. The default is "false", also if the node is omitted.

Note that the Moderator Controls only work if Xsi-Events are in permanent mode. For configuration of the Xsi-Events channel, see section [10.5.5 Xsi-Event Channel](#). Also, note that Moderator Controls have introduced two new Xsi paths in the configuration file. For more information to configure Xsi-Events, see section [10.5.1 Xtended Service Interface Basic Configuration – URL and Version](#). Meet-Me Moderator Controls are dependent on the Xsi-Events settings and scalability of the Xtended Services Platform (Xsp) can be impacted by the selection of the operation mode for Xsi-Events. Permanent mode needed for Meet-Me Moderator Controls in this release is typically the most resource consuming one for Xtended Services Platform (Xsp). For more information to configure Xsi-Events, see section [10.5.5 Xsi-Event Channel](#).

For more information on Cisco BroadWorks requirements in relation to Meet-Me Moderator Controls, see the *UC-One Solution Guide*. My Room currently requires XMPP to work fully.

Note that in Meet-Me, Video Server (UVS), and N-way conferences, participants get information about the full participants list via SIP NOTIFY using the conference event package. The prerequisite is that Communicator subscribes to this event package using a URI it receives in the *SIP Call-Info* event package NOTIFY. For this reason, a SIP SUBSCRIBE for the call-info event package is sent at login regardless of the value of the *bsoft-call-info* parameter. For more information on Cisco BroadWorks limitations on call-info subscriptions, see section [10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence](#).

For more information on enabling SIP NOTIFYs for participant lists, see section [10.1.29 My Room, N-Way, and N-Way Owner Participant List](#).

When Xsi-Events on-demand mode is used, room owner participant list is supported only when the owner dials into the room using Xsi. When Xsi-Events permanent mode is used, participant list for room owner is also supported when the owner dials into the bridge using SIP.

10.1.31 Video Server

Starting with Desktop Release 21.0.0, support for the new conferencing solution Video Server (UVS), replacing Meet-Me, was introduced. To use the Video Server, use the configuration parameter explained in this section. Note that the Video Server requires Cisco BroadWorks Release 21.0, as described in Cisco BroadWorks requirements listed in the *UC-One Solution Guide*. The Video Server has separate licenses that must be assigned for the feature to be enabled (for more information, see the *UC-One Solution Guide*). At login, the Video Server licenses are checked by the client (there is a separate license for Video Server audio and video). With My Room, some Xsi operations are also done by the owner of the room.

If the configuration file has the Video Server enabled, but there are no licenses, the client falls back to Meet-Me and N-way.

In addition, the Video Server requires XMPP (for XMPP configuration details, see section [10.3.1 Use Extensible Messaging and Presence Protocol](#)). It is recommended to use Moderator Controls, but they must be enabled separately. For more configuration details on Moderator Controls, see section [10.1.30 Meet-Me Moderator Controls and Participant List](#).

In the Video Server, the following Meet-Me-specific parameters are ignored:

- *Autodetect* – In a Video Server conference, details are provisioned outside of the client (the client only queries the Video Server for the available details). In the Video Server, the client does not create any conferences as in Meet-Me.
- *Direct-dial* – The Video Server always uses direct-dial.

The maximum participant limit for the Video Server is set on the server side. There is no configuration parameter for this or related XMPP chat room size.

Note that when using the Video Server, the following setting must always be used (these are located adjacent to the *service-uri* node) inside conference node:

- `<video-enabled>true</video-enabled>`
- `<xsi enabled="false" />` inside conference node

```
<config version="20">
  <services>
    <rooms enabled="true" >
      <conference-bridge type=" "%CONFERENCE_TYPE%"/>
    </rooms>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%CONFERENCE _TYPE %	meet-me	uvs, meet-me	<conference- bridge type ="uvs" />	When set to "uvs", the Video Server is enabled. When set to "meet-me", Meet-Me is enabled. The default is "meet-me". In addition, any other value defaults to "meet-me".

10.1.32 Team Telephony

Starting with Release 21.0.0, Team Telephony is supported. It is a lightweight implementation of the Busy Lamp Field (BLF) Cisco BroadWorks feature providing support for a subset of telephony presence states (*Available*, *Ringing*, and *Call*) for a preset list of contacts that is fetched over Xsi at login. XMPP is not required for Team Telephony. The Team Telephony window shows the predefined team members and their related call states.

Note that it is recommended to limit the team size to 15 participants to avoid issues in SIP signaling as the size of a SIP NOTIFY increases when the team size grows, which may cause fragmentation with UDP transport. Additionally, the amount of signaling grows significantly when the team size grows.

Team telephony contacts are also synchronized with Cisco BroadWorks enterprise directory over Xsi at login.

Even though the Team Telephony implementation depends on SIP, SIP calling does not necessarily have to be enabled for Team Telephony to work as Xsi calls can still be made and received. Nevertheless, SIP protocol nodes must be configured so Team Telephony notifications can be received with SIP NOTIFY (dialog event package).

Note that the client only looks at the user part of *userids* due to some solution level restrictions, so on the client side, it is not possible to have two contacts with the same user part and different domain part. For example, having joe@domain1.com and joe@domain2 in the Team Telephony list of contacts is not possible.

Regardless of SIP calling configuration, Xsi is used in this feature, mandating Xsi to be provisioned and configured correctly for Team Telephony to work.

The implementation is lightweight in that it does not offer a user interface to define monitored contacts, instead this must be done on the server side using the CommPilot portal.

The only action that a user can do for a ringing call is to pick it up. To enable this, the contacts in the monitored users list must have extensions defined and received by the client over Xsi so that calling is possible. Call pick-up depends on Cisco BroadWorks call pick-up groups to be properly configured. Similar to team definition, Communicator does not configure call pick-up on the server side, but only tries to use a Feature Access Code (FAC) when the pick-up action is issued by the user. Therefore, the necessary FACs must be provisioned on the server side.

In general, Team Telephony is enabled and configured via the BroadWorks CommPilot portal.

The Communicator user interface has been enhanced to provide a separate window for BLF contacts. The ability to pick up calls coming to the team as well as the ability to display the caller ID can be separately enabled or disabled in the configuration file.

See the *Communicator (Desktop, Mobile, iOS Tablet, and Android Tablet) Product Guide* and the *Communicator for Desktop User Guide* for more information on the feature itself and the *UC-One Solution Guide* for Cisco BroadWorks requirements.

NOTE 1: The BLF service must be assigned in Cisco BroadWorks for this configuration to have an impact in the user interface.

NOTE 2: In general, the Team Telephony contact list is not monitored after login. Any changes there only apply after logging out and logging back in.

Starting with Release 22.2.0, not having the Team Telephony service assigned on the Cisco BroadWorks side for the user automatically makes Communicator disable the configuration for the service.

Release 22.9.6 added a new sorting option to the Team Telephony window, based on server-side sorting order. For the configuration options, see the following table.

The following example shows the configuration node for this feature.

```

<config version="20">
  <services>
    <contacts>

      <busy-lamp-field
enabled="%ENABLE_BUSY_LAMP_FIELD_DESKTOP%">

        <allow-
pickup>%ENABLE_BLF_DIRECT_PICKUP_DESKTOP%/allow-pickup>

        <display-
caller>%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%/display-caller>

<utilise-server-sorting-order>%ENABLE_BLF_SERVER_SORTING_ORDER%/utilise-
server-sorting-order>%

      </busy-lamp-field>

```

The following tags, in the custom *BroadTouch_Tags* set, control this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	false	true, false	<busy-lamp-field enabled="true">	Enables Team Telephony features in the UI. When set to "false", the sub-nodes in the rest of this table are also treated as "false".
%ENABLE_BLF_DIRECT_PICKUP_DESKTOP%	false	true, false	<allow-pickup>true</allow-pickup>	Controls the ability to pick up team members' calls in the "Ringing" state. The recommended value is "true" when Team Telephony is enabled.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	false	true, false	<display-caller>true</display-caller>	Controls the availability of caller info for team members' line only when the incoming call is in the "Ringing" state. For active calls, Communicator never reveals the caller in the Team Telephony window. The recommended value is "true" when Team Telephony is enabled.
%BLF_ENABLE_SERVER_SORTING_ORDER%	false	true, false	<utilise-server-sorting-order>false</utilise-server-sorting-order>	Set to "true" to use the sorting order defined in CommPilot (server side) in Team Telephony window. Set to "false" to use the same sorting order that the contact list is using (first name or last name), as defined by the end-user settings.

In addition to the feature being enabled in DM as described in the previous table, the client must find a valid URI for <listURI> in the Xsi-Response to the following:

```
http(s)://<hostaddress:port>/com.broadsoft.xsiactions/v2.0/user/<userid>/services/busylampfield
```

before the Team Telephony window is enabled in the user interface.

The suggested settings to run Communicator as an assistant:

- opt-in TRUE

per each Executive set at least one of the following on:

- screening OR filtering

The best information for the user is provided if, under alerting, the following are configured:

- Alerting Calling Line ID Name: Originator Name
- Alerting Calling Line ID Number: Originator Number

10.1.33 Executive-Assistant

Starting with Release 21.0.0, the Executive-Assistant feature is supported. It allows an assistant to operate on behalf of an executive to screen, answer, and place calls as the "executive" (the caller ID is that of the executive). For more information about this feature, see the *Communicator (Desktop, Mobile, iOS Tablet, and Android Tablet) Product Guide* and the *Communicator for Desktop User Guide*. The service must be assigned on the Cisco BroadWorks side for this configuration to have an impact on the UI, as the server-side configuration is queried at login. The relevant roles must also be setup correctly for the feature to work. Note that the *sync-from* parameter (explained in section [10.19.2 Flexible Contact Card Field Configuration and Synchronization](#)) must be set to "xsi" when the Executive-Assistant feature is used as only the Cisco BroadWorks directory is used for the assistant to fetch the executive list and their details. Communicator does not monitor changes to provisioning changes actively. Client logout/login is required to take changed Executive-Assistant settings into use. In addition, FACs must be provisioned on the server side for this feature to work.

Starting with Release 22.2.0, not having Executive-Assistant service assigned on the Cisco BroadWorks side for the user will automatically make Communicator disable the configuration for the service.

The following example shows the configuration node for this feature.

```

    <config version="20">
      <services>
        <executive-assistant
enabled="%ENABLE_EXECUTIVE_ASSISTANT_DESKTOP%" />
  
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_EXECUTIVE_ASSISTANT_DESKTOP%	false	true, false	<executive-assistant enabled="false"/>	Enables Executive-Assistant features in the UI. The default is "false".

Note that when basic call logs are used, Cisco BroadWorks does not offer any details about calls placed on behalf of the executive. Instead, when assistant places a call on behalf of the executive, based on Cisco BroadWorks Basic Call Logs, the call appears to be from the assistant to the executive.

Cisco BroadWorks allows the assistant or executive to change the configuration of what name and number is presented in the SIP *From* header when the executive's line is ringing.

The Name can be one of the following (that is, "Eric Exec", "Eric Exec-Carol Caller", and so on):

- Executive
- Executive-Originator
- Originator-Executive
- Originator
- Custom

Independently of the previous list, the number can be:

- Executive
- Originator
- Custom

10.1.34 SIP SUBSCRIBE and REGISTER Refresh and SUBSCRIBE Retry

Communicator supports configuring the refresh intervals for SIP SUBSCRIBE and REGISTER. For SIP SUBSCRIBE, there is a separate parameter for the refresh interval (in seconds) and how long the client waits before it retries SIP SUBSCRIBE if there are errors (in seconds). The recommended maximum value for the *subscription-retry-interval* is 2000000 seconds while any negative, 0, or empty value results in 1800 seconds being used. Any negative value in for subscribe refresh leaves out the *Expires* header and thus creates a one-off SUBSCRIBE.

The SIP REGISTER refresh timer proposed by the client can be configured in seconds, but according to SIP specifications, the server can override the value. Currently, the client remembers the value proposed by the server for subsequent refreshes instead of always using the configured value.

Finally, the expires-value for SIP sessions (for SIP INVITE and SUBSCRIBE) can also be configured (in seconds). See the following example.

```
<config version="20">
    <protocols>
        <sip>
            <subscription-refresh-
interval>10800</subscription-refresh-interval>
            <subscription-retry-interval>60</subscription-
retry-interval>
            <registration-refresh-
interval>300</registration-refresh-interval> <!-- how often the client
refreshes SIP REGISTER, the server can override this value -->
        <session>
            <expires-value>3600</expires-
value> <!-- the value that goes into the SIP expires within a session -->
        </session>
    </sip>
</protocols>
</config>
```

10.1.35 Configure SIP URI or Tel URI in Outgoing Calls

Communicator supports configuring the target URI used in outgoing INVITEs in the dial pad, search, and dial field for some deployments. Either Tel URI or SIP URI can be used (parameter values tel and sip respectively). SIP is the recommended value. See the following example.

```
<config version="20">
    <services>
        <uri-handling>
            <prefer>
                <sip/><!--
possibilities are sip or tel, this applies to e.g. search and dial
field and dial pad, which URI is formed out of user input, a SIP URI or
a telURI -->
            </prefer>
        </uri-handling>
    </services>
</config>
```

Note that there is also another parameter to take the own URI from the *P-Associated-URI* in the SIP REGISTER response for outgoing SIP requests. For more information, see section [10.1.9 Use P-Associated-URIs in REGISTER](#).

10.1.36 SIP URI Validation

Communicator supports validating the user part of numeric SIP URIs provided in search and dial field as well as contacts (phone number fields only). When the SIP URI contains alphabet characters, validation is not done. This is to avoid side effects with SIP URIs that typically have alphabet characters and numbers. There is a regular expression parameter, which controls how validation is done. The default rule is `<search method="replace">[^\w+*\#]</search>`. This means remove (replace with empty string) anything which is NOT [a-zA-Z0-9_], '+', '*' and '#'.

See the following example for configuration details.

```

<config version="20">
  <services>
    <uri-handling>
      <sip-username-validation> <!-- allows to validate
SIP URIs to conform to certain rules using regexp. Is applied in the dial
and search field and contacts. -->

      <normalization>

<search method="replace">[^\w\+*\#\</search>

      </normalization>

      </sip-username-validation>

    </uri-handling

```

10.1.37 SIP UPDATE Support

Release 21.3.3 introduced support for SIP UPDATE. SIP UPDATE is needed in, for example, some IMS deployments, instead of the alternative re-INVITE. It allows a client to update parameters of a session such as the set of media streams and their codecs but has no impact on the state of a SIP dialog.

Typical use cases are related to early media when, for example, using ringback tone and pre-alert simultaneously.

SIP UPDATE is currently only supported when received in pre-dialog use cases (early media) and not during active dialog, for example, for call hold/resume where re-INVITE is still used.

It is not possible to add video to audio using SIP UPDATE (media change) in this release. Additionally, Communicator does not support full IMS long call flow with resource reservation.

A new configuration parameter is used to advertise support for SIP UPDATE in SIP signaling (as shown in the following example).

```

<config version="20">
  <protocols>
    <sip>
      <support-
update>%ENABLE_SIP_UPDATE_SUPPORT_DESKTOP%</support-update>

```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_SIP_UPDATE_SUPPORT_DESKTOP%	false	true, false	<support-update>true</support-update>	When set to "false", SIP UPDATE support is disabled. When set to "true", SIP UPDATE support is enabled.

10.1.38 Remote Control Event Package

Starting with Release 21.3.3, the Cisco BroadWorks Remote call control SIP event package is supported. It allows answering a call or putting it on hold from Receptionist or call center clients using the Communicator Desktop client. Answer and hold/resume buttons are visible in the Receptionist/Thin client to perform call management operations when this feature is enabled and when server-side provisioning and configuration has been done.

The implementation is based on SIP. Communicator places additional SIP header info into INVITE or *180 Ringing* messages: *Allow-Events: hold, talk* when this feature is enabled. This causes Cisco BroadWorks to send SIP NOTIFYs to Communicator when Receptionist/Thin client UI is used to answer/hold a call. Communicator answers the call (or resume a held call) without end user action in the Communicator UI when an unsolicited SIP NOTIFY within the SIP INVITE dialog is received, as the end user action has been performed in the Receptionist/Thin client.

There are two general options for devices to receive the remote-control notifications when, for example, the Receptionist Answer button is clicked. Either the remote-controlled device is “intelligent” and supports the remote-control event package (as Communicator Release 21.4.0 and later does) or the remote-controlled device is a “simple” end point which must be in the off-hook state (call already ongoing) for the Application Server to toggle between these two calls to the non-intelligent device.

The necessary remote-control notifications are only sent to one device.

If Communicator is one out of several SCA devices, either the Answer button on the Receptionist side would not be enabled when the primary device (non-intelligent phone) is on-hook or Communicator would not receive the necessary notifications to auto-answer the call and another intelligent device would receive the remote-control notifications.

If Communicator is provisioned as the only SCA device, things would work. However, if there are several SCA devices, the outcome of which device gets the notifications would be random.

If this feature is enabled, the recommended configuration on the Cisco BroadWorks side is to have Communicator as a primary device, as the talk-event is only allowed to one device.

```
<config version="20">
  <services>
    <calls>
      <remote-controlling
enabled="%ENABLE_REMOTE_CONTROL_EVENTS_DESKTOP%" />

```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_REMOTE_CONTROL_EVENTS_DESKTOP%	false	true, false	<remote-controlling enabled="true"/>	When set to “false”, Remote Control Event Package support is disabled. When set to “true”, Remote Control Event Package support is enabled.

10.1.39 SIP Auto-Answer

Starting with Release 21.5.0, Communicator supports the SIP call auto-answer feature. The SIP Call-Info header can contain a parameter “answer-after” indicating that the call is answered by Communicator after the indicated number of ring cycles. A value “0” designates immediate automatic answering without playing any ring tones.

There is no configurability for this feature in the DM configuration file, but it can be used in conjunction with selected Cisco BroadWorks services such as Push To Talk and Click To Dial.

10.1.40 Web Pop

Starting with Release 21.6.0, the web pop feature is supported for incoming and outgoing calls. It allows the end user to get more information about a ringing call by clicking a web button that launches a web browser to provide more information about the call. For outgoing calls only, a menu item is available. Web pop is not available in the Team Telephony window or for the assistant in the Executive-Assistant service.

The URL opened in the web browser can be configured. Additionally, the end user can override this URL in *Preferences*. The modified URL is only stored locally in the *user_settings.ini* file.

The following example shows the related parameter for enabling this feature.

```
<config version="20">
  <services>
    <web-pop
      enabled="%ENABLE_WEB_POP_DESKTOP%"
      allow-
edit="%WEB_POP_ALLOW_EDIT_DESKTOP%">%WEB_POP_URL_DESKTOP%</web-pop>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used to control enhanced call log availability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_WEB_POP_DESKTOP%	false	false, true	<web-pop enabled="true"	When set to “false”, web pop is disabled. When set to “true”, web pop is enabled.
%WEB_POP_ALLOW_EDIT_DESKTOP%	false	false, true	allow-edit="true" </web-pop>	When set to “false”, end user editing of web pop URL is disabled. When set to “true”, end user editing of web pop URL is enabled.
%WEB_POP_URL_DESKTOP%	empty	string	>http://example.com/caller?user=%(BWUserID)&caller=%(RemotePhone)</web-pop>	Configurable URL for web pop.

Web pop URL also supports variables in the same manner than in, for example, the configurable web button feature. The RemoteName variable is filled with the name that would be rendered to the user based on the first incoming SIP-request (the selection between the *From* header, *PAI*, and *Remote-party-ID* header). However, for clients running in Xsi-Only mode, the RemoteName and RemotePhone are picked from the Xsi-Event nodes <name> and <address>.

The supported tags in the URL are as follows:

- %(BWUserID) // BroadWorks User-ID
- %(FirstName) // Own First Name
- %(LastName) // Own Last Name
- %(EmailAddress) // Own email-address
- %(Group) // BroadWorks Group
- %(Phone) // Own phone number
- %(RemotePhone) // Phone number of the caller
- %(RemoteName) // Name of the remote party (if available)
- %(CallType) // “Incoming” OR “Outgoing”
- %(ServiceProvider) // NOT SUPPORTED

Example:

```
%(WEB_POP_URL_DESKTOP%=http://example.com/caller?user=%(BWUserID)&caller=%(RemotePhone)
```

would produce a config-node:

```
<web-pop enabled="true" allow-edit="true">http://example.com/caller?user=%(BWUserID)&caller=%(RemotePhone)</web-pop>
```

and the HTTP request would be sent to:

```
http://example.com/caller?user=darwin@broadsoft.com&caller=+12407200671
```

10.1.41 Auto-Show Dial Pad

Release 22.0.0 introduced a new feature where the UC-One dial pad can be configured to show automatically when a new call is made. The following options are available:

- Always – The *Main* window focus moves to dial pad. For parameter value recommendations, see section [10.20 UC-One Add-in for Microsoft Skype for Business \(S4B\)](#).
- API – Dial pad view is enabled only if the call is placed through the API or from other “non-user” sources.
- Never – The dial pad view never focuses automatically. This is the default value if nothing is defined or if the node is omitted.

The original intended use case is with S4B integration, to allow using UC-One dial pad more easily when calling PSTN numbers from S4B via UC-One. See the following example for a configuration example.

```
<config version="20">
  <services>
    <calls>
      <auto-show-dial-pad mode="%AUTO_SHOW_DIAL_PAD%" />
    </calls>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%AUTO_SHOW_DIAL_PAD%	never	always, api, never	<auto-show-dial-pad mode="always"/>	Selects the mode for auto-showing of the dial pad. See the description in the previous list.

10.1.42 SIP P-Early Media (PEM) Header

Release 22.5.3 introduced preview support for the SIP P-Early Media (PEM) header that can be used in, for example, IMS environments inside a trust domain to allow the network to authorize multiple SIP early media dialogs for instance in cases where another network allows all early media. Starting in Release 22.7.2, the feature is officially supported.

A new configuration parameter was introduced to enable advertising PEM support in SIP signaling. The actual early media handling logic is the same for both PEM and non-PEM cases, acting on supported PEM header values.

See the following for a configuration example.

```
<config version="20">
  <protocols>
    <sip>
      <support-p-early-media>%ENABLE_PEM_SUPPORT_DESKTOP%</support-p-early-media>
    </sip>
  </protocols>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_PEM_SUPPORT_DESKTOP%	false	true, false	<support-p-early-media>true</support-p-early-media>	Set to "true" to enable Communicator advertising PEM support in SIP signaling. Set to "false" to disable Communicator advertising PEM support in SIP signaling.

10.2 Real-Time Protocol

10.2.1 Real-Time Control Protocol Extended Report

Real-Time Control Protocol (RTCP) Extended Report (XR) reporting allows the client to send client-side statistics to a specified compatible server URI after a call using SIP PUBLISH. To enable RTCP XR reporting, set *audio-enabled* to “true” as shown in the following example and define the RTCP XR *service-URI* to match your reporting server deployment. RTCP XR reports for N-way calls do not include full data for the leg from the conference server towards the client, as the conference server does not support RTCP XR.

For more information on support for RTCP XR, see section [10.2.5 BroadSoft Media Engine \(from Cisco\)](#).

```
<config version="20">
    <protocols>
        <rtp>
            <call-quality-reporting audio-
enabled="%RTCP_XR_AUDIO_ENABLED%">
                <service-
uri>%RTCP_XR_SERVICE_URI%</service-uri>
<local-group>%RTCP_XR_LOCALGROUP_DESKTOP%</local-group> <!-- optional
identifier for grouping reports on the server side -->
                </call-quality-reporting>
        </rtp>
    </protocols>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set, control this capability.

Tag	Default if omitted	Value	Example	Description
%RTCP_XR_AUDIO_ENABLED%	false	true, false	<call-quality-reporting audio-enabled="true">	Enables RTCP XR reporting for audio calls. The default is “false”.
%RTCP_XR_SERVICE_URI%	empty	string	<service-uri>user@server.domain.com</service-uri>	The RTCP XR reporting server URI where the client sends the reports after a call. The default is empty.
%RTCP_XR_LOCALGROUP_DESKTOP%	empty	string	<local-group>test</local-group>	Optional identifier for grouping reports on the server side.

10.2.2 Real-Time Transport Protocol Port Range

Communicator can be configured to use a defined port range for Real-Time Transport Protocol (RTP) streams, which also applies for SRTP. This configuration is done by setting the port range limit values for both audio and video streams with the tags shown in the following example.

```
<config version="20">
    <protocols>
        <rtp>
<!-- notice the other sub-elements for RTP-tag -->
            <preferred-audio-port-start>8500</preferred-audio-port-start>
            <preferred-audio-port-end>8598</preferred-audio-port-end>
            <preferred-video-port-start>8600</preferred-video-port-start>
        </rtp>
    </protocols>
</config>
```

```
<preferred-video-port-end>8698</preferred-video-port-end>
</rtp>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used to set this port range.

Tag	Default if Omitted	Supported Values	Example	Description
%RTP_AUDIO_PORT_RANGE_START%	8500	number	<preferred-audio-port-start>8500</preferred-audio-port-start>	Start of the audio port range.
%RTP_AUDIO_PORT_RANGE_END%	8598	number	<preferred-audio-port-end>8598</preferred-audio-port-end>	End of the audio port range.
%RTP_VIDEO_PORT_RANGE_START%	8600	number	<preferred-video-port-start>8600</preferred-video-port-start>	Start of the video port range.
%RTP_VIDEO_PORT_RANGE_END%	8698	number	<preferred-video-port-end>8698</preferred-video-port-end>	End of the video port range.

NOTE: Port ranges should be set so that they never overlap.

10.2.3 Real-Time Transport Protocol Packet Maximum Transmission Unit

It is possible to specify the RTP Packet Maximum Transmission Unit (MTU) used for video packets. For audio packets, it would not be used, as typically the packets are quite small to obtain a smaller latency.

```
<config version="20">
  protocols
    <rtp>
      <mtu>%RTP_VIDEO_MTU%</mtu>
    </rtp>
  </protocols>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to select the video MTU. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%RTP_VIDEO_MTU%	Approximately 1400	Positive integer	<mtu>1200</mtu>	Select the value for video RTP packet MTU. If this is left empty, the MTU used is around 1400.

10.2.4 RTCP MUX

Starting with Release 22.2.0, using RTCP MUX is configurable. This feature makes Communicator use the same port for RTP and RTCP. In SIP/SDP signaling level, the line `a=rtcp-mux` is added to the SDP generated by Communicator. In addition, different modes are possible:

- Backward-compatibility mode (that is, line `a=rtcp-mux` does not appear in SDP)
- Multiplexing mode (the `a=rtcp-mux` line will appear twice in the SDP: once in the `m=audio` section, and a second time in the `m=video` section)

Video and audio do not use the same port in this release. See the following example.

```

<config version="20">
  protocols
    <rtp>
      <mux enabled="%ENABLE_RTC_P_MUX%"/>

```

Note that RTCP MUX cannot be used with SRTP calls.

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to select the video MTU. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
<code>%ENABLE_RTC_P_MUX%</code>	true	true, false	<code><mux enabled="true"/></code> <code>></code>	To enable RTPC MUX, set to "true". To disable RTCP MUX, set to "false".

10.2.5 BroadSoft Media Engine (from Cisco)

Starting with Release 21.0.0, Communicator comes with a different default media framework called the BroadSoft Media Engine (BME). Note that in this release, the BME does not support CPULC. In addition, the list of codecs is different. In general, the ARS and CPULC configuration parameters used previously are ignored with BME; however, the default bit rate configuration parameter (as explained in section 11 [Video Optimization](#)) is used in the BME as the maximum bit rate for a session unless BME DVBA is used. For more information on DVBA, see section 10.2.6 [Dynamic Video Bit Rate Adaptation](#).

RTCP must be used for video to work fully.

It is possible to continue using the previous media framework via configuration that has these features (as shown in the following example).

```

<config version="20">
  <services>
    <calls>
      <media-handler>%MEDIA_HANDLER%</media-handler>

```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to select the media framework. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%MEDIA_HANDLER %	bme	bme, spirit	<media-handler>bme</media-handler	Only BME media framework is supported in this release. The recommended value is “bme”.

The following table provides some general parameters about the BME.

Function	BME
Audio codecs	<ul style="list-style-type: none"> ▪ G.711 aLaw and uLaw ▪ G.729ab ▪ G.722 64kbit/sec ▪ Opus 48 kHz
Audio algorithms	<ul style="list-style-type: none"> ▪ Packet loss concealment ▪ Noise reduction ▪ Echo cancellation ▪ Adaptive jitter buffer ▪ Automatic gain control ▪ Comfort noise generation ▪ Voice activity detection ▪ Keyboard clicks suppression
Video codec	<ul style="list-style-type: none"> ▪ H.264 Baseline constrained profile (packetization mode 1 and 0)
Video resolutions	<ul style="list-style-type: none"> ▪ SQCIF ▪ QCIF ▪ CIF ▪ VGA ▪ 4CIF ▪ HD720p
Video algorithm	Dynamic Video Bit Rate Adaptation (DVBA).
Video frame rate	Up to 30 fps, depending on available bandwidth and CPU.
Transport	RTP, SRTP
DTMF transport	Out-of-band (<i>RFC 4733</i>)
Quality measurement	RTCP XR

Both SIP INFO and RTCP FB can be used to request video key frames, but RTCP FB is the default, with fallback to SIP INFO if RTCP FB is not supported on the other end point. This is discovered using SDP signaling at call setup. However, if both end points (clients) support RTCP FB, there is no fallback to SIP INFO within the call.

10.2.6 Dynamic Video Bit Rate Adaptation

Starting with Release 21.2.0, Dynamic Video Bit Rate Adaptation (DVBA) is supported with the BME for the H.264 codec. It is adapting video bit rate in adverse network conditions to improve video quality. When packet loss is detected via RTCP, BME reduces its video bit rate by lowering the frame rate and/or switching to lower video resolution. In this release, resolution is not increased once it has been decreased. Standard RTCP signaling is used. Lowering the frame rate is only performed to reduce the CPU load.

A new configuration node has been defined on Desktop to enable the feature with minimum, maximum, and default bit rates. Outgoing/encoded video starts with default bit rate and varies between minimum and maximum bit rates.

DVBA configuration works in conjunction with video profile configuration described in section [11.3 Video Bit Rate Selection](#) based on following logic:

- Although in SDP both video directions are negotiated separately, both sending and receiving video ends up using the same maximum bit rate settings. In practice, this means that the lower maximum bit rate of sending and receiving video is used for both directions.
- The SDP bandwidth parameter indicates to the remote party the maximum bit rate that the client can receive. The SDP bandwidth parameter *valueRFC* is always set to the selected profile maximum bit rate value. The Preferences-video tab can be used to select a video size and take into use the bit rate configuration settings for that video size.
- Maximum bit rate is the lower value of DVBA maximum bit rate and selected profile maximum bit rate.
- Default bit rate is the lower value of DVBA default bit rate and selected profile default bit rate.
- Minimum bit rate is the lower value of DVBA minimum bit rate and selected profile minimum bit rate.

See the following example and table for DVBA configuration.

```

<config version="20">
  <services>
    <video>
      <profiles>
        <dvb enabled="%ENABLE_DVBA%" min-bitrate="100" default-
bitrate="1024" max-bitrate="2048" />
      </profiles>
    </video>
  </services>
</config>

```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to enable DVBA.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_DVBA %	false	true, false	dvba enabled="true"	Set to "true" to enable DVBA. Set to "false" to disable DVBA.

10.2.7 Comfort Noise (CN) for Early Media

For IMS deployments, in particular firewall/NAT pinholes, there has been a need to open pinholes for media and keep them open as per 3GPP TS 24.229. To keep NAT bindings and firewall pinholes open with unidirectional RTP traffic and enable the C-BGF to perform address latching, Release 22.9.2 introduced a feature to send keep alive messages for each media stream for audio. These messages are sent regardless of the media stream being currently inactive, send only, recvonly, or sendrecv. The keepalive message is a comfort noise RTP packet. There are some codec-specific aspects:

- For G729, it is required to have vad=true and also annex=yes in the remote SDP to enable CN in addition to configuration.

- For other codecs, it is only required to use `vad=true` to enable CN in addition to configuration.
- For G711 and G722, CN is generated by BME with a CN payload type.
- For G711 (8kHz), the default payload type for 8kHz is used (13) and it is not configurable.

See the following example and table for comfort noise (CN) configuration for the following use cases:

- 1) When a call is on hold, the client will continue to send CN with the microphone muted. Upon resume, the microphone is unmuted and regular audio RTP is sent.
- 2) When there is PEM inactive during negotiation, the client will start sending CN with the microphone muted as long as the codec is already negotiated.

To enable sending CN, it is required to set `vad="true"` for all codecs.

```

<config version="20">
  <services>
    <calls>
      <audio>
        <send-on-inactive enabled="%ENABLE_SEND_ON_INACTIVE%">

```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to enable sending CN.

Tag	Default if Omitted	Supported Values	Example	Description
<code>%ENABLE_SEND_ON_INACTIVE%</code>	false	true, false	<code><send-on-inactive enabled="true"></code>	Set to "true" to enable CN for use cases 1 and 2. Set to "false" to disable CN for use cases 1 and 2.

10.3 Extensible Messaging and Presence Protocol

10.3.1 Use Extensible Messaging and Presence Protocol

The Extensible Messaging and Presence Protocol (XMPP) is turned on for chat (however, voice and video still use SIP) and presence in the main configuration file in the *protocols* section. There are also several more fine-grained configuration parameters for XMPP as shown in the following example file. The XMPP usernames (JID) are expected to be in lowercase and Communicator tries to perform normalization when it finds uppercase letters in a JID.

Communicator expects the time stamps in the received server updates to be in Greenwich Mean Time (GMT). This functionality is hard-coded to avoid complex error situations.

Example File

```

<config version="20">
  <protocols>
    <xmpp enabled="true">
      <domain srv-enabled="true" use-for-ssl-verification="true" use-as-backup-record="true">domain.com</domain>
      <credentials>
        <username>johndoe@domain.com</username>

```

```

                                <password>123abcpassword>
                                </credentials>
                                <domain srv
enabled="true">domain.im</domain>
                                <
                                <use-ssl>true</use-ssl>
<xmpp/>

```

NOTE: Communicator uses operating system primitives for DNS operations and typically, DNS responses are cached, honoring the Time to Live (TTL) of the DNS response with XMPP when configured. Not all protocols support DNS TTL. See the SIP and XMPP sections for DNS TTL support. There is also a new feature described in section [10.7.1 DNS TTL Management](#) for DNS TTL handling.

The following DM tags are supported.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_XMPP %	false	true, false	<xmpp enabled="true">	When set to "true", enables XMPP used for presence, chat, and file transfer. When set to "false", disables XMPP. For more information on configuring packages, see section 10.15 Communicator Packages and Device Management .
%BW_USER_IMP_ID-1%	empty	string	<username>johndoe</username>	Typically, the XMPP userid.
%BW_USER_IMP_PWD-1%	empty	string	<password>123abc</password>	Typically, the XMPP password.
%XMPP_SRV_ENABLED%	false	true, false	<domain srv-enabled="true"	When set to "true", enables XMPP usage of DNS SRV. When set to "false", disables XMPP usage of DNS SRV.
%USE_FOR_SSL_VERIFICATION %	false	true, false	use-for-ssl-verification="true"	When set to "true", TLS certificate verification is based on XMPP domain parameter. When set to "false", TLS certificate verification is done based on the domain part of the XMPP userid.

Tag	Default if Omitted	Supported Values	Example	Description
%USE_AS_BACKUP_RECORD%	true	true, false	use-as-backup-record="true"	Set to set to "true" to use the value of the domain parameter as a fallback (last resort) of finding a working XMPP server when SRV records have not yielded into a working server. Set to "false" to disable this fallback. When disabled, no A-query is made to the value of the domain parameter and no XMPP connection is attempted to the value of the domain parameter.
%BW_IMP_SERVER_NET_ADDRESS-1%	empty	string	<domain.com</domain>	XMPP server domain. Cannot be the same as the guest client domain. Depending on the previous configuration parameter, is also the domain used for SSL certificate verification in XMPP. For more information on XMPP certificates, see section 10.16.8 XMPP SRV Support and Certificate Validation .
%XMPP_SSL_ENABLED%	false	false, true	<use-ssl>true</use-ssl>	SSL not used for XMPP traffic. SSL used for XMPP traffic. The default is "true".

10.3.2 XMPP Service Discovery

The Communicator Desktop client supports the Service Locator (SRV) DNS query to find the XMPP server.

Communicator finds the right XMPP server based on DNS SRV and A-queries using the following steps:

- 1) Take the value of the XMPP domain parameter from the configuration file and resolve it using SRV (<domain srv enabled="true" use-for-ssl-verification="">domain.im</domain>).
- 2) Resolve all the items received using DNS A-queries.
- 3) When many items are received, they are ordered based on SRV priority. To create this ordering, SRV priority is used first. For items with equal priority, weight is looked at to determine the likelihood in which a certain server is tried first. When SRV results in several items with equal transport protocol, priority, and weight, any one received is selected at random.

When the domain is defined as an IP address, the client performs “TCP SYN” directly to the defined address. In the following configuration example, A-query for “domain.im” would be done: SRV _xmpp-client._tcp.domain.im. The *use-for-ssl-verification* attribute that can be used to control whether the value of the domain parameter or the domain part of the end user’s JID is used for certificate validation (added in Release 20.0.1) for this configuration node, is described in more detail in section [10.16.8 XMPP SRV Support and Certificate Validation](#).

```
<config version="20">
  <protocols>
    <xmpp enabled="true">
      <credentials>
        <username>johndoe@company.com</username>
        <password>mypassword1</password>
      </credentials>
      <domain srv-enabled="true">domain.im</domain>
    </xmpp>
  </protocols>
</config>
```

If the domain is omitted, the client performs an SRV-record query using the domain part of the defined XMPP username (SRV xmpp-client._tcp.domain2.com). The configuration for this is shown in the following example.

```
<config version="20">
  <protocols>
    <xmpp enabled="true">
      <credentials>
        <username>johndoe@domain2.com</username>
        <password>mypassword1</password>
      </credentials>
    </xmpp>
  </protocols>
</config>
```

If SRV queries do not result in finding a working XMPP server, the configured domain is used as a fallback. DNS A-query is done for the value of the domain parameter and XMPP connection setup is done to the resulting IP address.

Release 21.4.0 introduced a new attribute for the XMPP domain “use-as-backup-record”, which can be used to turn off this fallback option. This was since some XMPP domains do not resolve into working XMPP servers; therefore, the benefit of not using the domain fallback address is saving one unnecessary A-query for the domain and resulting XMPP connection setup towards the IP address of the XMPP domain.

The default value for this parameter is “true” and it only has effect if "srv-enabled" = true.

NOTE: Communicator uses operating system primitives for DNS operations and typically, DNS responses are cached, honoring the TTL of the DNS response with XMPP when configured. Not all protocols support DNS TTL. See the SIP and Xsi sections for DNS TTL support. There is also a new feature described in section [10.7.1 DNS TTL Management](#) for DNS TTL handling.

10.3.3 XMPP Failover

XMPP failover is also supported in this release. Following BroadCloud procedures, more than one XMPP server is needed.

XMPP failover process is as follows:

- 1) XMPP server discovery: Communicator resolves the XMPP server URL, typically using both DNS SRV and A-query lookups and receives multiple IP addresses. For more details on DNS operations and XMPP server discovery, see the preceding section.
- 2) Communicator starts using the received IP addresses in priority order and chooses the first one that works. When a failure is detected, Communicator goes back to step 1 XMPP server discovery. However, if an XMPP server connection failed while the network interface remains up, it is tried last even if it comes back as the top priority server from DNS in XMPP server discovery. The placement of the primary server to the end of the list is effective for one proxy discovery process, hence, in the next discovery process, the top priority server will again be the first to be used. For example, if the DNS TTL feature is used, the top priority server will again be used after the next DNS TTL expiry of the secondary server.

If all IP addresses fail, then Communicator displays a UI error for XMPP connectivity as per the current implementation. After network connectivity loss or a working XMPP server stops responding or TCP connection dies, the XMPP discovery is done again and Communicator starts trying the servers in priority order.

If server1 is not responding but the TCP connection remains up, XMPP ping is used to detect server failure. This should complete in 10 to 15 seconds. A configurable exponential backoff timer was introduced in Release 3.9.0/22.9.2 and only applies if UC-One loses its XMPP connection but the network in general remains up. It is intended to avoid a DOS situation when all clients try to reconnect to the server:

- A new timer parameter defines the retry delay in seconds, which is denoted as T in the following sub-list.
- When retrying to connect, UC-One wait time increases according to the Fibonacci series as follows:
 - 1 * T
 - 1 * T
 - 2 * T
 - 3 * T
 - 5 * T
 - 8 * T
 - 13 * T
 - 21 * T
 - 21 * T
 - ...
- Note that the delay does not grow beyond 21 times the unit delay.

- In addition to the increasing delay, a random factor is applied to prevent spikes of clients attempting to reconnect at the same time. This is implemented by drawing a random number from a uniform distribution between 0.3 and 1.7 and multiplying the delay by that number. A new random number should be drawn on each round.

For example, on round four, if T is 10 seconds, the expected delay time is 30 seconds (3 * T), but the actual wait time can vary between 9 seconds and 51 seconds, after applying the random factor.

If the configuration file has a domain but only a partial username, then the client assumes that the domain part of the username is the same as the domain. If the configuration has a full username but no domain, then the client uses the domain part of the username for the SRV-query and as the default (A-record) in case the SRV-query fails or is disabled.

The failover logic relies on the configuration parameters that are found in the existing configuration file. No new configuration parameters have been added for XMPP failover.

XMPP SRV support has been enhanced so that it can be enabled regardless of the domain. For more information, see section [10.16.8 XMPP SRV Support and Certificate Validation](#).

When a Multi-User Chat (MUC) server in an MUC cluster fails, all chat rooms are unavailable until they are re-created on another MUC server; however, persistent rooms are available for both servers. Communicator clients that are connected to an MUC (owner or participant) do not see a problem until they try to send a message to the MUC. When they do, they receive an error message and they automatically join the room again.

Failback is not supported in this release.

Starting in Release 22.9.12, the XMPP exponential backoff timer also applies to HTTP Messaging as XMPP reconnect also happens when the network connectivity is regained. No new parameters were added.

The following is an example configuration of the exponential backoff timer.

```
<config version="20">
  <protocols>
    <xmpp>
      <connection-retry-
timer>%CONNECTION_RETRY_PARAMETER_DESKTOP%</connection-retry-timer>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to control chat for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%CONNECTION_RETRY_PARAMETER_DESKTOP%	10	Positive integer (seconds)	<connection-retry-timer>15</connection-retry-timer>	Set the starting value for the exponential backoff timer. See the previous section for details.

10.3.4 Publish Location

Communicator Release 10.0.0 and higher allows the client to discover and publish the user's location and time zone information. This functionality no longer depends on the Web Collaboration feature and it can be configured separately with the following *XML-nodes* under *<services>*. If *webcollab* is not enabled, then the URL for location still needs to be provided using the collaboration configuration node. The URL used to retrieve the location is composed by using the *urlSubdomain* and *urlBaseDomain* parameters. By default, a BroadCloud server is always used for this. For more information, see section 10.6.1 [Desktop Sharing \(Sharing Server and Web Collaboration\)](#).

```
<config version="20">
  <services>
    <location enabled="%ENABLE_LOCATION%" />
  </services>
</config>
```

The tag identified in the following table is used to enable this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_LOCATION%	false	false, true	<location enabled="true"/>	When set to "false", Location is disabled. When set to "true", Location is enabled.

Location depends on XMPP; therefore, to use it, XMPP must be enabled.

10.3.5 File Transfer

Starting with Release 9.3.1, configuration of file sharing can be enabled. The high-level option is *<media-share>* *XML-element*, which then separates into sublevel options, where file transfer can be configured on (set to "true") or off (set to "false"). The following example has file transfer capability defined. To enable file transfer, both %ENABLE_MEDIA_SHARE% and %ENABLE_FILE_TRANSFER% must be set to "true".

Size limits for transfers can be defined with *XML-element* values set for *<maximum-out-size>* and *<maximum-in-size>*. The related DM tags are called %FT_MAX_OUT% and %FT_MAX_IN%. If variable values are set to "0", then there are no limitations for file sizes.

Release 20.0.0 added support for file transfer encryption using a new parameter shown in the following example. File transfer encryption algorithms or keys cannot be configured.

```
<config version="20">
  <services>
    <media-share enabled="%ENABLE_MEDIA_SHARE%" <!--true/false-->
      <file-transfer enabled="%ENABLE_FILE_TRANSFER%" encryption-
        required="%FT_REQUIRE_ENCRYPTION%">
        <maximum-out-size>%FT_MAX_OUT%</maximum-out-size>
        <maximum-in-size>%FT_MAX_IN%</maximum-in-size>
        <protocol>xmpp</protocol> <!-- xmpp/msrp/http -->
      </file-transfer>
    </media-share>
  </services>
</config>
```

For information on the Device Management tags, see the following table.

Tag		File Transfer
%ENABLE_MEDIA_SHARE%	%ENABLE_FILE_TRANSFER%	
Value		
false	*	Deactivated
true	false	Deactivated
true	true	Activated

There is no strict requirement imposed by the client for the maximum size limitation on the solution level. Any value can be used from client perspective; however, the recommended maximum value is currently 50 Mbytes. Note that there is an impact to stream host scalability in the Messaging Server (UMS) when sending very large files. XEP-0065 (SOCKS5 byte stream negotiation), and XEP-0096 (SI file transfer) are used for file transfer. To setup the file transfer connection, the sending Communicator uses the standard XEP-0096 SI FileTransfer offer that includes details about the file. It also includes an indication that secure-transport is possible in Release 20.0.0 and onwards.

Additionally, encryption for file transfer can be specified. In that case, the connection remains a plain TCP connection between each Communicator leg and the stream host (server) in the Messaging Server. Other XMPP traffic uses a separate connection so that a large file transfer would not block other XMPP traffic.

With encryption, the used algorithm is AES-CFB with no padding. A new key is generated for every accepted transfer and keys are never re-used or stored. The key is a random string with the length of 192 bits.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_MEDIA_SHARE%	false	true, false	<media-share enabled="true">	See the previous table for different combinations of %ENABLE_MEDIA_SHARE% and %ENABLE_FILE_TRANSFER% tags.
%ENABLE_FILE_TRANSFER%	false	true, false	<file-transfer enabled="true"	See the previous table for different combinations of %ENABLE_MEDIA_SHARE% and %ENABLE_FILE_TRANSFER% tags.
%FT_MAX_IN%	0	From 1 to 2147483648 bytes	<maximum-in-size>0</maximum-in-size>	0=no limits.
%FT_MAX_OUT%	0	From 1 to 2147483648 bytes	<maximum-out-size>0</maximum-out-size>	0=no limits.
%FT_REQUIRE_ENCRYPTION%	false	true, false	encryption-required="true"	When set to "true", file transfer encryption is enabled. When set to "false", file transfer encryption is disabled.

10.3.6 Chat

In order to enable chat in Communicator, XMPP must be enabled. In addition, the chat feature must be enabled separately. Offline notification in the *Communications* window can be enabled when the remote party is offline. The chat type must always be set to “im” in this release. For enabling group chat, see the next section. See the following example for configuration details.

```
<config version="20">
  <services>
    <chat enabled="%ENABLE_CHAT%"> <!--true/false to enable chat-->

                                <type>im</type> <!-- conversation/im/sms, in BC
only type IM is supported -->

                                <offline-message-indication>false</offline-
message-indication> <!-- Shows info in chat window when sending message
to offline user or receiving messages from one -->
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used to control chat for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_CHAT%	false	false, true	<chat enabled="true">	When set to “false”, chat is disabled. When set to “true”, chat is enabled.
%ENABLE_OFFLINE_I NDICATION%	false	false, true	<offline-message- indication>false</ offline-message- indication>	When set to “false”, offline indication is disabled. When set to “true”, offline indication is enabled.

10.3.7 Group Chat

In order to enable group chat in Communicator, XMPP must be enabled. In addition, starting with Release 21.6.0, the group chat feature must be enabled separately. When disabled, incoming group chat invitations are silently discarded. See the following example.

```
<config version="20">
  <services>
    <chat enabled="true"> <!--true/false to enable chat-->
                                <groupchat enabled="%ENABLE_GROUP_CHAT%">
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to control group chat for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_GROUP_ CHAT%	true	false, true	<groupchat enabled="true">	When set to “false”, group chat is disabled. When set to “true”, group chat is enabled.

10.3.8 Presence and Automated Presence

Presence can be enabled using a configuration parameter. XMPP must be enabled for Presence to work. Release 22.5.0 added support for automated presence (no-sub) where XMPP presence subscriptions are automatically accepted by the Messaging Server (UMS), when enabled on the server side for the domain. There is no client-side configurability for this, instead Communicator detects support for no-sub at login and acts accordingly. For more information on end user functionality impacts, see the *UC-One Desktop User Guide*. For configuration and provisioning impacts, see the *UC-One Solution Guide*.

See the following example.

```
<config version="20">
  <services>
    <presence enabled="%ENABLE_PRESENCE%" <!--true/false-->

      <xmpp/>

      <!--only supported value xmpp-->

      <subscription>

        <bsoft-call-info enabled="true">
        </bsoft-call-info>

      </subscription>

    </presence>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to control Presence for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_PRESENC E%	false	false, true	<presence enabled="true">	When set to "false", presence is disabled. When set to "true", presence is enabled.

See the following sections for related items:

- Telephony presence in section [10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence](#).
- Idle detection in section [10.3.10 Idle Detection](#).

10.3.9 Offline Presence Control

Release 22.9.16 introduced a new feature to control the availability of offline presence in presence menus to cater for situations where the mobile Connect client is also in use, not offering the same capability.

See the following example.

```
<config version="20">
  <services>
    <presence enabled="%ENABLE_PRESENCE%" <!--true/false-->
  </services>
</config>
```

```
<manual-offline-set enabled="%DISABLE_OFFLINE_PRESENCE%">
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to control Presence for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%DISABLE_OFFLINE_PRESENCE%	false	false, true	<manual-offline-set enabled="true">	When set to "false", using offline presence is disabled. When set to "true", using offline presence is enabled.

10.3.10 Idle Detection

Communicator supports idle detection in presence. After a configurable period of inactivity, presence is set to the *Away* status. Keyboard presses and mouse movement count as activity. Only the *Away* status is supported. The feature works in the same way on both OS X and Windows. See the following example.

```
<config version="20">
  <services>
    <idle-detection enabled="true"> <!-- used to enable automatic
    presence update when the keyboard or mouse has not been touched for a
    configurable period of time -->

        <timeout-minutes>5</timeout-minutes>

        <presence-away>true</presence-away> <!-- set
    presence to away when idle -->

    </idle-detection>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used to control idle detection for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_IDLE_DETECTION%	empty	false, true	<idle-detection enabled="true">	When set to "false", idle detection is disabled. When set to "true", idle detection is enabled. If the node is empty, then the whole feature is disabled.
%IDLE_DETECTION_TIMEOUT%	empty	Integer larger than 0	<timeout-minutes>5</timeout-minutes>	Idle timeout in minutes for triggering presence change. If the node is empty, then the whole feature is disabled.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_PRESENCE_AWAY%	empty	false, true	<presence-away>true</presence-away>	When set to "false", presence is not set to <i>Away</i> (as the <i>Away</i> status is currently the only supported status). When set to "true", setting presence to <i>Away</i> is enabled when idle. If the node is empty, then the whole feature is disabled.

10.3.11 Presence Rules

Starting with Release 21.2.0, Cisco BroadWorks Call Processing features can be combined with presence states. The following rules can be created:

- Silent alerting
- Call Forwarding to number
- No rules

All of these Call Processing elements can be combined with any presence state so that, for instance, when setting presence to "Busy", calls would be forwarded to a mobile number. This feature depends on XMPP, as custom presence states are sent to the Messaging Server (UMS), which communicates with Cisco BroadWorks to enable or disable Call Processing features. Therefore, XMPP must be provisioned. For more information on basic XMPP configuration, see section [10.3.1 Use Extensible Messaging and Presence Protocol](#).

Both Mobile and Desktop must have presence rules on in order to avoid side effects. For Messaging Server (UMS) patch requirements, see the *UC-One Solution Guide*.

The following example describes the configuration of this feature.

```
<config version="20">
  <services>
    <presence-rules enabled="%ENABLE_PRESENCE_RULES_DESKTOP%"/>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to control presence rules for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_PRESENCE_RULES_DESKTOP%	false	false, true	<presence-rules enabled="true"/>	When set to "false", presence rules are disabled. When set to "true", presence rules are enabled.

10.3.12 Presence on Demand

Starting with Release 21.3.0, Presence on Demand (PoD) provides a snapshot of presence status for contacts that are not permanently subscribed and added to user's contact list within the XMPP domain. The Presence on Demand data is primarily used for search results to offer approximate idea if searched contact is available for communication at the time the search was conducted. In communication sessions and history, should the client notice contacts that are not subscribed as part of a contact list, then the client also uses Presence on Demand to retrieve presence information.

The Messaging Server (UMS) must also support this feature to have a working solution. For server version requirements, see the *UC-One Solution Guide*.

For more information on limitations regarding Presence on Demand with full enterprise directory, see section [10.5.11 Enterprise Directory Listing](#). There are no significant client-side performance implications, but the limit is there to manage the Messaging Server (UMS) load. The limit is applied to the combined list of contacts from search results as well as history and communications sessions. Release 22.9.18 introduced a new configuration parameter for the maximum number of PoD requests for all use cases, such as full enterprise directory and search.

The following example describes the configuration of this feature.

```
<config version="20">
  <services>
    <presence-on-demand enabled="%ENABLE_PRESENCE_ON_DEMAND_DESKTOP %">
      <poll-interval
seconds="%PRESENCE_ON_DEMAND_POLL_INTERVAL_DESKTOP %" /> <!--interval
in seconds-->
      <maximum-limit>%PRESENCE_ON_DEMAND_MAXIMUM_LIMIT%</maximum-limit>
    </presence-on-demand>
  </services>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), are used to control Presence on Demand.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_PRESENCE_ON_DEMAND_DESKTOP%	false	false, true	<presence-on-demand enabled="true" />	When set to "false", Presence on Demand is disabled. When set to "true", Presence on Demand is enabled.
%PRESENCE_ON_DEMAND_POLL_INTERVAL_DESKTOP%	300	Positive integer larger than or equal to 60	<poll-interval seconds="300" />	Defines how often presence is polled as the server does not send it automatically. The recommended value is "300". When set to less than 60 seconds, the client defaults to 60-second intervals.
%PRESENCE_ON_DEMAND_MAXIMUM_LIMIT%	100	Positive integer	<maximum-limit>90</maximum-limit>	Defines the maximum number of contacts PoD will be fetched for in, for example, search and full directory.

10.3.13 vCard Download Options

Starting with Release 22.4.2, additional options are available for controlling how fast vCards are downloaded at login. These options are intended to help deployments control the load towards Messaging Servers in a way that is most suitable for the particular deployment.

The first parameter defines how many vCards are downloaded in one request and the second defines the time interval between these requests when the server answers to the previous request.

As a fallback, if there is no answer from the server to a vCard request, UC-One Communicator waits for 36 seconds (hard-coded value) before starting the timeout for the next vCard request, and there are no retries for vCard requests at login until the presence status changes for the contact whose vCard download failed. At that point, the vCard is downloaded again. In general, when a contact comes online (presence changes from offline to an online status), its vCard is downloaded if it is missing or if the four-hour vCard timer after login has expired. UC-One Communicator employs a cache for vCards it downloads at login.

When one or both of these new parameters omits, UC-One Communicator defaults to pre-Release 22.4.2 behavior where the vCard batches are not used and all vCards are fetched one by one at login in one stream and the timeout for vCard cache validity is 4 hours. vCard cache is valid only within a login session and is not stored at logout. Currently at login, UC-One typically fetches all vCards since the timeout for the cache is 4 hours and does not persist across logins.

Release 22.5.3 added one more configuration parameter to get a configurable maximum download time for a batch as an additional fallback mechanism. See the following table for details.

The Presence on Demand (PoD) feature automatically fetches vCards for the contacts whose presence is queried in for example directory searches. At login, vCard requests initiate by PoD obey the parameters specified in this section, but after login when, for example, making a directory search, the vCard requests initiated by the PoD feature do not. For more information about PoD, see section [10.3.12 Presence on Demand](#).

The following example describes the configuration of this feature.

```
<config version="20">
  <protocols>
    ...
    <xmpp>
      ...
      <vcard>
        <batch-size>%VCARD-BATCH-SIZE%/batch-size>
        <batch-timeout>%VCARD-BATCH-TIMEOUT%<batch-timeout>
        <batch-failed-timeout-per-item>%VCARD-BATCH-FAIL-
TIMEOUT%/batch-failed-timeout-per-item>
      </vcard>
    
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used to control vCard download options.

Tag	Default if Omitted	Supported Values	Example	Description
%VCARD-BATCH-SIZE%	0	Positive integer	<batch-size>5</batch-size>	When empty, vCard download control is disabled and vCards are downloaded as before in one go. When set to a positive integer, defines how many vCards are downloaded in one request.
%VCARD-BATCH-TIMEOUT%	0	Positive integer	<batch-timeout>10</batch-timeout>	When empty, vCard download control is disabled and vCards are downloaded as before in one go. When set to a positive integer, defines how many seconds UC-One Communicator waits between vCard download requests.
%VCARD-BATCH-FAILED-TIMEOUT%	45	Positive integer	batch-failed-timeout-per-item>45</batch-failed-timeout-per-item>	Defines a timer for downloading a batch of vCards. This timer is multiplied with the number of vCards in the batch to get the maximum download time for the batch. After the maximum download time for the batch has elapsed, Communicator moves to the next batch and no longer waits for results from the vCards of the previous batch.

10.4 Messaging HTTP API

10.4.1 Messaging HTTP API Service Discovery

Communicator finds the right HTTP Messaging Server based on DNS SRV and A-queries using the following steps:

- 1) Take the value of the *messaging-HTTP-host* parameter from configuration file and resolve using DNS SRV (<messaging-http-host srv-svc-name="gateway-client" address="server.domain.com" enable-sync="true">).
- 2) Resolve all the items received using DNS A-queries. If SRV provides no results, the UMS server address is resolved with DNS A-query as a fallback solution.

- 3) When many items are received, they are ordered based on SRV priority. To create this ordering, SRV priority is used first. For items with equal priority, weight is looked at to determine the likelihood in which a certain server is tried first. When SRV results in several items with equal transport protocol, priority, and weight, any one received is selected at random.

10.4.2 Message History and Badge Sync

Starting with Release 21.4.0, a server-based message history feature is fully supported. All sent and received have also been stored locally in the Chat History before, but the message history feature provides multi-device enhancements. It allows the client to fetch Chat History from the Messaging Server (UMS) over HTTP to offer an improved user experience in multi-device environments so that messages typed in one device are also visible in others.

Chat History is only fetched when any of the following conditions is met:

- XMPP connects / reconnects. Starting in Release 22.9.12 XMPP reconnection exponential backoff timer also applies to HTTP messaging. For more information on the XMPP exponential backoff timer, see section [10.3.3 XMPP Failover](#).
- User's own presence state changes from offline to any other state.
- XMPP presence idle detection triggers presence change to a non-idle state.
- New chat tab is opened.

The Messaging Server (UMS) must also support this feature to have a working solution. Badge sync requires the push notification (mobile) related patches on solution level. For patch information and server version requirements, see the *UC-One Solution Guide*.

To reduce the bandwidth usage, Communicator stores the last-used timestamp that triggered message history retrieval onto the server and uses that delimiter when fetching message history the next time. This reduces the number of messages returned and prevents the client from fetching identical messages several times. A specific message ID is used to support detection of duplicate messages, regardless of whether this feature is enabled or not.

Older versions of Communicator clients are sending messages without unique message IDs. It is assumed that these messages are not included in the message history or, if these messages are delivered as part of the messages, the client may render some messages several times in chat windows.

For this operation, Communicator assumes that the server operates in GMT, and thus based on the local clock, calculates the timestamp in GMT prior to sending a message history retrieval request. However, upon first login of a client version or after the feature has been enabled, the client fetches the whole IM history.

The same configuration node is also used to sync unread chat message badges in the UI using a different HTTP API. Communicator sends unread message info to the server for distribution to other client devices and retrieves unread message information from the Messaging Server (UMS).

Release 22.5.0 added Chat History synchronization with configured sources. For more information on synchronization sources, see section [10.19.2 Flexible Contact Card Field Configuration and Synchronization](#).

See the following example for message history configuration.

```
<config version="20">
  <services>
    <chat enabled="true">
      <type>im</type>
      <offline-message-indication>>false</offline-message-indication>
      <is-composing>
        <chat enabled="true" />
      <groupchat enabled="true" />
    </is-composing>
    <prevent-clicking-links></prevent-clicking-links>
  </services>
  <messaging-http-host>
    srv-svc-name="%UMS_HTTP_SRV_SERVICE_NAME_DESKTOP%"
    address="%UMS_SRV_ADDRESS_DESKTOP%"
    enable-sync="%ENABLE_MESSAGE_SYNC_DESKTOP%">
    <use-ssl>%UMS_USE_SSL%</use-ssl>
    <fetch-path>%MESSAGE_SYNC_FETCH_PATH_DESKTOP%</fetch-path>
    <post-path>%MESSAGE_SYNC_POST_PATH_DESKTOP%</post-path>
  </messaging-http-host>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used to control message history.

Tag	Default if Omitted	Supported Values	Example	Description
%UMS_HTTP_SRV_SERVICE_NAME_DESKTOP%	Unset	_http-client gateway-client In addition, other values can be used if DNS is set accordingly.	<messaging-http-host srv-svc-name="gateway-client">	Enables (DNS) SRV resolution with provided service name that the client uses to resolve Messaging Server (UMS). If unset, the client only performs an A-record query.
%UMS_SRV_ADDRESS_DESKTOP%	unset	string	<messaging-http-host address="example.domain.com">	Defines the address used to make DNS SRV-query for looking up Messaging Server service hosts.
%ENABLE_MESSAGE_SYNC_DESKTOP%	false	false, true	enable-sync="true">	When set to "false", server-based message history and badge sync are disabled. When set to "true", server-based message history and badge are enabled.
%UMS_USE_SSL%	true	false, true	<messaging-http-host <use-ssl>>true</use-ssl>	When set to "false", sets the Messaging Server HTTP service to use HTTP. When set to "true", sets the Messaging Server HTTP service to use HTTPS.

Tag	Default if Omitted	Supported Values	Example	Description
%MESSAGE_SYNC_FETCH_PATH_DESKTOP%	empty	string	<messaging-http-host <fetch-path>/gateway/v2/msg/history </fetch-path>	Messaging Server path for fetching sync-content. Use the value in the example.
%MESSAGE_SYNC_POST_PATH_DESKTOP%	/v2/gateway/msg/read	string	<messaging-http-host <post-path>/gateway/v2msg/read </post-path>	Messaging Server path for posting sync-signals. Only needed for badge sync.

10.4.3 IM Retention Policy

Release 22.3.0 introduced support for IM retention policy. It provides a way for the clients to self-delete messages older than a specified number of days and ignore any messages that are retrieved from the server that are older than the specified number days.

The number of days includes today, so if the number is 7 then it would be today minus 6 days. The actual message purging is done at login, at message sync, and once a day, (also unread messages are purged).

Communicator uses the local time in the machine, while message time stamps received from UMS are based on Epoch time. The UI only shows relevant Chat History links based on available messages.

The following example shows the related parameter for enabling this feature.

```
<config version="20">
  <chat>
    <message-retention-time-days>%CHAT_MESSAGE_RETENTION_TIME_DAYS_DESKTOP%</message-retention-time-days>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to control IM retention policy.

Tag	Default if Omitted	Supported Values	Example	Description
%CHAT_MESSAGE_RETENTION_TIME_DAYS_DESKTOP%	Unset=0	integer	<message-retention-time-days>3</message-retention-time-days>	Number of days the client retains the messages in local cache. Setting the value to "0" turns off IM retention, then all messages are saved, and nothing is automatically deleted.

10.4.4 Connect Messaging Support

Starting with Release 21.6.0, Connect messaging is also supported for sending group messages using either the “+” button or by multi-selecting contacts and starting a group chat in addition to receiving Connect group messages. This feature is implemented over a new HTTP API while one-on-one (1-1) chat sessions still use XMPP. Also, when 1-1 chat is expanded into a group chat using drag-and-drop, XMPP MUC is used and when a multi-party call has a chat component.

Release 22.7.6 added a new attribute for enabling Connect messaging in UC-One SaaS style to facilitate interworking with Connect clients that do not support XMPP. With UC-One SaaS style, the following behavior is provided:

- 1) Drag-and-drop is not possible for chats. Chat is not visible in active communications in the Main window.
- 2) If there is an active call (one-to-one call or group-call), a contact or other call can be drag-and-dropped to that, but not to communications area. Only the call is conferenced and XMPP MUC (group chat) is not started.

With Collaborate-style setting, full drag-and-drop is allowed and Release 22.7.5 functionality is retained. This is suitable for deployments not using Connect messaging or wishing to retain the wide possibility to use drag-and-drop and also have chat and share in ad hoc conference calls.

The following example shows the related parameter for enabling this feature.

```
<config version="20">
  <services>
    <group_messaging enabled=" %ENABLE_GROUP_MESSAGING_DESKTOP%"
use-collaborate-style-participant-
management="%USE_COLLABORATE_STYLE_PARTICIPANT_MANAGEMENT%" />
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), are used to control Connect group messaging support.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_GROUP_MESSAGING_DESKTOP%	false	false, true	<group_messaging enabled="true" />	When set to “false”, group messages are disabled. When set to “true”, group messages are enabled.

Tag	Default if Omitted	Supported Values	Example	Description
%USE_COLLABORATE_STYLE_PARTICIPANT_MANAGEMENT%	false	false, true	use-collaborate-style-participant-management="true"	<p>When set to "false", Communicator enables same behavior as the current UC-One SaaS-flavored client:</p> <ol style="list-style-type: none"> 1. DND is not possible for chats (and chat is not visible in active-comms row). 2. If there is an active call (one-to-one or group-call), a contact or other call can be dropped onto that (but not to the comms-area). Only the call is conferenced, MUC is not started underneath. <p>When set to "true", allow drag-and-drop and retain the functionality that Release 22.7.5 has. This is suitable for customers not using Connect messaging or wishing to retain the wide possibility to use contact drag-and-drop and also have chat and share in ad hoc calls.</p>

Starting with Release 22.4.0, Connect messaging is used for ad hoc group messaging whenever enabled while XMPP is always used in My Room and in 1-1 sessions.

10.4.5 Aggregated Presence

Aggregated presence is server functionality to calculate, aggregate, and publish presence states on behalf of all clients that a subscriber is logged into and using. In this model, Communicator is not storing or utilizing free-text stored locally or to the private storage, which is a significant simplification to client logic. The client just shows the status it gets from the server.

Starting with Release 21.6.0, aggregated presence is used via a new HTTP API for manual presence operations. However, presence notifications still arrive using XMPP as before. In addition, automated presence statuses (Busy-In Call, Away, Online, Offline, Busy-In Meeting, and so on) still use XMPP for updates. Aggregated presence also has an impact to the available options in the Busy-In Call configuration typically using a presence server. Release 22.9.2 added support for local Busy-In Call status generation with aggregated presence in certain deployments.

For more information on the Busy-In Call configuration, see section [10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence](#).

Note that aggregated presence must also be enabled on the Messaging Server (UMS) side. For the necessary Messaging Server patches, see the *UC-One Solution Guide*. If aggregated presence is not enabled, Communicator falls back to XMPP presence.

Deployments are recommended to turn this on only after a significant penetration of clients supporting aggregated presence has been reached.

Release 22.5.0 added an “Automatic” presence status in the UI. This new presence status requires aggregated presence to be enabled in order to show.

The following example shows the related parameter for enabling this feature.

```
<config version="20">
  <services>
    <presence>
      <server-presence-aggregation
enabled="%ENABLE_SERVER_PRESENCE_AGGREGATION_DESKTOP%" enable-local-busy-
in-call="%ENABLE_LOCAL_BUSY_IN_CALL_DESKTOP%" />

```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to control aggregated presence support.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_SERVER_PRESENCE_AGGREGATION_DESKTOP%	false	false, true	<server-presence-aggregation enabled="true"/>	When set to “false”, aggregated presence is disabled. When set to “true”, aggregated presence enabled.
%ENABLE_LOCAL_BUSY_IN_CALL_DESKTOP%	false	false, true	enable-local-busy-in-call="true" />	When set to “true”, local generation of Busy – In Call presence status is enabled. When set to “false”, local generation of Busy – In Call presence status is not enabled.

10.5 Use Cisco BroadWorks Xtended Services Interface Features

10.5.1 Xtended Service Interface Basic Configuration – URL and Version

The %XSI_NAMESPACE% tag is used to define the namespace in generated requests. This should be defined as “*http://schema.broadsoft.com/xsi*” for v2.0.

The following example shows the related parameters. For moderator control impacts to these parameters, see section *10.1.30 Meet-Me Moderator Controls and Participant List*.

```
<config version="20">
  <protocols>
    <xsi>
      <namespace>%XSI_NAMESPACE%</namespace>
      <version>%XSI_VERSION%</version>
      <paths root="%XSI_ROOT%">
        <action-root>com.broadsoft.xsi-actions/v2.0</action-root>

```

```

    <subscription-root>com.broadsoft.xsi-events/v2.0</subscription-root>
    <action>com.broadsoft.xsi-
actions/%XSI_VERSION%/user/%%1@%% (DOMAIN) </action>
    <directories>directories</directories>
    <services>services</services>
    <profile>profile</profile>
    <calls>calls</calls>
    <subscription>com.broadsoft.xsi-
events/%XSI_VERSION%/user/%%1@%% (DOMAIN) </subscription>
    <events>com.broadsoft.xsi-events/%XSI_VERSION%/channel</events>
    <async-events>com.broadsoft.async</async-events>
    </paths>
</xsi>

```

The Xsi-version tag value should be set to the version of the interface deployed on the Xtended Services Platform (Xsp), noting compatibilities with the Communicator client. For Xsi, signaling authentication device tokens are also supported since Release 21.4.0 for the DM-configuration retrieval part only, while remaining signaling employs the usual authentication procedure with 401 challenges.

Tag	Default if Omitted	Supported Values	Example	Communicator
%XSI_NAMESPACE %	empty	string	<namespace> http://schema.broadsoft.com/xsi </namespace>	The Xsi namespace used for Xsi operations.
%XSI_ROOT%	empty	string	<paths root="https://domain.com">	Xsi root is used for Xsi operations.
%XSI_VERSION%	v2.0	v2.0	<version>v2.0</version >	The version "v2.0" is used for 9.3.x and higher.

The Xtended Service Interface URL and XSI-server version must be configured with the XML section under <protocols><xsi>.

The possible value for the %XSI_VERSION% is "v2.0".

Release 20.2.0 introduced new elements shown in the previous example. Action-root and subscription-root are required for Meet-Me Moderator Controls. If they are omitted, Communicator still works with the older Xsi configuration; however, Meet-Me Moderator Controls will not work.

When the two new elements are included in the configuration, the older configuration parameters in the path's node are no longer used:

- <action>
- <directories>
- <services>
- <profile>
- <calls>
- <subscription>
- <events>
- <async-events>

The following items are example Cisco BroadWorks features that can be used via Xtended Services Interface APIs, typically Xsi-Actions:

- Network call logs in Call History, basic and enhanced
- Search and synchronization with Cisco BroadWorks enterprise directory
- Service management, for example, to turn on Call Forwarding
- Click To Dial as well as associated mid-call controls and conferencing
- Visual Voice Mail
- Team telephony
- Moderator Controls
- Executive-Assistant
- Call Center login
- Call recording
- Meet-Me conferencing and provisioning
- Password change
- My Room with Video Server (UVS) or Meet-Me
- Login procedures with DM-config file retrieval and license check

All features in the previous list use the same Xtended Services Interface module in the client and the following settings are used to turn them on (“on” is the default).

For more information on Xsi-Events used by a number of these features, see section [10.5.5 Xsi-Event Channel](#).

Example Files

Search and Add within Search Tag

```
<config version="20">
  <services>
    <search enabled="true">
      <xsi>
        <directory>Enterprise</directory> <!--
        directory to search in
        -->
        <search-locations> <!--
        location name="FullName" xsi_field="name" /
        -->
        <!--
        not supported for Enterprise directory
        -->
        <location name="First Name" id="firstname"
        xsi_field="firstName" />
        <location name="Last Name" id="lastname"
        xsi_field="lastName" />
        <location name="Phone" id="anyphone" xsi_field="number" />
        </search-locations>
      </xsi>
    </search>
  </services>
</config>
```

Supplementary Services without Toolbar

```
<config version="20">
  <services>

    <supplementary-services enabled="true">
      <xsi> <!-- xdm xsi -->
        <broadworks-anywhere enabled="true" />
        <remote-office enabled="true" />
        <call-forwarding-always enabled="true" />
        <call-forwarding-busy enabled="true" />
        <call-forwarding-not-reachable enabled="true" />
        <call-forwarding-no-answer enabled="true" />
        <do-not-disturb enabled="true" />
        <calling-line-id-delivery-blocking enabled="true" />
        <simultaneous-ring-personal enabled="true" />
        <connected-line-identification-presentation enabled="true" />
        <connected-line-identification-restriction enabled="true" />
      </xsi>
    </supplementary-services>
  </services>
</config>
```

Call Logs

```
<config version="20">
  <services>
    <call-history enabled="true">
  </call-history>
  </services>
</config>
```

10.5.2 Xsi Service Discovery

Communicator finds the right Xtended Services Platform (Xsp) based on DNS SRV and A-queries using the following steps:

- 1) Take the value of the Xsi paths root parameter from configuration file and resolve using SRV (<paths root="http://server.domain.com/">).
- 2) Resolve all the items received using DNS A-queries. If SRV provides no results, the Xsi root path is resolved with DNS A-query as a fallback solution.
- 3) When many items are received, they are ordered based on SRV priority. To create this ordering, SRV priority is used first. For items with equal priority, weight is looked at to determine the likelihood in which a certain server is tried first. When SRV results in several items with equal transport protocol, priority, and weight, any one received is selected at random.

10.5.3 Sticky Xsi 302 Response Support

In some deployments, Xtended Services Platforms are configured always to redirect incoming Xsi requests with 302 responses. For these deployments, Release 21.2.0 and onwards supports "sticky" 302 where the client remembers the forwarded to URI (HTTP location header) and uses that, avoiding excessive 302 signaling. This applies to both Xsi-Events and Xsi-Actions.

More detailed example steps when connecting to xsp.domain.com:

- 1) DNS SRV-query to resolve xsp.domain.com.
- 2) DNS A-query for received response, result IP 10.1.1.5.
- 3) Send HTTP GET to 10.1.1.5, HTTP Host header contains xsp.domain.com.
- 4) Received 302 response with xsp1.domain.com in the location header.

- 5) (Without additional DNS queries) send HTTP GET to 10.1.1.5 with Host header set to "xsp1.domain.com".
- 6) Receive *200 OK*.
- 7) Client treats the address received in 302 as a permanent change (despite it coming within 302) so additional HTTP GETs go to 10.1.1.5 without further DNS operations, with Host header set to xsp1.domain.com until the server stops responding.

When the server stops responding, failover uses the original list received in step 1 to get the next server to try.

There is no client-side configurability on top of basic Xsi configuration for this feature, but Xtended Services Platform (Xsp) configuration can be used.

10.5.4 Xtended Service Interface Failover

10.5.4.1 Configuration and DNS Operations

The Xtended Services Interface (Xsi) failover is also supported in this release, following Cisco BroadWorks procedures, more than one Xtended Services Platform (Xsp) is needed.

The URL used in the *Login* screen is used to fetch the config file, which contains the Xtended Services Platform (Xsp) root path used for all Xsi operations instead of the URL used in the *Login* screen (these two may be identical via configuration).

The failover triggering, and failover time logic relies on configuration parameters that are found in the existing configuration file. No new configuration parameters have been added for failover since the various paths for Xtended Services Interface operations are already supported in the configuration file.

Operating system (OS) caching is also used for DNS operations, controlled by the OS. Communicator uses OS primitives for DNS.

DNS operations are redone to get the list of IP addresses for Xtended Services Platforms at Xsp discovery, typically SRV records would also get resolved.

SRV is supported with Xsi starting with Release 21.4.0. Note that for failover to work fully, SRV records must be used. For more information on Xsi SRV-record setup, see the *UC-One Solution Guide*.

For Xsi-Actions, both client and lower level OS primitives for HTTP manage the TCP connection setup. When a new TCP connection is created, a DNS A-query is typically also done, even though there is session reuse when requests are done close to one another timewise.

The Xsi-Event heartbeats are typically sent using a new TCP connection every time, as a result a DNS A-query is done in the lower protocol stack levels and if the Xsp FQDN resolves to several IP addresses, the request may end up with a different Xsp causing an Xsi-Event channel error in the UI. For this reason, it is recommended to use a single IP address for each Xsp/FQDN received from SRV.

For more information on configuring Xsi-Events to be used either permanently or in other modes, see section [10.5.7 Xtended Services Interface Mid-Call Controls](#).

10.5.4.2 Failover Detection and Failover Time

Xsp discovery is the first step in the failover process and it is done in the following cases:

- Login. If login is successful and then the Xsp is lost, loss detection time depends on whether Xsi-Events are used (see the next bullet for Xsi-Events case). If Xsi-Events are not used, TCP setup process towards the Xtended Services Platform (Xsp) with associated timeouts dictates how long failover takes after initial login has taken place. When connecting to an Xtended Services Platform (Xsp), there is a TCP timeout of about 30 seconds before the client gives up on that server and tries the next.
- Network interface loss. Network loss is detected immediately with HTTP as it is done on top of TCP, triggering the failover process.
- Xsi-Event channel loss. For example, caused by TCP RST from the Xsp, a permanent TCP connection is used with Xsi-Events and if the associated TCP socket dies or if the server responds with 5xx that is detected immediately, and the failover process is triggered. TCP connection used for Xsi-Actions is not permanent but torn down after each required operation has been done. If Xsi-Events are used and the TCP socket remains alive, for instance, when a load balancer is used in front of the Xsp, Xsi-Events heartbeat in *config.xml* can be used to control failover times as one missed heartbeat from the Xsp triggers the failover process, which completes in about 30 seconds, when 15 seconds heartbeat value is used. For Xsi-Actions, there is no failover if the TCP connection fails during the short time interval used to perform a query. 503 errors and network failures cause one retry to be performed.

10.5.4.3 Failover Process

When the failover process is triggered the following steps are taken:

- 1) Xsp discovery: Communicator resolves the Xtended Services Platform URL using a DNS SRV and A-query lookups and receives multiple IP addresses.
- 2) Communicator starts using the received IP address in priority order and chooses the first one that works. When a failure is detected, Communicator goes back to step 1 Xsp discovery. However, if an Xsp connection failed while the network interface remains up, that Xsp is tried last even if it would come back as the highest priority Xsp from DNS.
- 3) The Xsi request itself is done using FQDN and not an IP address, for example:
`https://domain.com:443/com.broadsoft.xsiactions/v2.0/user/johndoe@domain.com/services`

If no working Xtended Services Platform (Xsp) is found, the client displays an UI error for Xsi connectivity as per the current implementation. Fail back to Xsp1 while Xsp2 still works is not supported in this release. Instead, the working Xsp is kept until it stops working, logout occurs, or network or connection loss occurs.

When *404* is received (user not found), there is no failover since it is assumed that the account does not exist on the server.

Furthermore, a *401* response (authentication failure) after several Xsi requests have succeeded and credentials are thus valid causes the client to log out since the current valid credentials are no longer working.

If an Xtended Services Interface failover takes place during login, the client only handles the ongoing message and drops the others. This is to be improved in upcoming releases. For the workaround, see the *Communicator for Desktop Release Notes* for this release.

The version control feature supports failover in this release.

An exponential backoff timer was introduced in Release 3.9.0/22.9.2 and only applies if UC-One loses its Xsi connection but the network in general remains up. It is intended to avoid a DOS situation when all clients try to reconnect to the server:

- A new timer defines the retry delay in seconds, which is denoted as T in the following sub-list. With Xsi, T has a value of 10.
- When retrying to connect, UC-One wait time increases according to the Fibonacci series as follows:
 - 1 * T
 - 1 * T
 - 2 * T
 - 3 * T
 - 5 * T
 - 8 * T
 - 13 * T
 - 21 * T
 - 21 * T
 - ...
- Note that the delay does not grow beyond 21 times the unit delay.
- In addition to the increasing delay, a random factor is applied to prevent spikes of clients attempting to reconnect at the same time. This is implemented by drawing a random number from a uniform distribution between 0.3 and 1.7 and multiplying the delay by that number. A new random number should be drawn on each round.

For example, on round four, when T is 10 seconds, the expected delay time is 30 seconds (3 * T), but the actual wait time can vary between 9 seconds and 51 seconds, after applying the random factor.

NOTE: Communicator uses operating system primitives for DNS operations and typically, DNS responses are cached. This release does not honor the TTL of the DNS response with Xsi. For information about other protocols, see section [10.7.1 DNS TTL Management](#).

10.5.5 Xsi-Event Channel

Xsi-Event channel is used for various services such as:

- Xsi mid-call controls
- Moderator Controls
- Terminating Xsi call control
- Incoming call notification in Xsi-Only mode
- Call Settings status notifications
- Participant list for My Room owner
- Participant list for ad hoc room owner (Video Server [UVS] only)

The Xsi-Event channel can be configured for use at login for the entire duration of the login session or only when an Xtended Services Interface call is started as shown in the following example. For the Xsi-Event channel to be enabled permanently at login, the *on-demand* parameter is set to “false”. Setting this to “false” also enables the call setting toolbar to be updated when other devices, such as desk phones, change Call Settings.

For the following services, a permanent event channel must be used:

- Moderator Controls
- Terminating Xsi call control
- Incoming call notification in Xsi-Only mode
- Participant list for room owner also using SIP calls
 - My Room owner
 - Ad hoc room owner in Video Server (UVS) only
- Immediate Call Settings status notifications (otherwise, the status of Call Settings is only refreshed when, for example, opening the *Call Settings* window or making Call Settings changes using the client).

Xsi-Events heartbeat is used to keep the Xsi-Event channel open and the heartbeat interval can be specified using the following parameter.

```

<config version="20">
    <protocols>
        <xsi>
<event-channel enabled="%ENABLE_XSI_EVENT_CHANNEL%" on-demand="
%CHANNEL_NOT_PERSISTENT%">
                                <heartbeatInterval>
%CHANNEL_HEARTBEAT%</heartbeatInterval> <!-- in milliseconds -->
                                </event-channel>

```

The following tags, in the custom *BroadTouch_Tags* set, are used for Xsi-Event channel.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_XSI_EVENT_CHANNEL%	false	true, false	<event-channel enabled="true"	This establishes an Xsi-Event channel. It must be set to “true” to receive, for example, mid-call control service-related events. The recommended value is “true”.
%CHANNEL_NOT_PERSISTENT%	false	true, false	on-demand="true"	This controls Xsi-Event channel persistence. The recommended value is “true”. Set to “true” to use on-demand mode. Set to “false” to use persistent event channel.

Tag	Default if Omitted	Supported Values	Example	Description
%CHANNEL_HEARTBEAT%	10000	number	<heartbeatInterval>10000</heartbeatInterval>	This is the Xsi-Event channel heartbeat (in milliseconds). The default is "10000".

10.5.6 Click To Dial

The Communicator Desktop client supports Click To Dial using basic call back functionality on Cisco BroadWorks. Through this option, an icon (representing “call from phone”) is shown in the UI.

When a user makes use of this option to invoke a call, there are many possible configurations in Cisco BroadWorks. For example, all of the user’s associated telephony endpoints or devices may ring (assuming the user has the Cisco BroadWorks Shared Call Appearance service configured) and the user can then choose to answer the call on any of the ringing devices.

The following example shows this parameter. For more information on the related mid-call controls, see section [10.5.7 Xtended Services Interface Mid-Call Controls](#).

```
<config version="20">
  <services>
    <calls>
      <extended-call-control enabled="%ENABLE_XSI_CALLS%" call-control-window="%ENABLE_XSI_MIDCALL_CONTROLS%"/>
    </calls>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to control the Click To Dial option for the client.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_XSI_CALLS%	false	false, true	<extended-call-control enabled="true"	When set to “false”, Click To Dial is disabled. When set to “true”, Click To Dial is enabled.

10.5.7 Xtended Services Interface Mid-Call Controls

Mid-call control services are provided to Communicator Desktop client users when initiating a Click To Dial call (that is, a call from a phone). An enhanced call-control-window appears providing mid-call actions such as:

- Hold or Resume
- Transfer (for more information, see section [10.1.20 Transfer Call](#))
- Call Park and Retrieve
- Conference
- Add participants
- End call

Note that the call control action taken controls the active call regardless of the alerted device or endpoint used to answer the call.

To provide Xtended Services Interface mid-call controls, the Xsi-Events channel must be enabled. Either permanent or on-demand mode can be used. For more information on Xsi-Events configuration, see section [10.5.5 Xsi-Event Channel](#).

Note that this release does support Xtended Services Interface mid-call controls for calls initiated using other devices such as desk phones. For more information on terminating Xsi call control, see section [10.5.8 Terminating Xsi Call Control](#).

The following example is from the call's node.

```
<config version="20">
    <services>
        <calls>
<extended-call-control enabled="%ENABLE_XSI_CALLS%" call-control-
window="%ENABLE_XSI_MIDCALL_CONTROLS%"/>

```

The following tags, in the custom *BroadTouch_Tags* set, are used with mid-call control services.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_XSI_CALLS%	false	true, false	<extended-call-control enabled="true"	This enables call control over the Xtended Services Interface. This must be set to "true" to access mid-call control services. The recommended value is "true".
%ENABLE_XSI_MIDCALL_CONTROLS%	false	true, false	call-control-window="true"/>	This enables activation of mid-call control services. The recommended value is "true". This parameter is in the calls section in the main XML configuration file.

10.5.8 Terminating Xsi Call Control

Starting with Release 21.1.0, Communicator can be used to control calls that have been initiated using other devices. In case of an incoming call, the actual answering action must happen with the other device. This terminating Xsi call control supports the same mid-call controls than calls initiated using Xsi from Communicator. Note that as this feature depends on Xsi-Events; therefore, the Xsi-Event channel must be persistent. For more information on Xsi-Event channel configuration, see section [10.5.7 Xtended Services Interface Mid-Call Controls](#).

Depending on Xsi-Event channel signaling, not all call controls may always be available (that is, holding or resuming a call may not always be possible).

Also note that for incoming call notifications to work with Xsi-Only Communicator, they must be separately enabled. For more information, see section [10.5.9 Incoming Call Notifications in Xsi-Only Mode](#).

```
<config version="20">
  <protocols>
    <xsi>
      <extended-call-control enabled="true" call-control-window="true"
terminating-controls="%ENABLE_TERMINATING_XSI_CALLS%" />
    </xsi>
  </protocols>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, is used to control this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_TERMINATING_XSI_CALLS%	false	false, true	terminating-controls="true"	When set to "false", terminating Xsi call control is disabled. When set to "true", terminating Xsi call control is enabled.

10.5.9 Incoming Call Notifications in Xsi-Only Mode

This feature, introduced in Release 21.5.0, provides an incoming call toaster in Communicator for calls ringing on a desk phone. Based on a received Xsi-Event, the client presents an incoming call toaster to the user to answer or decline a call when Communicator Desktop is run in Xsi-Only configuration (or with only Xsi and XMPP enabled).

Note that a persistent Xsi-Event channel is required for this feature. In addition, the desk phones deployed with the Xsi-Only client must support the Remote Control Event Package; only then is answering calls remotely in Communicator possible. For more information on the Remote Control Event Package in Communicator, see section [10.1.38 Remote Control Event Package](#).

In Xsi-Only mode, XMPP, chat, and presence can be enabled or disabled. However, SIP calls must be disabled when this feature is used. When SIP is enabled, Communicator only shows incoming calls received via SIP.

In addition, this feature also requires terminating Xsi call controls to be enabled.

See the following example for configuration.

```
<config version="20">
  <services>
    <calls>
      <extended-call-control enabled="true" call-control-window="true"
terminating-controls="true"
remote-answer-support="%ENABLE_XSI_REMOTE_ANSWER_DESKTOP%"/>
    </calls>
  </services>
</config>
```

The following tag in the custom *BroadTouch_Tags* set is used to enable the incoming call notification feature option in Xsi-Only mode.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_XSI_REMOTE_ANSWER_DESKTOP%	false	false, true	remote-answer-support="true"	When set to "false", incoming call notifications over Xsi are disabled. When set to "true", incoming call notifications over Xsi are enabled.

10.5.10 Call Settings and Call Settings Toolbar

The *Call Settings* toolbar in the main view, which allows easier management of Supplementary Services, must be enabled separately as shown in the following example. However, these features must be pre-assigned in a user's Cisco BroadWorks profile to provide this accessibility. Starting with Release 20.2, the Call Settings toolbar is a button in the left pane with right-click menus. The configuration parameters in Release 20.2.0 dictate which menu options and ToolTips are available.

The following individual services can be enabled or disabled (other parts of the feature cannot be configured):

- BroadWorks Anywhere
- BroadWorks Remote Office
- Forward Calls (Call Forwarding Always, Busy, or No Answer)
- Do Not Disturb
- Hide Number (Caller ID Blocking)
- Simultaneous Ringing Personal
- Anonymous Call Rejection
- Automatic Callback
- Call Waiting
- Voice Messaging Management
- Connected Line Identification Presentation (COLP)
- Connected Line Identification Restriction (COLR)

In addition, the Xsi-Events channel must be enabled to allow the toolbar to be updated dynamically when other devices change settings. Otherwise, the toolbar is only updated when the client itself makes changes. For information on the setup of the Xsi-Events channel, see section [10.5.7 Xtended Services Interface Mid-Call Controls](#).

If the toolbar setting is enabled for a service, then the corresponding service must also be enabled in the *Call Settings* window. The same configuration structure is used for both the *Call Settings* window and the toolbar, with different parameters as shown in the following example. Note that the toolbar parameter is not supported for all services.

```

<config version="20">
    <services>
```



```

<supplementary-services enabled="%ENABLE_XSI_SRV_MANAGEMENT%"
toolbar="true" toolbar-call-settings="%ACCESS_CALL_SETTINGS%"
    <xsi> <!-- xdm xsi -->
        <broadworks-anywhere enabled="true"
toolbar="true" />
        <remote-office enabled="true" toolbar="true" />
        <call-forwarding-always enabled="true"
toolbar="true" />
        <call-forwarding-busy enabled="true"
toolbar="true" />
        <call-forwarding-not-reachable enabled="true"
toolbar="true" />
        <call-forwarding-no-answer enabled="true"
toolbar="true" />
        <do-not-disturb enabled="true" toolbar="true"
/>
        <calling-line-id-delivery-blocking
enabled="true" />
        <simultaneous-ring-
personal
showAnswerConfirmationSetting="%SIM_RING_SHOW_ANSWER_CONFIRMATION%"
enabled="true" />
        <connected-line-
identification-presentation enabled="true" />
        <connected-line-
identification-restriction enabled="true" />
        <voice-messaging enabled="true" />
        <call-waiting enabled="true" />
        <anonymous-call-rejection
enabled="true" />
        <automatic-callback
enabled="true"/>
    </xsi>
</supplementary-
services>
    </supplementary-services>

```

The following tag, in the custom *BroadTouch_Tags* set, is used to enable the Service Management (Call Settings) option.

Tag	Default if Omitted	Supported Values	Example	Call Settings Option
%ENABLE_XSI_SRV_MANAGEMENT%	false	false, true	<supplementary-services enabled="true"	When set to "false", Service Management with Xsi is disabled. When set to "true", Service Management with Xsi is enabled.

Communicator Desktop client can be configured to display the Call Settings toolbar, at the top of the client user interface. To enable this function, the toolbar-related tags, defined in the *BroadTouch_Tags* set, must be set accordingly.

Call Settings Toolbar	Deactivated	Activated
Tag	Value	
%ENABLE_XSI_SRV_MANAGEMENT%	false	true
%ENABLE_TOOLBAR%	*	true

In addition to the tags already mentioned, the following tag enables a Call Settings icon to appear in the toolbar at the top of the *Main* window. When activated, the user can select this icon to access all their available Cisco BroadWorks services. The table also provides details on the toolbar enablement.

Tag	Default if Omitted	Supported Values	Example	Call Settings Icon
%ACCESS_CALL_SETTINGS%	false	false, true	toolbar-call-settings="true">	"false" = deactivated "true" = activated
%ENABLE_TOOLBAR%	false	false, true	toolbar="true"	When set to "false", the toolbar is disabled. When set to "true", the toolbar is enabled.
%SIM_RING_SHOW_ANSWER_CONFIRMATION%	true	false, true	showAnswerConfirmationSetting="true"	When set to "false", the simultaneous ringing answer confirmation is disabled. When set to "true", the simultaneous ring answer confirmation is enabled.

Furthermore, to allow the toolbar to dynamically update the status of its displayed services (regardless of the device or endpoint the user makes use of to modify their service), the Xsi-Event channel must be enabled and persistent. Otherwise, the toolbar is updated only when the user makes changes through the client itself. To enable this function, the toolbar-related tags, defined in the *BroadTouch_Tags* set, must be set accordingly.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_XSI_EVENT_CHANNEL%	false	false, true	<event-channel enabled="true"	This establishes the Xsi-Event channel needed for mid-call control. It must be set to "true" to access mid-call control services.

Tag	Default if Omitted	Supported Values	Example	Description
%CHANNEL_NOT_PERSISTENT%	false	false, true	on-demand="true">	This controls the Xsi-Event channel persistence. When set to "true", the on-demand mode is enabled. When set to "false", the on-demand mode is disabled (this means always on Xsi-Event channel).

The following services are directly accessible through the toolbar:

- BroadWorks Remote Office (see the following NOTE)
- Forwarding Calls (Call Forwarding Always, Busy, or No Answer)
- Do Not Disturb
- BroadWorks Anywhere

NOTE: Access to the Remote Office service through the toolbar may require specific Cisco BroadWorks patches to be deployed in situations where no telephone number has been specified for the service. Therefore, it is not recommended to use the Remote Office service with the toolbar without the Cisco BroadWorks patches. For patch requirements, see the *Communicator (Desktop) Release Notes*.

10.5.11 Enterprise Directory Listing

Starting with Release 10.1, contact listing from the enterprise directory (that is, the Showall directory) is again available as a service provider option.

This feature is intended for small and medium enterprises where the number of contacts in the telephony directory is limited as the usability of the feature heavily suffers due to additional scrolling when the number of users grows, and end users are likely to search. The directory contacts are downloaded at login. Therefore, the login time and traffic towards the Xtended Services Platform (Xsp) increase the more directory contacts the enterprise has. This is why the recommended maximum for the directory size is 100.

When Presence on Demand is used, presence is not fetched at all if there are more than 100 contacts to avoid performance issues. For more information about Presence on Demand, see section [10.3.12 Presence on Demand](#).

Communicator shows the received search results as is without any translations done on the client side.

Full contact listing from the enterprise directory can be configured by setting the `<full-enterprise-directory>-node` under `<contacts>` in the configuration XML file. The `%ENABLE_SHOW_ALL_DIRECTORY%` template variable is used to set the desired Boolean value. Result-limit parameter dictates how many results are shown from the directory, starting from the beginning of the received list. The maximum value for result-limit is 65535, values smaller than 50 will be treated the same as 0.

When searching in the full enterprise directory view, only the downloaded contacts are searched.

```
<config version="20">
```

```
<services>
  <contacts>
    <full-enterprise-directory enabled="%ENABLE_SHOW_ALL_DIRECTORY%">
      <result-limit>0</result-limit>
    </full-enterprise-directory>
```

The tag listed in the following table is used to control this capability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_SHOW_ALL_DIRECTORY%	false	false, true	<full-enterprise-directory enabled="true">	When set to "false", the Showall directory is disabled. When set to "true", the Showall directory is enabled.

10.5.12 Xsi Directory Search, Enable or Disable

Starting with Release 20.1.0, the enterprise directory search over Xsi can be enabled and disabled using the following parameter.

```
<config version="20">
  <services>
    <search>
      <xsi enabled="%ENABLE_XSI_SEARCH%">
```

Communicator shows the received search results as is without any translations done on the client side. The following fields are searched:

- First name
- Last name
- Hiragana first name
- Hiragana last name
- Work number
- Mobile phone
- Extension
- IM address
- BroadWorks ID
- Email address
- Department

The following table depicts the DM tag used.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_XSI_SEARCH%	false	true, false	<xsi enabled="true">	When set to "false", Xsi search is disabled. When set to "true", Xsi search is enabled.

Note that to use the multi-part search enhancements introduced in Release 22.4.0, additional Cisco BroadWorks patches must be installed. For more information on Cisco BroadWorks patches, see the *UC-One Solution Guide*.

For more information on the end user visible search examples, see the *Communicator for Desktop User Guide* for Release 22.4.0.

Release 22.9.1 introduced a change so that Xsi search is done with cards internally to align with Connect implementation when searching email and IM address fields. This behavior is not configurable.

10.5.13 Enhanced Search Options

Cisco BroadWorks has several different directories where user data can be stored. The various directories have different data for different purposes. Until Release 21.0.0, only the enterprise directory was used by Communicator Desktop.

Release 21.0.0 added the possibility to search additional directories. Note that all the directories must still be populated on the server side, as Communicator only reads the available data.

Any of the following Cisco BroadWorks directories, in addition to the enterprise directory, can be used when making searches. These directories have less data than enterprise directory:

- User's personal phone list
- Group's common phone list
- Enterprise's common phone list

This enhancement, when enabled, applies to all search operations done by Communicator. This include searches done by end users as well as synchronization operations done automatically by the client when adding contacts or retrieving data for display name that shows when receiving certain incoming calls where the display name cannot otherwise be found (when sync-from=xsi).

The following example depicts the usage of this parameter. Each of the four supported Cisco BroadWorks directories has its own parameter where search for only that directory can be enabled and disabled. Note that the previously used enterprise directory must be enabled separately in the new configuration node. To use all possible directories, they must all be enabled.

```

<config version="20">
  <services>
    <search enabled="true"> <!-- Enables search using various
sources (Xsi, LDAP, Outlook), XDM search not supported in 10.0.3 -->

      <max-result-size>50</max-result-size> <!-- How many
results are shown in the first search result page, 0 or less for showing
20 results, no maximum value in practice, but recommended value 50 as for
Xsi the server only gives 50 result -->

      <xsi enabled="%ENABLE_XSI_SEARCH%">
        <search-sources>
          <enterprise
enabled="%ENABLE_CONTACTS_ENTERPRISE_SEARCH_DESKTOP%" />

          <enterprise-common
enabled="%ENABLE_CONTACTS_ENTERPRISE_COMMON_SEARCH_DESKTOP%" />
          <personal
enabled="%ENABLE_CONTACTS_PERSONAL_SEARCH_DESKTOP%" />
        </search-sources>
      </xsi>
    </search>
  </services>
</config>

```

```

    <group-common
enabled="%ENABLE_CONTACTS_GROUP_COMMON_SEARCH_DESKTOP%" />
    </search-sources>

```

Note that Communicator retains support for the following existing search-related nodes “as is”.

```

<!-- minimum Xsi search phrase length, search operation only done
when min size trigger is met -->
<min-size>3</min-size>
<!-- directory to search in -->

```

The background for this parameter is that Communicator is trying to minimize the load on the Xtended Services Platform (Xsp) and other search sources when searching. When end users type search strings, it is likely that they provide those at the same time, thus it would make sense to wait until the search input has been provided. The parameter `<min-size>` provides configurability for a number of characters while the timeout that Communicator waits until it starts searching for matches in the local address book is hard-coded to 1 second. The previously used `defer-period` configuration parameter is no longer used.

Furthermore, the new configuration node `<search-sources>` replaces the previously used `<directory>` node when found. If `<search-sources>` is not used, the `<directory>` node is be used as before. This allows a single configuration file to be used for both Release 21.0.0 and previous releases.

The following tags, in the custom `BroadTouch_Tags` set, are used to enable the various search directories.

Tag	Default if Omitted	Supported Values	Example	Description
<code>%ENABLE_CONTACTS_ENTERPRISE_SEARCH_DESKTOP%</code>	false	false, true	<code><enterprise enabled="true" ></code>	When set to “false”, enterprise directory search is disabled. When set to “true”, enterprise directory search is enabled. It is recommended to have enterprise directory search enabled as other client features depend on that since other supported directories do not have the necessary data such as JID (unique ID).
<code>ENABLE_CONTACTS_ENTERPRISE_COMMON_SEARCH_DESKTOP</code>	false	false, true	<code><enterprise-common enabled="true" ></code>	When set to “false”, enterprise common directory search is disabled. When set to “true”, enterprise common directory search is enabled.

Tag	Default if Omitted	Supported Values	Example	Description
ENABLE_CONTACTS_PERSONAL_SEARCH_DESKTOP	false	false, true	<personal enabled="true">	When set to "false", personal directory search is disabled. When set to "true", personal directory search is enabled.
ENABLE_CONTACTS_GROUP_COMMON_SEARCH_DESKTOP%	false	false, true	<group-common enabled="true">	When set to "false", group common directory search is disabled. When set to "true", group common directory search is enabled.

10.5.14 Enable Xsi Ad Hoc Conference Calls

Starting with Release 21.1.0, a new configuration parameter has been added to allow enabling and disabling Xsi conference calls for ad hoc conferences. See the following example.

```
<config version="20">
  <services>
    <conference>
      <xsi enabled="%DESKTOP_ENABLE_XSI_CONFERENCE%"
/>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to enable ad hoc Xsi conferences. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%DESKTOP_ENABLE_XSI_CONFERENCE%	true	true, false	<xsi enabled="true"/>	Set to "true" to enable Xsi ad hoc conferences. Set to "false" to disable the feature.

10.5.15 Visual Voice Mail

Starting with Release 21.2.0, Visual Voice Mail (VVM) is supported in the Communicator Desktop client for audio only. It allows users to view incoming voice mails in a list view in the *Main* window history where individual items can be played. This feature is based on Xsi, but notifications of new voice mail are provided over SIP; therefore, SIP must be enabled for the notifications to work. In addition, SIP SUBSCRIBE for MWI configuration is needed for the notifications to arrive and MWI must be enabled for Visual Voice Mail to work. For more information on MWI configuration, see section [10.1.25 Voice Mail Number and Message Waiting Indicator](#). For more information on SIP configuration, see section [10.1.1 Change Basic SIP Server Settings](#). For basic Xsi configuration, section [10.5.1 Xtended Service Interface Basic Configuration – URL and Version](#).

When voice mails are received from Cisco BroadWorks, they come with a Cisco BroadWorks userid that Communicator uses to make a directory search to match the sender to existing contacts.

Primarily UC-One Desktop client is syncing on BroadWorks userid, secondarily based on the user part of the SIP address and as a last resort showing the number if there is no name to show.

Release 22.9.2 added support for refreshing the voice mail view using the Xsi API when opening the voice mail view. This is in addition to the previously supported usage of the h API at login and 24 hours after the last usage of the API if still logged in.

For Cisco BroadWorks release and patch requirements for Visual Voice Mail, see the *UC-One Solution Guide*.

Release 21.2.0 introduced a slightly different UI for history where calls, chat, and voice mail are separated into their own tabs. The order of these tabs can be configured. For more information, see section [10.19.12 Configurable History Tab Order](#).

Visual Voice Mail must be separately enabled in the configuration.

The following settings are needed on the CommPilot portal to have Visual Voice Mail:

- Voice messaging enabled
- “When message arrives, use unified messaging” option enabled
- “Use Phone Message Waiting Indicator” option enabled

Starting with Release 22.2.0, not having the Visual Voice Mail service assigned on the Cisco BroadWorks side for the user automatically makes Communicator disable the configuration for the service.

Release 22.3.1 introduced a new configuration parameter to hide the voice mail preferences tab. For more information, see section [10.19.16 Hide Voice Mail Settings](#).

Release 22.7.5 added support for refreshing the voice mail list for purged messages at login and once every 24 hours after that.

The following example shows Visual Voice Mail configuration. Note that the voice mail number must still be set as specified in section [10.1.25 Voice Mail Number and Message Waiting Indicator](#).

```
<config version="20">
  <services>
    <voice-mail enabled="false" settings="false" visual-voicemail="%ENABLE_VISUAL_VOICE_MAIL%">
      <timeline>
        <chat q="1"/>
        <calls q="2"/>
        <voicemail q="3" />
      </timeline>
      <center-number>%BWVOICE-PORTAL-NUMBER-1%</center-number> <!-- number for MWI, can be used without enabling voicemail tab -->
    </voice-mail>
  </services>
</config>
```

Note that a new Xsi path is also required for Visual Voice Mail, as shown in the following example.

```
<config version="20">
  <protocols>
    <xsi>
      <paths>
        <voicemail>voicemailmessages</voicemail>
      </paths>
    </xsi>
  </protocols>
</config>
```


The following tag, in the custom *BroadTouch_Tags* set, is used to enable Visual Voice Mail and control the history tab order.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_VISUAL_VOICE_MAIL%	false	false, true	<voice-mail enabled="false" visual-voicemail="true">	When set to "false", VVM is disabled. When set to "true", VVM is enabled. Note that voice-mail enabled=false before the actual VVM attribute is still used for backward compatibility.

For timeline parameter tags, see section [10.19.12 Configurable History Tab Order](#).

10.5.16 Call Center Agent Login

Starting with Release 21.2.0, at login it is also possible to log into a call center and view the available call queues in a separate window as well as join queues and set call center statuses. This feature depends on Xsi-Actions so Xsi must be configured and enabled. Also, note that as a result dynamic Automatic Call Distribution (ACD) status updates are not supported in the UI if the ACD status is changed somewhere else. For more information on basic Xsi configuration, see section [10.5.1 Xtended Service Interface Basic Configuration – URL and Version](#).

Starting with Release 22.2.0, not having the Call Center Basic/Premium/Standard service assigned on the Cisco BroadWorks side for the user automatically makes Communicator disable the configuration for the service.

The following example shows the related parameter for enabling this feature.

```
<config version="20">
<services>
  <call-center-agent enabled="%ENABLE_CALL_CENTER_DESKTOP%" />
</services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to control call center login.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_CALL_CEN TER_DESKTOP%	empty	false, true	<call-center-agent enabled="true" />	When set to "false", call center integration is disabled. When set to "true", call center integration is enabled. If the node is empty, then the feature is disabled.

10.5.17 Call History – Basic Call Logs

Cisco BroadWorks basic call logs are used by default in the Call History over Xsi. Call History can be enabled using the configuration parameter in the following example.

In special deployments, Xsi-based Call History can be disabled via a separate configuration parameter (see the following example). When disabled, the history view itself cannot be disabled in user interface. When Xsi Call History is disabled, some Call History data may be available via local history, but it will not be complete. In general, usage of local Call History is not recommended.

Release 22.5.0 added support for syncing Call History items with configured sync sources. For more information on sync sources, see section [10.19.2 Flexible Contact Card Field Configuration and Synchronization](#).

The following example shows the related parameter to enable this feature.

```
<config version="20">
  <services>
    <call-history enabled="true"/>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to control basic call log availability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_CALL_HISTORY_DESKTOP%	true	false, true	<call-history enabled="true" enhanced="true"/>	When set to "false", basic call logs are disabled in Call History. When set to "true", basic call logs are enabled in Call History.

Display names in Call History are primarily taken from the Xsi call log response received from the Xsp. However, local contact display names override the server response, there is no automatic sync towards any directories for call log entries.

Release 22.5.0 introduced support for syncing Call History items with configured sources. For more information on syncing, see section [10.19.2 Flexible Contact Card Field Configuration and Synchronization](#).

10.5.18 Call History – Enhanced Call Logs

Starting with Release 21.6.0, Cisco BroadWorks enhanced call logs are supported in addition to the basic call logs, a different Xsi API is used in this case for retrieving Call History data. For more information on basic Xsi configuration, see section [10.5.1 Xtended Service Interface Basic Configuration – URL and Version](#).

Enhanced call logs offer more history data than basic call logs such as call duration and additional caller information, which is needed for instance for showing full information in some Call Forwarding and hunt group scenarios.

The following example shows the related parameter for enabling this feature.

```
<config version="20">
  <services>
    <call-history enabled="true"
      enhanced="%ENABLE_ENHANCED_CALL_HISTORY_DESKTOP%" />
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to control enhanced call log availability.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_ENHANCED_CALL_HISTORY_DESKTOP%	false	false, true	<call-history enabled="true" enhanced="true"/>	When set to "false", enhanced call logs are disabled. When set to "true", enhanced call logs are enabled. If the node is empty, then the feature is disabled.

10.5.19 Single Sign-On

Single Sign-On (SSO) is supported but without additional DM configuration parameters on top of the existing Xsi parameters, introduced initially in Release 22.2. For more information on related branding recommendations, see the *UC-One Desktop Branding Guide*. The branded SSO context is used as one part of the URL needed to connect to the Xsp authentication service.

Release 22.4.0 introduced additional SSO options that have branding and server configuration impacts. In addition, support was added for using custom Identity Providers (IdPs).

Release 22.5.0 added support for dynamic detection of IdPs. For more information on related branding options, see the *UC-One Desktop Branding Guide*.

Release 22.9.4 added support for the Save Login feature replacing the previous Remember Password feature in SSO (no configurability changes were introduced). For the end-user visible changes, see the *UC-One Desktop User Guide*. As a result, the password is not saved, only the login token.

It is possible to hide Cisco BroadWorks credentials with SSO so that only SSO is used by using a new IdP option "broadworks". If that is returned by the Xsp authentication service to Communicator, the Cisco BroadWorks (username and password) will be available to the user as a sign-in option. If "broadworks" IdP is not returned, the Cisco BroadWorks username and password fields will not be visible in the login screen.

Same Communicator can support both SSO and non-SOS users. Note that Communicator checks the availability of the authService at login via Xsi-Actions before the SSO login procedure. When authService is enabled in the deployment, Communicator assumes that long lived token is in use for non-SSO users and save password checkbox is therefore hidden in the UI as long-lived token is assumed to be used instead. Using Exit instead of Logout makes Communicator remember the entered password so it does not need to be re-entered. Communicator does not proactively monitor the validity of the long-lived token. If the long-lived token expires, any new request to Cisco BroadWorks will be challenged and Communicator will perform a forced logout. It is not possible to change the userid without closing the browser.

The new "broadworks" IdP will therefore control if Cisco BroadWorks authentication (username and password) should be available for the user as a sign-in option or not. The email field at login should only be visible when branding has not defined any sso_context and only at first login after which the user input is cached and user is taken directly to the login view.

The following rules related to the Cisco BroadWorks login apply:

- 1) Select the SSO context that Communicator uses to ask for the IdPs configured on the server side. The URL where the IdPs are checked at login is constructed by using the *dm_url* parameter value combined with a hard-coded string “authService/providers/” combined with the value of *sso_context* parameter.
 - If the branded *sso_context* is empty, the end user can define the *sso_context* by using the email address UI field at login. The domain part of the provided email address before the last comma will be used as the *sso_context*. In the second login, the provided email address is remembered, and the email address field should not appear but going back to the first view is possible via a menu item.
 - If branded *sso_context* is available, use that.
- 2) Request the IdP list from the server and present options to the user depending on the server response:
 - If the Xsp authentication service is not configured, present the Cisco BroadWorks login option on the *Sign In* screen.
 - If just the “broadworks” IdP is returned, present the Cisco BroadWorks login option on the *Sign in* screen.
 - If a non-BroadWorks IdP(s) is returned, instead of the Cisco BroadWorks username and password section, display a button with some text on the *Sign in* screen.
 - If both the “broadworks” IdP and non-BroadWorks IdP(s) are returned at the same time, present the Cisco BroadWorks and SSO options on the *Sign in* screen (current behavior).

NOTE 1: If DM URL is defined for the “broadworks” IdP, it is not used.

NOTE 2: If the Xsp authentication service is configured, but retrieving the SSO providers fails, at sign-in with the Cisco BroadWorks credentials, Communicator uses long-lived token authentication only.

Additionally, the deployment must configure the Xsp authService to not provide other IdPs than the desired one under the name “Custom IdP 1” and ensure also that the name “broadworks” is not listed in the authService response. For more information on Xsp configuration, see the *UC-One Solution Guide*. For more information on server-side SSO, see the *SAML Authentication Integration Solution Guide*.

Finally, DNS must also be provisioned for localhost.ucclient.net to resolve to 127.0.0.1.

10.5.20 Personal Assistant and Nordic Presence

Release 22.5.0 introduced support for a Personal Assistant feature that provides the end user with additional presence statuses as well as the ability to configure them by selecting expiration time, transfer number, and silent alerting.

This feature depends on both Xsi, HTTP messaging, and XMPP. At login, UC-One checks both Personal Assistant service assignment over Xsi and Messaging Server (UMS) support for Personal Assistant over HTTP and downloads the existing Personal Assistant service values over Xsi. The results for expiration time, transfer number, and ring splash are populated in the options view.

New Personal Assistant presence states are sent using HTTP when selected in the UI. XMPP is used to receive the new presence states. Note that aggregated presence must be enabled to use Personal Assistant.

The Personal Assistant presence states are added to the existing drop-down menu if the Personal Assistant feature is enabled in DM. If the Personal Assistant service is assigned in Cisco BroadWorks, the pop-up with the advanced options will also appear.

The directory used for transfer number should match the existing contact list search configuration. For more information on directory search configuration, see sections [10.5.13 Enhanced Search Options](#) and [10.5.12 Xsi Directory Search, Enable or Disable](#).

To utilize Personal Assistant fully, the user must be provisioned on a Messaging Server (UMS) supporting Personal Assistant and additional presence states and must have the Personal Assistant service assigned in Cisco BroadWorks. In addition, the DM configuration file must have this feature enabled. Failing to provide all these will result in a sub-optimal user experience. The existing Cisco BroadWorks workflow for providing the Personal Assistant service to users will continue to be used.

If the Messaging Server (UMS) gateway supports Personal Assistant presence, but the user does not have the Personal Assistant service assigned in Cisco BroadWorks, the user may still be able to see the Personal Assistant status of other users.

Existing customers upgrading to the Release 22.5.x client will not have any impact on the Personal Assistant feature unless they explicitly modify their DM configuration and enable this feature regardless of how their Messaging Server is patched and/or Cisco BroadWorks services are assigned.

Release 22.7.0 added support for hiding and showing the silent alert setting when setting up Personal Assistant states such as “Gone for the day”. Release 22.7.0 also added support for “Alert me first” setting. The following table shows the different cases when both features are used, and silent alert may or may not be hidden. The “Alert me first” feature also requires support in the Messaging Server (UMS) and Cisco BroadWorks. See the *UC-One Solution Guide* for more details on required Messaging Server (UMS) and Cisco BroadWorks versions. Communicator stores silent alert setting changes in Cisco BroadWorks.

Release 22.7.5 added a new configuration parameter to control whether S4B presence is overriding the PA presence when both are being used. When set to “true”, setting S4B presence will not clear PA presence. Instead PA presence overrides and stays. When disabled, presence change in S4B clears the PA state as today. Additionally, setting PA presence via system tray brings the Main window to foreground when the PA UI is opened. Personal Assistant must also be enabled in the Messaging Server (UMS) for the system tray PA setting to work. For more information on this parameter, see section [10.20 UC-One Add-in for Microsoft Skype for Business \(S4B\)](#).

Setting the PA presence will also be mapped to a relevant S4B presence status.

Selected Radio Button in UI	Ring Splash Setting (in the received JSON from Cisco BroadWorks)	Alert Me First Enabled
No Alert	OFF (hidden by config)	OFF
No Alert	ON (hidden by config)	OFF
No Alert	OFF (visible by config)	OFF
Ring splash	ON (visible by config)	OFF

Selected Radio Button in UI	Ring Splash Setting (in the received JSON from Cisco BroadWorks)	Alert Me First Enabled
Alert me first	OFF (hidden by config)	ON
Alert me first	ON (hidden by config)	ON
Alert me first	OFF (visible by config)	ON
Alert me first	ON (visible by config)	ON

Table 1 Alert Me First and Silent Alert Interworking

The following example shows the related parameter for enabling this feature.

```
<config version="20">
<services>
<presence>
<personal-assistant enabled="%DESKTOP_PERSONAL_ASSISTANT_ENABLED%">
<silent-alert show="%ENABLE_SILENT_ALERT_SHOW%" />
</personal-assistant/>
</presence>
</services>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), are used to control enhanced call log availability.

Tag	Default if Omitted	Supported Values	Example	Description
%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	false	false, true	<personal-assistant enabled="true" />	When set to "false", the Personal Assistant feature is disabled. When set to "true", the Personal Assistant feature is enabled. See the next table for details regarding hybrid scenarios.
%ENABLE_SILENT_ALERT_SHOW%	true	false, true	<silent-alert show="true" />	When set to "false", the Personal Assistant (PA) silent alert setting is hidden when managing PA statuses such as "Gone for the day". When set to "true", the Personal Assistant silent alert setting is shown when managing PA statuses such as "Gone for the day".

The following table shows the impact of various combinations of Messaging Server (“UMS” in the following table) support and Cisco BroadWorks (“BW” in the following table) configuration for Personal Assistant (“PA” in the following table).

DM Configuration File	Messaging Server State	Cisco BroadWorks PA Service State	Display in UC-One Desktop
DM configuration option NOT enabled	UMS NOT supporting the additional states	BW PA service NOT assigned to the user	No new PA states No configuration of states
DM configuration option enabled	UMS NOT supporting the additional states	BW PA service NOT assigned to the user	No new PA states No configuration of states
DM configuration option enabled	UMS supporting the additional states	BW PA service NOT assigned to the user	Show new PA states No configuration of states
DM configuration option enabled	UMS supporting the additional states	BW PA service assigned to the user	Show new PA states Allow configuration of states

10.6 Share

10.6.1 Desktop Sharing (Sharing Server and Web Collaboration)

Communicator Release 10.0.1 introduced a new feature that allows users to share their desktop. This feature is enabled with the `<webcollab>-node`, where `urlSubDomain` and `urlBasedomain` attributes define the user’s *WebCollaboration-server*.

By default, *webcollab* is disabled.

```
<config version="20">
  <services>

    <webcollab enabled="%ENABLE_WEBCOLLAB%"
urlSubdomain="%WEBCOLLAB_SUBDOMAIN%"
urlBaseDomain="%WEBCOLLAB_BASEDOMAIN%"></webcollab>
```

Release 20.0.1 introduced support for a different server-side implementation, called the Sharing Server (USS). For this type of implementation, the configuration is slightly different as shown in the following example. For more information on the required provisioning of DNS A and SRV records, see the *UC-One Solution Guide*. There is no client-side configuration for SRV records as they are resolved automatically when available. By default, *webcollab* is disabled.

```
<config version="20">
  <services>
    <webcollab enabled="true" useXmppCredentials="true" type="uss"
urlSubdomain="broadsoft" urlBaseDomain="domain.com" uss-
address="http://uss.domain.com:1234/uss">

    </webcollab>
```

- `urlSubdomain` – This is the subdomain part of the server URL used for location.
- `urlBaseDomain` – This is the base domain part of the server URL used for location.

- **useXmppCredentials** – This parameter is used for flow-through provisioning in general with older Web Collaboration solution but not anymore used for selecting the Sharing Server (USS) authentication mode since both XMPP and Xsi credentials are always sent to the server. For more information regarding XMPP credential usage for Web Collaboration authentication, see section 10.8.1 [Flow-Through Provisioning](#). If XMPP credentials are not used for Sharing Server authentication, the Xsi credentials are used instead to obtain the Xsp login token needed for final USS authentication. The flow used by Communicator to obtain the token is described in more detail in the *Optimizing Bandwidth Usage for Sharing Server Feature Description*, which is available on cisco.com. For server-side configuration instructions regarding Xsp login token usage for Sharing Server authentication, see the *UC-One Solution Guide*. In Release 22.2.1 and onwards, Web Collaboration is again supported using an external browse window, using XMPP credentials only.
- **type** – This defines the type of server implementation used. For valid values, see the following Device Management Tag table.
- **uss-address** – This defines the Sharing Server address. Releases 21.6 to 22.2.0 do not support older Web Collaboration but USS only. In Release 22.2.1 and onwards, Web Collaboration is again supported using an external browser window, using XMPP credentials only. XMPP credentials must be used. For more information, see section [10.8.1 Flow-Through Provisioning](#).

Starting with Release 21.1.0, the maximum number of Sharing Server participants is no longer enforced on the client side. It is only enforced on the server side as the limit varies depending on available resources. In collaboration, the server informs the client about the maximum number of participants when the session is created.

To enable the Desktop Share service, configure the tags as shown in the following table.

Tag		Desktop Share
%ENABLE_PRESENCE%	%ENABLE_WEBCOLLAB%	
Value		
false	*	Deactivated
true	false	Deactivated
true	true	Activated

Web Collaboration Tag	Default if Omitted	Supported Values	Example	Description
%WEBCOLLAB_BASED_OMAIN%	empty	string	urlBaseDomain="companymeeting.com"	Base domain of the collaboration server URL (required for the feature to work).
%WEBCOLLAB_SUBDOMAIN%	empty	string	urlSubdomain="company"	Subdomain of the collaboration server URL (required for the feature to work).

Web Collaboration Tag	Default if Omitted	Supported Values	Example	Description
%SHARE_TYPE%	broadcloudmeeting	string (case insensitive)	type="broadcloudmeeting"	This is the type of the Sharing Server (USS). Currently supported values are "uss" and "broadcloudmeeting". An empty value defaults to "broadcloudmeeting" whereas other value disables the feature. The broadcloudmeeting takes the older Web Collaboration feature into use with an external browser window.
%USS_ADDRESS%	empty	string	uss-address="http://uss.domain.com:1234/uss"	This is the URI for a compatible Sharing Server (USS). If the value is left empty, the feature is disabled.
%ENABLE_WEBCOLLAB%	false	true, false	webcollab-enabled="true"	Set to "true" to enable sharing. Set to "false" to disable sharing.

Additionally, to share their desktop, each user must have an enabled Web Collaboration account, for which associated credentials must be known to the client. This, in turn, activates the Desktop Share option icon on the client's interface (assuming the credentials are valid). If the Web Collaboration account is not enabled, joining the share fails. On the Sharing Server (USS), this limitation does not apply. In Web Collaboration, the retirement process may be disabled to avoid manual labor as one alternative.

In both Sharing Server (USS) and Web Collaboration, the Collaborate – Sharing license must also be assigned to the account for the share icon to become visible in the UI.

Starting with Release 21.0, it is always possible to join a share even when starting a share is not enabled in the configuration (that is, webcollab enabled="false"). Sharing, however, always requires sharing to be enabled in the configuration. In deployments where some users have share and some do not, a single DM tag %ENABLE_WEBCOLLAB% can be used to control the behavior.

Note that although the values can be configured, BroadCloud servers are used by default to get location information. The following values are typically used:

- urlSubdomain="webservice12" urlBaseDomain="broadcloudmeeting.com" and, in EU
- urlSubdomain="webservice-eu" urlBaseDomain="broadcloudmeeting.com"

Starting with Release 21.4.0, usage of Cisco BroadWorks login tokens is supported for Sharing Server (USS) room creation. In addition, HTTP proxy with the Sharing Server is supported in Release 21.4.0 and later.

Starting with Release 21.6.0, only the Sharing Server (USS) is supported. Web Collaboration is not supported.

10.6.2 Share Service Discovery

Communicator finds the right share server (Sharing Server or Web Collaboration) based on DNS SRV and A-queries using the following steps (the following example is for the Sharing Server):

- 1) Take the value of the *uss-address* parameter from the configuration file and resolve using SRV (*uss-address*="http://uss.domain.com:1234/uss").
- 2) Resolve all the items received using DNS A-queries. If there are no SRV records, then the configured server address is resolved with an A-query.
- 3) When many items are received, they are ordered based on SRV priority. To create this ordering, SRV priority is used first. For items with equal priority, weight is looked at to determine the likelihood in which a certain server is tried first. When SRV results in several items with equal transport protocol, priority, and weight, any one received is selected at random.

With the Sharing Server (USS), the share server is contacted only once the end user clicks on the share button, and not during login sequence.

10.6.3 Sharing Server (USS) Failover

Sharing Server (USS) client implementation also supports failover. For SRV requirements for failover, see the *UC-One Solution Guide*. If only A-records are used, failover is not supported, as connection setup is done using a single URL and underlying HTTP protocol libraries can only handle one IP address for that URL. SRV allows having several URLs for the server so that failover can also be supported.

The failover process is as follows:

- 1) Sharing Server (USS) discovery: Communicator resolves the Sharing Server URL using a DNS SRV and A-query lookups and receives multiple IP addresses.
- 2) Communicator starts using the received IP address in priority order and chooses the first one that works. When a failure is detected, Communicator goes back to step 1 Xsp discovery (the previous step). However, if a Sharing Server connection failed while the network interface remains up, that Sharing Server is tried last even if it would come back as the highest priority Sharing Server from DNS.

If the primary server stops working during an ongoing share, failover is started once the end user manually starts a new share.

10.6.4 Share Passing

Starting with Release 21.2.0, Sharing Server (USS) share participants can also share and not just the owner (as in previous releases); however, only one person can share at any one time within a session and individual users can only share in one session if they have many sessions. In addition, share passing is only supported in My Room and when the Sharing Server (USS) is used (and not in older webcollab). This feature must be enabled in the configuration and, in order to share, a sharing license must be assigned. See the following example. For more information on basic share configuration, see section [10.6.1 Desktop Sharing \(Sharing Server and Web Collaboration\)](#).

Note that this feature depends on XMPP that must also be configured and enabled on the server side. For more information on basic XMPP configuration, see section [10.3.1 Use Extensible Messaging and Presence Protocol](#).

```
<config version="20">
  <services>
    <webcollab enabled="%ENABLE_WEBCOLLAB%"
useXmppCredentials="%WEBCOLLAB_USE_XMPP_CREDENTIALS%" type="%SHARE_TYPE%"
urlSubdomain="%WEBCOLLAB_SUBDOMAIN%"
urlBaseDomain="%WEBCOLLAB_BASEDOMAIN%" uss-address="%USS_ADDRESS%">
  <participant-share enabled="%ENABLE_PARTICIPANT_SHARE%"/>
    </webcollab>
  <max-participants></max-participants>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, is used to enable share passing.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_PARTICIPANT_SHARE%	false	false, true	<participant-share enabled="true"/>	When set to "false", share passing is disabled. When set to "true", share passing is enabled.

10.7 DNS

10.7.1 DNS TTL Management

A separate configuration parameter has been added for managing the way DNS resolving is redone when the TTL of the DNS record of the currently used server expires. The following parameter, when enabled, forces Communicator to redo DNS operations once the TTL of the DNS SRV or A-record of the currently used server expires.

After the DNS resolving is redone, this parameter also forces Communicator to reconnect to the top priority server received if it is different from the currently used server, even in the case when the current connection is working fully. However, for SIP, reconnection is only done after ongoing calls have finished.

Furthermore, if the newly returned DNS records no longer contain the server that is currently used, reconnection is done immediately even if calls are ongoing. For XMPP, reconnection is always done if the currently used server is not the top priority one in the updated list.

If the TTLs for servers A and SRV records are different, the smaller value is chosen.

When this parameter is disabled, DNS operations are not redone when TTL expires.

This parameter only works for SIP and XMPP in this release. Note that it must be enabled separately for SIP and XMPP in the *config.xml* file. Release 22.9.16 added a minimum value for DNS TTL. For more information, see section [10.1.6.2 Failover Triggering and Failover Time](#).

Note that the DNS TTL management feature cannot be used when an IP address is used in the proxy address parameter described in section [10.1.1 Change Basic SIP Server Settings](#).

Also note that Release 22.9.16 introduced a separate configuration parameter for utilizing a minimal value for DNS TTL for SIP only. For more information, see section [10.1.6.1 Configuration and DNS Operations](#).

```
<config version="20">
  <services>
    <sip>
      <refresh-on-ttl enabled="%SIP_REFRESH_ON_TTL%" />
    </sip>
    <xmpp>
      <refresh-on-ttl enabled="%XMPP_REFRESH_ON_TTL%" />
    </xmpp>
  </services>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set, are used to enable DNS TTL management.

Tag	Default if Omitted	Supported Values	Example	Description
%SIP_REFRESH_ON_TTL%	false	false, true	<refresh-on-ttl enabled="true"/>	When set to "false", DNS TTL management is disabled for SIP. When set to "true", DNS TTL management is enabled for SIP.
%XMPP_REFRESH_ON_TTL%	false	false, true	<refresh-on-ttl enabled="true"/>	When set to "false", DNS TTL management is disabled for XMPP. When set to "true", DNS TTL management is enabled for XMPP.

10.8 Provisioning

10.8.1 Flow-Through Provisioning

Starting with Release 20.0.1, the retrieval of Web Collaboration credentials is automated. When the parameter shown in the following example is set to "true", the client re-uses the user's XMPP credentials as their Web Collaboration credentials. There is a new configuration parameter to enable this, as shown in the following example.

```
<config version="20">
  <services>
    <webcollab enabled="true" urlSubdomain="company"
urlBaseDomain="domain.com" useXmppCredentials="true">
    </webcollab>
  </services>
</config>
```

If the *useXmppCredentials* parameter is set to "true", then the client does not allow the user to manually enter their Web Collaboration credentials (this section is hidden in *Preferences*). If the connection still fails, then an error message appears indicating that there is a server error.

If this parameter is set to “false”, then the client works as in previous releases whereby the Web Collaboration credentials can be manually entered as shown in the following figure.

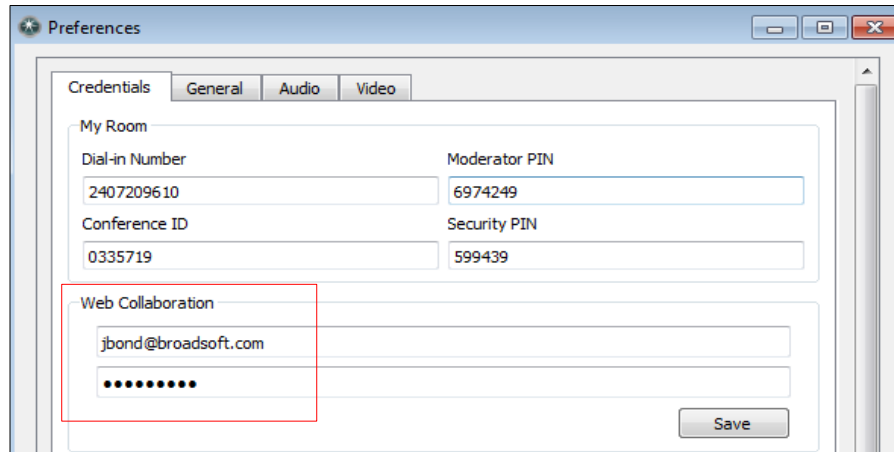


Figure 3 Desktop Share Credentials

For information on the automated provisioning of the My Room conference bridge, see section 10.8.2 [Meet-Me Conference Bridge Auto-Provisioning and Silent Dialing](#). Note that the *Title* parameter must be used for flow-through provisioning to work.

For My Room Device Management tags and configuration information, see section 10.8.2 [Meet-Me Conference Bridge Auto-Provisioning and Silent Dialing](#).

The following tag enables auto-provisioning of the user’s Web Collaboration credentials.

Web Collaboration Tag	Default if Omitted	Supported Values	Example	Description
%WEBCOLLAB_USE_XMPP_CREDENTIALS%	false	true, false	useXmppCredentials="true"	This enables auto-provisioning of the Web Collaboration credentials settings. The default is “false”. In that case, the Xsp login token is used for Sharing Server (USS) authentication.

10.8.2 Meet-Me Conference Bridge Auto-Provisioning and Silent Dialing

Meet-Me conferencing is typically used in My Room. For more information about My Room, see section [10.9.1 Enable My Room](#). The parameters for conference bridge auto-provisioning in Meet-Me are described in the following example.

```

<config version="20">
<services>
    <rooms enabled="%ENABLE_ROOMS%">
        <myroom enabled="%ENABLE_MYROOM%" />
        <projectrooms enabled="false"
create="false" />
        <default-room-history-size>%ROOMS_HISTORY_SIZE%</default-room-history-size>
    </rooms>
</services>

```

```

                <conference-bridge type=""
autodetect="%AUTODETECT_CONFERENCE%" title="%CONFERENCE_TITLE%"
default-bridge="%BRIDGE_ID%" direct-dial="%DIRECT_DIAL%" />

                <!-- if true, disable editing of conf
details in preferences and use XSI r

```

For conference bridge manual provisioning (auto-retrieval/provisioning deactivated), users must configure, through their client's *Preferences* → *Credentials* tab settings, their audio or video conference bridge-related details as shown in the following figure. For the type-attribute, see section [10.1.31 Video Server](#).

Both "type" and "autodetect" with empty values is not allowed.

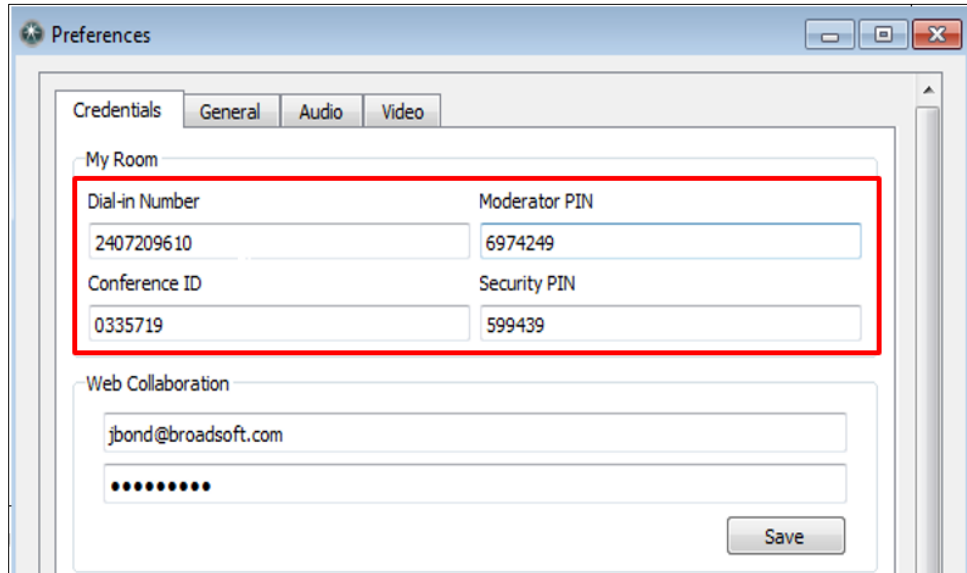


Figure 4 Conference Bridge Settings

NOTE: For manual provisioning, audio or video conferencing resources are not restricted to the Cisco BroadWorks Meet-Me Conferencing service. The conference bridge number and access details can be provided by any valid third-party platform or provider.

Creating the following *BroadTouch_Tags* enables the client to automate the provisioning of a user's My Room audio conference bridge settings (*Preferences* → *Credentials*). The client queries the user's predefined Cisco BroadWorks Meet-Me audio bridges and conferences based on the tag set search criteria.

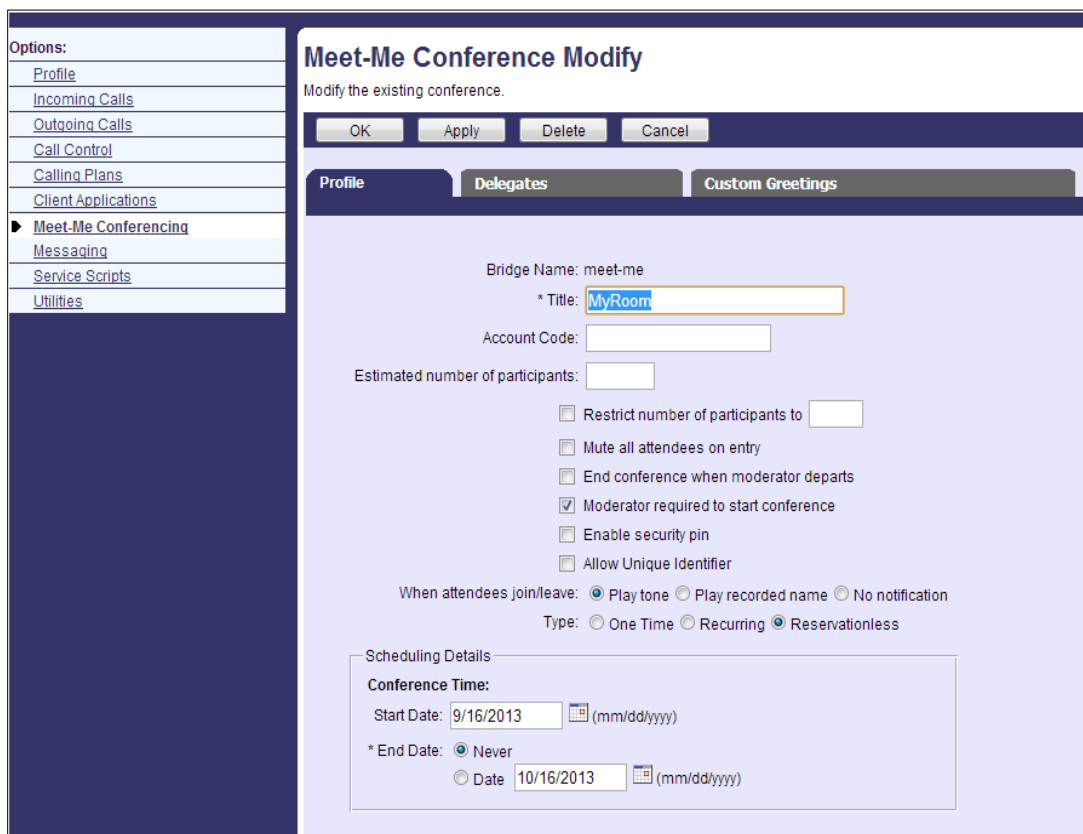
Conference Bridge Tags	Default if Omitted	Supported Values	Example	Description
%AUTODETECT_CONFERENCE%	false	true, false	<conference-bridge autodetect="true">	This enables auto-provisioning of <i>My Room</i> conference bridge settings. The default is "false".

Conference Bridge Tags	Default if Omitted	Supported Values	Example	Description
%BRIDGE_ID%	empty	string	default-bridge="meet-me@domain.com"	<p>This should be set to the bridge ID corresponding to the Cisco BroadWorks Meet-Me bridge hosting the user's primary conference.</p> <p>This parameter is used by the client, in an Xsi query, to retrieve that bridge's telephone (dial-in) number.</p>
%CONFERENCE_TITLE%	empty	Example, My Bridge	title="My Bridge"	<p>This should be set to the generic <i>Title</i> corresponding to users' primary personal conference in Cisco BroadWorks.</p> <p>The <i>Title</i> is used (by the client) to search through the list of conferences associated with the user's primary bridge in an attempt to establish a match. If a match is found, then the client subsequently sends an Xtended Services Interface query to retrieve the conference's respective Moderator PIN and Security PIN (if one exists). If no match is found, then the client attempts to create one.</p> <p>NOTE: A <i>Title</i> must be defined; otherwise, auto-provisioning is not possible.</p>
%DIRECT_DIAL%	false	true, false	direct-dial="true"	<p>This enables the silent dialing into Meet-Me conferences where, instead of using DTMF, the PIN codes are already provided in the SIP INVITE, for example, sip:9726994519;confid=45678;pin=1234@host;user=phone.</p>

The new client-created bridge has the following default Cisco BroadWorks settings:

- Bridge Name: fixed
- Title: <CONFERENCE_TITLE tag>
- Account Code: <empty>
- Estimated number of participants: <empty>
- Restrict number of participants to: <empty>
- Mute all attendees on entry: <not selected>

- End conference when moderator departs: <not selected>
- Moderator required to start conference: <selected>
- Enable security PIN: <not selected>
- Allow Unique Identifier: <not selected>
- When attendees join/leave: *Play tone*
- Type: Reservationless
- Scheduling Details
- Conference Time:
 - Start Date: <current date>
 - End Date: *Never*



Options:

- Profile
- Incoming Calls
- Outgoing Calls
- Call Control
- Calling Plans
- Client Applications
- ▶ **Meet-Me Conferencing**
- Messaging
- Service Scripts
- Utilities

Meet-Me Conference Modify

Modify the existing conference.

OK Apply Delete Cancel

Profile Delegates Custom Greetings

Bridge Name: meet-me

* Title:

Account Code:

Estimated number of participants:

Restrict number of participants to

Mute all attendees on entry

End conference when moderator departs

Moderator required to start conference

Enable security pin

Allow Unique Identifier

When attendees join/leave: Play tone Play recorded name No notification

Type: One Time Recurring Reservationless

Scheduling Details

Conference Time:

Start Date: (mm/dd/yyyy)

* End Date: Never Date (mm/dd/yyyy)

Figure 5 Meet-Me Conference Default Settings

Following is a list of more detailed information regarding each parameter for the conference-bridge node:

- *Title*
 - Search term for the conference when auto-provisioning (autodetect) is enabled. If a match is found, then the necessary details (for example, dial-in number and Moderator PIN) are used to provision the *My Room* conferencing service. If no match is found (and assuming the user was preconfigured with the Meet-Me Conferencing service), then the client attempts to reuse an existing bridge assigned to the user or create a new one (through Cisco BroadWorks) if one had not been assigned. Subsequently, if successful, it uses the newly created bridge details for the *My Room* conference bridge settings. If no title is specified, the room is not created nor is there a search; therefore, the title is a mandatory parameter for flow-through provisioning.
- *Default-bridge*
 - If the *default-bridge* is provided in configuration, then this bridge should be used when creating a conference. The client does not create bridges but only uses existing ones for the conferences. The bridge ID specified for this parameter is the bridge ID that is used when the conference is created by the client. In this case, the exact value of the *title* parameter is used as the title of the conference.
 - If a *default-bridge* attribute is not provided or is empty, the first available active bridge should be used. In the following cases, the creation of a conference should be abandoned.
 - When a *default-bridge* is provided in the configuration but is not available or is not active.
 - When no *default-bridge* is provided in the configuration and no bridge is available or active.
- *Direct-dial*
 - This feature enhances user experience by allowing the Meet-Me conference dialing to be silent without any audible DTMF.
 - This feature depends on Cisco BroadWorks Release 20.0 and works for Xsi calls where a new Xsi API request is used, including the required PINs in the single API request. The client auto-detects the Cisco BroadWorks version to use this feature.
 - Recommended value (default) is true in order to encourage the usage of this feature, but if the configuration parameter is omitted it defaults to false.
 - If set to “true”, the client tries to call Meet-Me without using DTMF, providing the required PINs in the SIP INVITE or Xsi request.
 - Defaults to “false” when the configuration node is omitted.
 - The bridge used must be assigned to the user for the Direct Dial feature to work.
- *Autodetect*
 - If set to “true”, the client tries to find the conference automatically using the Xtended Services Interface.
 - If set to “false”, the user can set it manually. The conference information can be copied and pasted even when *autodetect* is on.

The process for automatic detection of a conference is as follows:

- 1) The client gets all bridges assigned to the user over the Xsi.
- 2) For each bridge found, the client searches for existing conferences using the *Title* parameter as the search criteria, a partial match is sufficient. If several results are found, the first one is selected.
- 3) If no search results are found, the client creates a conference using the bridge ID in the *default-bridge* parameter, the exact value of the *Title* parameter as the title.
- 4) If no active one is found, or no bridge is available, then the automatic detection of a conference fails.

For information on Cisco BroadWorks requirements in relation to Meet-Me bridge auto-provisioning, see the *Cisco BroadWorks Requirements* section in the *UC-One Solution Guide*.

10.9 My Room

10.9.1 Enable My Room

The Communicator Desktop client, through the My Room feature set, provides users access to group chat, audio and/or video conferencing, and Desktop Share. My Room can be enabled and disabled in the configuration file for deployments that do not offer My Room, as shown in the following example.

```
<config version="20">
    <services>
        <rooms enabled="%ENABLE_ROOMS%">
            <myroom enabled="%ENABLE_MYROOM%" />
            <projectrooms enabled="false"
create="false" />
            <default-room-history-
size>%ROOMS_HISTORY_SIZE%</default-room-history-size>
            <conference-bridge
autodetect="%AUTODETECT_CONFERENCE%" title="%CONFERENCE_TITLE%" default-
bridge="%BRIDGE_ID%" direct-dial="%DIRECT_DIAL%" />
            <!-- if true, disable editing of conf
details in preferences and use XSI r
```

Defined as part of the *BroadTouch_Tags*, the tags listed in the following table enable this option. Once enabled, the client shows the *My Room* icon in the left-side pane, just below the presence status flag.

My Room Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_ROOMS%	false	true, false	<rooms enabled="true">	This enables the rooms feature. The default is "false".

My Room Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_MYROOM%	false	true, false	<myroom enabled="true" />	Set to "true" to enable My Room. Set to "false" to disable My Room. The default is "true".
%ROOMS_HISTORY_SIZE%	10	integer	<default-room-history-size>10<default-room-history-size>	The default is "10". However, this parameter does not apply to My Room where the history is "0" for security reasons. It only applies to ad hoc chat rooms.

The following table describes the usage of rooms and My Room tags.

Tag		My Room
%ENABLE_ROOMS %	%ENABLE_MYROOM%	
Value		
false	*	Deactivated
true	false	Deactivated
true	true	Activated

My Room can also be moderated (moderated My Room) but there is no configurability for that feature but Communicator learns server support for it during login. However HTTP messaging needs to be enabled for this feature to fully work. For more information about this feature, see the *Communicator for Desktop User Guide* or the *Communicator (Desktop, Mobile, iOS Tablet, and Android Tablet) Product Guide*.

There is also active talker support in My Room but without configuration parameters. It is based on Xsi-Events.

10.9.2 Guest Client

In previous releases, it was not been possible to join a full Communicator My Room session with a web browser. Guest client support allows this functionality with invitations that can be generated in My Room. Guest client can be enabled using the parameters described in the following example. For requirements on Collaborate and Cisco BroadWorks versions, see the *UC-One Solution Guide*. XMPP must be enabled for the guest client feature to work.

Communicator assumes that all users using guest client join My Room with the JID's domain set to match the configured <guest-client-domain>. Guest client domain therefore cannot be the same as the usual XMPP domain.

Release 22.6.0 introduced a behavioral change using existing configuration parameters, making Communicator auto-accept guest client My Room join requests when "Allow everyone to join automatically" is selected. No server-side changes are required for this.

When moderated My Room is not enabled, the existing guest client auto-accept configuration parameter dictates if guest clients are automatically accepted or not.

For more information about this feature, see the *Communicator (Desktop, Mobile, iOS Tablet, and Android Tablet) Product Guide*.

```

<config version="20">
  <services>
    <myroom enabled="true" >
      <guest-client-support enabled="%GUEST_CLIENT_ENABLE%">
        <guest-client-url>%GUEST_CLIENT_URL%
      </guest-client-url>
      <guest-client-domain>kowabunga-
guest.%GUEST_CLIENT_DOMAIN%
      </guest-client-domain>
      <auto-accept-all></auto-accept-all>
    </guest-client-support>
  </myroom>

```

The following tags, defined in the custom *BroadTouch_Tags* set, are used to enable guest client.

Tag	Default if Omitted	Supported Values	Example	Description
%GUEST_CLIENT_URL%	empty	String	<guest-client-url>https://xsp.do main.com/cgc </guest-client-url>	URL used as a base to generate a link for guest clients to join My Room. When empty, disables the guest client feature.
%GUEST_CLIENT_DOMAIN%	empty	String	<guest-client-domain>guest.do main.com</guest-client-domain>	Used for identifying guest clients. This is their XMPP domain. When empty, disables the guest client feature. In addition, other tags have been used in deployments instead of this, for example, %BW_IMP_SERVICE_NET_ADDRESS-1%.
%GUEST_CLIENT_ENABLE%	false	true, false	<guest-client-support enabled="true">	When set to "true", guest client support is enabled. When set to "false", guest client support is disabled.

Tag	Default if Omitted	Supported Values	Example	Description
%GUEST_CLIENT_AUTO_ACCEPT%	false	true, false	<auto-accept-all enabled="false">	When set to "true", guest client auto-accept support is enabled so that guests automatically join My Room when moderated My Room is not used. When set to "false", guest client auto-accept support is disabled. The feature is not supported in UMS Release 21.0 and must always be set to "false".

NOTE: The *auto-accept* parameter must be kept to "false" in this release as the auto-accept feature for joining guest users is not yet supported.

10.10 Search

10.10.1 Contact Search

The Communicator client automatically and simultaneously searches through its respective contact sources. The Desktop client supports the following contact sources:

- Local contacts (added manually in the client)
- XMPP contact list (created through presence authorization)
- Cisco BroadWorks telephony directory
- LDAP Corporate Directory
- Outlook local address book for Windows only. For the supported versions of Outlook, see the *Communicator (Desktop, Mobile, iOS Tablet, and Android Tablet) Product Guide*.

For LDAP and Outlook search configuration, see the following subsections. For Cisco BroadWorks directory search, see section [10.5.12 Xsi Directory Search, Enable or Disable](#). Search in general must be enabled separately, and in addition to that, each of the search sources must be enabled separately.

10.10.2 LDAP Search

LDAP is used for search operations when the feature is enabled. In the user interface, a search results in the group “Corporate Directory” originating from the LDAP server. Currently, only the Microsoft Active Directory server is supported, but the configuration parameters allow the feature to try other LDAP servers such as OpenLDAP. Only the default values for LDAP have been tested.

First name and last name fields as well as fields with a phone number in the LDAP server are searched, while several other fields can be requested to be present in the results. These fields can be configured using the schema settings described in the following example.

Starting with Release 21.5.0, the format of the credentials sent in the LDAP Bind request is configurable. Before Release 21.5.0, it was always in the form of “userid@domain.com”, where the userid is taken from the *Preferences-Credentials* tab as provided by the end user and domain.com from the LDAP domain parameter.

Starting with Release 21.5.0, when the LDAP domain parameter is empty, only the contents of the preferences *userid* field is used in the LDAP Bind request. This allows using various kinds of formats for LDAP userid, for example, NT4 (domain\userid), UPN (userid@domain.com), or Bind (cn=User Fullname,ou=name,dc=domain,dc=com) styles.

More detailed descriptions of the *domain-name* parameter follow.

Release 22.0.1 introduced support for LDAP credentials in the configuration file. When LDAP credentials are present in the configuration file, the preferences LDAP credentials section is hidden.

Release 22.5.2 introduced support for new attributes for few search-location values to control whether the wildcard-character (asterisk) is appended or prepended to the searched value:

```
omit-preceding-wildcards="true"
omit-succeeding-wildcards="true"
```

The search-locations in the following list also support these new controls:

```
MobilePhone
WorkPhone
```

Example

```
<ldap-schema-entry ldap-attr="mobile">
<query search-location="MobilePhone"
omit-preceding-wildcards="true"
omit-succeeding-wildcards="true" />
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="telephoneNumber">
<query search-location="WorkPhone"
omit-preceding-wildcards="true"
omit-succeeding-wildcards="true"/>
</ldap-schema-entry>
```

It is important to notice that when these attributes are set to “true”, the search results from LDAP might not match the search results from Xsi. These are intended to be used only in special cases when LDAP-structure is inefficient.

For more information on LDAP server certificate validation and DNS, see section [10.16.10 LDAP Certificate Validation](#).

Release 22.9.2 introduced sorting parameters for LDAP to cater to some deployments.

The following example provides information to enable an LDAP search.

```

<config version="20">
  <services>
    <search enabled="true">
      <ldap-search enabled="%ENABLE_LDAP_SEARCH%"/>
    ..
  </services>

  <protocols>
  ..
    <ldap>
      <server name="ldap">
        <uri>%LDAP_SERVER_URI%</uri>
        <port>%LDAP_SERVER_PORT%</port>
        <base-object>%LDAP_BASE_OBJECT%</base-object>
        <object-
filter>(objectClass=user) (objectCategory=person)</object-filter>
        <protocol>%LDAP_PROTOCOL_VERSION%</protocol>
        <security>
          <tls enabled=="true"/>
        </security>
        <authentication use="%LDAP_AUTHENTICATION%">
          <domain-name>%LDAP_DOMAIN%</domain-name>
        <method>SASL</method>
        </authentication>
        <credentials>
          <username>user@domain.com</username>
          <password>lpqotr fuhwepfiböjwpobj</password>
        </credentials>
        <sorting enabled="%ENABLE_LDAP_SORTING
">
          <sort-control
enabled="%ENABLE_LDAP_SORT_CONTROL%"> </sort-control>
        </sorting>
        <schema name="schema-name">
          <ldap-schema-entry ldap-attr="displayName">
            <query search-location="FullName"/>
          </ldap-schema-entry>
          <ldap-schema-entry ldap-attr="givenName">
            <query search-location="FirstName"/>
          </ldap-schema-entry>
          <ldap-schema-entry ldap-attr="l">
            <query search-location="City"/>
          </ldap-schema-entry>
          <ldap-schema-entry ldap-attr="mail">
            <query search-location="Email"/>

```

```

</ldap-schema-entry>
<ldap-schema-entry ldap-attr="postalCode">
  <query search-location="postalCode"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="sn">
  <query search-location="LastName"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="streetAddress">
  <query search-location="street"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="st">
  <query search-location="Country"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="mobile">
  <query search-location="MobilePhone"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="telephoneNumber">
  <query search-location="WorkPhone"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="telexNumber">
  <query search-location="Extension"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="hphone">
  <query search-location="HomePhone"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="confphone">
  <query search-location="ConfNumber"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="confid">
  <query search-location="ConfID"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="securitypin">
  <query search-location="SecurityPin"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="weburl">
  <query search-location="Web"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="collab">
  <query search-location="collabroom"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="imp">
  <query search-location="IMPID"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="departmentNumber">
  <query search-location="Department"/>
</ldap-schema-entry>
<ldap-schema-entry ldap-attr="title">
  <query search-location="Title"/>
</ldap-schema-entry>
</schema>
</server>
</ldap>

```

The LDAP Corporate Directory search is enabled through the tag identified in the following table. When enabling the Desktop client, the user interface lists all search results (matches found in the configured LDAP server) against its *Corporate Directory* contact category.

The following tags, in the custom *BroadTouch_Tags* set, are used to control LDAP search. Note that leaving a parameter value empty results in an invalid configuration (except for the security and domain nodes).

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_LDAP_SEARCH%	false	false, true	<ldap-search enabled="true"/>	When set to "false", LDAP search is disabled. When set to "true", LDAP search is enabled.
%LDAP_SERVER_URI%	empty (invalid)	string	<uri>example.com</uri>	LDAP server URI. A valid URI is needed for a working LDAP connection.
%LDAP_SERVER_PORT%	389	number	<port>389</port>	LDAP server port.
%LDAP_BASE_OBJECT%	empty (invalid)	string	<base-object>DC=example,DC=com</base-object>	The name of the LDAP base-object entry (or possibly the root) relative to the search that is to be performed. Valid base-object is needed for a working LDAP search. Currently, only domain component (DC) parameters have been tested. Must match LDAP server provisioning for search operations to succeed.
%LDAP_PROTOCOL_VERSION%	empty	2, 3	<protocol>3</protocol>	LDAP protocol version used. Version 3 is recommended for faster error handling.
%LDAP_AUTHENTICATION%	no	yes, no	<authentication use="yes">	Set to "no" to disable LDAP authentication. Set to "yes" to enable LDAP authentication.
%LDAP_DOMAIN%	empty	string	<domain-name>example.com</domain-name>	Contents of the LDAP username domain part. See the preceding section for details about when this is left empty.

Tag	Default if Omitted	Supported Values	Example	Description
%LDAP_USERNAME%	empty	String	<username>user@domain.com</username>	LDAP username.
%LDAP_PASSWORD%	empty	string	<password>1pqrtrfuhwepfiböjwpobj</password>	LDAP password.
%ENABLE_TLS%	false	true, false Any other value defaults to "true".	<tls enabled="true"/>	Set to "false" to disable LDAP over TLS. Set to "true" to enable LDAP over TLS.
%ENABLE_LDAP_SORTING%	true	true, false	<sorting enabled="true">	Set to "true" to enable LDAP result sorting, which is required in certain deployments. Set to "false" to disable overall LDAP result sorting.
%ENABLE_LDAP_SORT_CONTROL%	true	true, false	<sort-control enabled="true" />	Set to "true" to enable sort-control in the search request with sn and givenName hard-coded. Additionally, ldap sorting must be enabled for sort-control to work. Set to "false" to disable sort-control in the search request, in this case, sorting takes place on the client side. However, client-side sorting is not implemented in this release.

The LDAP configuration parameters are of the following main categories:

- Enable LDAP search. This is done in the search section.
- Server parameters – Specify the LDAP server to which the client connects:
 - *URI* – Server address.
 - *Port* – Port to be used.

- *Object-filter* – Object filters limit values to actual persons. In general, it is not recommended that it be changed in this release. However, small changes can be done as long as the LDAP server supports the configuration and the returned objects are persons. The *object-filter* parameter is not the final LDAP search query *object-filter*, but it is used to create it based on the actual search string that the end user provided in the UI. If objects are defined in the *object-filter* node, they are combined with an AND operation with the end-user provided search string in the actual *object-filter* of the search query towards the LDAP server. The search string is looked up in several fields in the LDAP server. In the actual LDAP search operation, the searched fields are combined with an OR operation. For instance, if only person *objectClass* is configured in the *object-filter* and the end user searched for “1234”, the following *object-filter* would be used in the actual LDAP search query when the schema only has telephone number and mobile number:

Filter: (&(objectClass=person)((telephoneNumber=1234*)(mobile=1234*))).

Specifically, operators like AND or OR cannot be used in the *object-filter* configuration node.
- *Base-object* – The name of the LDAP base-object entry (or possibly the root) relative to the search that is to be performed. Currently only the domain component (DC) parameters have been tested. It is needed to have base objects defined in the configuration that match the provisioning of the records done on the LDAP server side.
- *Protocol* – The supported values are “2” or “3”. This corresponds to LDAPv2 and LDAPv3. In the past, this has been required, for example, to handle special characters like “ä”.
- *Security* – Only “tls” is currently supported. “Kerberos” and “ssl” are not supported.
- *Authentication* – Only the SASL parameter value is currently supported; however, the actual implementation uses SIMPLE mechanism with octet password. In addition, authentication must be enabled for LDAP search to work.
- *Credentials* – Username and password can be provided in configuration. When provided, the preferences LDAP credentials section is hidden.
- *Domain-name* – The value of this parameter is appended to the username provided in preferences if that does not have a domain part. If the username provided in preferences has a domain part, it will also be used for LDAP search queries.
- *Sorting* – Defines if the server is requested to do sorting and if client-side sorting is enabled.
- **Schema settings** – Specifies the LDAP server fields retrieved in searches. It consists of many LDAP schema entries, where the *ldap-attr* is the attribute name used in the reply that the server sends for the search and refers to the field in the LDAP server. An *ldap-attr* in the configuration means that the client needs this attribute (from the server) for the contact. The *search-location* parameter is used for internally mapping the LDAP attribute to the corresponding contact property inside the client. Multi-value attributes are not supported; instead, the last received one is used. The *ldap-attr* cannot currently be empty for *firstname* or *lastname* fields. However, for other fields, it can be left empty. This causes that parameter to be ignored. In principle, any server field can be mapped to any client field using these two configuration parameters (*ldap-attr* for the server and *search-location* for client).

Schema parameters also have one Device Management tag. For more information on Device Management, see the *UC-One Solution Guide*.

The schema has been updated by removing redundant parts to have only the *ldap-attr* and *search-location*.

10.11 Outlook Integration

Release 10.0.1 introduced two integration points to Outlook. Outlook integration is supported on Windows. The client supports the Outlook search for Contact discovery. However, searching Outlook will not return Distribution List objects (Contact Groups) or contacts without any communications capabilities (phone number or email address). There is no hard-coded limit to the Outlook Address Book size although at some point delays will increase, a local address book with at least 500 Outlook contacts can be searched. Outlook integration is enabled as follows.

```
<config version="20">
    <services>
        <search enabled="true">
            <outlook-search
enabled="%ENABLE_OUTLOOK_SEARCH%" />
        </search>
    </services>
</config>
```

Outlook search also works when several Outlook accounts are in use, but only one account is used at a time (default selected, which can be changed in Outlook).

Additionally, there are other related considerations as follows:

- The client searches for Contacts and Calendar entries in the default Outlook account. The account is set to the default via *File* → *Info* (left pane) → *Account Settings* → *Account Settings* → *Data Files*. Select an account and mark it as "Set as Default". After making this change, sign out and sign back into the client and it now searches that account for Contacts and Calendar entries.
- For some users, the client shows Outlook's proprietary Access/Deny security pop-up. This is triggered every 30 minutes when trying to read Outlook contacts and putting them into the client's local cache. This Outlook security pop-up is triggered when the customer's computer does not have anti-virus software installed or if it is not up to date with the latest virus definitions. For some users, it is possible to disable the Outlook security pop-ups in the Trust Center. These Outlook pop-ups should no longer be seen in Release 20.0.0 and later.
- The client searches the Outlook contacts only on the local machine (that is, the Outlook Address Book). There is no Exchange server lookup performed. In addition, all directories in Outlook are searched for contacts, even deleted folders. The Contacts directory can also have multiple levels of subfolders. With Office 365, the search operation may end up to the cloud server.

Note that if local caching is disabled in Outlook, searching can be slow.

Starting with Release 10.0.4, Communicator supports integration with Outlook's Calendar so that appointments trigger automated presence state changes. This is configured as follows.

```
<config version="20">
    <services>
        <outlook-calendar-presence
enabled="%ENABLE_OUTLOOK_CALENDAR_PRESENCE%" />
    </services>
</config>
```

If a user has multiple Outlook profiles and *Control Panel* → *Mail* → *Show Profiles* → *Prompt for a profile to be used* is set. Then the client asks for the profile selection every minute when trying to check the Calendar entry; however, this only happens when Outlook is not running. In other cases, no profile selection pop-up is shown, and the client works as expected.

An Outlook local address book search is independently controlled through the tag identified in the following table.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_OUTLOOK_SEARCH%	false	false, true	<outlook-search enabled="true" />	When set to "false", Outlook search is disabled. When set to "true", Outlook search is enabled.

The tag in the following table is used to enable Calendar presence. Using it requires presence to be enabled.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_OUTLOOK_CALENDAR_PRESENCE%	false	false, true	<outlook-calendar-presence enabled="true" />	When set to "false", calendar presence is disabled. When set to "true", calendar presence is enabled.

Integration is supported for Windows-only Desktop clients. For the supported versions of Microsoft Outlook, see the *Communicator (Desktop, Mobile, iOS Tablet, and Android Tablet) Product Guide* or the *Communicator for Desktop User Guide*.

10.12 Outlook – Plugin

Starting with Release 21.5.0, the Outlook Plugin is also installed using the standard Desktop client installation package. Starting in Release 22.9, a separate DLL file is no longer used so the plugin is not visible on the Outlook Add-in list. The installers are available on cisco.com (as a zip file) from the software download area.

Release 22.9.2 added support for a revised user experience (UX) whereby the right-click menus are removed in favor of hovering actions and buttons. For more information and examples of the user experience, see the *Communicator for Desktop User Guide*. To avoid side effects, it is not a supported deployment model to install and run Release 22.9 clients while keeping the earlier client versions as well. The Release 22.9 version should replace the older version.

There is no configuration option for this feature; instead, it must be enabled while branding. For more information, see the *Communicator for Desktop Branding Guide*. Note that Outlook Add-in installation requires administrator rights. For Outlook Add-in platform requirements, see the *Communicator for Desktop User Guide*.

Once installed, the Add-in enables Outlook to display the presence status for the user's Desktop client contacts, and allows the user to invoke the following click-to-communicate functions in Outlook:

- Chat

- Call from computer
- Call from phone
- Video call

For more information, see the *Communicator for Desktop User Guide*. DNS must also be provisioned for localhost.uccclient.net to resolve to 127.0.0.1. For more information, see the *UC-One Solution Guide*.

NOTE: For an optimal user experience, the Outlook privacy option must be used to disable security notifications.

Release 22.3.0 introduced a new feature to allow the end user to also make PSTN calls from Outlook via UC-One and have S4B or UC-One presence in Outlook.

For this, a new configuration parameter was introduced to specify the presence source for Outlook Add-in, either S4B or Communicator. This is in conjunction of the single installer for S4B integration and Outlook Add-in. This parameter also dictates how other functionality is performed in Outlook Add-in as follows:

- Calling SIP addresses from Outlook Add-in is done either using S4B or Communicator.
- Chat is done either using S4B or Communicator.

PSTN calls are however always done using Communicator, and not S4B.

Example for configuration

```
<config version="20">
  <services>
    <outlook-presence-source name="%OUTLOOK_PRESENCE_SOURCE%"/>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, is used to control the Outlook Add-in presence source.

Tag	Default if Omitted	Supported Values	Example	Description
%OUTLOOK_PRESENCE_SOURCE%	See the table that follows.	s4b, communicator or	<outlook-presence-source name="s4b"/>	When set to "s4b", Outlook Add-in presence, SIP calling, and chat come from S4B. When set to "communicator", Outlook Add-in presence, chat, and SIP calling come from UC-One Communicator.

Package	Config File Value for Outlook-presence-Value	Outlook Add-in Presence Source
Lync and Outlook Add-in enabled	<outlook-presence-source name="communicator"/>	Communicator
Lync and Outlook Add-in enabled	<outlook-presence-source name="s4b"/>	S4b

Package	Config File Value for Outlook-presence-Value	Outlook Add-in Presence Source
Lync and Outlook Add-in enabled	<outlook-presence-source name=""/>	S4b
Lync and Outlook Add-in enabled	Without configuration node	S4b
Only Outlook Add-in enabled	<outlook-presence-source name="communicator"/>	Communicator
Only Outlook Add-in enabled	<outlook-presence-source name="s4b"/>	S4b
Only Outlook Add-in enabled	<outlook-presence-source name=""/>	Communicator
Only Outlook Add-in enabled	Without configuration node	Communicator

10.13 UC-One Hub Integration

Release 22.0.0 introduced support for UC-One Hub and the related banner and contextual gadget. UC-One Hub is the special functionality that allows the UC-One client to be extensible and provides customers with the ability to better integrate the client into their business processes.

UC-One Hub integrates UC-One real-time communications with cloud applications by allowing users to stay inside UC-One to also access cloud applications. For this purpose, the Hub banner in the bottom of the *Main* window allows viewing content from other applications inside the *Main* window. Additionally, contextual intelligence is supported using the contextual gadget to display related data from configured applications when chat view is opened.

In terms of the user experience (UX), this feature also adds a new Hub button next to the existing web button in the left pane and a Hub banner instead of the existing banner in the bottom of the *Main* window as well as a contextual gadget to the far right in the *Main* window. The order of the Hub button in the left-side button navigation bar, the display, and URL of the Hub button, Hub banner, and contextual gadget are configured as in the following example.

In general, the following configuration logic is applied:

- The whole Hub feature is disabled by setting `uchub enabled=false`, and when enabled, the `hub-button` must also be enabled and have a URL.
- Other sub-features can be disabled individually using the `enabled` attribute.
- Token-based authentication for Hub signaling is enabled by defining the login URL. Communicator gets the token from Xsp; therefore, the Cisco BroadWorks version that is used must also support login token.

```
<services>
  <uchub
    enabled="%ENABLE_HUB%"
    login_url="%HUB_LOGIN_URL%"
    <hub-button
      enabled="%ENABLE_HUB_BUTTON%"
      url="%HUB_BUTTON_URL%" />
    <hub-banner
      enabled="%ENABLE_HUB_BANNER%"
      url="%HUB_BANNER_URL%"
      height="%HUB_BANNER_HEIGHT%" />
```

```

<contextual-gadget
  enabled="%ENABLE_CONTEXTUAL_GADGET%"
  url="%CONTEXTUAL_GADGET_URL%"/>
<hub-analytics
  enabled="%ENABLE_HUB_ANALYTICS%"
  serviceproviderid="%HUB_ANALYTICS_SERVICE_PROVIDERID%"
  resellerid="%HUB_ANALYTICS_RESELLERID%"
  companyid="%HUB_ANALYTICS_COMPANYID%" />
</uchub>

```

See the following table for the related DM tags.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_HUB%	false	true, false	<uchub enabled="true"	Set to "true" to enable the login dialog. Set to "false" to disable the login dialog.
%HUB_LOGIN_URL%	false	string	login_url="https://domain.com"	This URL is used to enable token-based authentication for the URL for the Hub feature.
%ENABLE_HUB_BANNER%	false	true, false	enabled="true"	Set to "true" to enable the Hub banner. Set to "false" to disable the Hub banner.
%HUB_BANNER_HEIGHT%	40	40 to 240	height="50"	This is used to set the height of the Hub banner with a minimum of 40px and a maximum of 240px. A value below 40 is considered as 40 and a value above is considered as 240. Any other invalid values are considered as 40.
%HUB_BANNER_URL%	empty	Allowed values are valid http/https URL or empty ("").	url="https://labs.com/app/notifications?xsp=%(xsp)&id=%(BWUserID)&password=%(Password)"	This links to the actual URL used for the Hub banner URL.
%ENABLE_HUB_BUTTON%	false	true, false	encode="true"	Set to "true" to enable the Hub button. Set to "false" to disable the Hub button.

Tag	Default if Omitted	Supported Values	Example	Description
%HUB_BUTTON_URL%	empty	Allowed values are valid http/https URL or empty ("").	url="http://domain.com"	This links to the actual URL used for the Hub button URL.
%ENABLE_CONTEXTUAL_GADGET%	false	true, false	<contextual-gadget enabled="true"	Set to "true" to enable the contextual gadget. Set to "false" to disable the contextual gadget.
%CONTEXTUAL_GADGET_URL%	empty	Allowed values are valid http/https URL or empty (""). Any other values are considered as empty.	url="https://labs.com/app/contextual?xsp=%(xsp)∓id=%(BWUserID)&password=%(Password)"	This links to the actual URL used for the contextual gadget.

10.14 Google Analytics

Release 22.2.0 introduced support for Google Analytics in the UC-One client in addition to the previously supported Hub Analytics. The configuration parameter and related DM tag in the following example are used to enable client-side analytics. This parameter is independent of the Hub Analytics parameter depicted in more detail in section [10.13 UC-One Hub Integration](#).

If either Hub Analytics or UC-One client analytics are enabled, sending data from UC-One is enabled. However, the end user can enable or disable sending of analytics data in *Preferences*. In addition, Google Analytics can also be enabled and disabled in branding. For more information, see the *Communicator for Desktop Branding Guide*. For more information on the general process for enabling Google analytics, see the *UC-One Google Analytics Client Reference Guide*.

```
<services>
  <analytics enabled="%ENABLE_ANALYTICS_DESKTOP%" />
```

See the following table for details on the DM tag.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_ANALYTICS_DESKTOP%	False (only if the whole node omits, having "" defaults to true)	false, true	<analytics_enabled="true" />	When set to "false", UC-One client analytics is disabled. When set to "true", UC-One client analytics is enabled.

10.15 Communicator Packages and Device Management

10.15.1 Packages

Communicator has five different packages, each enabled by a separate combination of parameters. This section also shows the Device Management (DM) template tags used for each package.

Through the corresponding tags defined in the *BroadTouch_Tags* set, each of the communication services provided through Communicator – Audio, Video, and Instant Messaging & Presence (or chat) can be independently controlled. Consequently, the following service packages can be created:

- Instant Messaging and Presence (IM&P) only
- Audio only
- IM&P + Audio
- Audio + Video
- IM&P + Audio + Video
- Xtended Services only (default package)
- Presence + Audio
- Presence + Video

Notably, features associated with the Xtended Services package use the Xsi. By default, this package is a sub-package of all service packages. Therefore, the following Xtended Services package features are inherent to all service packages by default:

- Call logs
- Directory search (local contacts can be added, modified, and deleted)
- Service Management (Call Settings)
- Click To Dial

Service packages can be configured as shown in the following table. Note that turning off calls does not disable SIP. For more information on SIP settings and instructions on how to disable SIP, see section [10.1.1 Change Basic SIP Server Settings](#). For more information on telephony presence-related configuration details and the Xsi-Only package, see section [10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence](#). For audio and video call button enablement in the UI, see section [10.1.5 Enable SIP Audio and Video Calls](#). For basic XMPP settings, see section [10.3.1 Use Extensible Messaging and Presence Protocol](#). For enabling chat, see section [10.3.6 Chat](#). For enabling presence, see section [10.3.8 Presence and Automated Presence](#).

Note that for presence without chat packages, share and My Room must be disabled.

NOTE: The client device type is associated with the tag set; therefore, once a service package is provisioned, it applies to all client users through their assigned device type.

Service Package	IM&P	Audio	IM&P + Audio	Audio + Video	IM&P + Audio + Video	Xtended Services	Presence + Audio	Presence + Video
Tag	Value							
%ENABLE_AUDIO CALLS%	false	true	true	true	true	false	true	true
%ENABLE_CHAT %	true	false	true	false	true	false	false	false
%ENABLE_PRESENCE%	true	false	true	false	true	false	true	true
%ENABLE_VIDEO CALLS%	false	false	false	true	true	false	false	true
%ENABLE_XMPP %	true	false	true	false	true	false	true	true
%ENABLE_WEBCOLLAB%	true	false	true	false	true	false	false	false
%ENABLE_MY_ROOM%	true	false	true	false	true	false	false	false

10.15.2 Xsi-Only Deployments Without SCA

When deploying Communicator as a basic click-to-call application, it may be beneficial to be able to deploy Communicator without the use of the Cisco BroadWorks Shared Call Appearance (SCA) feature. For more information regarding configuration file creation, license, and service assignment as well as provisioning steps for this deployment model, see the *UC-One Solution Guide*.

In this configuration, only the following functionality is available by default:

- Click To Dial with call control
- Directory search
- Basic call logs
- Call Settings
- Configurable web button
- Contact list (not synchronized across devices)

For instructions on how to enable/disable features, see the corresponding sections in this document.

For a high-level overview of deployment packages, see section 4 in the *Communicator (Desktop, Mobile, iOS Tablet, and Android Tablet) Product Guide*.

10.15.3 Partial Match Enhancements for Device Type Selection

To allow increased flexibility when selecting functionality packages for user groups or individual users, Release 21.6.0 introduced support for a (first) partial match in the device profile type selection. This allows customers to use different device types without making a new branded build as previously required.

The general Device Management procedure specifies that the Cisco BroadWorks Application Server provides a UC-One Device Profile Type. The default is named “Business Communicator – PC”. A Device Profile of “Business Communicator – PC” can be created and assigned to the user. The Application Server then builds a configuration file and stores it on the Profile Server.

At login, Communicator queries the assigned device list via Xsi and, in previous releases, performs an exact match search for “Business Communicator – PC”.

Communicator uses the device profile configuration data (configuration file) associated with this device profile to enable and disable various features.

The enhancement introduced with Release 21.6.0 is that a partial match for the device profile type is done instead of an exact match. Communicator uses the first matching device profile type it finds from the device list XML it receives as a result of the device list Xsi query at login that contains “Business Communicator – PC” in the very beginning of the device profile type string.

This allows the same client executable to be used with various device profile types, so the service provider can change feature packages for individual users or groups of users by just changing the device profile type in DM for a user or group of users.

For instance, the service provider could have any number of device profile types based on user roles, such as “Business Communicator – PC Basic”, “Business Communicator – PC Executive”, or “Business Communicator – PC Assistant” and change the functionality available for individual users by just changing the device profile type for them.

Note that it is not expected to have many matching device profile types in the received device list XML but only one.

This approach also allows flexibility regarding the number of DM tags and they could have different configuration file templates, for example:

- Configuration file with custom tags definitions:
 - Contains dynamic tags (%BW-x% tags) and custom tags.
- Configuration file with default parameter values:
 - Contains dynamic tags and minimal custom tags; all other parameters are defined with default values within in the configuration file.

This way, the service provider can define what parameters they want to expose using custom tags.

10.15.4 Forced DM Configuration File Update

Starting with Release 22.5.0, forced DM configuration file update is supported, allowing deployments to more easily, for example, introduce new features that require configuration changes.

Communicator periodically re-downloads the DM configuration file and compares it with the file it already has. If the file has been updated, Communicator shows a pop-up to the end user where restart or ignore options are presented. If there are ongoing calls, group chats, or share sessions, re-login is not done.

Periodic re-download of the DM configuration file is done based on the time interval specified in the automatic upgrade feature. For more information on automatic upgrade, see section [13 Version Control and Automatic Upgrade](#).

Example for configuration:

```
<config version="20">
  <services>
    <auto-reconfigure enabled="%ENABLE_AUTOMATIC_RECONFIGURE_DESKTOP%"
  />
```

The following tag, in the custom *BroadTouch_Tags* set, is used to control the capability.

Tag	Default if Omitted	Supported Values	Example	Description
ENABLE_AUTOMATIC_RECONFIGURE_DESKTOP	false	true, false	<auto-reconfigure enabled="true" />	When set to "true", forced DM file update is enabled. When set to "false", forced DM file update is disabled.

10.16 Security

10.16.1 Pinned SSL Certificate in Client

The UC-One client uses SSL certificate internally for secured communication with other related internal processes. This certificate has validity priority of maximum eight months to one year after the client release. After this period has passed, some of the UC-One client functionality may not work correctly. For example, Client login via SSO, Calling, Messaging, Outlook plugin, and S4B plugin may be implicitly affected by the SSL internal certificate expiry issue.

Clients must be upgraded before this pinned SSL certificate expiry date, and there will be a warning pop-up message shown before configured number of days, which can be configured in the DM config file as follows.

```
<config>
<services>
<internal-cert-expiry-notification enabled="true"
warn-before-days= "90"
warn-frequency-days = "7"/>
```

The default values are shown in the above xml, if this tag is ignored.

10.16.2 Installer Certificates

Communicator installer version 22.7.0 uses certificate issued to "Cisco, Inc.". Previous application releases used certificates issued to "BroadSoft Inc.". Therefore, automatic upgrades directly from client versions earlier than 22.5.5 and 22.6.1 is not possible due to security checks. The earlier Communicator versions demand that the installed version and upgraded versions are signed with the same certificate. The future proofing fixes in 22.5.4 and 22.6.1 are required intermediate upgrade steps prior to automatically upgrading to 22.7.0. If manual client installation is possible, there are no similar limitations.

10.16.3 SSL/TLS Certificates

In general, SSL/TLS Certificates bind together:

- A domain name, server name, or host name. For Communicator, the host name is typically used on the server side.
- An organizational identity (that is, the company name) and location.

In Communicator, only server-side TLS certificates are used. TLS 1.2 is supported, but since Release 21.3, Communicator denies SSLv3 connections that do not upgrade to TLS. This is done to authenticate the server to the client while the username and password are used to authenticate the client to the server so that mutual authentication is achieved. SIP, XMPP, Share, and HTTP use the same SSL Library internally for checking the certificates (CiscoSSL).

SSL certificates must be issued from a trusted Certificate Authority's (CA) Root Certificate. Self-signed certificates are not accepted, and the certificate verification chain must be intact when chained certificates are used. Wild-carded certificates can be used.

However, self-signed certificates can be used in the verification chain.

Certificate validation Common Name (CN) is supported for the certificate validation. If the CN of the certificate does not match the CN of the domain to which the client is connected, validation fails. Release 22.1.0 also added a new branding parameter that makes the configured domain to be used for TLS certificate validation instead of the connected-to domain for SIP, Xsi, and Share. XMPP remains configurable both ways as before. Release 22.7.0 uses the more secure certificate validation branding option by default. For more information about the branding parameter, see the *UC-One Branding Guide*.

SSL certificate SAN is also supported in this release for Xsi, SIP, XMPP, and Sharing Server (USS). For more information, see the sections that follow.

For Xsi, if the configured URL is not branded to be used for certificate validation, and if the DM URL is `xsp.domain.com` is redirected to `xsp1.domain.com` and `xsp2.domain.com` for redundancy, then the certificate must match either `xsp1.domain.com` or `xsp2.domain.com` since the connection is set up to use those addresses. The same principle also applies to SIP and XMPP.

Release 22.7 added support Server Name Indication (SNI) for Transport Layer Security (TLS) certificate validation in TLS. Release 22.9.8 changed the Sharing Server (USS) behavior so that the SNI is populated with the resolved server URL when safer certificate validation is used to align with industry load balancing practices. For other protocols, the configured server URL is placed into the SNI. When safer certificate validation is not used, the connected-to server URL is placed on the SNI.

For the safest certificate validation option for other protocols than USS, see the following figure.

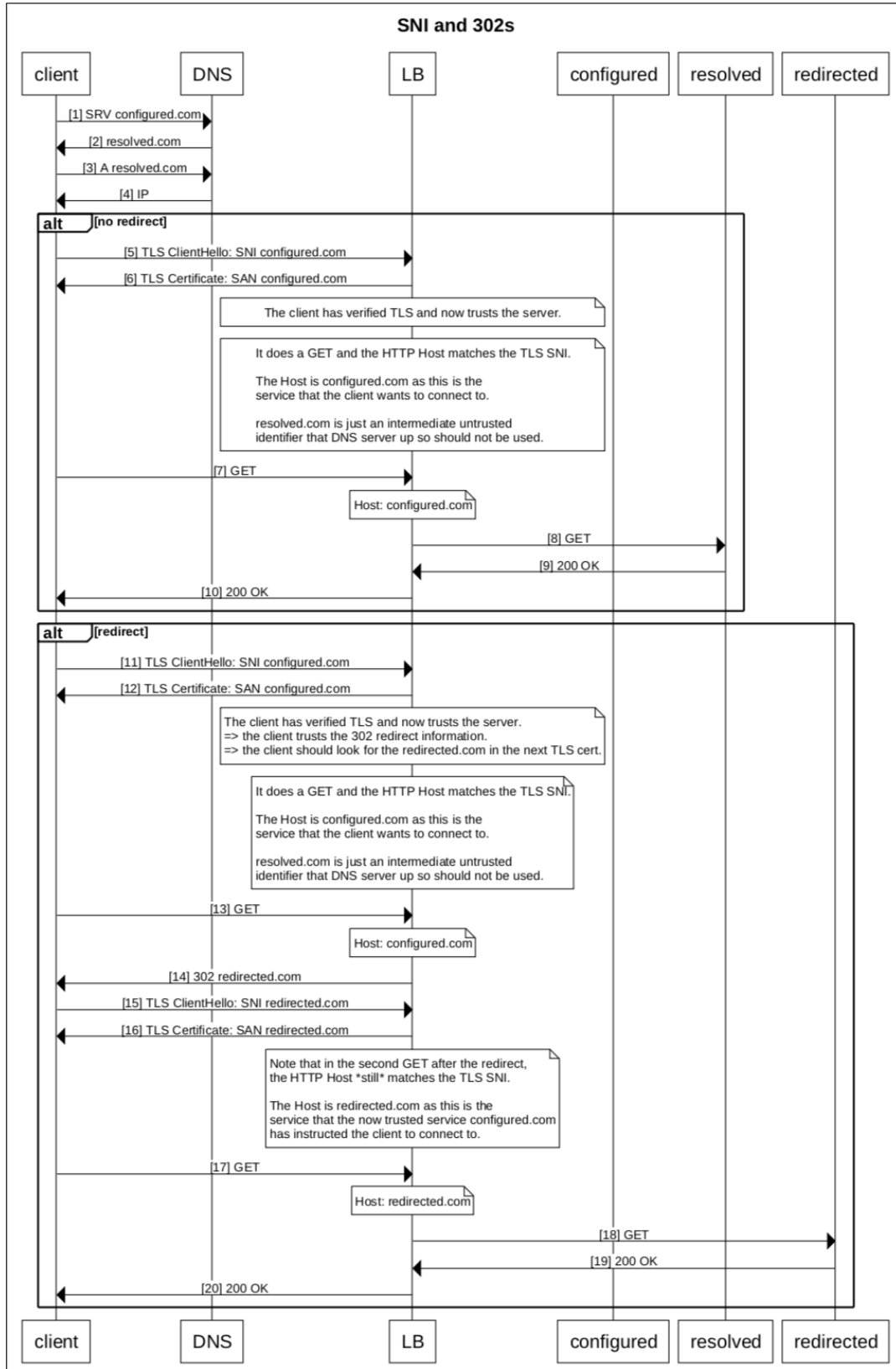


Figure 6 SNI and TLS Certificate Validation

TLS certificate validation specifics with related DNS operations are slightly different for each protocol and described in more detail in the corresponding protocol sections:

- For Sharing Server certificate handling, see section [10.16.9 Sharing Server \(USS\) Certificate Validation](#).
- For XMPP and Messaging Server (UMS) HTTP certificate handling, see section [10.16.8 XMPP SRV Support and Certificate Validation](#). This section also contains some examples of XMPP domains, SRV, and certificate validation on the XMPP side.
- For SIP certificate handling, see section [10.16.5 SIP TLS Certificate Validation](#).
- For HTTP Messaging certificate handling, see section [10.16.7 Messaging API SRV Support and Certificate Validation](#).
- For Xsi certificate handling, see section [10.16.6 Xtended Service Interface TLS Certificate Validation](#).
- For LDAP certificate handling, see section [10.16.10 LDAP Certificate Validation](#).

The differences in certificate validation is related to whether the final connected-to server address used for validation or not (related to DNS SRV address resolution).

A potential tool to validate a secure URL for HTTP is available at <https://www.sslshopper.com/ssl-checker.html>

or

<https://www.digicert.com/help/>

This tool takes, for example the login URL, as input and checks the validity of the SSL certificate. If the certificate passes this test, then it should be accepted by the Release 10.0.4 and later Communicator clients. If the certificate does not pass the validity test of the SSL Library, login fails.

In general, the certificate verification process for each protocol is the following (a separate certificate may be needed for different protocols depending on the domains):

- Server administration purchases a server certificate that is signed by a well-known CA.
- Client tries to contact the server at x.domain.com, and as part of TLS setup, downloads the certificate tied with *.domain.com (CN field in the certificate or even SAN field equals *.domain.com). Typically, the client can also download chained intermediate certificates that can be used to verify the server certificate. Intermediate certificates may also exist in the local OS certificate store of the desktop machine, so in one way or another they must be obtained on client side. In this case, the verification chain must be intact for the connection setup to succeed. On Mac OS, the root certificate must be in the end of the chain for verification to succeed. The certificate chain can be checked also using the certificate check web site previously listed. Note that the site may not detect out of order certificate chains, so it is sometimes beneficial to run OpenSSL from the command line to see the certificate chain issues (the following configured DM URL would be server.domain.com and the TLS port here would be 443):

```
openssl s_client -showcerts -connect server.domain.com:443
```

- Client applications have access to root certificates from some trusted source. For Communicator, the OS holds a list of CA root certificates. The list is maintained by OS updates and in exceptional cases manually (can be viewed in the keychain app on Mac OS for instance).

- Communicator uses the openssl SSL Library, which accesses the OS certificate store to get the root certificates needed to verify the server certificate. The SSL Library uses the root CA certificate from OS to verify the CA signature on the server certificate, as part of the required checks before establishing a secure connection.
- If verification succeeds, then the TLS connection is setup; otherwise, an error message is printed onto the *UCOneLog.log* file, indicating what kind of an error prevented TLS setup.

The following figure depicts this process.

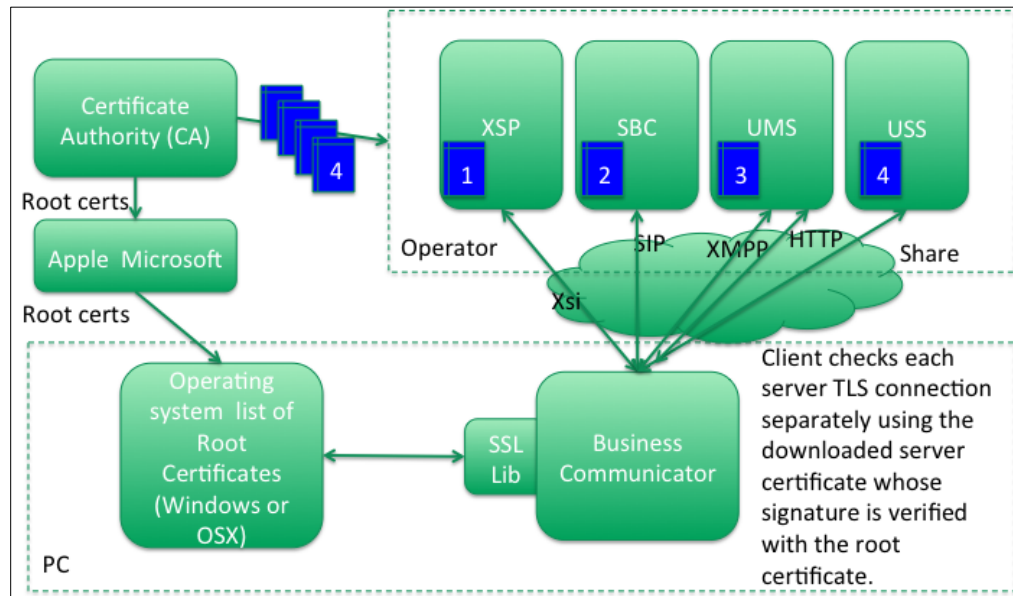


Figure 7 TLS Certificate Verification

The following TLS options are supported in negotiation:

- TLS 1.1
- Secure renegotiation
- Session tickets

TLS compression is not supported.

10.16.4 SIP Over TLS and Secure Real-time Transport Protocol

The Communicator Desktop client can be configured to use SIP signaling over TLS and Secure Real-time Transport Protocol (SRTP) for media encryption. However, these features must be enabled in the configuration as shown in the following example. Note also that when dynamic SIP proxy discovery is used, DNS SRV priorities override static parameters such as this one, and non-TLS transport is used if it has a higher priority in DNS SRV. For more information on dynamic SIP proxy discovery, see section [10.1.4 Dynamic SIP Proxy Discovery](#).

When dynamic proxy discovery is not used, enabling TLS for SIP takes it into use.

For details on SIP port and transport protocol recommendations when SIP ALGs are used in the network, see the *UC-One Solution Guide*.

```
<config>
    <protocols>
        <sip>
            <secure>%USE_TLS%</secure> <!-- if true
use TLS for SIP-->
```

Note that the certificate used must be valid. Furthermore, the certificate chain must be intact so that the intermediate certificate is also linked. It is recommended that a widely used certificate be employed so that is already present, by default, in the desktop devices. It is also possible to add certificates locally on the desktop machine either manually or by using bulk provisioning, although this is not typically done.

To enable the related SRTP for media encryption, there is a separate setting.

In addition to RTP, RTCP traffic can be secured with the same mechanisms as RTP using the preceding configuration.

For SIP/TLS ciphers, see [Appendix A: TLS Ciphers](#).

The SRTP is used to provide security for the media stream in three different aspects:

- Confidentiality (data is encrypted)
- Authentication (assurance of the identity of the other party or parties)
- Integrity (measures against, for example, replay attacks)

The current version of the media framework supports AES 128 Counter Mode for protection and Hash Message Authentication Code (HMAC)-SHA-1 for authentication. The master key size is 16 bytes and master salt is 14 bytes.

The media framework supports both the full (80-bit) and short (32-bit) authentication tag. Communicator exchanges the keys inside the SDP as part of SIP signaling, both sides of the call send the key they use to the other side.

SRTP can be enabled using the configuration shown in the following example. The current implementation uses only the SDP secure RTP profile and supports multiline SDP for Audio Visual Profile (AVP) and Secure Audio Visual profile (SAVP) entries. The SRTP implementation has been tested successfully in its usual deployment configuration with various SBCs. Interoperability Testing (IOT) with endpoints that only support encryption using the AVP profile is not supported.

The multiline SDP procedures related to SRTP was added in Desktop Release 10.1.2 and higher so that multiple m-lines are always used. Separate m-lines for AVP and SAVP are used.

Note, however, careful consideration must be given to the SBC configuration; particularly ensuring that the incoming “m=” line, associated with RTP/SAVP in the SDP, is not removed because in certain cases SRTP calls may be blocked.

Several different network configurations are however possible, in some deployments the SBC is not involved with the media traffic while in other deployments each client RTP media leg towards the SBC is separately encrypted and negotiated via the SBC. In some deployments, the SBC does not allow multiple SDP lines.

The SBC can also modify the order of the SDP m-lines at call setup, putting the AVP (non-encrypted) or SAVP (encrypted) m-line first. Therefore, clients that select the first working m-line are made to prefer either encrypted or unencrypted traffic. The various SRTP configuration options are as follows:

- **Mandatory** – At call setup, the initial SDP includes only the SAVP m-line when offering and the client accepts only the SAVP m-line in the SDP when answering, therefore only SRTP calls are possible.
- **Preferred** – At call setup, the initial SDP includes both the AVP and SAVP m-lines, but SAVP is first when offering, indicating the order of preference. When answering, the client selects SAVP if available even if is not the first m-line (as per SIP specifications the order of the m-lines is not changed when answering).
- **Optional** – At call setup, the initial SDP includes both the SAVP and AVP m-lines when offering but AVP is first indicating the order of preference. When answering, the client selects the first m-line, AVP or SAVP.
- **SRTP not enabled** – There is no SAVP m-line in the initial SDP when offering. When answering, SAVP is not accepted, therefore only RTP calls are possible.
- **Transport** – New configuration option introduced in Release 21.6.1 to automatically select the SRTP mode based on transport protocol. If TLS is used, mandatory SRTP mode is enabled. If TCP or UDP is used, no SRTP is utilized.

SRTP versus RTP is symmetric in both directions of the call, that is, sending and receiving profiles are the same.

```

<config version="20">
    <protocols>
        <rtp>
            <secure
mode="%SRTP_PREFERENCE%">%USE_SRTP%</secure> <!--true/false, enables
SRTP. Attribute (mandatory|preferred|optional) controls preferred
behavior in r20 -->

```

The Secure Real-Time Control Protocol (SRTCP) is also used if SRTP is enabled.

The following tags, in the custom *BroadTouch_Tags* set, are used to enable TLS and SRTP.

Tag	Default if Omitted	Supported Values	Example	Description
%USE_TLS%	false	false, true	<secure> true</secure>	When set to "false", TLS is deactivated. When set to "true", TLS is activated. If the <secure> tag omits, then the default is "false". If it is declared and the value omits, it defaults to "true". It is recommended to explicitly define what is the desired value, and not leave the node content empty.
%USE_SRTP%	false	false, true	<secure mode="mandatory">true</secure>	When set to "false", SRTP is deactivated. When set to "true", SRTP is activated.
%SRTP_PREFERENCE%	optional	mandatory, preferred, optional, transport	mode="mandatory"	Defines how preferred SRTP is at call setup. The default value is "optional".

10.16.5 SIP TLS Certificate Validation

When SIP is run over TLS, certification validation follows the generic procedures described in section [10.16.3 SSL/TLS Certificates](#). However, there are a few SIP-specific details described via the following example.

Certificate validation process:

- 1) Perform DNS operations to the URI specified in <record-name>, <domain-override> or <domain> parameter in that priority order : first NAPTR, then SRV, and finally A-query.
- 2) Set up SIP/TLS connection to server specified in proxy address (no SRV case) or to the URI given by DNS SRV response (SRV case). In the following example, SRV is used.
- 3) Certificate received from server, CiscoSSL validates the certificate using CN or SAN. With the less safe TLS certificate branding option, the address to which the client is connected must match CN or SAN for validation to succeed. When the TLS certificate branding option is not used (default in Release 22.7.0 and later), the configured domain must match CN or SAN. The following parameters are used in this order: record-name, domain-override, and domain. In the following figure where the less safe TLS certificate branding option is used, connection is towards sbc1.server.domain.com at 1.2.3.4; therefore, CN would work while SAN would fail.

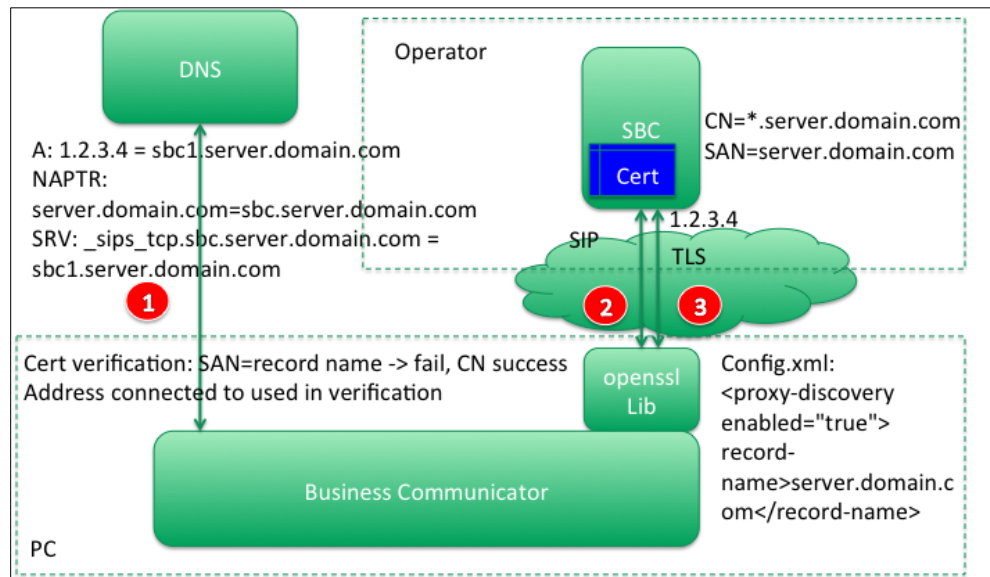


Figure 8 SIP Certificate Validation with Less Safe Branding Option

[Figure 9](#) depicts the case where the default safer certificate validation procedure is used.

Certificate validation process:

- 1) Perform DNS operations to the URI specified in <record-name>, <domain-override>, or <domain> parameter in that priority order : first NAPTR, then SRV, and finally A-query.
- 2) Set up SIP/TLS connection to server specified in proxy address (no SRV case) or to the URI given by DNS SRV response (SRV case). In the following example, SRV is used.

- 3) Certificate received from server, CiscoSSL validates the certificate using CN or SAN. With the safer TLS certificate procedure, the configured server address must match CN or SAN for validation to succeed. The following parameters are used in this order: record-name, domain-override, and domain. In the following figure where the safer TLS certificate procedure is used, connection is towards sbc1.server.domain.com at 1.2.3.4. CN would fail as there is a "." after the wild card, while SAN would work as that is an exact match.

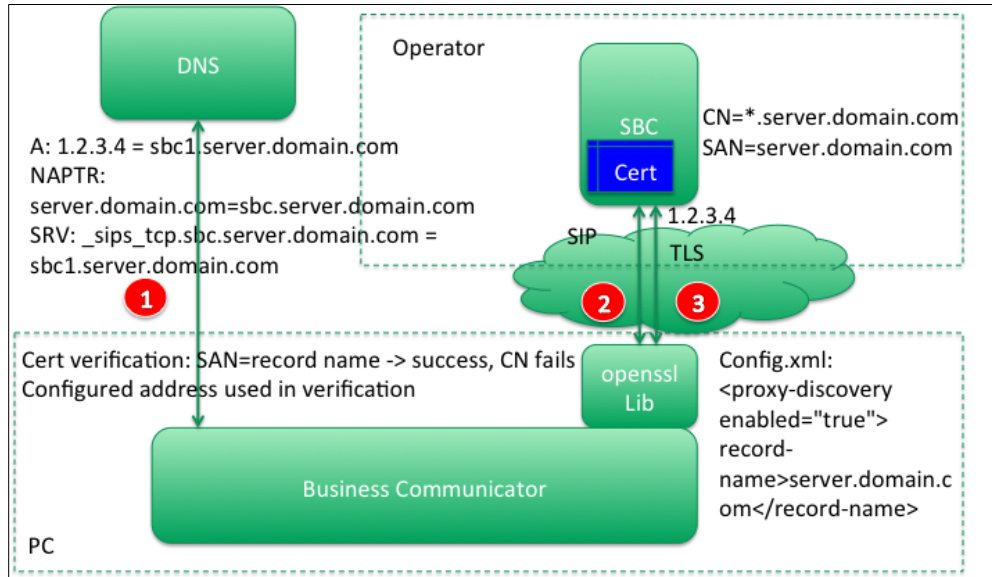


Figure 9 SIP Certificate Validation with Safer Certificate Validation (Default)

For SIP failover scenarios where the safer TLS certificate validation mechanism is used and the configured server address resolves to, for example, two servers, both servers need to return a certificate that has a CN or SAN matching to the configured address. Multi-SAN certificates can be used for this purpose as one alternative.

The scenarios for certificate provisioning are depicted in the following figure, indicating which values need to be provided in the certificate when enhanced security branding is used to validate the received certificate based on configured addresses.

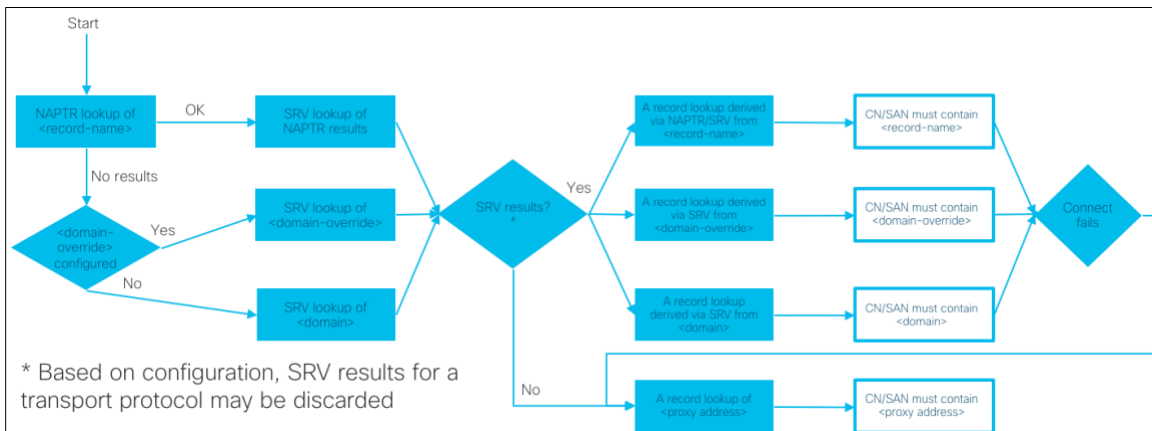


Figure 10 SIP Certificate Validation and Configuration Options

10.16.6 Xtended Service Interface TLS Certificate Validation

Starting with Release 22.1.0, TLS certificate validation for Xsi can operate in two different ways:

- Connected-to address is used for TLS certificate validation
- Configured address is used for TLS certificate validation (default from Release 22.7.0 onwards)

Figure 11 depicts the Xsi certificate validation process when TLS certificate branding options are not used. The figure after that depicts the case where TLS verification branding option is used. The difference is whether the connected to or the configured address is used for TLS certificate validation.

- 1) Perform DNS SRV-query operations to the URI given at login (<https://xsp.server.domain.com>) or after login constructed via Xsi path parameters. Resolve the received items via DNS A-queries and select the highest priority server. For more information on Xsi service discovery (selecting Xsp), see section [10.5.2 Xsi Service Discovery](#).
- 2) Set up HTTP connection towards 1.2.3.4.
- 3) Set up Xsi TLS connection.
- 4) Certificate received from server, OpenSSL validates the certificate using CN or SAN and the URI used (xsp1.server.domain.com). In the following figure, CN works but SAN fails.

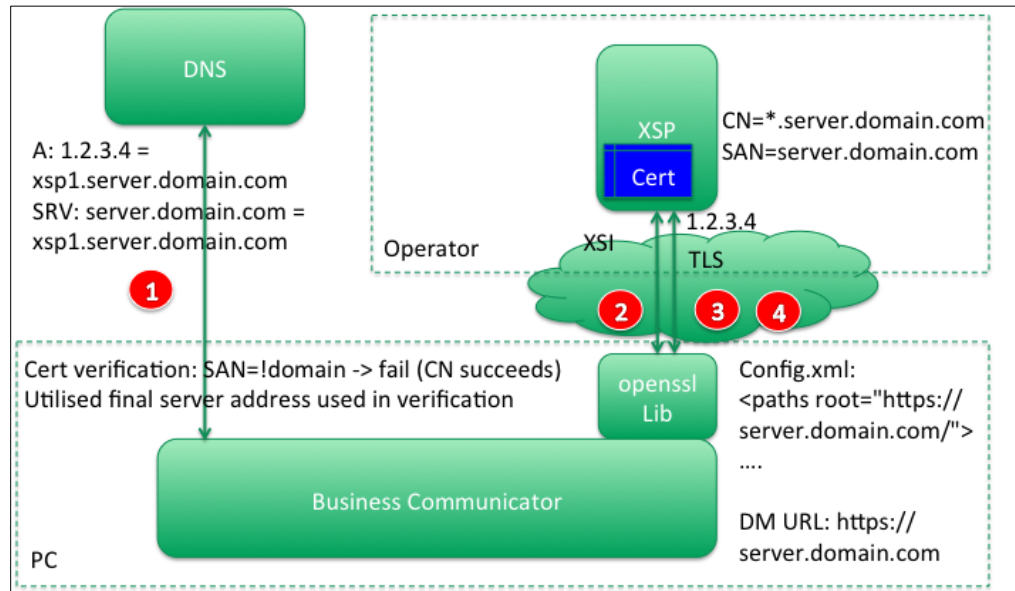


Figure 11 Xsi Certificate Validation – Non-Branded

When TLS certificate branding option is used, the following steps are employed:

- 1) Perform DNS SRV-query operations to the URI given at login (<https://xsp.server.domain.com>) or after login constructed via Xsi path parameters. Resolve the received items via DNS A-queries and select the highest priority server. For more information on Xsi service discovery (selecting Xsp), see section [10.5.2 Xsi Service Discovery](#).

- 2) Set up HTTP connection towards 1.2.3.4.
- 3) Set up Xsi TLS connection.
- 4) Certificate received from server, OpenSSL validates the certificate using CN or SAN and the configured URI (server.domain.com). In the following figure, CN fails but SAN works.

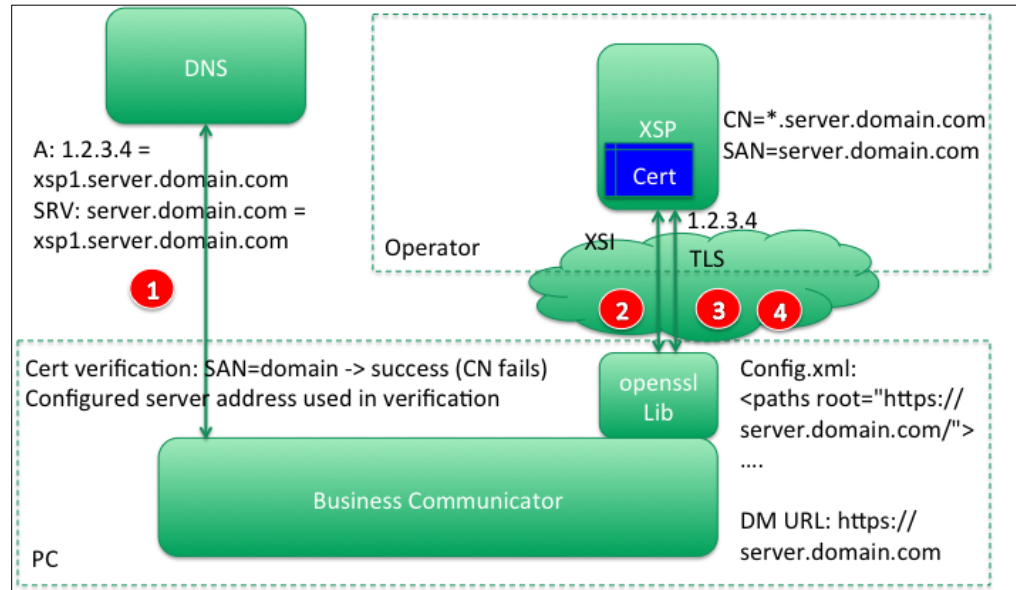


Figure 12 Xsi Certificate Validation – Branded

10.16.7 Messaging API SRV Support and Certificate Validation

When the HTTP API is used for message sync, the DNS SRV is also used. TLS certificate validation is done using the server address received from DNS. For more information on message sync configuration, see section [10.4 Messaging HTTP API](#).

The following steps are used for an HTTP API certificate validation:

- 1) Perform DNS SRV-query operations to the URI given in the configuration file (in the following example, https://ums.server.domain.com). Resolve the received items via DNS A-queries and select the highest priority server. For more information on HTTP API service discovery (selecting UMS), see section [10.5.2 Xsi Service Discovery](#).
- 2) Set up HTTP connection towards 1.2.3.4.
- 3) Set up the Xsi TLS connection.

- 4) The certificate is received from the server. OpenSSL validates the certificate using CN or SAN and the configured URI (server.domain.com). As shown in the following figure, CN fails but SAN works.

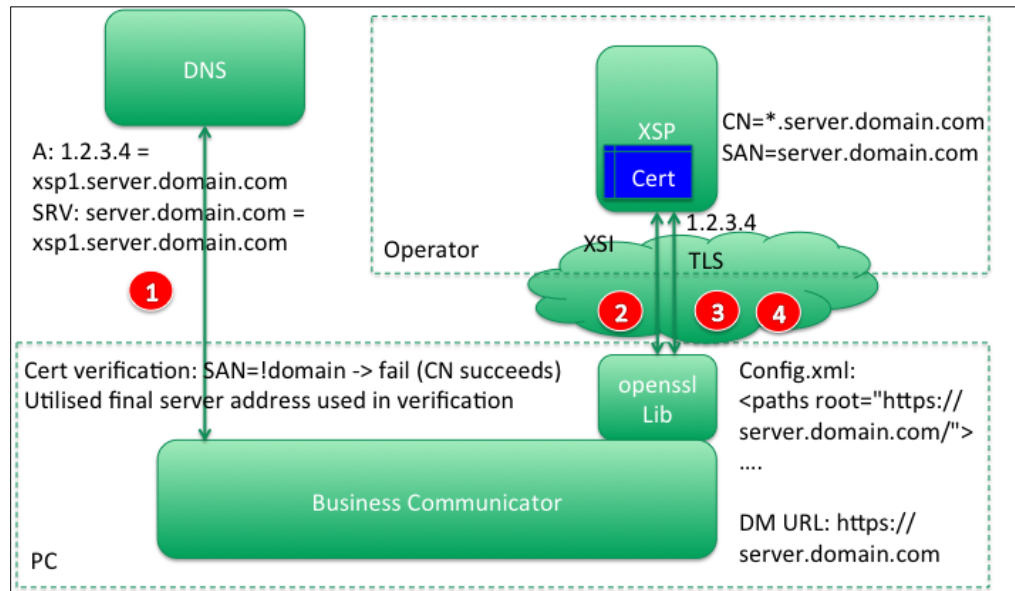


Figure 13 Messaging HTTP API Certificate Validation

10.16.8 XMPP SRV Support and Certificate Validation

With XMPP, certificate validation is done either with the domain part of the XMPP userid (JID) or the value of the domain parameter. For more information on the domain parameter, see the previous section. In some cases, one deployment must support several different companies with different domains. In this case, the domain of the XMPP username may be different from the value of the domain parameter. To use the value of the domain parameter for certificate validation allowing to keep the same certificate for each company, a new attribute *use-for-ssl-verification* (added in Release 20.0.1) is to be used. It defaults to "false". Without this parameter, TLS certificate verification is done against the XMPP username domain part. Both CN and SAN fields can be used in the certificate in XMPP.

With SRV, the final address received from the DNS is not used for certificate validation but the value of the domain parameter, which also defines where DNS operations are started. See the following example.

Steps:

- 1) Perform DNS operations to the URI specified in the <domain> parameter, in the following figure, server.domain.com is resolved with SRV resulting in ums1.server.domain.com being returned, which is the final address to which to connect. DNS A-query gives 1.2.3.4 as the IP address.
- 2) Set up XMPP TCP connection to server specified in <domain> or to the URI given by the DNS (SRV case). In this case, SRV returned ums1.server.domain com at 1.2.3.4.
- 3) Add TLS to the successful XMPP session.

- 4) Certificate received from server, OpenSSL library validates the certificate using CN or SAN. The *use-for-ssl-verification* parameter dictates if the domain part of XMPP JID or the value of the <domain> parameter is used in validation, whose configured value must match CN or SAN for validation to succeed. In the following figure, *use-for-ssl-verification=true*, thus the domain (server.domain.com) must match either SAN or CN. In the following figure, it only matches SAN, because CN has an additional "." and therefore, does not match.

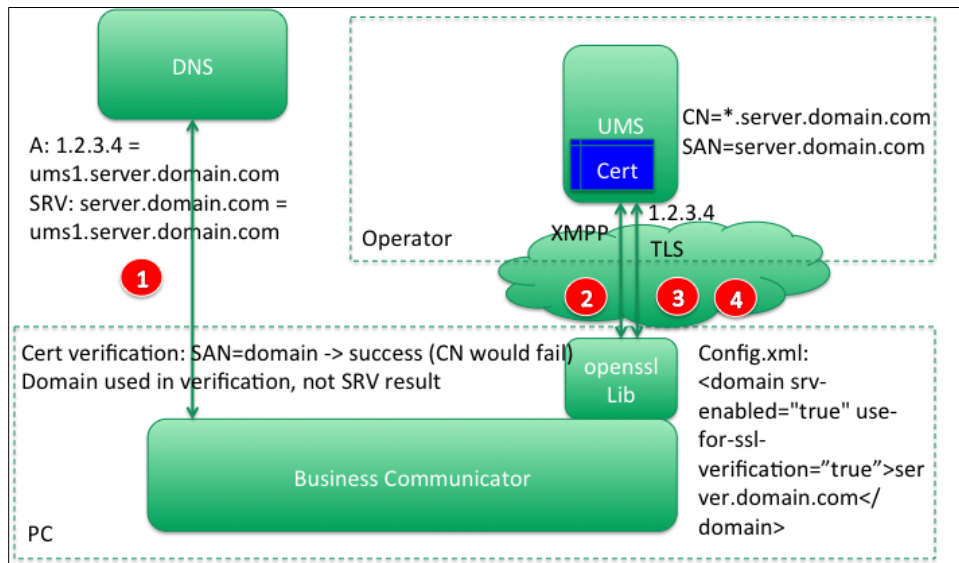


Figure 14 XMPP Certificate Validation

The following table provides examples of the usage of the different parameters and certificates.

XMPP <domain> Tag in Config File %BW_IMP_SERV_ICE_NET_ADDRESS-1%	JID= user@domain-Y.com	DNS SRV-Record (Has No Impact on Certificate Validation)	SSL Verification Domain Attribute (%USE_FOR_SSL_VERIFICATION%)	Expected SSL Cert on XMPP Server
Null	domain-Y.com	IP address returned in SRV response	empty=false	domain-Y.com
Null	domain-Y.com	domain-Z.com returned in SRV	empty=false	domain-Y.com
Null	domain-Y.com	IP address returned in SRV response	invalid option	domain-Y.com
Null	domain-Y.com	domain-Z.com returned in SRV	FALSE	domain-Y.com
domain-X.com	domain-Y.com	IP address returned in SRV response	empty=false	domain-Y.com
domain-X.com	domain-Y.com	domain-Z.com returned in SRV	empty=false	domain-Y.com

XMPP <domain> Tag in Config File %BW_IMP_SERVICE_NET_ADDRESS-1%	JID= user@domain-Y.com	DNS SRV-Record (Has No Impact on Certificate Validation)	SSL Verification Domain Attribute (%USE_FOR_SSL_VERIFICATION%)	Expected SSL Cert on XMPP Server
domain-X.com	domain-Y.com	IP address returned in SRV response	TRUE	domain-X.com
domain-X.com	domain-Y.com	IP address returned in SRV response	FALSE	domain-Y.com
domain-X.com	domain-Y.com	domain-Z.com returned in SRV	TRUE	domain-X.com
domain-X.com	domain-Y.com	domain-Z.com returned in SRV	FALSE	domain-Y.com

Use the custom DM tag %USE_FOR_SSL_VERIFICATION% for the SSL verification domain parameter.

For more information on basic XMPP configuration, see section 10.3.1 [Use Extensible Messaging and Presence Protocol](#). To enable XMPP SRV, see the following example.

```

<config version="20">
  <protocols>
    <xmpp enabled="true">

                                <credentials>

<username>user@domain.com</username>

                                <password>abc123</password>

                                </credentials>

                                <domain srv-enabled="%XMPP_SRV_ENABLED%"
use-for-ssl-
verification="%USE_FOR_SSL_VERIFICATION%">%BW_IMP_SERVICE_NET_ADDRESS-
1%</domain> <!-- XMPP server domain -->

                                <use-ssl>%XMPP_SSL_ENABLE%</use-ssl> <!-- enable
SSL for XMPP, default on -->

```

10.16.9 Sharing Server (USS) Certificate Validation

The Sharing Server may have self-signed certificates, but the Communicator Desktop client does not allow them. Instead, CA certificates must be used with Communicator Desktop.

On the Sharing Server, when the TLS certificate branding options is not used, the URI received from SRV is used for certificate validation, so the CN or SAN of the certificate must match that URI. *Figure 15* depicts the process.

- 1) Server address from configuration file parameter “uss-address=“https://server.domain.com.” is resolved in DNS SRV (A-record fallback also exists) to another URI (uss1.server.domain.com) which is resolved using DNS A-queries.
- 2) HTTP connection setup to 1.2.3.4.
- 3) TLS connection setup.
- 4) Certificate received from server and validated using OpenSSL. CN or SAN field of the received certificate must match the final server address received from SRV where the connection is made (uss1.server.domain.com). In the following figure, CN would match since it is wild-carded, but SAN would fail (for participants interworking with older Communicator versions, a pure IP address may still be used for connecting, in this case, the host name from configuration is used for verification).

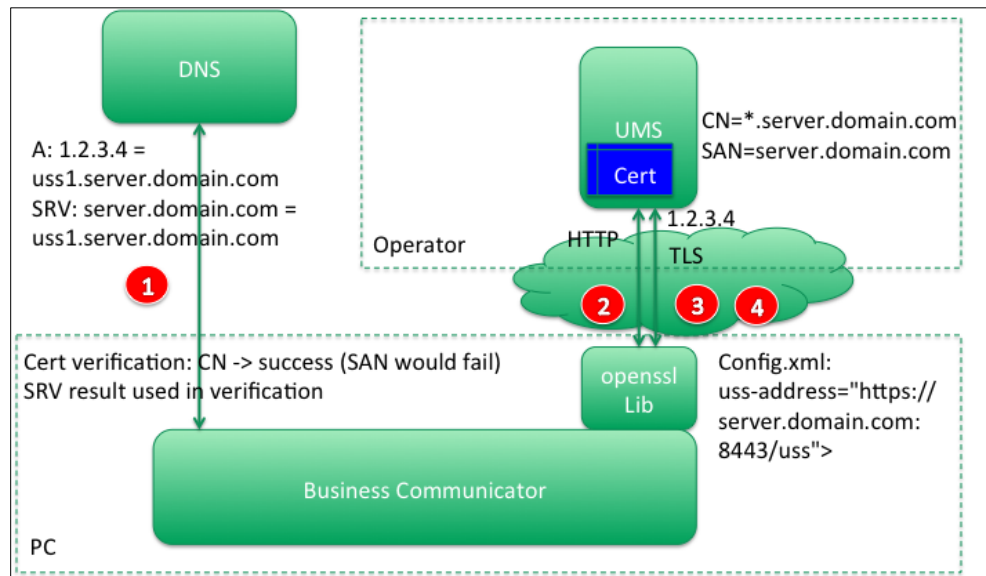


Figure 15 Sharing Server (USS) Certificate Validation

10.16.10 LDAP Certificate Validation

LDAP certificate validation works in the same manner as other protocols except that SRV is not used typically. In general, the LDAP server URL in the configuration file must match the SAN or CN field in the server certificate and the root certificates in the OS keychain must be compatible with the server certificate. There is no configurability for this in LDAP.

- 1) Server address from configuration file LDAP node <uri>/server.domain.com </uri> is resolved in DNS A-query.
- 2) LDAP connection set up to 1.2.3.4.
- 3) TLS connection setup.

- 4) Certificate received from the server and validated using OpenSSL. CN or SAN field of the received certificate must match the configured LDAP server address received from SRV where the connection is made (server.domain.com). In the following figure, CN would fail since it is wild-carded, but SAN would work, as there is an exact match.

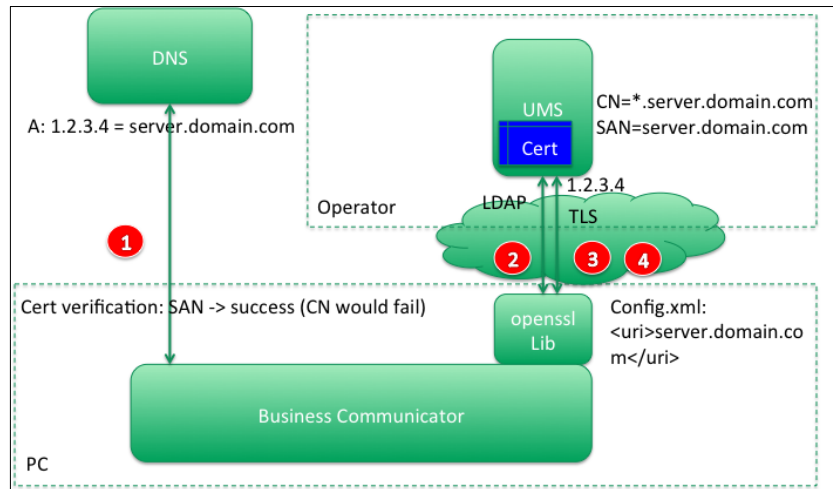


Figure 16 LDAP Certificate Validation

The service provider LDAP server administrator should have a signed <name>.cert certificate or equivalent, such as, .pem, (self-signed is not supported), which the LDAP server uses to manage TLS connections. The service provider administrator can either remotely install (for example, using a script) or otherwise install <name>.cert onto each machine or let individuals install it if they have admin rights. For additional instructions, go to:

<https://manuals.gfi.com/en/kerio/connect/content/server-configuration/ssl-certificates/adding-trusted-root-certificates-to-the-server-1605.html>

Note that OS UI tools can also be used.

10.16.11 Change Password

Starting with Release 21.3.x, the Xsi password can be changed at any time by the end user. Xsi-Actions is used for this purpose by the client. Client configuration defines if the user can change the password and how many days prior to password expiration Communicator warns the user about password expiration. Xsi password expiration is checked at login once a day and at connection reconnect.

When client-side password change notifications are not enabled and when Xsi password is changed on the server side while the client is logged in, the old password can be tried three times, after which Xsi is disabled until the next login. This behavior is not configurable, but Cisco BroadWorks can be configured regarding how many authorization failures are allowed until the account is locked.

If password is changed from some other own device such as mobile, the behavior depends on whether long-lived token (LLT) is in use or not. If LLT is not used, the next Xsi request will trigger authentication and forced logout so that the end user can provide the updated password. If LLT is used and long-lived token has not expired, Xsi operations continue to work until the long-lived token expires and the end user must re-enter the password.

The following example shows password change configuration.

```
<config version="20">
  <services>
    <password-update enabled="%ENABLE_PASSWORD_UPDATE%">
      <warn-before-
days>%PASSWORD_UPDATE_WARN_BEFORE_DAYS%</warn-before-days>
    </password-update>
  </services>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), are used to enable password change features. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_PASSWORD_UPDATE%	true	true, false	password-update enabled="true">	Select "true" to enable password change at any time. Select "false" to disable the feature.
%PASSWORD_UPDATE_WARN_BEFORE_DAYS%	0	positive integer	<warn-before-days>10</warn-before-days>	Specifies how many days prior to password expiration Communicator warns the user about password expiration. The warning is shown if the <i>expirydays</i> value from the server is less than or equal to the one defined in configuration here. The client warns if the credentials are expiring today (= 0) or they have already expired in the past (< 0). There is no warning for expiry in the future (> 0).

The following example shows how to control token expiry notification.

```
<config version="20">
  <services>
    <login-token-expiry-notification
enabled="%ENABLE_LOGIN_TOKEN_EXPIRY_NOTIFICATION%" />
  </services>
</config>
```

The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_LOGIN_TOKEN_EXPIRY_NOTIFICATION%	true	true, false	login-token-expiry-notification enabled=true	Select "true" to enable token expiry notification at any time. Select "false" to disable the feature.

10.16.12 Cisco BroadWorks MAC Field and Specific Configuration File Name

Starting with Release 21.3.0, using a specific Cisco BroadWorks feature, the DM configuration file can be tied to a specific device's MAC address so that no other device can download that configuration file. Once started, Communicator generates a device ID, and once Cisco BroadWorks has the same ID, the name of the config file is changed from *config.xml* to *<device ID>.xml*.

There is no client-side configurability for this feature. Instead, this feature can be enabled per installer via branding. For more information, see the *Communicator for Desktop Branding Guide*.

10.16.13 XMPP Security Enhancement for Unauthorized File Types

Starting with Release 21.1.0, it is possible to specify unauthorized file types for a file transfer. This feature is sometimes required by corporate IT policies.

Blocking of unauthorized file types in file transfer applies for both the sending and receiving sides. The unauthorized file types can be specified in a configuration parameter (as shown in the following example). Release 22.9.1 made the file extension list case insensitive so that the same file extensions would not need to be provided both in lower case and upper case.

```
<config version="20">
    <services>
        <media-share>
            <file-transfer enabled="%ENABLE_FILE_TRANSFER%" encryption-
required="%FT_REQUIRE_ENCRYPTION%">
                <limit-file-extensions enabled="
%ENABLE_FILE_TRANSFER_FILE_EXTENSION_LIMIT%">%FILE_TRANSFER_FORBIDDEN_EXT
ENSIONS%</limit-file-extensions>
            </file-transfer>
        </media-share>
    </services>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), are used to enable file type blocking and to specify the blocked file types. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_FILE_TRANSFER_FILE_EXTENSION_LIMIT%	false	true, false	<limit-file-extensions enabled="true"></limit-file-extensions>	Select "true" to enable blocking of unauthorized file types in file transfer. Select "false" to disable the feature.
%FILE_TRANSFER_FORBIDDEN_EXTENSIONS%	empty	comma-separated list of file extensions	<limit-file-extensions enabled="true">exe,zip,tar,dmg,jpg,tar.gz,pcapng</limit-file-extensions>	Defines the list of blocked file types.

10.16.14 XMPP Security Enhancement for Preventing Clickable Links

Starting with Release 21.1.0, clickable links can be prohibited in chat. This feature is sometimes required by corporate IT policies. However, the link can be copied and pasted into a web browser. This feature can be enabled using a configuration parameter (as shown in the following example).

```
<config version="20">
    <services>
        <chat>
            <prevent-clicking-
links>%CHAT_PREVENT_CLICKABLE_LINKS%</prevent-clicking-links>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to enable this feature. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%CHAT_PREVENT_CLICKABLE_LINKS%	false	true, false	<prevent-clicking-links>true</prevent-clicking-links>	Select "true" to prevent clickable links in chat. Select "false" to allow clickable links in chat.

10.16.15 HTTP Proxy Support

There are several ways of get an HTTP proxy:

- Static proxy
- Proxy Auto-Configuration (PAC)
- Proxy Auto-Detection

In this release, the client supports the static proxy option as well as the PAC and Proxy Auto-Detection options. For potential limitations, see the *Communicator (Desktop) Release Notes*. PAC and auto-configuration are part of the system proxy setting. The client also allows accessing the HTTP proxy preferences from the *Login* screen:

- For OS X, this is a menu option added to the top menu.
- For Windows, the top-corner menu is enabled in the *Login* window and it contains the "preferences" item.

The *Proxy* settings tab has three options as follows:

- 1) No proxy – Set to "ignore" in the *proxy_settings.ini* file. The client connects directly.
- 2) Use system proxies – Set to "system" in the *proxy_settings.ini* file. The client uses the proxy settings from the underlying operating system.
- 3) Use Communicator proxy settings – Set to "application" in the *proxy_settings.ini* file. The following fields are used:
 - Web Proxy Server
 - Port
 - Secure Web Proxy Server
 - Port

Note the following:

- Communicator Proxy settings are stored in a separate *proxy_settings.ini* file.
- The *proxy_settings.ini* file is read at startup.
- The *proxy_settings.ini* file can be distributed by system administrators. Communicator uses the settings from that even without a user's interaction with the proxy settings. Note that client logout or login is required for the proxy settings changes to take effect.

- The *proxy_settings.ini* uses the following format. The *type* field can be set to “application”, “system”, or “ignore”. If the *proxy_settings.ini* parsing fails, then “system” is the default. If “application” is selected, then the *httpserver*, *httpport*, *httpsserver*, and *httpsport* fields are relevant. Note that with other settings, they are overlooked.

```
[proxy_settings]
type=application
httpserver=proxy.server.com
httpport=8080
httpsserver=secure-proxy.server.com
httpsport=433
```

10.16.15.1 Static HTTP Proxy

Static proxy configuration means configuring the proxy statically on a workstation by defining the HTTP and HTTPS proxy addresses. For Windows, the proxy settings are found from the *Control Panel* → *Internet options* → *Connections* → *LAN settings* → *Proxy server* → *Advanced*.

- “HTTP” for normal HTTP connections
- “Secure” for HTTPS

For OS X, the configurations are under *System Preferences* → *Network* → *Wi-Fi* → *Advanced* → *Proxies*. Again, there are two separate settings, one for HTTP, and another for HTTPS.

NOTE: If a cabled connection is used on OS X, follow the previous proxy settings but under *System Preferences* → *Network* → *Ethernet*.

Static proxy settings are supported for both HTTP and HTTPS proxies. The following are exceptions:

- 1) The Login URL provided in the *Login* window must include the used protocol by containing the schema at the beginning (HTTP:// or HTTPS://).
- 2) Web Collaboration does not work on OS X if proxies are used.

Even if credentials for proxy authentication are provided in the *System Preferences* or *Internet options*, the application (Communicator) queries the username and password from the user and stores them for future use. This is how other applications work and cannot be changed due to operating system restrictions.

These credentials are stored in an encrypted format in the *application_settings.ini* file along with the other user profile settings. The relevant section is called [*http_proxy*].

```
[http_proxy]
username=user_basic
password_encrypted=<encrypted data>
```

10.16.15.2 Proxy Authentication

If proxy authentication is used, Communicator only asks for the credentials once and stores them for subsequent use. Proxy authentication can be applied regardless of how the operating system finds the proxy (for example, via static configuration or a PAC file).

If the proxy password changes during the session, the user starts to see network errors and must log in again (SIP and XMPP functionality does continue to work despite the issues).

10.16.16 3GPP SIP Headers for SRTP

Newer 3GPP specifications require additional SIP headers in order to use SRTP. See *3GPP TS 24.229* for more details as well as the following:

<https://tools.ietf.org/html/draft-dawes-dispatch-mediasec-parameter-07>

The headers required by this specification may break SIP calling in deployments where this specification is not used. Therefore, it is recommended that these headers be used only in environments where the server side supports them.

Only enabling the usage of the headers is configurable. No further configurability exists for individual headers. All headers are either enabled or disabled.

See the following example for configuration.

```
<config version="20">
    <protocols>
        <sip>
            <use-mediasec
enabled="%USE_MEDIASEC_DESKTOP%" />
        </sip>
    </protocols>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Value	Example	Description
%USE_MEDIASEC_DESKTOP%	false	true, false	<use-mediasec enabled="true" />	Enables 3GPP SIP headers for SRTP. The default is "false".

10.16.17 SRTP Re-keying Configurability

In some deployments, re-keying for SRTP is not supported. Therefore, Release 21.3.0 added a new configuration parameter for enabling/disabling SRTP re-keying. However, new keys are always taken into use when received. Configurability only pertains to sending new keys.

See the following example for configuration.

```
<config version="20">
    <protocols>
        <rtp>
            <secure mode="mandatory" rekey-
always="%ENABLE_RE-KEYING_DESKTOP%">true</secure>
        </rtp>
    </protocols>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Value	Example	Description
%ENABLE_RE-KEYING_DESKTOP%	true	true, false	<secure mode="mandatory" rekey-always="true">true</secure>	Enables SIP (SDP) re-keying for SRTP. The default is "true", which is the behavior in 21.2.

10.16.18 PIV URL

Release 22.5.0 introduced a new configuration parameter, URL for Personal Identity Verification (PIV) to specify a PIV-capable Xsp in case the Xsp used for non-PIV-authentication is not capable of also supporting PIV-authentication so that the same deployment can support both PIV and non-PIV users. The deployment must ensure that the utilized F5 load balancer address in branding matches the piv-enabled-root address in the DM configuration file. At the same time, Xsi root path (%XSI_ROOT%) still needs to point to the Xsp. The corresponding Xsp URL branding parameter must also point to the Xsp.

The two URLs are needed in both branding and DM configuration as there is some required SSO signaling before the configuration file is retrieved and the branding URLs are used for that. Therefore, these URLs must be the same both in branding and DM configuration.

If only PIV is used in Release 22.5.0, the utilized F5 address must match the Xsi root path address in the DM configuration file. This also means that in branding, only one URL is defined.

For more information on the required PIV branding parameters, see the *UC-One for Desktop Branding Guide*.

See the following example for configuration.

```
<config version="20">
    <protocols>
        <xsi>
            <paths root="%XSI_ROOT%" piv-enabled-
root="%PIV_XSI_ROOT%">
```

The following tag, in the custom *BroadTouch_Tags* set, controls this capability.

Tag	Default if Omitted	Value	Example	Description
%PIV_XSI_ROOT%	empty	string	<paths root="%XSI_ROOT%" piv-enabled-root="https://piv.domain.com"/>	The address of the PIV Xsi root. When empty, Communicator falls back to using %XSI_ROOT%

10.17 Emergency Calling

10.17.1 Banner Support

Communicator can render the Hypertext Markup Language (HTML) banner to the contact list view. To enable the banner and to define which HTML resource is rendered, the following configuration should be present under <services>.

```
<config version="20">
    <services>
        <banner enabled="true" url="http://domain.com" height="200"/>
```

The HTML rendered in the banner area can contain links. These links are opened in the browser, in the email client, and so on, based on the URL schema used in the links. The banner has been verified with basic HTML code only, for example, complex or newer JavaScript APIs may not work. For branding and sizing instructions, see the *Communicator for Desktop Branding Guide*.

The height value defines the banner area's vertical size in pixels. If the height is not defined, the client defaults to 40 pixels (height in centimeters or inches depends on the display resolution), which is also the minimum value accepted.

In the HTML code used in the banner, only HTML links with target="_blank" are opened in the external browser.

The template tags %ENABLE_BANNER%, %BANNER_URL%, and %BANNER_HEIGHT% are used to control the attribute values for the <banner>-node. For more information on the Device Management tags, see the following table.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_BANNER%	false	true, false	banner enabled="true"	When set to "true", the banner is enabled. When set to "false", the banner is disabled.
%BANNER_URL%	empty	string	url="http://domain.com"	Banner URL used to fetch content.
%BANNER_HEIGHT%	40	Number, 40 or more	height="200"	Height of the banner.

10.17.2 Disable Emergency Calls

Starting with Release 10.0.2, the client supports a new configuration node for controlling blocking of emergency calling.

The following is an example of a configuration that blocks calls to numbers 112, 911, and 999, and enables a static error message in the *Main* window and dial pad.

```
<config version="20">
  <services>
    <calls>
      <emergency-call enabled="%ENABLE_EMERGENCY_CALLING%">
        <emergency-call-notification enabled=
"%ENABLE_EMERGENCY_CALL_NOTIFICATION%" />
        <emergency-call-numbers>%EMERGENCY_NUMBER_LIST%</emergency-
call-numbers>
      </emergency-call>
    </calls>
  </services>
</config>
```

Make sure to have the emergency numbers without spaces. The number length can be something other than three. There are no other restrictions.

All settings under <emergency-call> are irrelevant when the feature is disabled (that is, <emergency-call enabled="true">).

The following table describes the different configuration options and Device Management tags.

Parameter	Default if Omitted	Supported Values	Example	Description
<code>%ENABLE_EMERGENCY_CALLING%</code>	true	true, false	<code><emergency-call enabled="false" /></code>	Emergency calls are blocked when set to "false". The default is "true". If the end user tries to make an emergency call when it is not allowed, a pop-up displays.
<code>%ENABLE_EMERGENCY_CALL_NOTIFICATION%</code>	false	true, false	<code><emergency-call-notification enabled="true" /></code>	Enables static error message ("No Emergency Calls") in error message/status area in top of the contact list. The default is "false".
<code>%EMERGENCY_NUMBER_LIST%</code>	empty	comma-separated list of emergency numbers (spaces not allowed)	<code><emergency-call-numbers>112,911,999</emergency-call-numbers></code>	Calls to numbers in this list are blocked when <code>%ENABLE_EMERGENCY_CALLING%</code> is set to "false".

Starting with Release 21.4.0, banner URLs can also be constructed using variables and encoded. For more information on the variables and related encoding functionality, see section [10.19.10 Pass Parameters and Encoding Web Button URLs](#).

10.17.3 Login Dialog

It is possible to enable a separate dialog shown after the *Login* window, which is used to show the user important information. The default text describes emergency calling, however, as part of the branding process it can be customized by a service provider.

The *Login* dialog has two buttons: OK and Cancel. The following options are supported for the Cancel button once the *Login* dialog feature has been enabled:

- 1) Hide the Cancel button.
- 2) Show the Cancel button and once clicked, return the user to the *Login* window. The *decline-button-action* parameter value is "logout".
- 3) Show the Cancel button and once clicked, exit the client. The *decline-button-action* parameter value is "exit".
- 4) Show the Cancel button and once clicked, login proceeds as usual. The *decline-button-action* parameter value is "login".

As a separate configuration parameter for options 2 through 4 in the previous list, a URL can be defined to open a browser window with that URL. The following example shows a configuration where the *Login* dialog feature is enabled and clicking on the **Cancel** button logs in and opens a web browser for www.domain.com. Note that in this dialog, the native buttons are used and cannot be branded.

```
<config version="20">
  <services>
    <login-informational-dialog
enabled="%ENABLE_LOGIN_INFORMATIONAL_DIALOG%">
      <decline-button-action>%DECLINE_BUTTON_ACTION%</decline-button-
action> <!-- disabled|login|logout|exit -->
      <decline-button-url>%DECLINE_BUTTON_URL%</decline-button-url>
    </login-informational-dialog>
```

The following table describes the DM tags.

Parameter	Default if Omitted	Supported Values	Example	Description
%ENABLE_LOGIN_INFORMATIONAL_DIALOG%	false	true, false	<login-informational-dialog enabled="true">	Enables and disables the <i>Login</i> dialog.
%DECLINE_BUTTON_ACTION%	disabled	disabled, login, logout, exit	<decline-button-action>login</decline-button-action>	Defines the Cancel button action in the <i>Login</i> dialog.
%DECLINE_BUTTON_URL%	empty	string	<decline-button-url>http://www.domain.com</decline-button-url>	URL for options 2 to 4 in the previous list.

10.17.4 Emergency Call Address Change Service

The Emergency Call Address Change Service (ECACS) exposes web services that allow Communicator to create a web browser session that allows a user to configure their emergency call address. At login, end users receive a dialog asking if the Emergency Call Service Address needs to be updated. If the end user selects “yes”, the ECACS service is invoked in a web browser.

Starting with Release 21.1.0, it is also possible to specify a separate menu item for ECACS independently of the ECACS procedure done at login. The menu item either starts the same ECACS procedure as it does for login or opens a web browser without the ECACS APIs using the specified URL.

For information about server-side implementation requirements from the client perspective, see the *Communicator Emergency Call Address Change Service Guide*. Release 21.3.0 introduced support for a new URL format described in the following table, however, it has been removed in Release 22.6.0 since it is no longer required.

See the following example for client configuration.

```
<config version="20">
  <services>
    <external-service-verification
enabled="%ENABLE_EXT_SERVICE_VERIFICATION%">
      show-menu=" %SHOW_EXT_VERIFICATION_MENU%" use-
session="%USE_SESSION_EXT_SERVICE_VERIFICATION%"
      <url>%EXT_SERVICE_VERIFICATION_URL%%BWDN-1%</url>
```

```
</external-service-verification>
```

The following table describes the DM tags.

Parameter	Default if Omitted	Supported Values	Example	Description
%ENABLE_EXT_SERVICE_VERIFICATION%	false	true, false	<external-service-verification enabled="true">	Enables and disables the Emergency Call Service Address Change feature.
%SHOW_EXT_VERIFICATION_MENU%	false	true, false	show-menu="true"	Set to "true" to enable the ECACS menu item. Set to "false" to disable the menu item.
%USE_SESSION_EXT_SERVICE_VERIFICATION%	true	true, false	use-session="true"	Defines if the ECACS API session is used in the menu. Set to "false" to deny the use of ECACS APIs in the address change process (instead in an independent web browser session). Set to "true" to use the same ECACS APIs as in the login case.
%EXT_SERVICE_VERIFICATION_URL%	empty	string	<url>http://server.domain.com</url>	Defines the URL that the client contacts at login or when menu item is invoked if the user wants to configure the Emergency Call Service Address. Accompanied with user's telephone number as in the example earlier in this section. From the URL, the client retrieves two other URLs that are used for launching the actual web page and retrieving status updates of the address change process. Depending on the <i>use-session</i> parameter, the ECACS APIs may not be used when the feature is invoked from the menu.

The following table describes various configuration possibilities.

Enabled	Show-menu	Use-session	Description
true	true	true (or omits)	ECACS API environment, user is prompted at login and the menu is available, using ECACS APIs.
true	false	true (or omits)	As above but with no possibility to operate via the menu.
false	true	true	ECACS APIs are used but only via a menu item.
false	true	false	ECACS APIs are not used. Only the menu can be used for setting the Emergency Call Service Address.

Enabled	Show-menu	Use-session	Description
false	false	false	Feature disabled.
true	true or false	false	Invalid setting. Only ECACS APIs can be used for login prompt.

10.18 Logging

10.18.1 Release 20.0.0 Enhancements

Logging was enhanced in Release 20.0.0 and later with the following changes:

- The log file *communicator_stderr.txt* is now called *UCOneLog.log*. *QXMPPClientLog.log* is called *XMPPLog.log*, but since the same information is available in *UCOneLog.log* file, the *XMPPLog.log* file may not be present.
- Use of logging levels – The current log levels are FATAL, ERROR, WARNING, INFO, DEBUG, and TRACE and are listed from the most severe to the least severe. Each log entry in a file states the severity level to which it belongs. By default, release builds contain logging information from all the supported levels, but this can be configured in the *LogConfig.xml* file.
- Several different log files can be used for different purposes, in addition to the all-encompassing *UCOneLog.log*, which is typically the only log file present. However, end users should provide the entire logs directory when reporting issues. The benefit of this additional logging is that a certain category of logging data can be more easily seen instead of searching the much larger generic *UCOneLog.log* file when needed.
- The number, size, logging level of log files, and the number of their backup files are defined in a new configuration file called *LogConfig.xml*. *LogConfig.xml* also determines if a log file is generated or not. This selection is done at build time but can be modified by editing the *LogConfig.xml* file.
- Rotating logs are cleared and re-used when the defined maximum size has been exceeded, starting from the oldest file. Several backup files are also created for the log files; they are named with a number that is appended at the end. For example, for the main log file, it is *UCOneLog.log.x* where “x” can be defined in the configuration. The larger the “x”, the older the backup configuration file. The default for “x” is “10”, so in addition to *UCOneLog.log* file, ten backup files would be used.
- The log file location has been changed slightly as follows:
 - OS X: */Users/USERNAME/Library/Application Support/BroadSoft/Communicator/logs*
 - Windows: *C:\Users\USERNAME\AppData\Local\BroadSoft\Communicator\logs*

The log levels are defined as follows:

- FATAL – The FATAL level designates very severe error events that presumably lead the application to abort.
- ERROR – The ERROR level designates error events that might still allow the application to continue running.
- WARN – The WARN level designates potentially harmful situations.
- INFO – The INFO level designates informational messages that highlight the progress of the application at coarse-grained level.

- **DEBUG** – The DEBUG level designates fine-grained informational events that are useful to debug an application.
- **TRACE** – The TRACE level designates finer-grained informational events than the DEBUG level.

NOTE: Log files generated with previous versions, such as *communicator_stderr.txt*, are not automatically deleted, however, they are no longer used in Release 20.0 and later. Also, note that advanced logs related to third-party applications (needed in special cases only) are stored in the default Communicator logging directory and not in the branded directories.

10.18.2 Standard HID Logging

A separate log file called *CommunicatorStandardHID.log* is used for standard Human Interface Device (HID) Add-in. It contains various events about standard HID operations. This file is essential for headset troubleshooting.

The *CommunicatorStandardHID.log* is automatically created when the standard HID Add-in is used.

10.18.3 Preferences User Interface for Logging

The recommended way to enable logging is to use the user interface in the *Preferences* window. Basic logging enables logging for everything else other than audio and video calls while the advanced logging also enables heavier logging for audio and video calls. It is not recommended to have advanced logging on when not needed, as it consumes much more disk space. In addition to the *Preferences* UI, logging can be enabled in the *application_setting.ini* configuration file by setting the following parameters (if login fails and the logging needs to be enabled):

- *loggingenabled* – Enables generic error logging.
- *xmpploggingenabled* – Enables XMPP logging.
- *advloggingenabled* – Enables advanced logging for audio and video calls in both the BME and the previous media framework.

To enable the XMPP logs and the *UCOneLog.log* (with XMPP information), add the following lines to the *application_setting.ini* file:

- `loggingenabled=true`
- `xmpploggingenabled=true`

To enable audio and video logs, add the following lines to the *application_setting.ini* file:

- `advloggingenabled=true` (with BME and previous media framework)

Release 10.0.1 introduced a way to enable logging through *Preferences* without the need to change values in the *application_setting.ini* file, while retaining the possibility to use the *.ini* file for choosing basic or advanced logging.

When using the Clear all logs button in the *Preferences*, the client clears all the logs, but it must be restarted for the media engine logs to be created again. Note that only logs for the configured media engine are cleared.

10.18.4 Outlook Add-in Logging

Starting with Release 21.6.0, additional Outlook Add-in log files are generated:

- OutlookPluginDLL_<DATE>.log – UI dll log, date rolling.
- OutlookPluginWrapper_<DATE>.log – wrapper log, date rolling.
- OutlookPluginGW.log – presence gw log, maximum two files rolling.

These files reside inside the Communicator *logs/* folder (the main logging directory).

If failures happen with certain registry settings, these files reside in the *\$TEMP/btbc_outlook_plugin/* folder.

These files are always created when logging is enabled in Communicator *Preferences*.

10.18.5 Disable Logging

Starting with Release 21.6.0, it is possible to disable logging using a branding option. For more information, see the *Communicator for Desktop Branding Guide*.

The following logging options are available:

- 1) Logging disabled, no user interface to turn it on.
- 2) Logging off by default, user interface present, but both basic and enhanced logging are turned off by default.
- 3) Basic logging is enabled by default and the preferences UI contains both basic and advanced logging options with advanced disabled. End users can toggle the logging options.
- 4) Both basic and advanced logging are enabled by default. The Preferences UI is available. End users can toggle the logging options.

In case of an upgrade installation, the following takes place for logging settings for cases 1 through 4 in the previous list:

- 1) Logging disabled: logging is turned off, even if it was on previously.
- 2) For 2 through 4, previous user settings are not altered.

10.19 User Interface

10.19.1 Configurable Left Pane Order

This feature allows the order of the left pane icons to be configured. The order is dictated by the *q-value* parameters in the following configuration node, with the smallest on top. However, the presence icon is always the first icon. In addition, the default icon selected after installation can be specified in the configuration. At subsequent logins, the client remembers and selects the previously used icon.

Note that Contacts, History, Chat History, and dial pad icons cannot be removed. Release 22.0.0 introduced a separate Chat History icon and removed the room's icon in the left pane.

Release 22.5.0 introduced three new web buttons and their order in the left pane can be specified using the same configuration parameters structure. For more information on the additional web buttons, see section [10.19.9 Configurable Web Button and Web Tab View](#).

See the following example for configuration parameter details.

```

<config version="20">
  <services>
    <leftpane default="%LEFT_PANE_DEFAULT%"> <!--
Configurable left pane button order -->
    <contacts q="%LEFT_PANE_CONTACTS_Q%" />
    <rooms q="%LEFT_PANE_ROOMS_Q%" />
    <history q="%LEFT_PANE_HISTORY_Q%" />
    <chat-history q="%LEFT_PANE_CHAT_HISTORY_Q%" />
    <dialpad q="%LEFT_PANE_DIALPAD_Q%" />
    <directory q="%LEFT_PANE_DIRECTORY_Q%" />
    <web-button q="%LEFT_PANE_WEB_BUTTON_Q%" />
    <web-button-2 q="%LEFT_PANE_WEB_BUTTON_2_Q%" />
    <web-button-3 q="%LEFT_PANE_WEB_BUTTON_3_Q%" />
    <web-button-4 q="%LEFT_PANE_WEB_BUTTON_4_Q%" />
    <hub-button q="%LEFT_PANE_HUB_BUTTON_Q%" />
  </leftpane>

```

The following table describes the DM tags for configurable left pane order.

Tag	Default if Omitted	Supported Values	Example	Description
%LEFT_PANE_DEFAULT%	contacts	contacts, rooms, history, dialpad, directory	<leftpane default="dialpad">	This is any of the names of the left pane icons. The default is "contacts".
%LEFT_PANE_CONTACTS_Q%	1	Any integer from "1" onwards. The default is "1".	<contacts q="1" />	Placement of the Contacts icon.
%LEFT_PANE_HISTORY_Q%	3	Any integer from "1" onwards. The default is "3".	<history q="3" />	Placement of the History icon.
%LEFT_PANE_CHAT_HISTORY_Q%	2	Any integer from "1" onwards. The default is "3".	<chat-history q="2" />	Placement of the Chat History icon.
%LEFT_PANE_DIALPAD_Q%	4	Any integer from "1" onwards. The default is "4".	<dialpad q="4" />	Placement of the Dial Pad icon.
%LEFT_PANE_DIRECTORY_Q%	5	Any integer from "1" onwards. The default is "5".	<directory q="5" />	Placement of the Directory icon.
%LEFT_PANE_WEB_BUTTON_Q%	6	Any integer from "1" onwards. The default is "6".	<web-button q="6" />	Placement of the web button icon.

Tag	Default if Omitted	Supported Values	Example	Description
%LEFT_PANE_WEB_BUTTON_2_Q%	8	Any integer from "1" onwards. The default is "6".	<web-button-2 q="8" />	Placement of the web button 2 icon.
%LEFT_PANE_WEB_BUTTON_3_Q%	9	Any integer from "1" onwards. The default is "6".	<web-button-3 q="9" />	Placement of the web button 3 icon.
%LEFT_PANE_WEB_BUTTON_4_Q%	10	Any integer from "1" onwards. The default is "6".	<web-button-4 q="10" />	Placement of the web button 4 icon.
%LEFT_PANE_HUB_BUTTON_Q%	7	Allowed values are numbers. Any other value is considered to be 1.	<hub-button q="7" />	This is used for the Hub button in the left-side button navigation bar.

10.19.2 Flexible Contact Card Field Configuration and Synchronization

Starting with Release 20.1.0, all contact card fields can be made editable and each field can be hidden by configuration. The user interface also has a button, allowing the contact card details to be synchronized with the Cisco BroadWorks enterprise directory or other sources when manual mode is used. With automatic mode, the contact card must be opened for data synchronizing to occur. Additionally in Release 22.9.10 and later, contact syncing is done when entering the call history view to be able to show better names there. This was done in order to spare Xsp capacity in some deployments.

Matching of server data in sync against the local data is done by JID, and if that is not available, by phone numbers and email address in the following order:

- 1) Email address
- 2) Work phone
- 3) Extension

If XMPP is enabled and the contact has no JID, synchronizing with the server is not done. The contact card is synchronized with Cisco BroadWorks when the contact is added via Cisco BroadWorks directory search.

Contact synchronizing is done automatically when a new contact is added when automatic synchronizing is in use. If manual synchronizing is in use, then the end user must click on the sync button (cloud symbol).

If XMPP is enabled but it is not working, adding, or modifying a contact is disabled.

"Automatic" is the default value for the *contact-card sync-from* parameter. If the whole <contact-card>-node is omitted, "automatic" is again the default. The possible values are:

- "Xsi" – The Cisco BroadWorks enterprise directory is used for manual synchronizing.

- “Automatic” – The client behaves as in Release 20.0.2. The contact card is automatically synchronized with Cisco BroadWorks directories and only some fields are editable. The *edit* and *show* parameter values are ignored.
- “LDAP” – The LDAP directory is used for manual synchronizing.
- “Automatic-ldap” – The client behaves as in Release 20.0.2, but automatic synchronizing is done with LDAP.
- “Outlook” – Local Outlook is used for manual synchronizing.

Starting with Release 22.0.0 and later, the value of attribute *sync-from* has no significance in display name matching. It only affects the synchronization of contact-card details from configured directory. It no longer defines what source is used for caller name lookup.

Release 21.5.0 added more contact card fields. For backward compatibility reasons, they are hidden by default and they use a different parameter syntax. In addition, only these fields have custom DM tags. The DM tags are used to control the visibility of the <additional-field> in the contact card regardless of the value of the *sync-from* attribute in the parent node <contact-card>. Editing of these additional fields, as well as most other contact card fields, is disabled if *sync-from* is set to “automatic”.

- title
- department
- hiragana-firstname
- hiragana-lastname
- region
- location
- yahooid
- pager
- bw-userid

Note that the old field’s *show-value* should default to “true” omitting and the *edit-value* should default to “false” except for following fields: *displayname*, *personal-phone*, *conference-phone*, *conference-id*, *conference-pin*, and *web-url*.

Release 22.5.0 added support for syncing chat and Call History items with configured sources.

See the following example for configuration details.

```

<config version="20">
  <services>
    <contacts>
      <contact-card sync-from="xsi">
        <field id="displayname" show="true" edit="true"/>
        <field id="firstname" show="true" edit="true"/>
        <field id="lastname" show="true" edit="true"/>
        <field id="mobile-phone" show="true" edit="true"/>
        <field id="work-phone" show="true" edit="true"/>
        <field id="personal-phone" show="true" edit="true"/>
        <field id="extension-phone" show="true" edit="true"/>
        <field id="street" show="true" edit="true"/>
        <field id="city" show="true" edit="true"/>
        <field id="postalcode" show="true" edit="true"/>
        <field id="country" show="true" edit="true"/>
        <field id="JID" show="true" edit="true"/>
        <field id="email" show="true" edit="true"/>
      </contact-card>
    </contacts>
  </services>
</config>

```

```

<field id="conference-phone" show="true" edit="true"/>
<field id="conference-id" show="true" edit="true"/>
<field id="conference-pin" show="true" edit="true"/>
<field id="web-url" show="true" edit="true"/>
<field id="collaboration-room" show="true" edit="true"/>
<additional-field id="title" show="%SHOW_TITLE%"
edit="%ALLOW_EDIT_TITLE%"/>
<additional-field id="department" show="%SHOW_DEPARTMENT%"
edit="%ALLOW_EDIT_DEPARTMENT%"/>
<additional-field id="hiranaga-firstname"
show="%SHOW_HIRAGANAFIRSTNAME%" edit="%ALLOW_EDIT_HIRAGANAFIRSTNAME%"/>
<additional-field id="hiranaga-lastname"
show="%SHOW_HIRAGANALASTNAME%" edit="%ALLOW_EDIT_HIRAGANALASTNAME%"/>
<additional-field id="region" show="%SHOW_REGION%"
edit="%ALLOW_EDIT_REGION%"/>
<additional-field id="location" show="%SHOW_LOCATION%"
edit="%SHOW_LOCATION%"/>
<additional-field id="yahooid" show="%SHOW_YAHOOID%"
edit="%ALLOW_EDIT_YAHOOID%"/>
<additional-field id="pager" show="%SHOW_PAGER%"
edit="%ALLOW_EDIT_PAGER%"/>
<additional-field id="group-id" show="%SHOW_GROUPID%"
edit="%ALLOW_EDIT_GROUPID%"/>
<additional-field id="bw-userid" show="%SHOW_BWUSERID%"/>
</contact-card>

```

The following table describes the DM tags for contact synchronizing.

Tag	Default if Omitted	Supported Values	Example	Description
%CONTACT_SOUR CE_SYNC%	automatic	Xsi, automatic, ldap, automatic- ldap, outlook	<contact-card sync- from="xsi">	Specifies the contact sync source. The default is "automatic".
%SHOW_TITLE%	false	true, false	<additional- field id="title" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%SHOW_DEPARTM ENT%	false	true, false	<additional- field id="departmen t" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%SHOW_HIRAGAN AFIRSTNAME%	false	true, false	<additional- field id="hiranaga- firstname" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%SHOW_HIRAGAN ALASTNAME%	false	true, false	<additional- field id="hiranaga- lastname" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.

Tag	Default if Omitted	Supported Values	Example	Description
%SHOW_REGION%	false	true, false	<additional-field id="region" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%SHOW_LOCATION%	false	true, false	<additional-field id="location" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%SHOW_YAHOOID%	false	true, false	<additional-field id="yahood" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%SHOW_PAGER%	false	true, false	<additional-field id="pager" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%SHOW_GROUPID%	false	true, false	<additional-field id="group-id" show="true" edit="true"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%SHOW_BWUSERID%	false	true, false	<additional-field id="bw-userid" show="true" edit="false"/>	When set to "false", the field is not shown. When set to "true", the field is shown.
%ALLOW_EDIT_TITLE%	false	true, false	<additional-field id="title" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable.
%ALLOW_EDIT_DEPARTMENT%	false	true, false	<additional-field id="department" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable. Editing is disabled if <i>sync-from</i> is set to "automatic".
%ALLOW_EDIT_HIRANAGAFIRSTNAME%	false	true, false	<additional-field id="hiranaga-firstname" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable. Editing is disabled if <i>sync-from</i> is set to "automatic".
%ALLOW_EDIT_HIRANAGALASTNAME%	false	true, false	<additional-field id="hiranaga-lastname" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable. Editing is disabled if <i>sync-from</i> is set to "automatic".
%ALLOW_EDIT_REGION%	false	true, false	<additional-field id="region" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable. Editing is disabled if <i>sync-from</i> is set to "automatic".

Tag	Default if Omitted	Supported Values	Example	Description
%ALLOW_EDIT_LOCATION%	false	true, false	<additional-field id="location" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable. Editing is disabled if <i>sync-from</i> is set to "automatic".
%ALLOW_EDIT_YAHOOID%	false	true, false	<additional-field id="yahooid" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable. Editing is disabled if <i>sync-from</i> is set to "automatic".
%ALLOW_EDIT_PAGER%	false	true, false	<additional-field id="pager" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable. Editing is disabled if <i>sync-from</i> is set to "automatic".
%ALLOW_EDIT_GROUPID%	false	true, false	<additional-field id="group-id" show="true" edit="true"/>	When set to "false", the field is not editable. When set to "true", the field is editable. Editing is disabled if <i>sync-from</i> is set to "automatic".

10.19.3 Integrated Call Window

This feature allows end users to have the call window integrated with the *Main* window. It reduces the number of Communications windows; however, a separate call window can still be opened using an active Communications menu. This configuration setting also applies to Xsi calls. Chats still open in their own window.

See the following example for configuration details.

```
<config version="20">
  <services>
    <auto-show-comm-window
enabled="%SHOW_COMM_WINDOW%"/> <!-- By default BTBC 20.1 will hide
communication windows for audio-only sessions -->
```

The following table describes the DM tag.

Tag	Default if Omitted	Supported Values	Example	Description
%SHOW_COMM_WINDOW%	true	true, false	<auto-show-comm-window enabled="true"/>	The default is "false" to use the integrated call window. If the parameter is omitted, it defaults to "true", which is the behavior in previous releases.

10.19.4 Display Name for Contacts

It is possible to specify the order in which the display name for contacts is provided using the contact card data. Possibilities include:

- Display name.
- First name and last name.

- XMPP name. This was added in Release 21.4.0 for Receptionist interworking. This typically comes from the XMPP roster.
- XMPP address (JID).
- Email address.
- Any of the phone numbers (the first one detected is chosen). The search order for the phone number is:
 - Work phone
 - Extension
 - Mobile phone
 - Home phone
 - Conference number

Note that for Receptionist interworking, the display name is only read and is displayed from the XMPP roster item when configured so that XMPP name entry is present and located before the *JID* entry in the entry list and there are no preceding entries.

Note that the format of the entries is as specified in the following example and cannot be changed. One `<entry>` node is needed for each and cannot be combined.

See the following example for configuration details.

```

<config version="20">
  <contacts>
    <displayname-order> <!-- Sets the ordering of the
displayname selection, in contact list in the contact list entries (which
entry is shown as the display name) -->
      <entry>DisplayName</entry>
      <entry>FirstNameLastName</entry>
      <entry>XmppName</entry>
      <entry>Jid</entry>
      <entry>Email</entry>
      <entry>AnyPhoneNumber</entry>
    </displayname-order>
  </contacts>
</config>

```

10.19.5 Select Service Name Over First Name in Directory Search

Release 22.7.0 introduced a new configuration parameter to select whether the service name parameter or system-wide first name parameter (for instance “Voice Messaging Group” in many cases for conference bridges) from Xsi directory search results is used in the UI when showing search results for virtual subscribers. In general, the service name parameter is only present for virtual subscribers in Cisco BroadWorks, so this parameter only impacts those contacts when returned in search results.

Release 22.7.3 changed the search result UI so that no display name is shown in the contact card of search results for virtual subscribers. The parameter below dictates whether the service name is used as the first name instead of a system-wide string which cannot be localized as the service name can. Deployments intending to localize the search results for virtual subscribers are recommended to set `use-service-name=true` so that the contact cards of search results can have localized values.

For configuration details, see the following example.

```
<config version="20">
  <services>
    <contacts>
      <use-service-name
enabled="%ENABLE_SERVICE_NAME_IN_SEARCH%"/>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to enable showing display name instead. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_DISPLAY_NAME_IN_SEARCH%/>	true	true, false	<use-service-name enabled="true"/>	Set to "true" to show service name parameter contents in search results as the first name for virtual subscribers. Set to "false" to show system-wide first name parameter in search results as the first name for virtual subscribers.

10.19.6 Active Communications Extra Buttons

Starting with Release 20.2.0 (except 22.9.2 through 22.9.8), additional buttons can be configured to be visible in the active Communications area in the *Main* window. The following buttons can be activated:

- Call transfer
- Conferencing
- Call Park

For single-click mode these parameters are disabled. The end user can enable single-click mode in Preferences.

For configuration details, see the following example.

```
<config version="20">
  <services>
    <calls>
      <active-comms>
        <buttons>
          <transfer-button
enabled="%ACTIVE_COMMS_ENABLE_TRANSFER_BUTTON" />
          <conference-button enabled="
ACTIVE_COMMS_ENABLE_CONFERENCE_BUTTON" />
          <call-park-button enabled="
ACTIVE_COMMS_ENABLE_CALL_PARK_BUTTON" />
        </buttons>
      </active-comms>
```

The following table describes the DM tags.

Tag	Default if Omitted	Supported Values	Example	Description
%ACTIVE_COMM_ENABLE_TRANSFER_BUTTON%	false	true, false	<transfer-button enabled="true" />	When set to "true", the Transfer button is enabled. When set to "false", the Transfer button is disabled. The default is "false".
%ACTIVE_COMM_ENABLE_CONFERENCE_BUTTON%	false	true, false	<conference-button enabled="true" />	When set to "true", the Conference button is enabled. When set to "false", the Conference button is disabled. The default is "false".
%ACTIVE_COMM_ENABLE_CALL_PARK_BUTTON%	false	true, false	<call-park-button enabled="true" />	When set to "true", the Call Park button is enabled. When set to "false", the Call Park button is disabled. The default is "false".

Note that the minimum width of the *Main* window increases for each button added.

10.19.7 Minimize After Login

Communicator can be minimized to the system tray after login using a separate configuration parameter. When the Communicator window is active, it also shows in the task bar.

See the following example for configuration details.

```
<config version="20">
  <services>
    <minimize-after-login
enabled="%MINIMIZE_AFTER_LOGIN%" />
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used to enable minimization. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%MINIMIZE_AFTER_LOGIN%	false	true, false	<minimize-after-login enabled="true" />	Set to "true" to minimize Communicator after login.

10.19.8 Auto-Close S4B PSTN Call Window

Release 22.6.0 introduced support to automatically close the Communicator window that was used for a call triggered by a S4B PSTN call. This is related to the typical usage model whereby presence, chat, and VoIP calls take place on the S4B side while Communicator is only used for PSTN calls, triggered via S4B. After login, Communicator is sent to background as "closed", so that it is only accessible through the system tray. If Communicator is either minimized or in the background when a call is triggered outside of Communicator, or a call is answered with Communicator, upon terminating the last call, Communicator is sent to the background.

All other communications related to that call, such as chat, are terminated and the *tab/communications* window is closed prior to sending the application to background. This happens regardless of the user being engaged in ongoing chats, share, or other activities inside or outside the last call that was terminated.

If Communicator is brought manually to the foreground this new behavior does not apply.

The new configuration parameter only applies to S4B branded builds, where the existing configuration option *<minimize-after-login>* is ignored, instead S4B builds a new configuration parameter *<s4b-windowing-model>*. For information on the branding aspects, see the *UC-One Communicator for Desktop Branding Guide*.

For configuration details, see the following example.

```
<config version="20">
  <services>
    <lync-integration enabled="%ENABLE_LYNC_INTEGRATION%">
      <s4b-windowing-model
enabled="%ENABLE_S4B_WINDOWING_MODEL_DESKTOP%" />
    </lync-integration>
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used to enable the configurable web button. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_S4B_WINDOWING_MODEL_DESKTOP%	true	true, false	<s4b-windowing-model enabled="true"/>	Set to "true" to enable the S4B window to auto-close after the call. Set to "false" to disable S4B window to auto-close after the call.

10.19.9 Configurable Web Button and Web Tab View

Starting with Release 21.1.0, it is possible to have an additional left pane icon in the main window. This allows configurable links to web pages added. The web content can be opened either in a web browser or inside the Communicator *Main* window. The feature can be configured to have either one link specified in the main configuration file or several links using a separate XML file that must be configured to show in a web browser. In the latter case, the main configuration file must point to the separate XML file on a web server.

Release 22.2.0 introduced support for web tab view where web content can be opened onto a tab. The same variables are supported as with the web button feature. A new attribute value "tab" is added to the existing web button configuration node.

Release 22.5.0 introduced support for three additional web buttons that follow the same configuration parameter structure. For information on specifying the UI location in the left pane for these new web buttons, see section *10.19.1 Configurable Left Pane Order*.

For configuration details, see the following example.

```
<config version="20">
  <services>
    <web-button
enabled=" %DESKTOP_WEBBUTTON_ENABLED%" type=" %DESKTOP_WEBBUTTON_TYPE%"
target=" %DESKTOP_WEBBUTTON_TARGET%"
url="
http://%BWDEVICEACCESSFQDN%:80/%BWDMSCONTEXT%/ %BWDEVICEACCESSURI%webbut
ton_config.xml">
    </web-button>
  </services>
</config>
```

```

<tooltip language=" %DESKTOP_WEBBUTTON_TOOLTIP_LANGUAGE-
1%">%DESKTOP_WEBBUTTON_TOOLTIP-1%</tooltip>
</web-button>
<web-button-2 enabled="%DESKTOP_WEBBUTTON_2_ENABLED%"
type="%DESKTOP_WEBBUTTON_2_TYPE%"
target="%DESKTOP_WEBBUTTON_2_TARGET%"
url="%DESKTOP_WEBBUTTON_2_URL%">
<tooltip language="%DESKTOP_WEBBUTTON_2_TOOLTIP_LANGUAGE-
1%">%DESKTOP_WEBBUTTON_2_TOOLTIP-1%</tooltip>
</web-button-2>
<web-button-3 enabled="%DESKTOP_WEBBUTTON_3_ENABLED%"
type="%DESKTOP_WEBBUTTON_3_TYPE%"
target="%DESKTOP_WEBBUTTON_3_TARGET%"
url="%DESKTOP_WEBBUTTON_3_URL%">
<tooltip language="%DESKTOP_WEBBUTTON_3_TOOLTIP_LANGUAGE-
1%">%DESKTOP_WEBBUTTON_3_TOOLTIP-1%</tooltip>
</web-button-3>
<web-button-4 enabled="%DESKTOP_WEBBUTTON_4_ENABLED%"
type="%DESKTOP_WEBBUTTON_4_TYPE%"
target="%DESKTOP_WEBBUTTON_4_TARGET%"
url="%DESKTOP_WEBBUTTON_4_URL%">
<tooltip language="%DESKTOP_WEBBUTTON_4_TOOLTIP_LANGUAGE-
1%">%DESKTOP_WEBBUTTON_4_TOOLTIP-1%</tooltip>
</web-button-4>

```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used to enable the configurable web button. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%DESKTOP_WEBBUTTON_ENABLED%	false	true, false	<web-button enabled="true">	Set to "true" to enable the web button. Set to "false" to disable the web button.
%DESKTOP_WEBBUTTON_TYPE%	ext	direct, ext	type="direct"	Specifies if a separate XML file is used to specify many links or if a single link is used inside the configuration file.
%DESKTOP_WEBBUTTON_TARGET%	ext	main, ext, tab	target="ext"	Specifies where the web content is rendered, inside the main window or in a separate web browser (default browser).
Many	empty	string	url="http://domain.com:80/docs/webbutton_config.xml">	This is either the link to a single web page or a link to an XML document listing many links.
%DESKTOP_WEBBUTTON_TOOLTIP_LANGUAGE-1%	en	Communicator languages are listed in the <i>Communicator Language Guide</i> .	<tooltip language="en">Link</tooltip> </web-button>	This is the Communicator language specified for the tooltip.

Tag	Default if Omitted	Supported Values	Example	Description
%DESKTOP_WEBBUTTON_TOOLTIP-1%	empty	string	<tooltip language="en">Link</tooltip>	This is the tooltip text shown in the UI.
%DESKTOP_WEBBUTTON_2_ENABLED%	false	true, false	<web-button-2 enabled="true">	Set to "true" to enable the web button 2. Set to "false" to disable the web button 2.
%DESKTOP_WEBBUTTON_2_TYPE%	ext	direct, ext	type="direct"	Specifies if a separate XML file is used in web button 2 to specify many links or if a single link is used inside the configuration file.
%DESKTOP_WEBBUTTON_2_TARGET%	ext	main, ext, tab	target="ext"	Specifies where the web content is rendered in web button 2, inside the main window or in a separate web browser (default browser).
%DESKTOP_WEBBUTTON_2_URL%	empty	string	url="http://domain.com:80/docs/webbutton2_config.xml">	This is either the link to a single web page or a link to an XML document listing many links for web button 2.
%DESKTOP_WEBBUTTON_2_TOOLTIP_LANGUAGE-1%	en	Communicator languages are listed in the <i>Communicator Language Guide</i> .	<tooltip language="en">Web button 2</tooltip> </web-button>	This is the Communicator language specified for the tooltip in web button 2.
%DESKTOP_WEBBUTTON_2_TOOLTIP-1%	empty	string	<tooltip language="en">Web button 2</tooltip>	This is the tooltip text shown in the UI for web button 2.
%DESKTOP_WEBBUTTON_3_ENABLED%	false	true, false	<web-button-3 enabled="true">	Set to "true" to enable the web button 3. Set to "false" to disable the web button 3.
%DESKTOP_WEBBUTTON_3_TYPE%	ext	direct, ext	type="direct"	Specifies if a separate XML file is used in web button 3 to specify many links or if a single link is used inside the configuration file.
%DESKTOP_WEBBUTTON_3_TARGET%	ext	main, ext, tab	target="ext"	Specifies where the web content is rendered in web button 3, inside the main window or in a separate web browser (default browser).

Tag	Default if Omitted	Supported Values	Example	Description
%DESKTOP_WEBBUTTON_3_URL%	empty	string	url="http://domain.com:80/docs/webbutton3_config.xml">	This is either the link to a single web page or a link to an XML document listing many links for web button 3.
%DESKTOP_WEBBUTTON_3_TOOLTIP_LANGUAGE-1%	en	Communicator languages are listed in the <i>Communicator Language Guide</i> .	<tooltip language="en">Web button 3</tooltip></web-button>	This is the Communicator language specified for the tooltip in web button 3.
%DESKTOP_WEBBUTTON_3_TOOLTIP-1%	empty	string	<tooltip language="en">Web button 3</tooltip>	This is the tooltip text shown in the UI for web button 3.
%DESKTOP_WEBBUTTON_4_ENABLED%	false	true, false	<web-button-4 enabled="true">	Set to "true" to enable the web button 4. Set to "false" to disable the web button 4.
%DESKTOP_WEBBUTTON_4_TYPE%	ext	direct, ext	type="direct"	Specifies if a separate XML file is used in web button 4 to specify many links or if a single link is used inside the configuration file.
%DESKTOP_WEBBUTTON_4_TARGET%	ext	main, ext, tab	target="ext"	Specifies where the web content is rendered in web button 4, inside the main window or in a separate web browser (default browser).
%DESKTOP_WEBBUTTON_4_URL%	empty	string	url="http://domain.com:80/docs/webbutton4_config.xml">	This is either the link to a single web page or a link to an XML document listing many links for web button 4.
%DESKTOP_WEBBUTTON_4_TOOLTIP_LANGUAGE-1%	en	Communicator languages are listed in the <i>Communicator Language Guide</i> .	<tooltip language="en">Web button 4</tooltip></web-button>	This is the Communicator language specified for the tooltip in web button 4.
%DESKTOP_WEBBUTTON_4_TOOLTIP-1%	empty	string	<tooltip language="en">Web button 4</tooltip>	This is the tooltip text shown in the UI for web button 4.

The following table shows configuration parameter combinations.

	Target=main	Target=ext	Target=tab
Type=direct	One web link (web contents is opened within the <i>Main</i> window).	One web link (web contents is opened in an external browser window).	One web link (web contents is opened in a tab).
Type=ext	External links configuration file. The list is rendered in the Communicator window.	Invalid configuration.	External links configuration file. The list is rendered in the Communicator tab.

See the following example for the separate XML file that specifies a number of links.

```
?xml version="1.0"?>
<web-button-list> <!-- root-node for all web-button configurations-->
<group id="1"> <!-- UI groups, one groups is required -->
  <name language="en">Group 2</name>
  <name language="de">Gruppe 2</name>
  <link target="ext" url="http://google.com">
    <title language="en">Search engine</title>
    <title language="de">Suchmaschine</title>
    <description language="en">Google
searches</description>
    <description language="de">Google</description>
  </link>
</group>
<group id="2"> <!-- UI groups, one groups is required -->
  <name language="en">Group 2</name>
  <name language="de">Gruppe 2</name>
  <link target="ext" url="http://twitter.com">
    <title language="en">Tweet</title>
    <title language="de">Ziepen</title>
    <description language="en">Access your
Twitter</description>
    <description language="de">Greifen Sie auf Ihre
Twitter</description>
  </link>
</group></web-button-list>
```

It is also possible to use Communicator variables in dynamic links. Some of the variables are known by the client and some are part of their own profile information.

For more information on the supported variables, see section [10.19.10 Pass Parameters and Encoding Web Button URLs](#).

The following example depicts the usage of the variables. The web-link URL contains JID and language variables:

```
http://domain.com/chatroulette/members/%(JID)/join?lang=%(Language)
```

For user “neil@domain.com” running Communicator in Chinese (simplified), the previous link would lead to an actual request to:

```
http://domain.com/chatroulette/members/neil@domain.com/join?lang=cn_Zh
```

When rendering web content inside Communicator, cookies are supported in Release 21.3.0 and onwards, but the following limitations apply:

- No navigation buttons, address-bars, refresh-buttons, or similar are supported. All navigation shall be implemented inside the HTML that is loaded from the configured URL.

- No guaranteed support for any browser plugins including but not limited to Java, Flash, and Shockwave. It is recommended to use only simple HTML with rudimentary JavaScript.
- Email links or opening a separate browser window from the *Main* window is not supported.
- When rendering content inside the *Main* window, the service provider must make the content match the space available.

Pressing the web-button (on the left pane) returns to the configured URL when already navigated to the linked web content. The *Main* window renders received content, including HTML-error pages.

10.19.10 Pass Parameters and Encoding Web Button URLs

Release 21.4.0 introduced preview support for a new encode-attribute that allows the URI's query part to be encoded (URL-encode on base64-encoding) in the banner and the web button. It also applies to external web button XML. Note that this is not encryption, so the security impact is limited, but it also allows keeping the parameters intact when they are passed through several systems.

Encoding is supported for the following configuration nodes:

- <banner>
- <web-button>
- <link> in external web-button configuration XML

Additionally, the same Communicator variables that were supported for web button previously can be used with the banner as well. Note that these variables only work within Communicator and are independent of DM tags. The variables allow creating dynamic links for web pages.

The following variables are supported:

- %(BWUserID)
- %(FirstName)
- %(LastName)
- %(Username) #This is sip-user name from DM-config
- %(JID)
- %(EmailAddress)
- %(WorkPhone)
- %(MobilePhone)
- %(Extension)
- %(Language) #Currently used language in Communicator
- %(XSP)
- %(BWToken)

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_BANNER_QUERY_ENCODING%	false	true, false	encode="true"	
%ENABLE_WEBBUTTON_QUERY_ENCODING%	false	true, false	encode="true"	

The following examples depict the way in which the variables and encoding work.

All examples use two dynamic parameters: %(xsp) and %(BWUserID). In the examples, the user is using the following values:

- xsp: xsp.goo.org
- BWUserID: dave@domain.net

Banner DM Configuration

The following configuration is in use in this example.

```
<config version="20">
  <services>
    <banner enabled="true" encode="true"
url=https://example.com/users/?xsp=%(xsp) &id=%(BWUserID)
height="50"/>
```

As a result, the following URI is constructed:

https://example.com/users/?xsp=xsp.goo.org&id=dave@domain.net

The final URI used in the UI then becomes (encode=true):

https://example.com/users/?eHNwPXhzcC5nb28ub3JnJmlkPWRhdmVAZG9tYWluLm5ldA%3D%3D

Direct URL for web-button

The following configuration is used in this example.

Note that the configured URI contains additional customer-specific extra query parameters (type and junk). The whole section is encoded.

```
<config version="20">
  <services>
    <web-button
enabled="true" type="direct" target="main" encode="true"
url="https://example.com/users/?type=agent&junk=%(junk) &xsp=%(xsp) &id=%(BWUserID) ">
<tooltip language="en">Labs test apps</tooltip>
</web-button>
```

As a result, the following URI is constructed:

https://example.com/users/?type=agent&junk=%(junk)&xsp=xsp.goo.org&id=dave@domain.net

The final URI then becomes (encode = true):

```
https://example.com/users/?dHlwZT1hZ2VudCZqdW5rPSUoanVuaykmeHNwPXhzcC5nb28ub3JnJmIkPWRhdmVAZG9tYWluLm5ldA%3D%3D
```

External web-button configuration XML

The URI pointing to the external web-button configuration file is not encoded in this example, but the external configuration file is. In addition, using parameters and encoding for the <web-button> node with external XML is allowed as long as the host serving the external web-button XML file supports encoded query string.

The user is running the UC-One in “English”.

The following DM configuration node is used in this example.

```
<config version="20">
    <services>
        <web-button
enabled="true" type="direct" target="main" encode="false"
url=" https://example.com/webbutton/?lang=% (Language) ">
<tooltip language="en">Web Things</tooltip>
</web-button>
```

As a result, the following URI is constructed:

```
https://example.com/webbutton/?lang=en
```

The final URI used in the client UI then becomes (encode = false):

```
https://example.com/webbutton/?lang=en
```

The client is then provided with an external web button XML file based on the previous request as the content of the URL is received.

```
<uc-one-portal> <!-- root-node for all web-button configurations-->
<group id="1"> <!-- UI groups, one groups is required -->
    <name language="en">Internal Sites</name>
    <name language="en">Internal Sites</name>
    <link target="ext" encode="true"
url="https://example.com/users/?xsp=% (xsp) &amp;id=% (BWUserID) ">
    <title language="en">Unite</title>
    <description language="en">Example Site</description>
    </link>
</group>
</uc-one-portal>
```

The web-button in the client’s UI operates now as follows:

Constructed URI:

```
https://example.com/users/?xsp=xsp.goo.org&amp;id=dave@domain.net
```

Final URI rendered in the UI (encode = true):

```
https://example.com/users/?eHNwPXhzcC5nb28ub3JnJmIkPWRhdmVAZG9tYWluLm5ldA%3D%3D
```

When using DM tags in a config template, note that all the variables previously listed must be preceded by another “%” character, for instance:

```
url="http://marketing.domain.com/server/DialogTest/?userID=%%(BWUserID)&jid=%%(JID)&lastname=%%(LastName)"
```

Additionally, the “&” character must be escaped as in the previous example.

When creating a DM tag, the double %% is not needed.

10.19.11 Hide My Room Email Invitation BTBC Link

Release 21.5.2 introduced a new configuration parameter to hide the btbc link (it uses btbc: scheme in the clickable link) in the invitation part from the My Room Email Meeting Invitation in environments where it cannot work. The remaining My Room invitation parts are preserved, that is, the audio details and guest link.

Release 22.6.1 introduced another parameter dictating whether the btbc link is included in Copy Guest Link invitation while the existing configuration only impacts the Email Meeting Invitation feature. This way, service providers can fully control the existence of btbc link in My Room invitations to, for instance, include it in the Copy My Room invitation, and exclude it in the Email Meeting Invitation.

Note that in deployments where the value for include-btbc-link-to-email-invitation is “true”, the value for include-btbc-link-to-copy-guest-link is also “true”. Additionally, when include-btbc-link-to-email-invitation is omitting, its default value “true” is also assigned to include-btbc-link-to-email-invitation. Therefore, the btbc-link would be enabled by default in both the email invitation and copy guest link (to clipboard) if the whole node is omitting.

Release 22.9.8 added another configuration parameter to control the visibility of the My Room email guest invitation menu. See the table that follows for additional details.

See the following example for configuration of this feature.

```
<config version="20">
  <services>
    <rooms enable d="true">
      <myroom enabled="true">
        <guest-client-support enabled="true">
          <guest-client-url>https://xsp.domain.com/cgc/</guest-client-
url>
          <guest-client-domain>kowabunga-guest.broadsoft.com</guest-
client-domain>
          <auto-accept-all>>false</auto-accept-all>
        </guest-client-support>
        <include-btbc-link-to-email-
invitation>%ENABLE_BTBC_LINK_INVITATION%</</include-btbc-link-to-email-
invitation>
        <include-btbc-link-to-copy-guest-
link>%ENABLE_BTBC_LINK_TO_COPY_GUEST_LINK%</include-btbc-link-to-copy-
guest-link>
        <include-email-invitation-
menu>%ENABLE_EMAIL_INVITATION_MENU%</include-email-invitation-menu>
      </myroom>
    </rooms>
  </services>
</config>
```

The following DM tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_BTBC_LINK_INVITATION%	true	true, false	<include-btbc-link-to-email-invitation>>false</include-btbc-link-to-email-invitation>	Select “false” to hide the btbc link from the email invitation. Select “true” to keep the btbc link in the email invitation.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_BTBC_LINK_TO_COPY_GUEST_LINK%	See description	true, false	<include-btbc-link-to-copy-guest-link>true</include-btbc-link-to-copy-guest-link>	Select "false" to not include the btbc-link in the Copy Guest Room invitation. Select "true" to include the btbc-link in the Copy Guest Link invitation. If the <i>include-btbc-link-to-copy-guest-link</i> is omitted, to retain the old behavior by default, its value is considered to be whatever value is currently set for <i>include-btbc-link-to-email-invitation</i> or, if also <i>include-btbc-link-to-email-invitation</i> is omitted, then the value is considered to default to "true".
%ENABLE_EMAIL_INVITATION_MENU%	true	true, false	<include-email-invitation-menu>true</include-email-invitation-menu>	Set to "true" to enable email guest invitation accessibility menu as well as the corresponding icon for sending an email invitation in the My Room UI. Set to "false" to hide the email invitation accessibility menu as well as the corresponding icon for sending an email invitation in the My Room UI.

10.19.12 Configurable History Tab Order

Starting with Release 21.2, the *History* tab order can be configured as shown in the following example.

```
<config version="20">
  <services>

    <timeline>
      <chat q="%TIMELINE_CHAT_Q%"/>
      <calls q="%TIMELINE_CALLS_Q%"/>
      <voicemail q="%TIMELINE_VOICEMAIL_Q%" />
    </timeline>
  </services>
</config>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), are used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%TIMELINE_CHAT_Q%	Middle tab	integer	<calls q="1"/>	Smallest number indicates a position on the far left, and largest on the far right. A value between the largest and the smallest is a position in the middle.

Tag	Default if Omitted	Supported Values	Example	Description
%TIMELINE_CALLS_Q%	Left-most tab	integer	<voicemail q="2"/>	Smallest number indicates a position on the far left and largest on the far right. A value between the largest and the smallest is a position in the middle.
%TIMELINE_VOICEMAIL_Q%	Right-most tab	integer	<chat q="3"/>	Smallest number indicates a position on the far left and largest on the far right. A value between the largest and the smallest is a position in the middle.

10.19.13 Enable Main Window Communications Buttons

Starting with Release 21.6.0, the Communications buttons in the *Main* window are hidden by default. They can be enabled using a new configuration parameter. See the following example.

```
<config version="20">
  <services>

    <bottom-bar visible="%ENABLE_BOTTOM_BAR%" />
  </services>
</config>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 [Communicator Device Type – Custom Tags](#), is used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_BOTTOM_BAR%	false	true, false	<bottom-bar visible="true"/>	Set to "true" to enable <i>Main</i> window bottom-bar Communications buttons. Set to "false" to disable <i>Main</i> window bottom-bar Communications buttons.

10.19.14 Hide Communications Window Notifications and Tones

Release 22.0.0 introduced support for controlling the Communications window notifications and tones.

The following features are supported via configuration:

- Communications window tones controlled by CC-One.
- Notifications (toasters) can be disabled.

See the following example.

```
<config version="20">
  <services>
    <hide-communication-notifications
mode="%HIDE_NOTIFICATIONS_MODE_DESKTOP%" />
    <mute-communication-alert
s mode="%MUTE_ALERTS_MODE_DESKTOP%" />
```

The configuration node controlling the hiding of toasters only affects toasters starting new sessions. Upgrading an audio call to video call is possible from the user with the prompt overlay in the Communications window.

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%HIDE_NOTIFICATIONS_MODE_DESKTOP%	none	all, call, message, none	<hide-communication-notifications mode="all" />	Controls which notification windows (toasters) are hidden based on media-type of the incoming communication.
%MUTE_ALERTS_MODE_DESKTOP%	none	all, call, message, none	<mute-communication-alerts mode="all" />	Controls which audible alert tones are hidden based on media-type of the incoming communication.

The impact of the toaster parameter is depicted in the following table. Share requests are considered to be of type “message” since the invitation to share-session travels over XMPP. Similarly, all chat and message types are considered equal and are controlled as type “message”.

Toaster	Toaster DM Configuration (hide-communication-notifications-mode)			
	all	call	message	none
Incoming call	hidden	hidden	visible	visible
Incoming chat	hidden	visible	hidden	visible
Incoming share	hidden	visible	hidden	visible
Incoming Connect message	hidden	visible	hidden	visible
Invitation to room or group chat	hidden	visible	hidden	visible
Buddy request	visible	visible	visible	visible
Error toaster about forced logout	visible	visible	visible	visible
Error toaster for lost connectivity	visible	visible	visible	visible
BLF window, line ringing	visible	visible	visible	visible

Toaster	Toaster DM Configuration (hide-communication-notifications-mode)			
	all	call	message	none
Call upgrade to video offer in call window	visible	visible	visible	visible

For audible alerts, the previous chart can be used by substituting the hidden with “inaudible” and visible with “audible”.

10.19.15 Communications Window UI Control via API

Release 22.0.0 introduced support for controlling the Communications window UI functionality. This is especially intended for CC-One interworking. In CC-One integration, CC-One modifies the Communicator Desktop client to operate in a mostly hidden mode. When configured, the client’s main UI can remain hidden, and when used for communications, only the relevant parts can be launched by the CC-One client. This feature is also used in conjunction with S4B integration. For more information, see section [10.20 UC-One Add-in for Microsoft Skype for Business \(S4B\)](#).

The following feature is supported via configuration:

- Untabbed Communications window

Additionally, the Desktop API has been enhanced so that CC-One can control the UI of the Communications window.

See the following example.

```
<config version="20">
  <services>

    <use-communication-window type="%COMMUNICATION_WINDOW_TRIGGER%" />
  </services>
</config>
```

Additionally, an existing node is utilized to achieve required end user experience for CC-One:

```
<minimize-after-login enabled="true" />
```

For more information, see section [10.19.7 Minimize After Login](#).

Communicator can be configured to support specific features (that is, video is enabled), but the CC-One client might guide the Communicator client to omit specific functionality for a specific session. For example, CC-One might signal UC-One to place a call and omit video-buttons. Despite this guideline from CC-One, UC-One does not completely hide all references to the Video calling from all locations in the client. If the end user brings the *Main* window to the foreground to access preferences or places a second call with the UC-One client, the video-calling capability will be present. CC-One’s preferences only affect calls started from CC-One.

CC-One cannot enable features that are disabled by the DM configuration file or that are not enabled in the UC-One’s licenses. For example, if the video license omits, CC-One cannot enable video calls from UC-One.

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%COMMUNICATION_WINDOW_TRIGGER%	never	always, api, never	<use-communication-window type="api" />	Switch to control new communication windows, open in tab or in own new window. For S4B integration, the value "never" is recommended to utilize a tab for video calls (audio calls would still only use <i>Main</i> window). The default value "never" takes tabs or <i>Main</i> window into use. While "always" takes Communications window into use. The value "api" is to be used with the Communicator API to show the Communications window when invoked via the Communicator API.

10.19.16 Hide Voice Mail Settings

Release 22.3.1 introduced support to hide voice mail settings (tab). For information on Visual Voice Mail, see section [10.5.15 Visual Voice Mail](#). Release 22.4.0 enhanced the configurability to add the option to only hide the on/off switch for voice mail while leaving all other settings visible. For backward compatibility, the older Boolean values can also still be used (true = "show", false = "hide").

See the following example for configuration details.

```
<config version="20">
  <services>
    <voice-mail enabled="false"
settings="%VOICEMAIL_SETTINGS_ENABLED%" visual-voicemail="true">
    ....
  </voice-mail>
```


The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%VOICEMAIL_SETTINGS_ENABLED%	show	show, hide, hideswitch	<voice-mail settings="show" visual-voicemail="true">	Possible values: <ul style="list-style-type: none"> “show”: Shows all the Voice mail settings including the main switch. This is the default. “hide”: Hides all the voice mail settings (entire Preferences tab). “hideswitch”: Hides only the main voice mail switch but all the other voice mail settings are visible. With this the voice mail cannot be turned on/off from the client at all. One must go to the web portal to do that.

10.19.17 Control Number of Rings for Call Forwarding

Release 22.6.0 introduced support for client-side UI control of the *Preferences* → *Incoming Calls* setting for the maximum number of rings before an incoming call is forwarded when it is not answered. This parameter controls the maximum number of rings visible in the Preferences UI. The deployment requirement is that the corresponding server-side parameter is set to the same value; otherwise, the Communicator UI may show values that are not enabled on the server side or may also show a subset of the values enabled on the server side. This parameter also affects the upper limit of Number of rings before greeting setting under *Voicemail* tab in *Preferences*. Release 22.7.6 introduced a minimum value for the number of rings parameter.

For configuration details, see the following example.

```
<config version="20">
  <services>
    <services>
      <supplementary-services
enabled="%ENABLE_XSI_SRV_MANAGEMENT%" toolbar="%ENABLE_TOOLBAR%"
toolbar-call-settings="%ACCESS_CALL_SETTINGS%">
        <xsi> <!-- Any service can be individually
enabled/disabled, xdm services not supported in BTBC. xdm xsi -->
          <number-of-rings-range
min="%NUMBER_OF_RINGS_RANGE_MIN_VALUE_DESKTOP%"
max="%NUMBER_OF_RINGS_RANGE_MAX_VALUE_DESKTOP%" />
        ....
      </supplementary-services>
    </services>
  </services>
</voice-mail>
```

The following tags, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, are used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%NUMBER_OF_RINGS_RANGE_MAX_VALUE_DESKTOP%	20	0, 2-20	<number-of-rings-range max="8"/>	Set the maximum number of rings before the call is routed to voice mail.

Tag	Default if Omitted	Supported Values	Example	Description
%NUMBER_OF_RINGS_RANGE_MIN_VALUE_DESKTOP%	0	0, 2-20	<number-of-rings-range min="3"/>	Set the minimum number of rings before the call is routed to voice mail.

10.19.18 Hide Spell Checker Settings

Release 22.5.3 introduced support for disabling spell checker and auto-correction as well as hiding the related preferences UI for deployments where the English language is not used.

See the following example for configuration details.

```
<config version="20">
  <services>
    <spell-checker enabled="%ENABLE_SPELL_CHECK_DESKTOP%"/>
    ....
  </voice-mail>
```

The following tag, in the custom *BroadTouch_Tags* set defined in section 3.2 *Communicator Device Type – Custom Tags*, is used for this feature.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_SPELL_CHECK_DESKTOP%"/>	true	true, false	<spell-checker enabled="false"/>	Set to "true" to enable spell checker UI in preferences. The feature itself is disabled by default in the UI when the preferences UI for it is visible. Set to "false" to disable spell checker and auto-correction and hide the related preferences UI.

10.20 UC-One Add-in for Microsoft Skype for Business (S4B)

Microsoft integration allows Communicator to be used for non-S4B calls together with Cisco BroadWorks that manages those calls. The integration works in a different fashion in Release 22.1.0 than in older UC-One clients; therefore, some configuration parameters have been removed.

In this deployment scenario, S4B-to-S4B calls, presence, and chat are typically managed by S4B. For more information on this feature, see the *UC-One Add-in for Microsoft S4B Product Guide*. A separate client module can be enabled for S4B integration. Note that the coloring scheme for the reference client with S4B integration enabled is different from a reference client without S4B enabled.

Release 22.0.0 introduced a new configuration option for auto-showing the dial pad when a new call is made. This is especially intended for the S4B integration cases where a PSTN call is made via S4B and handled by UC-One. For more information, see section [10.1.41 Auto-Show Dial Pad](#).

Release 22.7.5 added a new configuration parameter for selecting whether Personal Assistant (PA) presence or S4B presence overrides when both are used. When set to “true”, setting S4B presence will not clear PA presence, instead PA presence overrides and stays. When disabled, presence change in S4B clears PA state as today. See the table that follows.

See the following example for configuration details.

```

<config version="20">
  <services>
    <lync-integration
enabled="%ENABLE_LYNC_INTEGRATION%">

<pa-presence-precedes-lync-
presence>%PA_PRESENCE_PRECEDES_LYNC_PRESENCE%</pa-presence-precedes-lync-
presence>

<s4b-windowing-model enabled="true" />
  </lync-integration>

```

The following tags, in the custom *BroadTouch_Tags* defined in section 3.2 [Communicator Device Type – Custom Tags](#), are used to enable Lync Integration. The default value is applied when the node is omitted.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_LYNC_INTEGRATION%	false	true, false	<lync-integration enabled="true">	Select “true” to enable Lync Integration. It enables loading the required libraries and makes the client try to connect with Lync. This parameter also enabled default call type calls menu before Release 2.1.5.0. In Release 21.5.0 and later, the default call type menu is always enabled. Note the other recommended settings for minimizing the <i>Main</i> window in section 10.19.7 Minimize After Login as well as other items in the following table.
%PA_PRESENCE_PRECEDES_LYNC_PRESENCE%	false	true, false	<pa-presence-precedes-lync-presence>true</pa-presence-precedes-lync-presence>	Set to “true” to make PA presence take precedence. Set to “false” to make S4B presence to take precedence.

Due to the special deployment model, it is in general recommended to use Lync Integration with the following general settings that assume that S4B is used for presence and chat. It is also possible to use the Minimize After Login feature depending on the usage profiles of S4B and Communicator. This feature minimizes Communicator automatically after login, which can be useful when S4B is the main client being used. For more information on this feature, see section [10.19.7 Minimize After Login](#).

The following table depicts the various configuration parameters related to S4B integration. The recommended default setup in Release 22.1.0 is to use the *Main* window without tabs and with dial pad auto-showing for calls initiated from S4B while otherwise keeping UC-One minimized.

Communicator Feature	Recommended Configuration	Reference Section
XMPP (protocol, presence, and chat) disabled	<pre><protocols> <xmpp enabled="false"> </protocols> <services> <presence enabled="false"> </services> <chat enabled="false"> </chat></pre>	10.3.1 Use Extensible Messaging and Presence Protocol
Video enabled	<pre><services> <video enabled="true"> </services></pre>	10.15 Communicator Packages and Device Management
Full enterprise directory disabled	<pre><services> <contacts> <full-enterprise-directory enabled="false"> <result-limit>0</result-limit> </full-enterprise-directory> </services></pre>	10.5.11 Enterprise Directory Listing
Call history with Xsi	<pre><services> <call-history enabled="true"> </call-history></pre>	10.5.1 Xtended Service Interface Basic Configuration – URL and Version
Live search disabled	<pre><services> <search enabled="false"> <xsi enabled="false"> <outlook-search enabled="false"/> <ldap-search enabled="false"/> </services></pre>	10.5.12 Xsi Directory Search, Enable or Disable 10.10 Search 10.11 Outlook Integration
Auto-show communications window enabled	<pre><services> <auto-show-comm-window enabled="false"/> </services></pre>	10.19.3 Integrated Call Window
Minimize after login enabled	<pre><minimize-after-login enabled="true" /></pre>	10.19.7 Minimize After Login
Auto-show dial pad enabled	<pre><auto-show-dial-pad mode="always" /></pre>	10.1.41 Auto-Show Dial Pad
Lync Integration enabled	<pre><lync-integration enabled="true"></pre>	10.20 UC-One Add-in for Microsoft Skype for Business (S4B)
Communications window type	<pre><use-communication-window type="never" /></pre>	10.19.15 Communications Window UI Control via API

For more information related to Busy-In Call configuration when in Xsi-Only mode, see section [10.1.10 Enable Shared Call Appearance and Automatic Busy – In Call Presence](#).

10.21 API for Third-Party Applications

Starting with Release 20.1.0, an API for third-party applications is supported. For more information, see the *Communicator for Desktop SDK*. The API has different components that can be enabled via configuration as follows:

- HTTP API (always enabled in Release 22.0.0 and later)
- C++ wrapper for the HTTP API in a form of a DLL. This has been deprecated and it is recommended that the HTTP API is used. The DLL wrapper will be removed in upcoming releases, the earliest being Release 23.0.

Cisco made add-ins using the API as well as partners. The following add-ins can be enabled using the configuration parameters in this section:

- Outlook Add-in.
- Compatible headsets, such as Plantronics or Jabra. Note that both the *api-provider* parameter and the *allow-connectors* parameter are needed as per the following table to use third-party add-ins.
- Compatible USB phones. For a non-exhaustive list of tested devices and link to further documentation, see the *Communicator (Desktop, Mobile, and Tablet) Product Guide* or the *Communicator for Desktop User Guide*.

For configuration details, see the following example.

```

<config version="20">
  <services>
    <api-provider enabled="%ENABLE_API_PROVIDER%">
      <allow-connectors>%ALLOW_CONNECTORS%</allow-
connectors> <!-- all|first-party -->
    </api-provider>
  </services>
</config>
```

When *<api-provider>* is "false":

- Nothing connects (including Outlook Add-in): whole tab in preferences is hidden and the *allow-connectors* parameter has no meaning.

When *<api-provider>* is "true":

- Outlook Add-in connects always.
- First-party and third-party applications follow *<allow-connectors>*:
 - all = first-party and third-party add-ins are possible, user controls the acceptance through Preferences
 - "first-party"; only first-party add-ins are possible, user controls then through preferences, user is not asked specifically about them (by default allowed); third-party add-ins are always rejected without user being noticed about them

Release 22.0.0 simplified the API configuration by making HTTP API always enabled.

The following table describes the DM tags.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_API_PROVIDER%	false	true, false	<api-provider enabled="true">	When set to "true", the API is enabled. When set to "false", the API is disabled. The default is "false".
%ALLOW_CONNECTORS%	empty	all, first-party	<allow-connectors>all</allow-connectors>	Either "all" or "first-party" can be specified. "First-party" means that only Cisco-provided add-ins are accepted while "all" means that third-party add-ins can also be used.

10.22 Help URL

Starting with Release 9.3.1, the `<url-help>` element was made obsolete. Clients have a built-in help URL, which is defined when the build is made. This is to handle the case for the *Login* window when no configuration file with a URL is yet available. The help system is accessible from the *Login* screen, which is accessible before the DM configuration file is downloaded by the client. For more information regarding the help URL and its associated parameters, see the branding guides for Desktop, Mobile, and Tablet.

10.23 IPv6

IPv6 is supported as a preview feature in Release 22.4.0 and as an official feature in Release 22.5.0; however, there is no configuration parameter for enabling it. Communicator uses IPv4 when both IPv6 and IPv4 are available. To use IPv6, DNS should return only IPv6 entries for the selected protocol. Mixed protocol operations are also possible so that, for example, SIP uses IPv6 while XMPP would employ IPv4. This is based on DNS resolution. For generic DNS provisioning instructions, see the *UC-one Solution Guide*.

The local machine must have at least one IPv4 network interface also enabled due to OS restrictions.

10.24 BTBC URL Scheme

Communicator Desktop supports its own URL scheme that is used in My Room invitations. It is used to allow an invitation recipient to simply click a link to go into My Room using the native UC-One client instead of using web-based guest client functionality. UC-One client registers the "btbc" uri scheme with the underlying operating system. For Windows, this is done through the Windows registry and for OS X, this is done with the *plist-file* in the *app-package*.

Starting with Release 22.4.0, a similar registration procedure is supported for Callto and Tel URL schemes in *Preferences*. For more information, see the *UC-One Communicator for Desktop User Guide*.

Starting with Release 22.7.0, branding of the supported URL schemes is supported. For more information, see the *UC-One Communicator for Desktop Branding Guide*.

11 Video Optimization

In previous Communicator for Desktop releases, video quality was good when both parties had a good uplink and downlink, good cameras, enough CPU power, and the client had been configured to use a higher bandwidth. However, for Release 20.0.0 and higher, DVBA has been introduced to automatically adjust the frame rate, bit rate, and resolution during a call based on changing network conditions. For more information on DVBA, parameters, see section [10.2.6 Dynamic Video Bit Rate Adaptation](#). Release 21.0.0 uses a different media framework (BME) by default. For more information on the BME, see section [10.2.5 BroadSoft Media Engine \(from Cisco\)](#). The following sections provide more background information and the generally recommended video configurations.

The quality of the video depends on several parameters as follows:

- Video resolution – The higher the resolution, then the better the quality per individual video frame. Lower resolution results in a smaller video size and a less accurate picture.
- Available bandwidth – This must be high enough to allow the video frames to go through without significant packet loss, jitter, or delay.
- Frame rate – If the video frame rate is low, then the video becomes “robotic” since the video frames are not updated fast enough even when the received frames have a high resolution.

Perceived video quality is a compromise between these three parameters. These parameters and their settings in Communicator are described in more detail in the following section.

For better video quality and optimization, the RTCP must be enabled between the caller and the callee to exchange call-related information. The client uses proprietary RTCP signaling, for example, to tell the other endpoint to send less data when it cannot handle all the incoming data and when to tell the other endpoint to send more. Note that this only applies to the previous media framework. The BME does not support this proprietary signaling in this release and only uses standard RTCP.

11.1 Default Video Parameter Values

The following list provides the default values used for the relevant parameters:

- Default video size – Large size can be changed by the end user; corresponds to an H.264 profile level according to the following table.
- Default bit rate – See the following table (configurable per video size). The default for RTP bit rate is “512” (as a fallback).
- Default frame rate – See the following table for the values for each H.264 profile. With BME, the best possible frame rate is selected when the session is started.

Recommended Codecs	Communicator Video Size	H.264 Profile Level	Video Size	FPS Default	Recommended CPU	Default Maximum Bit Rate (Kbps)	Minimum RAM (GB)	H.263 Resolutions
Any supported codec	Small	1.1	174 x 144	15 through 30	Pentium Dual Core 1.7 GHz	192	1	SQCIF
Any supported codec	Medium	2	352 x 288	15 through 30	Pentium Dual Core 1.7 GHz	384	1	QCIF
Any supported codec	Large	3	640 x 480	15 through 30	Pentium Dual Core 1.7 GHz	512	1	CIF

Recommended Codecs	Communicator Video Size	H.264 Profile Level	Video Size	FPS Default	Recommended CPU	Default Maximum Bit Rate (Kbps)	Minimum RAM (GB)	H.263 Resolutions
G.722 for audio, H.264 for video	HD	3.1	1280 x 720	15 through 30	Pentium Quad Core	4096	2	4CIF

11.2 Video Parameter Selection Algorithm

11.2.1 General

Communicator tries to use the largest resolution that fits within the constraints of the maximum bit rate and the maximum frame rate for an H.264 profile level. This applies to both media frameworks used in Release 21.0.0. Several frame sizes (width x height y) are possible within a single H.264 profile level as described in the examples. The client chooses the largest one that still fits within the constraints.

This section describes values for bit rate, frame rate, and resolution that can be used in various cases.

The steps to select the frame rate and the H.264 profile level (resolution) are as follows:

- 1) The H.264 profile level that the client proposes is based on the video size setting in *Preferences*. For the default values for each H.264 profile level for various video sizes, see the table in section 11.1 [Default Video Parameter Values](#).
- 2) The SIP/SDP negotiation with the B-party results in an H.264 profile level being selected. Typically, the same resolution is used for both directions, but asymmetric resolutions are also possible.
- 3) The media framework calculates the best frame rate possible based on the selected H.264 profile level and the configured bit rate as it tries to stay within the bounds specified. The best possible frame rate is selected when the session is started. The closest available camera resolution is used for sending video. For the default bit rates and frame rates, see section 11.1 [Default Video Parameter Values](#). Note that the actual resulting frame rate may be lower than the default requested from the media framework.

At some point, the CPU load becomes a limiting factor for all machines as the frame rate, resolution, and bit rate increase. When the CPU load reaches close to 100%, video quality is impacted. For the measurements that have influenced the current default values for bit rate and frame rate, see the examples.

11.2.2 SIP/SDP Signaling

SIP/SDP signaling negotiates an H.264 profile level (resolution) for the video call. Both parties propose an H.264 profile level based on what they can receive and the callee chooses the outcome. For information on SIP signaling, see *RFC 3261* and *RFC 3264*. In addition, the maximum possible bit rate that can be accepted is shared mutually by the A-party and B-party.

The following video parameters are used for the H.264 profile that the client proposes to the B-party:

- The video size setting found in the *Video* tab of Communicator's *Preferences* page. Each video size maps to a corresponding H.264 profile level.
- The video size-specific default and the minimum and maximum bit rate configuration parameters in the configuration file, determine the upper limit of the RTP bandwidth for the corresponding video size.

- This is the largest available camera resolution that can be used with the H.264 profile in question. Camera resolutions are obtained from the camera.

The H.264 profile level is selected based on the previous parameters and it is the resolution that the client offers to receive in the negotiation.

While the H.264 profile level is negotiated through the SDP, the transmitted bit rate and frame rate are managed dynamically by each client during the call.

H.264 is the recommended video codec for higher quality video, while H.263 was previously used as a backup codec for devices with small resolutions or limited capabilities. Both parties of the video call propose one H.264 profile level to be used. Communicator proposes the best one it can use, while lower profiles are also accepted as part of the negotiation.

11.3 Video Bit Rate Selection

The bit rate can be selected separately for each video size in the BME. The configured default bit rate is used as the maximum. As a fallback, if video size-specific bit rates are not available, then the client uses only the single bit rate parameter in the RTP-section of the configuration file (to select the upper limit for the RTP bit rate for all video resolutions). It does not include the audio bit rate, which is handled separately.

However, the client does not use the bandwidth at the upper limit if it is not necessary. In previous releases, the bit rate had to be set to a lower value to handle office locations, that is, ones with high available bandwidth and remote locations with very limited bandwidth (for roaming users).

Starting with Release 21.0.0, the bit rate can be configured so that each video size set in *Preferences*, has its own upper and lower limits. In Release 21.0.0, this still applies when the previous media framework is used. For more information on how DVBA interacts with video profile bit rate configuration, see section [10.2.6 Dynamic Video Bit Rate Adaptation](#). With the previous media framework, the client starts with the default bit rate trying to keep the bit rate within the bounds specified by the maximum and minimum values. For example, HD requires a higher bandwidth for frame rates higher than 15 fps. The bit rate parameters are independent of the resolution selection and therefore degrade the video quality when the values are too low for the selected resolution.

NOTE: The *bitrate* is determined by the configuration parameters. For higher resolutions, the video maximum, default, and minimum *bitrate* parameters must be set accordingly. In the following example, the maximum *bitrate* for the *Large* video is set to "2048".

```
config>
        <services>
          <calls>
            <video>
              <profiles> <!-- Bitrate is kb/s not kilobyte!
-->

<small enabled="true" min-bitrate="128" default-bitrate="160" max-
bitrate="192" />
<medium enabled="true" min-bitrate="256" default-bitrate="512" max-
bitrate="1024" />
<large enabled="true" min-bitrate="384" default-bitrate="768" max-
bitrate="2048" />
  <hd enabled="true" min-bitrate="512" default-bitrate="1024" max-
bitrate="4096" />
              </profiles>
```

11.4 Video Frame Rate Selection

With BME, the configured bit rate and negotiated H.264 profile level dictates the best possible frame rate that the client tries to take in use in the beginning of the session.

The frame rate is an important factor to provide the best-perceived video quality and in many cases, a lower resolution is better. For example, to avoid a “robotic” video, it is recommended that the frame rate is at least 20 fps. This can be achieved by having a smaller resolution for the individual video frames while still having the bandwidth consumption remain within the upper limit. The media framework automatically adjusts the frame rate depending on the network conditions.

11.5 Optimization Examples

The following table provides generic examples that show how different H.264 profile levels are mapped to resolutions, maximum bit rates, and frame rates.

Level	VBV ¹ Maximum Bit Rate (1000 bits/s)	VBV Buffer Size (1000 bits)	Macroblocks per Second	Resolution and Frame Rate
1	64	175	1485	128x96@30 or 176x144@15
1b	128	350	1485	128x96@30 or 176x144@15
1.1	192	500	3000	176x144@30 or 320x240@10
1.2	384	1000	6000	176x144@60 or 320x240@20
1.3	768	2000	11880	352x288@30
2	2000	2000	11880	352x288@30
2.1	4000	4000	19800	352x288@50
2.2	4000	4000	20250	352x288@50 or 640x480@15
3	10000	10000	40500	720x480@30 or 720x576@25
3.1	14000	14000	108000	1280x720@30
3.2	20000	20000	216000	1280x720@60
4	20000	25000	245760	1920x1088@30 or 2Kx1K@30
4.1	50000	62500	245760	1920x1088@30 or 2Kx1K@30
4.2	50000	62500	522240	1920x1088@60 or 2Kx1K@60
5	135000	135000	589824	2560x1920@30
5.1	240000	240000	983040	4Kx2K@30 or 4096x2304@25

¹ VBV = Video Buffering Verifier

Note that bit rates much lower than the maximum bit rate listed in the previous table are typically used to scale corporate network bandwidth consumption. Subsequent tables provide information specific to Communicator.

The mapping of H.264 profile levels to Communicator (BC) video sizes is as follows:

- HD – H.264 profile level 3.1 is not recommended for sub-optimal network conditions. This is because it results in lower quality for the initial video, that is, before DVBA dynamically adjusts the video quality.
- Large – H.264 profile level 3.0. This is the default.

- Medium – H.264 profile level 2.0. This is to be used when “Large” is not performing well.
- Small – H.264 profile level 1.1 and lower. This is used mainly with mobile devices, often with limited displays and limited network and processing power.

The following table lists examples of combinations of different parameters from actual tests. The tests had lower fps values in favor of lower bit rate settings, which are used in many current deployments. These test results influenced the recommended parameter values described in the previous section. Note that perceived quality also depends on the device drivers and display adapters on a particular machine.

Codec	Communicator Video Size	H.264 Profile Level	Camera Video Size	FPS	CPU	CPU Load	Bit Rate Default (kbps)
H.264	Small	1.1	174 x 144	30	i7-2640M @2.8GHz	N/A	512
H.264	Medium	2	352 x 288	25	i7-2640M @2.8GHz	20%	512
H.264	Large	3	640 x 480	20	i7-2640M @2.8GHz	40%	512
H.264	HD	3.1	1280 x 720	15	i7-2640M @2.8GHz	45%	512
H.264	Small	1.1	174 x 144	30	C2Duo E6850 @3GHz	N/A	512
H.264	Medium	2	352 x 288	25	C2Duo E6850 @3GHz	20%	512
H.264	Large	3	640 x 480	20	C2Duo E6850 @3GHz	50%	512
H.264	HD	3.1	1280 x 720	15	C2Duo E6850 @3GHz	100%	512

11.6 Symmetric Versus Asymmetric Video

By default, Communicator attempts to have symmetric video, that is, the same resolution for both directions, although this is not mandatory.

If the “Large” video size is selected, Communicator offers to receive the “Large” video in SDP. In this case, a specific third-party device such as a desk phone can answer with “Small” but still send “Large”, resulting in a non-symmetric video.

Typically, if Communicator receives an offer with “Small”, then it answers with “Small” and the resolution is the same for both directions. However, the negotiated bit rate can be different.

12 Typical Bandwidth Consumption Scenarios

Video bandwidth is discussed in the previous section while this section focuses on other use cases.

The following table describes the estimated bandwidth consumption for audio calls (RTP).

Audio Codec	Bit Rate (kbps)	Audio Bandwidth (kbps) NEB
G.711	64	87
G.722	64	87
G.729	8	31

13 Version Control and Automatic Upgrade

Version Control uses an XML file on a standard web server. At login, the client checks its version and compares it to the one specified in the network to see if a new version should be used. Downgrade is not supported. Before Release 21.6.0, the XML file is typically located on the Device Management server in Cisco environments. It also supports failover.

Starting with Release 21.6.0, the separate XML is no longer used, and the necessary parameters are provided inside the configuration file to reduce the number of different provisioning files to simplify system setup. See the following example.

If the <Upgrade> tag is missing but an <url> tag is present, the client fetches the file from the URL (that is, retains the previous functionality). If both <Upgrade> and <url> are present, the URL is ignored. For more information, see the *UC-One Solution Guide*. Provisioning steps for version control are also listed in that document.

Release 22.3.0 introduced support for an automatic upgrade where the new software is installed with minimum end-user intervention. In automatic an upgrade, the new software is downloaded silently in the background and validated using a certificate while software installation is done with the previously used settings, for instance Outlook Add-in enabled/disabled, installation done for a single user or all users, shortcuts created, and so on.

Once the software is downloaded, the hash (checksum) is used to confirm the download was successful, only after that will the end user be notified. The service provider is responsible for finding or creating the hash and populating the corresponding DM tags. Additionally, the downloaded installer is validated against the Cisco certificate by the operating system.

The hash specific to each installer file is created by the Cisco branding service when making a branded build, that file is to be placed as the value for the hash DM tag. This is needed for each installer separately. The hash file is available in the branding portal together with the actual installer.

There are three automatic upgrade channels available and the user belongs to only one: alpha, beta, or stable. The channel can be selected by the end user in *Preferences*. The intention of the three independent channels is to assist in deployments where some users first test a new version such as alpha or beta while other users can continue to use the versions they have. The new version is checked only the channel for which the user is configured. For alpha and beta channels, the version specified in configuration is the recommended version while the mandatory version still comes from the default channel.

The values of the DM tags related to automatic upgrade can be managed in the usual manner such as device types or groups in DM to, for instance, limit certain versions to only a subset of users.

New configuration parameters were introduced to the version control configuration node for automatic upgrade, shown in the following example. One parameter enables/disables the automatic upgrade while the polling interval defines how often the client downloads the full configuration file to determine if the software update is available. A 25% random factor is added to the polling interval to distribute the server load more evenly. In addition, the channels have their own parameters. The general login steps for an automatic upgrade are as follows:

- 1) The need for an upgrade is checked using the available versions in the configuration file (downloaded regularly as per the polling interval parameter).
- 2) If there is an upgrade available, then the package is silently downloaded.

- 3) If the download is successful, then the end user is asked whether to upgrade the product.
- 4) If the end user replies “yes”, then the client is exited, and the auto-upgrade starts.

Note that previously by default for users without administrator rights, the automatic upgrade only shows pop-ups in the mandatory upgrade case. Release 22.6.1 added support for a new configuration attribute that allows hiding all automatic upgrade menus and pop-ups if the user does not have administrator rights on the PC. Release 3.9.0/22.9.1 removed the requirement of the end user needing administrator rights.

Release 22.9.6 added a new attribute to hide automatic upgrade preferences items and also re-added the previously used parameter to hide automatic upgrade menus and preferences for non-admins.

The following table shows the different combinations of the two attributes when automatic upgrade has been enabled and also shows how they impact the UI elements.

hide-for-non-admin	hide-settings	Preferences		Menu (check for updates)		Automatic Upgrade Popup	
		Admin	Non-admin	Admin	Non-admin	Admin	Non-admin
true	true	not shown	not shown	shown	not shown	shown	not shown
false	false	shown	shown	shown	shown	shown	shown
false	true	not shown	not shown	shown	shown	shown	shown
true	false	shown	not shown	shown	not shown	shown	not shown

Table 2 Automatic Upgrade Hiding Options

Example DM configuration (note that in this node, the XML is currently case-sensitive):

```

<config>
  <services>
    <version-control enabled="%ENABLE_VERSION_CONTROL_DESKTOP%">
<url>http://%BWDEVICEACCESSFQDN%:80/%BWDMSCONTEXT%/%BWDEVICEACCESSURI%ver
sion_check.xml</url>
    <automatic-upgrade enabled="%ENABLE_AUTOMATIC_UPGRADE_DESKTOP%" auto-
hide-for-non-admin="%HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMIN%" hide-
settings="%HIDE_AUTOMATIC_UPGRADE_SETTINGS%"/>
    <Upgrade>
      <Interval>%AUTOMATIC_UPGRADE_INTERVAL_MINUTES%</Interval>
      <Windows>
        <Must>%MUST_VERSION_WINDOWS%</Must>
        <Recommended>%RECOMMENDED_VERSION_WINDOWS%</Recommended>
        <Download
hash="%URL_HASH_WINDOWS%">%DOWNLOAD_URL_WINDOWS%</Download>
        <alpha
          version="%ALPHA_VERSION_WINDOWS%"
hash="%ALPHA_HASH_WINDOWS%">%ALPHA_URL_WINDOWS%</alpha>
        <beta
          version="%BETA_VERSION_WINDOWS%"
hash="%BETA_HASH_WINDOWS%">%BETA_URL_WINDOWS%</beta>
      </Windows>
      <OSX>
        <Must>%MUST_VERSION_OSX%</Must>

```

```

    <Recommended>%RECOMMENDED_VERSION_OSX%</Recommended>
    <Download hash="%URL_HASH_OSX%">%DOWNLOAD_URL_OSX%</Download>
    <alpha
version="%ALPHA_VERSION_OSX%"
hash="%ALPHA_HASH_OSX%">%ALPHA_URL_OSX%</alpha>
    <beta
version="%BETA_VERSION_OSX%"
hash="%BETA_HASH_OSX%">%BETA_URL_OSX%</beta>
    </OSX>
    </Upgrade>
</version-control>

```

The following custom DM tags can be used.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_VERSION_CONTROL_DESKTOP%	true	true, false	<version-control enabled="true">	Set to "false" to disable version control. Set to "true" to enable version control.
%RECOMMENDED_VERSION_WINDOWS%	none	string	<Recommended>21.0.0.159</Recommended>	Minimum Windows version recommended to be used by end users, as recommended by service provider. Not mandatory to use this version and login can proceed even with older versions although the dialog is shown at every login.
%MUST_VERSION_WINDOWS%	none	string	<Must>21.0.0.159</Must>	Minimum Windows version mandated to be used by end users, as recommended by service provider. Mandatory to use this version or higher, and login cannot proceed with older versions. In addition, the dialog is shown at every login.
%DOWNLOAD_URL_WINDOWS%	none	string	<Download>http://domain.com/client</Download>	URL to the Windows client installer.
%RECOMMENDED_VERSION_OSX%	none	string	<Must>21.0.1.</Must>	Minimum OS X version recommended to be used by end users, as recommended by service provider. Not mandatory to use this version and login may proceed even with older versions although the dialog is shown at every login.
%MUST_VERSION_OSX%	none	string	<Recommended>21.0.1.140</Recommended>	Minimum OS X version mandated to be used by end users, as recommended by service provider. Mandatory to use this version or higher, and login cannot proceed with older versions. In addition, the dialog is shown at every login.
%DOWNLOAD_URL_OSX%	none	string	<Download>http://domain.com/client</Download>	URL to the OS X client installer.

Tag	Default if Omitted	Supported Values	Example	Description
%ENABLE_AUTOMATIC_UPGRADE_DESKTOP%	false	true, false	<automatic-upgrade enabled="true">	Set to "false" to disable automatic upgrade. Set to "true" to enable automatic upgrade.
%AUTOMATIC_UPGRADE_INTERVAL_MINUTES%	0	integer	<Interval>480</Interval>	Polling interval (in minutes) which specifies how often UC-One fetches the full configuration file to see if new software is available. A value of "0" means no polling.
%HIDE_AUTOMATIC_UPGRADE_UI_FOR_NON_ADMINS%	false	true, false	<automatic-upgrade enabled="true" auto-hide-for-non-admin="true/false" hide-settings="true/false" />	Set to "true" to hide all automatic upgrade preferences, menus, and pop-ups for users without administrator rights. Note that if this parameter is set to "true", the non-admin user is able to log in and use Communicator even if it does not fulfill the minimum version requirement. Additionally, even if the auto-upgrade feature is disabled, this parameter (defined under it) still affects the basic version control behavior by also blocking the version control checks for non-admin. Set to "false" to show automatic upgrade preferences, as well as menus and pop-ups for users without administrator rights. For parameter combinations, see Table 2 Automatic Upgrade Hiding Options .
%HIDE_AUTOMATIC_UPGRADE_SETTINGS%	false	true, false	<automatic-upgrade enabled="true" auto-hide-for-non-admin="true/false" hide-settings="true/false" />	Set to "true" to hide automatic upgrade preferences, actual pop-ups and the menu remains. Set to "false" to show automatic upgrade preferences. For parameter combinations, see Table 2 Automatic Upgrade Hiding Options .
%URL_HASH_WINDOWS%	empty	string	<Download hash="https://foobar/btbc-win.hash">	URL to a hash file to validate the upgrade binary (Windows). For the URL and version, the existing tags are used so they are not listed here but in the previous section.
%ALPHA_VERSION_WINDOWS%	empty	string	version="22.2.0.1077"	Alpha client version number (Windows).
%ALPHA_HASH_WINDOW_S%	empty	string	<Download hash="https://foobar/btbc-win.hash">	URL to an alpha channel hash file for validating the upgrade binary (Windows).
%ALPHA_URL_WINDOWS%	empty	string	<Download>http://domain.com/client</Download>	URL to the alpha Windows client installer.

Tag	Default if Omitted	Supported Values	Example	Description
%BETA_VERSION_WINDO WS%	none	string	version="22.2.0.10 78">	Beta client version number (Windows).
%BETA_HASH_WINDOWS %	empty	string	<Download hash="https://foob ar/btbc-win.hash">	URL to a beta channel hash file used to validate the upgrade binary (Windows).
%BETA_URL_WINDOWS%	empty	string	<Download>http:// domain.com/client </Download>	URL to the beta Windows client installer.
%URL_HASH_OSX%	empty	string	<Download hash="https://foob ar/btbc-osx.hash">	URL to a hash file used to validate the upgrade binary (OS X). For URL and version, the existing tags are used so they are not listed here but in the previous section.
%ALPHA_VERSION_OSX%	empty	string	version="22.2.0.11 77"	Alpha client version number (OS X).
%ALPHA_HASH_OSX%	empty	string	<Download hash="https://foob ar/btbc-osx.hash">	URL to an alpha channel hash file for validating the upgrade binary (OS X).
%ALPHA_URL_OSX%	empty	string	<Download>http:// domain.com/client </Download>	URL to the alpha OS X client installer.
%BETA_VERSION_OSX%	none	string	version="22.2.0.11 78">	Beta client version number (OS X).
%BETA_HASH_OSX%	empty	string	<Download hash="" https://foobar/btbc- osx.hash">	URL to a beta channel hash file used to validate the upgrade binary (OS X).
%BETA_URL_OSX%	empty	string	<Download>http:// domain.com/client </Download>	URL to the beta OS X client installer.
%ENABLE_MIGRATION_D ESKTOP%	false	true, false	<migration- upgrade enabled="true" >	Migration enabled or not. True indicates enabled.
%MANDATORY_MIGRATIO N_DESKTOP%	false	true, false	<migration- upgrade enabled=true mandatory=false>	Migration is mandatory. True indicates the user cannot skip.
%MIGRATION_LINK_DESK TOP%	string	string	<migration- link="https://domai n.dom">	Link of the to be migrated application installer. If it is empty or if the link is missing, normal version control is utilized.
%INTERNAL_CERT_EXPIR Y_NOTIFICATION%	true	true, false	<internal-cert- expiry-notification enabled="true">	Internal SSL certificate expiry notification enabled here. When set to "true", indicates it is enabled, and a pop-up will be shown X days before the SSL certificate expires.
%INTERNAL_CERT_EXPIR Y_WARN_BEFORE_DAYS %	90	string	<internal-cert- expiry-notification enabled="true" warn-before-days= "90">	Internal SSL certificate expiry notification shown 90 days before internal SSL certificate expiry date.

Tag	Default if Omitted	Supported Values	Example	Description
%INTERNAL_CERT_EXPIRY_WARN_FREQUENCY_DAYS%	7	string	<internal-cert-expiry-notification-enabled="true" warn-frequency-days = "7" />	Internal SSL certificate expiry notification shown every 7 days in case of SSL certificate expiry date in the given days range.

Full build number is not required. The client is looking at the information it has. Examples for version 21.0.0.159 in use by end user:

Version control example 1:

```
<OSX>
<Must>21.0.0.159</Must>
<Recommended>21.0.1.</Recommended>
<Download>http://domain.com/client</Download>
</OSX>
```

This one recommends an upgrade but does not mandate it since the current version is lower than recommended but the mandated version is the same.

Version control example 2:

```
<OSX>
<Must>21.0.1.</Must>
<Recommended>21.0.1.140</Recommended>
<Download>http://domain.com/client</Download>
</OSX>
```

This one mandates an upgrade since 21.0.1 is newer than 21.0.0.159.

Release 22.9.20 introduced migration pop-up enhancements.

Today when migrating from UC-One to Webex using version control, there are two pop-ups shown. The product has only specified one pop-up while the customer would like to have two with a separate migration link for the Webex landing page or the actual installer.

To cater to both, a new configuration parameter is to be added in the scope of this ticket inside version control node:

```
<version-control enabled="true">
<migration-upgrade enabled=true/false mandatory=false/true migration-link="https://domain.dom">
```

DM tags:

```
%ENABLE_MIGRATION_DESKTOP%
%MANDATORY_MIGRATION_DESKTOP%
%MIGRATION_LINK_DESKTOP%
```

Default values also when node omitting:

```
migration-upgrade enabled=false
mandatory=false
migration-link=empty (=not used)
```

If this node is omitted, migration-upgrade is set to “false, or migration-link is missing, normal version control is utilized. When this node is present with migration-link populated, a migration pop-up would be shown where the end user can accept or reject the upgrade. The migration pop-up indicates to the end user that a new application is being taken into use. The following text is proposed:

“You are migrating to WebEx application. Your contact list or history will not be automatically migrated.”

If the optional migration-link is present, the value from that parameter would be used instead of the <download> parameter inside version control configuration for downloading the Webex installer. If it is not present, the existing <download> parameter and version control is used.

14 Appendix A: TLS Ciphers and OpenSSL

The following table lists the supported TLS ciphers for SIP/TLS on Windows. The SSL Library is integrated with the client on both Windows and Mac OS. Release 21.0.0 (and later) supports TLS 1.2 and other more secure ciphers. CiscoSSL 1.7.1 is the currently used version, roughly matching OpenSSL 1.1.1g. The cipher list cannot be configured in this release. No additions, order changes, or removals are possible via configuration.

The following table lists the supported ciphers on both Mac OS and Windows, where the SSL Library is integrated with Communicator, in the usual case where FIPS is not used. The ciphers are in priority order as proposed by the client to the server in the Client Hello TLS message.

Cipher
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305
DHE-RSA-CHACHA20-POLY1305
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA256
ECDHE-ECDSA-AES256-SHA
ECDHE-RSA-AES256-SHA
DHE-RSA-AES256-SHA
ECDHE-ECDSA-AES128-SHA
ECDHE-RSA-AES128-SHA
DHE-RSA-AES128-SHA
RSA-PSK-AES256-GCM-SHA384
DHE-PSK-AES256-GCM-SHA384
RSA-PSK-CHACHA20-POLY1305

Cipher
DHE-PSK-CHACHA20-POLY1305
ECDHE-PSK-CHACHA20-POLY1305
AES256-GCM-SHA384
PSK-AES256-GCM-SHA384
PSK-CHACHA20-POLY1305
RSA-PSK-AES128-GCM-SHA256
DHE-PSK-AES128-GCM-SHA256
AES128-GCM-SHA256
PSK-AES128-GCM-SHA256
AES256-SHA256
AES128-SHA256
ECDHE-PSK-AES256-CBC-SHA384
ECDHE-PSK-AES256-CBC-SHA
SRP-RSA-AES-256-CBC-SHA
SRP-AES-256-CBC-SHA
RSA-PSK-AES256-CBC-SHA384
DHE-PSK-AES256-CBC-SHA384
RSA-PSK-AES256-CBC-SHA
DHE-PSK-AES256-CBC-SHA
AES256-SHA
PSK-AES256-CBC-SHA384
PSK-AES256-CBC-SHA
ECDHE-PSK-AES128-CBC-SHA256
ECDHE-PSK-AES128-CBC-SHA
SRP-RSA-AES-128-CBC-SHA
SRP-AES-128-CBC-SHA
RSA-PSK-AES128-CBC-SHA256
DHE-PSK-AES128-CBC-SHA256
RSA-PSK-AES128-CBC-SHA
DHE-PSK-AES128-CBC-SHA
AES128-SHA
PSK-AES128-CBC-SHA256
PSK-AES128-CBC-SHA

15 Appendix B: UC-One Communicator DM Tag Provisioning Script

The number of custom DM tags has grown in each release, as many customers prefer to have tags for the new configuration parameters. In an effort to offer mechanisms for provisioning those custom DM tags more easily, this section contains a script that can be run on the Xsp side to assign values to the custom DM tags. This script is intended especially for new deployments where most of the custom DM tags are intended to be used.

Note that this script is only valid for new deployments where custom DM tags are being created. In order to modify existing custom DM tags, the command in the following script must be changed from “add” to “set”.

Script template with only a few custom tags set (in a real deployment, you would need to populate a bigger list of custom tags).

```

%% ***** BroadTouch_Tags - read file *****
%%
%% Instructions:
%% -----
%% - This read file can be used to create, add and set UC-One Communicator
%%   client custom tags
%% - Use %% to comment out any steps not required based on deployment specific
%%   service requirements:
%%     Step 1 -- for new deployments only, create initial tag set label
%%     Step 2 -- add a new custom tag (an entry is required for each new tag)
%%     Step 3 -- set value for an existing custom tag (entry required for each applicable tag)
%%     Step 4 -- display and visually verify tag settings
%%
%% - Edit, modify file as needed respecting command syntax. Save file (e.g. BroadTouch_Tags.txt)
%% - SFTP read file to AS under directory /tmp
%% - Login to AS, bwcli (login as admin)
%% - Execute the following command from bwcli: AS_CLI> r /tmp/BroadTouch_Tags.txt
%% - Verify results
%%
%% -----
%% Step 1: Create Communicator tag set label - BroadTouch_Tags
%% -----
quit all;System;DeviceTagSet
add BroadTouch_Tags
%% -----
%% Step 2: Add Communicator custom tags
%% -----
quit all;System;DeviceTagSet;Tags
add tagSetName BroadTouch_Tags %RTP_VIDEO_MTU% 1200
add tagSetName BroadTouch_Tags %USE_AS_BACKUP_RECORD% false
add tagSetName BroadTouch_Tags %ENABLE_SIP_UPDATE_SUPPORT_DESKTOP% false
add tagSetName BroadTouch_Tags %ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP% true
add tagSetName BroadTouch_Tags %ENABLE_REMOTE_CONTROL_EVENTS_DESKTOP%
true
add tagSetName BroadTouch_Tags %ENABLE_OUTLOOK_SEARCH% false
%% -----
%% Step 3: Set Communicator custom tags (if tag already exists)
%% -----
set tagSetName BroadTouch_Tags %ENABLE_LOCATION% tagvalue true
set tagSetName BroadTouch_Tags %ENABLE_EXECUTIVE_ASSISTANT_DESKTOP% tagvalue
true
%% -----
%% Step 4: Verify custom tags have been correctly defined and set
%% -----

```

```
quit all;System;DeviceTagSet;Tags
get tagSetName BroadTouch_Tags
quit all
```

The following lists most Desktop custom tags with example values. Note that several values such as server URLs must be modified for the deployment and the example values will not work as is.

```
add tagSetName BroadTouch_tags %ACCESS_CALL_SETTINGS% true
add tagSetName BroadTouch_tags %ALLOW_CONNECTORS% all
add tagSetName BroadTouch_tags %AUTODETECT_CONFERENCE% false
add tagSetName BroadTouch_tags %BANNER_HEIGHT% 50
add tagSetName BroadTouch_tags %BANNER_URL% https://domain.com/notifications/
add tagSetName BroadTouch_tags %BRIDGE_ID% meet-me@domain.com
add tagSetName BroadTouch_tags %BSOFT_CALL_INFO% false
add tagSetName BroadTouch_tags %CALL_QUALITY_LOCAL_GROUP%
add tagSetName BroadTouch_tags %CALL_QUALITY_SERVICE_URI%
add tagSetName BroadTouch_tags %CHANNEL_HEARTBEAT% 10000
add tagSetName BroadTouch_tags %CHANNEL_HEARTBEAT_MOBILE% 10000
add tagSetName BroadTouch_tags %CHANNEL_NOT_PERSISTENT% false
add tagSetName BroadTouch_tags %CONFERENCE_TITLE% MyRoom
add tagSetName BroadTouch_tags %CONFERENCE_TYPE% uvs
add tagSetName BroadTouch_tags %DESKTOP_ENABLE_XSI_CONFERENCE% true
add tagSetName BroadTouch_tags %DESKTOP_MWI_ENABLE% true
add tagSetName BroadTouch_tags %DESKTOP_MWI_MODE% explicit
add tagSetName BroadTouch_tags %DESKTOP_WEBBUTTON_ENABLED% true
add tagSetName BroadTouch_tags %DESKTOP_WEBBUTTON_TARGET% main
add tagSetName BroadTouch_tags %DESKTOP_WEBBUTTON_TOOLTIP-1% Web Button
add tagSetName BroadTouch_tags %DESKTOP_WEBBUTTON_TOOLTIP_LANGUAGE-1% en
add tagSetName BroadTouch_tags %DESKTOP_WEBBUTTON_TYPE% ext
add tagSetName BroadTouch_tags %DIRECT_DIAL% true
add tagSetName BroadTouch_tags %DOMAIN_OVERRIDE%
add tagSetName BroadTouch_tags %DOWNLOAD_URL_OSX%
https://btbc.ihs.broadsoft.com:443/dms/bc/pc/BTBC-mac.dmg
add tagSetName BroadTouch_tags %DOWNLOAD_URL_WINDOWS%
https://btbc.ihs.broadsoft.com:443/dms/bc/pc/BTBC-win.exe
add tagSetName BroadTouch_tags %EMERGENCY_NUMBER_LIST%
add tagSetName BroadTouch_tags %ENABLE_ADD_REMOVE_VIDEO% false
add tagSetName BroadTouch_tags %ENABLE_API_PROVIDER% true
add tagSetName BroadTouch_tags %ENABLE_AUDIOCALLS% true
add tagSetName BroadTouch_tags %ENABLE_BANNER% false
add tagSetName BroadTouch_tags %ENABLE_BLF_DIRECT_PICKUP_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_BLF_DISPLAY_CALLER_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_BUSY_LAMP_FIELD_DESKTOP% false
add tagSetName BroadTouch_tags %ENABLE_CALL_CENTER_DESKTOP% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PARK_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_CALL_PULL_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_CALL_RECORDING_DESKTOP% false
add tagSetName BroadTouch_tags
%ENABLE_CALL_SECURITY_CLASSIFICATION_DESKTOP% false
add tagSetName BroadTouch_tags %ENABLE_CHAT% true
add tagSetName BroadTouch_tags %ENABLE_CHAT_RECORD_DESKTOP% false
add tagSetName BroadTouch_tags %ENABLE_CONNECTORS% false
add tagSetName BroadTouch_tags
%ENABLE_CONTACTS_ENTERPRISE_COMMON_SEARCH_DESKTOP% true
add tagSetName BroadTouch_tags
%ENABLE_CONTACTS_ENTERPRISE_SEARCH_DESKTOP% true
add tagSetName BroadTouch_tags
%ENABLE_CONTACTS_GROUP_COMMON_SEARCH_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_CONTACTS_PERSONAL_SEARCH_DESKTOP%
true
```

```

add tagSetName BroadTouch_tags %ENABLE_DND% false
add tagSetName BroadTouch_tags %ENABLE_DVBA% true
add tagSetName BroadTouch_tags %ENABLE_EXECUTIVE_ASSISTANT_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_EXT_SERVICE_VERIFICATION% false
add tagSetName BroadTouch_tags %ENABLE_FILE_TRANSFER% true
add tagSetName BroadTouch_tags %ENABLE_FORCED_LOGOUT% false
add tagSetName BroadTouch_tags %ENABLE_FRAME_RESIZE% true
add tagSetName BroadTouch_tags %ENABLE_FT% true
add tagSetName BroadTouch_tags %ENABLE_IDLE_DETECTION% true
add tagSetName BroadTouch_tags %ENABLE_IM_SECURITY_CLASSIFICATION_DESKTOP%
false
add tagSetName BroadTouch_tags %ENABLE_LOCATION% true
add tagSetName BroadTouch_tags %ENABLE_LYNC_INTEGRATION% true
add tagSetName BroadTouch_tags %ENABLE_MEDIA_SHARE% true
add tagSetName BroadTouch_tags %ENABLE_MEETME_MODERATOR_CONTROLS% true
add tagSetName BroadTouch_tags %ENABLE_MYROOM% true
add tagSetName BroadTouch_tags %ENABLE_NWAY_VIDEO% true
add tagSetName BroadTouch_tags %ENABLE_OFFLINE_INDICATION% false
add tagSetName BroadTouch_tags %ENABLE_OUTLOOK_CALENDAR_PRESENCE% true
add tagSetName BroadTouch_tags %ENABLE_OUTLOOK_SEARCH% true
add tagSetName BroadTouch_tags %ENABLE_PARTICIPANT_SHARE% true
add tagSetName BroadTouch_tags %ENABLE_PASSWORD_UPDATE% true
add tagSetName BroadTouch_tags %ENABLE_PRESENCE% true
add tagSetName BroadTouch_tags %ENABLE_PRESENCE_AWAY% true
add tagSetName BroadTouch_tags %ENABLE_PRESENCE_ON_DEMAND_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_PRESENCE_RULES_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_ROOMCREATION% false
add tagSetName BroadTouch_tags %ENABLE_ROOMS% true
add tagSetName BroadTouch_tags %ENABLE_SHOW_ALL_DIRECTORY% false
add tagSetName BroadTouch_tags %ENABLE_TELEPHONY_PRESENCE% false
add tagSetName BroadTouch_tags %ENABLE_TERMINATING_XSI_CALLS% true
add tagSetName BroadTouch_tags %ENABLE_TEST_CALLS_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_TEST_SERVICES_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_TOOLBAR% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_CALLS% true
add tagSetName BroadTouch_tags %ENABLE_VIDEOCALLS% true
add tagSetName BroadTouch_tags %ENABLE_VISUAL_VOICE_MAIL% true
add tagSetName BroadTouch_tags %ENABLE_WEBCOLLAB% true
add tagSetName BroadTouch_tags %ENABLE_WEB_API% true
add tagSetName BroadTouch_tags %ENABLE_XMPP% true
add tagSetName BroadTouch_tags %ENABLE_XSI_CALLS% true
add tagSetName BroadTouch_tags %ENABLE_XSI_EVENT_CHANNEL% true
add tagSetName BroadTouch_tags %ENABLE_XSI_MIDCALL_CONTROLS% true
add tagSetName BroadTouch_tags %ENABLE_XSI_SEARCH% true
add tagSetName BroadTouch_tags %ENABLE_XSI_SRV_MANAGEMENT% true
add tagSetName BroadTouch_tags %EXT_SERVICE_VERIFICATION_URL%
add tagSetName BroadTouch_tags %FORCED_LOGOUT_APPID% BTBC-DT
add tagSetName BroadTouch_tags %FT_MAX_IN% 50485760
add tagSetName BroadTouch_tags %FT_MAX_OUT% 50485760
add tagSetName BroadTouch_tags %FT_REQUIRE_ENCRYPTION% false
add tagSetName BroadTouch_tags %GUEST_CLIENT_AUTO_ACCEPT% false
add tagSetName BroadTouch_tags %GUEST_CLIENT_DOMAIN% kowabunga-guest
add tagSetName BroadTouch_tags %GUEST_CLIENT_ENABLE% true
add tagSetName BroadTouch_tags %GUEST_CLIENT_ENABLED% true
add tagSetName BroadTouch_tags %GUEST_CLIENT_URL% https://xsp.domain.com/cgc
add tagSetName BroadTouch_tags %IDLE_DETECTION_TIMEOUT% 10
add tagSetName BroadTouch_tags %IMP_SERVER% domain.im
add tagSetName BroadTouch_tags %IM_SECURITY_LEVEL% unclassified
add tagSetName BroadTouch_tags %LEFT_PANE_CONTACTS_Q% 2
add tagSetName BroadTouch_tags %LEFT_PANE_DEFAULT% contacts
add tagSetName BroadTouch_tags %LEFT_PANE_DIALPAD_Q% 5

```



```

add tagSetName BroadTouch_tags %LEFT_PANE_DIRECTORY_Q% 4
add tagSetName BroadTouch_tags %LEFT_PANE_HISTORY_Q% 3
add tagSetName BroadTouch_tags %LEFT_PANE_ROOMS_Q% 1
add tagSetName BroadTouch_tags %LEFT_PANE_WEB_BUTTON_Q% 7
add tagSetName BroadTouch_tags %MAX_CONF_PARTIES% 10
add tagSetName BroadTouch_tags %MUST_VERSION_OSX% 21.0.0.159
add tagSetName BroadTouch_tags %MUST_VERSION_WINDOWS% 20.0.6.3
add tagSetName BroadTouch_tags %NETWORK_HELP_URL%
http://broadtouch.bc.im/BTBC/help/
add tagSetName BroadTouch_tags %PASSWORD_UPDATE_WARN_BEFORE_DAYS% 10
add tagSetName BroadTouch_tags
%PRESENCE_ON_DEMAND_POLL_INTERVAL_DESKTOP% 300
add tagSetName BroadTouch_tags %RECOMMENDED_VERSION_OSX% 21.2.2.18
add tagSetName BroadTouch_tags %RECOMMENDED_VERSION_WINDOWS% 21.2.2.24
add tagSetName BroadTouch_tags %REJECT_WITH_486_DESKTOP% false
add tagSetName BroadTouch_tags %ROOMS_HISTORY_SIZE% 10
add tagSetName BroadTouch_tags %RTCP_XR_AUDIO_ENABLED% false
add tagSetName BroadTouch_tags %RTCP_XR_LOCALGROUP_DESKTOP%
add tagSetName BroadTouch_tags %RTCP_XR_SERVICE_URI%
add tagSetName BroadTouch_tags %SBC_PORT% 5060
add tagSetName BroadTouch_tags %SHARE_TYPE% uss
add tagSetName BroadTouch_tags %SHOW_COMM_WINDOW% false
add tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL%
add tagSetName BroadTouch_tags %SOURCE_PORT% 5060
add tagSetName BroadTouch_tags %SRTP_PREFERENCE% optional
add tagSetName BroadTouch_tags %TCP_SIZE_THRESHOLD% 0
add tagSetName BroadTouch_tags %TEST_NUMBER_DESKTOP-1% +1-234567
add tagSetName BroadTouch_tags %TEST_NUMBER_DESKTOP-2%
add tagSetName BroadTouch_tags %TEST_NUMBER_LANGUAGE_DESKTOP-1% en
add tagSetName BroadTouch_tags %TEST_NUMBER_LANGUAGE_DESKTOP-2%
add tagSetName BroadTouch_tags %TIMELINE_CALLS_Q% 1
add tagSetName BroadTouch_tags %TIMELINE_CHAT_Q% 2
add tagSetName BroadTouch_tags %TIMELINE_VOICEMAIL_Q% 3
add tagSetName BroadTouch_tags %TRANSFER_CALL_TYPE% full
add tagSetName BroadTouch_tags %USE_ALTERNATIVE_IDENTITIES% true
add tagSetName BroadTouch_tags %USE_PROXY_DISCOVERY% false
add tagSetName BroadTouch_tags %USE_SRTP% false
add tagSetName BroadTouch_tags %USE_TLS% false
add tagSetName BroadTouch_tags %USS_ADDRESS% https://uss.ihs.broadsoft.com:8443/uss
add tagSetName BroadTouch_tags %USS_ADDRESS_LIST%
wss://uss1.domain.com:8443/uss,wss://uss2.domain.com:8443/uss
add tagSetName BroadTouch_tags %VERSION_NUMBER% 0
add tagSetName BroadTouch_tags %WEBCOLLAB_BASEDOMAIN% domain.com
add tagSetName BroadTouch_tags %WEBCOLLAB_SUBDOMAIN% webservice
add tagSetName BroadTouch_tags %XMPP_ENCRYPTION% false
add tagSetName BroadTouch_tags %XMPP_REFRESH_ON_TTL%
add tagSetName BroadTouch_tags %XMPP_SRV_ENABLED% true
add tagSetName BroadTouch_tags %XMPP_SSL_ENABLE% false
add tagSetName BroadTouch_tags %XSI_ACTIONS_ENABLED% true
add tagSetName BroadTouch_tags %XSI_ACTIONS_URL%
https://bc.domain.com/com.broadsoft.xsi-actions/v2.0/user/
add tagSetName BroadTouch_tags %XSI_NAMESPACE% http://schema.broadsoft.com/xsi
add tagSetName BroadTouch_tags %XSI_ROOT% https://bc.domain.com/
add tagSetName BroadTouch_tags %XSI_VERSION% v2.0
add tagSetName BroadTouch_tags %ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP% true
add tagSetName BroadTouch_tags %ENABLE_BANNER_QUERY_ENCODING% true
add tagSetName BroadTouch_tags %ENABLE_WEBBUTTON_QUERY_ENCODING% true
add tagSetName BroadTouch_tags %USE_AS_BACKUP_RECORD% v2.0
add tagSetName BroadTouch_tags %ENABLE_REMOTE_CONTROL_EVENTS_DESKTOP% true
add tagSetName BroadTouch_tags %USE_RPORT_IP% true
add tagSetName BroadTouch_tags %ENABLE_EMERGENCY_CALLING% false

```

```
add tagSetName BroadTouch_tags %ENABLE_EMERGENCY_CALL_NOTIFICATION% false
add tagSetName BroadTouch_tags %ENABLE_LOGIN_INFORMATIONAL_DIALOG% false
add tagSetName BroadTouch_tags %DECLINE-BUTTON_URL% http://www.domain.com
add tagSetName BroadTouch_tags %DECLINE-BUTTON_ACTION% disabled
add tagSetName BroadTouch_tags %SHOW_EXT_VERIFICATION_MENU% false
add tagSetName BroadTouch_tags %USE_SESSION_EXT_SERVICE_VERIFICATION% false
add tagSetName BroadTouch_tags %ENABLE_SIP_UPDATE_SUPPORT_DESKTOP% true
add tagSetName BroadTouch_tags %ACTIVE_COMMS_ENABLE_TRANSFER_BUTTON% true
add tagSetName BroadTouch_tags %ACTIVE_COMMS_ENABLE_CONFERENCE_BUTTON%
false
add tagSetName BroadTouch_tags %ACTIVE_COMMS_ENABLE_CALL_PARK_BUTTON% false
add tagSetName BroadTouch_tags %MINIMIZE_AFTER_LOGIN% false
add tagSetName BroadTouch_tags %CONTACT_SOURCE_SYNC% automatic
add tagSetName BroadTouch_tags %ENABLE_LDAP_SEARCH% false
add tagSetName BroadTouch_tags %USE_FOR_SSL_VERIFICATION% false
add tagSetName BroadTouch_tags %UMS_HTTP_SRV_SERVICE_NAME_DESKTOP% _http-
client
add tagSetName BroadTouch_tags %UMS_SRV_ADDRESS_DESKTOP% http://domain.com
add tagSetName BroadTouch_tags %ENABLE_MESSAGE_SYNC_DESKTOP% false
add tagSetName BroadTouch_tags %UMS_USE_SSL% false
add tagSetName BroadTouch_tags %MESSAGE_SYNC_FETCH_PATH_DESKTOP% false
add tagSetName BroadTouch_tags %MESSAGE_SYNC_POST_PATH_DESKTOP% false
add tagSetName BroadTouch_tags %CHAT_PREVENT_CLICKABLE_LINKS% false
add tagSetName BroadTouch_tags %ENABLE_FILE_TRANSFER_FILE_EXTENSION_LIMI T%
false
add tagSetName BroadTouch_tags %WEBCOLLAB_USE_XMPP_CREDENTIALS% true
add tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_START% true
add tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_END% true
add tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_START% true
add tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_END% true
add tagSetName BroadTouch_tags %RTP_VIDEO_MTU% true
add tagSetName BroadTouch_tags %MEDIA_HANDLER% bme
add tagSetName BroadTouch_tags %USE_MEDIASEC_DESKTOP% false
add tagSetName BroadTouch_tags %ENABLE_RE-KEYING_DESKTOP% false
add tagSetName BroadTouch_tags %ENABLE_VERSION_CONTROL_DESKTOP% true
```

Acronyms and Abbreviations

This section lists the acronyms and abbreviations found in this document. The acronyms and abbreviations are listed in alphabetical order along with their meanings.

ACD	Automatic Call Distribution
AE	Assistant–Enterprise
AES	Advanced Encryption Standard
AGC	Automatic Gain Control
ALG	Application Layer Gateway
AMR	Adaptive Multi-Rate
API	Application Programming Interface
ARS	Automatic bitRate Selection
AS	Application Server
AVP	Audio Visual Profile
BLF	Busy Lamp Field
BME	BroadSoft Media Engine (from Cisco)
BWA	BroadWorks Anywhere
BWCLI	BroadWorks Command Line Interface
CA	Certificate Authority
CLI	Command Line Interface
CN	Common Name
CPU	Central Processing Unit
CPULC	CPU Load Control
CSWV	Call Settings Web View
DM	Device Management
DND	Do Not Disturb
DNS	Domain Name System
DOS	Denial of Service
DTAF	Device Type Archive File
DTMF	Dual-Tone Multi-Frequency
DVBA	Dynamic Video Bit Rate Adaptation
ECACS	Emergency Call Address Change Service
EULA	End-User License Agreement
FAC	Feature Access Code
FIPS	Federal Information Processing Standards
FIR	Full Intra Request

FPS	Frames per Second
FQDN	Fully Qualified Domain Name
GMT	Greenwich Mean Time
HID	Human Interface Device
HMAC	Hash Message Authentication Code
IdP	Identity Provider
iLBC	internet Low Bitrate Codec
IM&P	Instant Messaging and Presence
IMS	IP Multimedia Subsystem
IOT	Interoperability Testing
JID	Jabber Identifier
LDAP	Lightweight Directory Access Protocol
LLT	Long-Lived Token
MSI	Microsoft Installer
MSRP	Message Session Relay Protocol
MTU	Maximum Transmission Unit
MUC	Multi-User Chat
MWI	Message Waiting Indicator
NAPTR	Naming Authority Pointer
NAT	Network Address Translation
NSIS	Nullsoft Scriptable Install System
OS	Operating System
PAC	Proxy Auto-Configuration
PAI	P-Asserted-Identity
PEM	P-Early Media
PIV	Personal Identity Verification
PN	Push Notification
PoD	Presence on Demand
PPI	P-Preferred-Identity
PSTN	Public Switched Telephone Network
RTCP	Real-Time Control Protocol
RTP	Real-Time Transport Protocol
SaaS	Software as a Service
SAN	Subject Alternative Name
SASL	Simple Authentication and Security Layer
SAVP	Secure Audio Visual Profile

SBC	Session Border Controller
SCA	Shared Call Appearance
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SFTP	Secure File Transfer Protocol
SIP	Session Initiation Protocol
SNI	Server Name Indication
SRTCP	Secure Real-Time Control Protocol
SRTP	Secure Real-Time Transport Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time to Live
UC	Unified Communications
UCaaS	Unified Communications as a Service
UI	User Interface
UMS	Messaging Server (Cisco BroadWorks)
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USS	Sharing Server (Cisco BroadWorks)
UVS	Video Server (Cisco BroadWorks)
VAD	Voice Activity Detection
VBV	Video Buffering Verifier
VVM	Visual Voice Mail
VXML	Voice Extensible Markup Language
WebRTC	Web Real-Time Communication
WME	Webex Media Engine
WRS	WebRTC Server
XMPP	Extensible Messaging and Presence Protocol
XR	Extended Report
Xsi	Xtended Services Interface
Xsp	Xtended Services Platform