Webex for Cisco BroadWorks Configuration Guide

Release 45.11

Document Version 1

Table of Contents

1 Summary of Changes 1
1.1 Changes for Release 45.11, November 2025 1
1.2 Changes for Release 45.10, October 2025 1
1.3 Changes for Release 45.9, September 2025 1
1.4 Changes for Release 45.8, August 2025 2
1.5 Changes for Release 45.7, July 2025 2
1.6 Changes for Release 45.6, June 2025 2
1.7 Changes for Release 45.5, May 2025 2
1.8 Changes for Release 45.4, April 2025 2
1.9 Changes for Release 45.3, March 2025 2
1.10 Changes for Release 45.2, February 2025 2
1.11 Changes for Release 45.1, January 2025 3
1.12 Changes for Release 44.12, December 2024 3
1.13 Changes for Release 44.11, November 2024 3
1.14 Changes for Release 44.10, October 2024 3
1.15 Changes for Release 44.9, September 2024 3
1.16 Changes for Release 44.8, August 2024 3
1.17 Changes for Release 44.7, July 2024 3
1.18 Changes for Release 44.6, June 2024 3
1.19 Changes for Release 44.5, May 2024 3
1.20 Changes for Release 44.4, April 2024 4
1.21 Changes for Release 44.3, March 2024 4
1.22 Changes for Release 44.2, February 2024 4
1.23 Changes for Release 44.1, January 2024 4
2 Changes for Configuration Files 5
2.1 Changes for Configuration Files for Release 45.11 5
2.2 Changes for Configuration Files for Release 45.10 5
2.3 Changes for Configuration Files for Release 45.9 7
2.4 Changes for Configuration Files for Release 45.8 7
2.5 Changes for Configuration Files for Release 45.7 7
2.6 Changes for Configuration Files for Release 45.6 8
2.7 Changes for Configuration Files for Release 45.5 8
2.8 Changes for Configuration Files for Release 45.4 9
2.9 Changes for Configuration Files for Release 45.3 9
2.10 Changes for Configuration Files for Release 45.2 9
2.11 Changes for Configuration Files for Release 45.1 9
2.12 Changes for Configuration Files for Release 44.12 9
2.13 Changes for Configuration Files for Release 44.11 9
2.14 Changes for Configuration Files for Release 44.10 10

Cisco Confidential

2.15 Changes for Configuration Files for Release 44.9 ... 10
2.16 Changes for Configuration Files for Release 44.8 ... 10
2.17 Changes for Configuration Files for Release 44.7 ... 10
2.18 Changes for Configuration Files for Release 44.6 ... 10
2.19 Changes for Configuration Files for Release 44.5 ... 11
2.20 Changes for Configuration Files for Release 44.4 ... 11
2.21 Changes for Configuration Files for Release 44.3 ... 11
2.22 Changes for Configuration Files for Release 44.2 ... 12
2.23 Changes for Configuration Files for Release 44.1 ... 14

3 Introduction ... 15

4 Installation ... 16
4.1 Localized Client Download ... 16
4.2 Android Client ... 16
4.3 iOS Client ... 16
4.4 Desktop Client ... 16

5 Device Management ... 17
5.1 Device Management Tags ... 17
5.2 Partial Match Enhancements for Device Type Selection ... 18
5.3 Client Configuration ... 19
5.4 Deployment of config-wxt.xml ... 19
5.5 Configuration File (config-wxt.xml) ... 19
5.6 System Default Tags ... 20
5.7 Cisco BroadWorks Dynamic Built-in System Tags ... 20

6 Custom Tags ... 23
6.1 Common Features ... 35
6.1.1 SIP Server Settings ... 35
6.1.2 SIP Over TLS and Secure Real-time Transport Protocol ... 38
6.1.3 3GPP SIP Headers for SRTP ... 40
6.1.4 Force TCP, TLS or UDP Usage and Keepalives ... 40
6.1.5 Configurable Timeout for Opening SIP Socket ... 42
6.1.6 Dynamic SIP Proxy Discovery ... 43
6.1.7 Preferred-Port Usage for SIP ... 48
6.1.8 SIP Failover and Failback ... 48
6.1.9 SIP SUBCSRIBE and REGISTER Refresh and SUBSCRIBE Retry ... 53
6.1.10 Use P-Associated-URIs in REGISTER ... 53
6.1.11 SIP P-Early Media (PEM) Header ... 54
6.1.12 SIP UPDATE Support ... 54
6.1.13 Legacy SIP INFO FIR ... 55
6.1.14 SIP rport Management for NAT Traversal ... 55
6.1.15 SIP Session ID ... 56
6.1.16 Incoming Call Rejection Behavior ... 56

Cisco Confidential

6.1.17 Real-Time Transport Protocol Port Range ... 57
6.1.18 ICE Support (Webex Calling only) ... 57
6.1.19 RTCP MUX ... 58
6.1.20 Transfer ... 58
6.1.21 N-Way Conference Calls ... 59
6.1.22 Call Pull ... 61
6.1.23 Call Park/Retrieve ... 62
6.1.24 Call Statistics ... 63
6.1.25 Call Auto Recovery / Seamless Call Handover ... 63
6.1.26 Call Recording ... 64
6.1.27 Voicemail, Visual Voicemail, Message Waiting Indicator ... 65
6.1.28 Voicemail Transcription for Webex Calling ... 66
6.1.29 Call Settings ... 67
6.1.30 Settings Portal and Web-based Call Settings ... 69
6.1.31 Call Center / Call Queue Login/Logout ... 72
6.1.32 Xtended Services Interface (XSI) ... 72
6.1.33 Codec Configuration ... 76
6.1.34 SIP-URI Dialing ... 78
6.1.35 Call History ... 78
6.1.36 Disable Video Calls ... 79
6.1.37 Emergency (911) Calling - Location Reporting with E911 Provider ... 79
6.1.38 PAI as Identity ... 81
6.1.39 Disable Screen Sharing ... 81
6.1.40 Spam Call Indication ... 81
6.1.41 Noise Removal and Bandwidth Extension for PSTN/Mobile Calls ... 82
6.1.42 QoS DSCP Marking ... 82
6.1.43 Primary Profile ... 83
6.1.44 Block List (Webex Calling only) ... 84
6.1.45 Media Adaptation and Resilience Implementation (MARI) ... 85
6.1.46 Simultaneous Calls with Same User ... 87
6.1.47 RTCP-XR ... 87
6.1.48 Call Forwarding Info ... 88
6.1.49 Caller ID ... 88
6.1.50 Multi-line ... 91
6.1.51 Enhanced SIP Authorization ... 92
6.1.52 Personal Assistant (Away Presence) ... 93
6.1.53 End-to-End Encryption (Webex Calling only) ... 94
6.2 Desktop Only Features ... 95
6.2.1 Forced Logout ... 95
6.2.2 Call Pickup ... 95
6.2.3 Boss-Admin (Executive-Assistant) Support ... 96
6.2.4 Escalate SIP Calls to Meeting (Webex Calling only) ... 97

Cisco Confidential

6.2.5 Desk Phone Control Calling – Auto Answer ... 97
6.2.6 Auto Answer with Tone Notification ... 98
6.2.7 Desk Phone Control – Mid Call Controls – Conference ... 98
6.2.8 Call Pickup Notifications ... 98
6.2.9 Remote Control Event Package ... 100
6.2.10 Survivability Gateway (Webex Calling only) ... 101
6.2.11 Remote Mute Control Event Package (Webex Calling only) ... 101
6.2.12 Move Call ... 102
6.3 Mobile Only Features ... 104
6.3.1 Emergency Calling ... 104
6.3.2 Push Notifications for Calls ... 105
6.3.3 Single Alerting ... 107
6.3.4 Click to Dial (Call Back) ... 107
6.3.5 MNO Support ... 108
6.3.6 Incoming Caller ID ... 112
7 Early Field Trial (BETA) Features ... 114
7.1 Emergency (911) Calling - Cisco Emergency Location Information Service (Webex Calling only) and Configuration Cleanup ... 114
8 Custom Tags Mapping between Webex for Cisco BroadWorks and UC-One ... 118
9 Appendix A: TLS Ciphers ... 126
10 Appendix B: DM Tag Provisioning Script ... 127
10.1 Desktop ... 128
10.2 Mobile ... 131
10.3 Tablet ... 134
10.4 System Tags ... 137
11 Acronyms and Abbreviations ... 138

Cisco Confidential

1 Summary of Changes

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

1.1 Changes for Release 45.11, November 2025

This version of the document includes the following changes:

- Updated section *6.1.35 Call History* – added details about the secondary lines support. Removed section *Unified Call History for Secondary Lines (Webex Calling only)* from the BETA features.
- Moved section *6.1.53 End-to-End Encryption (Webex Calling only)* out of BETA.
- Updated section *6.3.5.3 Outgoing Calling Line Identity (CLID) – Dual Persona*
    - Removed the Hide Caller ID option as now it is part of the common section *6.1.49.1 Outgoing Caller ID*.
    - Updated the config option (config tag and custom tag) for the dual persona.
- Added section *6.1.32 Xtended Services Interface (XSI)* – combining XSI related information.
- Added section *6.1.32.2* XSI Dynamic Proxy Discovery.
- Updated section *6.1.32.2 XSI Dynamic Proxy* Discovery

The Webex App accesses the XSI (XSI-Actions & XSI-Events) and Device Management Service (DMS) services on the XSP. To find the XSI service host(s), the Webex App performs DNS SRV lookup for _xsi-client._tcp.. The SRV points to the configured URL for the XSP hosts or load balancers for the XSI service. If SRV lookup is not available, the Webex App falls back to A/AAAA lookup.

The client attempts to locate the XSP nodes using the following DNS flow:

- Webex app initially retrieves Xsi-Actions/Xsi-Events URLs from Cisco Webex Cloud (entered when creating the associated BroadWorks Calling Cluster). The XSI hostname/domain is parsed from the URL and the client performs SRV lookup as follows:
    - Webex app performs an SRV lookup for _xsi-client._tcp.<xsi domain>
    - If the SRV lookup returns one or more targets:
        - Webex app makes A/AAAA lookup of the XSI hostname and if it is a valid IP address, the XSI hostname is added at the back of the cached list, as a backup service.
        - The client connects to one of the targets based on the SRV priority, then weight (or at random if they're all equal).
    - If the SRV lookup does not return any targets:
        - The Webex app makes A/AAAA lookup of the Root XSI parameter and if it is a valid IP address, this is the only address added to the cached list. This could be a load balancing edge element, or it could be the XSP server itself.

Cisco Confidential

        - The A/AAAA record must resolve to a single IP address for the same reasons.

- Custom XSI-Actions/XSI-Events paths can be set in the DMS config file, as described in the previous section:
    - If there is a difference in the initial XSI Root or Actions paths, the client will re-initialize the XSI Actions/XSI Events connectivity. The first step in this is to perform the same DNS lookup process listed under step 1 - this time requesting a lookup for the value in the %XSI_ROOT_WXT% parameter from its configuration file.
    - Note: Make sure to create the corresponding SRV records if you use this tag to change the XSI interfaces.

The Webex app also has a configurable option to control the XSI proxy discovery. The XSI proxy discovery mode can be used to control the combination of the main XSI hostname (used for the SRV lookup) and/or DNS SRV resolved XSI targets used for the XSI communication. To download the config file, the Webex app initially uses the *srv-host* mode. After the config file is downloaded, the configured proxy discovery *mode* is applied. The proxy discovery *mode* can be one of:

- *host-only* - use only the main XSI hostname, do not trigger DNS SRV lookup
- *srv-only* - do not use the main XSI hostname, rely on the DNS SRV lookup only
- *prefer-srv* - if there are DNS SRV records found, use only them. If not, use the main XSI hostname only
- *srv-host* - (default) if there are DNS SRV records found, use them with priority and append the main XSI hostname at the end of the list as a backup service. If not, use the main XSI hostname

After the DMS config file is downloaded:

- If there is an empty XSI Root or it has the same value as the main XSI hostname, and the proxy discovery mode is different than *srv-host*:
    - *host-only* - update the resulting XSI targets and leave just the main XSI hostname
    - *srv-only* - update the resulting XSI targets and leave just the SRV addresses
    - *prefer-srv* - if there is just one address, it should be the main XSI hostname. If there are more, the main XSI hostname is removed from the list
- If the XSI Root is non-empty and its value is different than the main XSI hostname:
    - Perform new DNS lookup process using the XSI Root value
    - Order the DNS results respecting the proxy discovery mode configured
    - Re-initialize its XSI Actions and XSI Events connectivity

```
<config>
<protocols><xsi>
   <proxy-discovery mode="%XSI_PROXY_DISCOVERY_MODE_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%XSI_PROXY_DISCOVERY_MODE_WXT%	srv-host	host-only, srv-only, prefer-srv, srv-host	Controls how the Webex app should build the list of XSI targets used by the application after the download of the config file. The initial discovery, before the DMS config download, always uses srv-host mode.

- XSI Event Channel – added details about the new inactivity timer and updates related to blacklisting of the XSI hosts.

1.2 Changes for Release 45.10, October 2025

This version of the document includes the following changes:

- Updated section *6.1.21 N-Way Conference Calls* – merged the BETA section *N-Way Conference Calls Enhancement (Webex calling only)*.
- Updated section *6.1.22 Call Pull* – merged the BETA section *Call Pull Enhancements*.
- [**Important**] Added section *Emergency (911) Calling - Cisco Emergency Location Information Service (Webex Calling only) and Configuration Cleanup* in BETA.
    - Document Version 3 – additional details have been included regarding the availability of the Cisco Emergency Location Information service exclusively for the Webex calling deployment type.
- Added section ***Error! Reference source not found.*** in BETA.
- Updated section *6.1.35 Call History* – added clarification that the call history is synchronized across all devices just for the primary line of the user.
- Added section *End-to-End Encryption (Webex Calling only)* in BETA.

1.3 Changes for Release 45.9, September 2025

This version of the document includes the following changes:

- Updated section ***Error! Reference source not found.Error! Reference source not found.*** – added more details.
- Updated section *6.1.22 Call Pull* – added more details regarding the feature dependency on the server-side service configuration.
- Updated section *6.1.25 Call Auto Recovery / Seamless Call Handover* – added more details regarding the feature's dependency on the Call pull feature and the tone played during call recovery.

1.4 Changes for Release 45.8, August 2025

This version of the document includes the following changes:

Cisco Confidential

- Updated section *6.1.33 Codec Configuration* – added details about the maximum H.264 video resolution per platform and the update for the Desktop version of the Webex app.

1.5 Changes for Release 45.7, July 2025

This version of the document includes the following changes:

- Added section ***Error! Reference source not found.Error! Reference source not found.*** in BETA.
- Added section ***Error! Reference source not found.Error! Reference source not found.*** in BETA.

1.6 Changes for Release 45.6, June 2025

There were no changes to this document for this release.

1.7 Changes for Release 45.5, May 2025

This version of the document includes the following changes:

- Removed section Call Queue Agent CLID Selection – deprecated by *6.1.49.1 Outgoing Caller ID*.
- Removed deprecated tags and attributes.

1.8 Changes for Release 45.4, April 2025

This version of the document includes the following changes:

- Moved section *6.1.33.1 AI Codec* – out of BETA.
- Added section *6.1.50 Multi-line* – combined the desktop-only and mobile BETA sections.
- Moved section *6.1.51 Enhanced SIP Authorization* – out of BETA.
- Moved section *6.1.52 Personal Assistant (Away Presence)* as common for Desktop and Mobile

1.9 Changes for Release 45.3, March 2025

There were no changes to this document for this release.

1.10 Changes for Release 45.2, February 2025

This version of the document includes the following changes:

- Added section *Enhanced SIP Authorization****Error! Reference source not found.*** in BETA.

1.11 Changes for Release 45.1, January 2025

This version of the document includes the following changes:

- Moved section *Personal Assistant (Away Presence)* out of BETA.
- Moved section *6.3.2.3 Delivery Mode (Webex Calling only)* out of BETA.

Cisco Confidential

1.12 Changes for Release 44.12, December 2024

There were no changes to this document for this release.

1.13 Changes for Release 44.11, November 2024

This version of the document includes the following changes:

- Added section *Mobile (Webex Calling only)* in BETA.

1.14 Changes for Release 44.10, October 2024

This version of the document includes the following changes:

- Added section *Personal Assistant (Away Presence)* in BETA***Error! Reference source not found.***.
- Added section *Delivery Mode (Webex Calling only)* in BETA.

1.15 Changes for Release 44.9, September 2024

There were no changes to this document for this release.

1.16 Changes for Release 44.8, August 2024

This version of the document includes the following changes:

- Updated section *6.1.33 Codec Configuration* – added clarification about the DTMFs and supported delivery mechanisms.

1.17 Changes for Release 44.7, July 2024

This version of the document includes the following changes:

- Added section *AI Codec* in BETA.
- Updated section *6.1.44 Primary Profile* – removed details about the Webex app behavior priori to Release 43.2.

1.18 Changes for Release 44.6, June 2024

This version of the document includes the following changes:

- Updated section *6.3.6. Incoming Caller ID* – added more details about the native experience and how the feature works.

1.19 Changes for Release 44.5, May 2024

This version of the document includes the following changes:

- Updated section *6.1.18 ICE Support (Webex Calling only)* – added IPv6 support via NAT64.
- Updated section *6.1.49 Caller ID* - added sub-section *6.1.49.2 Remote Caller ID Name*.

1.20 Changes for Release 44.4, April 2024

This version of the document includes the following changes:

- Updated section *6.1.49.1 Outgoing Caller ID*.

Cisco Confidential

- Updated section *Changes for Configuration Files for Release 44.3* – added details about the keepalive updates in 44.3.

1.21 Changes for Release 44.3, March 2024

This version of the document includes the following changes:

- Updated section *6.3.6. Incoming Caller ID*
    - Moved section *6.1.49.1 Outgoing Caller ID* as common for Desktop and Mobile, and updated it with more details.
- Updated section *6.1.4 Force TCP, TLS or UDP Usage and Keepalives* – added details about the configurable keepalives using custom tags.

1.22 Changes for Release 44.2, February 2024

This version of the document includes the following changes:

- Added section *6.3.6 Incoming Caller ID*
- Updated section *6.2.8 Call Pickup Notifications*
    - Added subsection *6.2.8.1 Busy Lamp Field* - moved BLF specifics in it.
    - Added subsection *6.2.8.2 Call Pickup Group (Webex Calling only)*.
- Added section *6.1.48 Call Forwarding Info*.
- Updated section *6.1.8.3 Enforce IP Version* – added details for the new *nat64* mode.
- Updated section *6.1.41 Noise Removal and Bandwidth Extension for PSTN/Mobile Calls* – added details for the new Bandwidth Extension support and the Noise Removal updates. Section *Speech Enhancements for PSTN Calls* is removed from BETA.

1.23 Changes for Release 44.1, January 2024

There were no changes to this document for this release.

Cisco Confidential

2 Changes for Configuration Files

2.1 Changes for Configuration Files for Release 45.11

- The config tag <services><dialing><mobility-persona-management> and the corresponding custom tag %ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT% are deprecated and now part of the unified caller ID config section as tag <services><calls><caller-id><outgoing-calls><mobility>, using the new custom tag %ENABLE_CLID_OUTGOING_CALLS_MOBILITY_WXT%.
- The config tag <services><dialing><calling-line-id-delivery-blocking> and the corresponding custom tag %ENABLE_CLID_DELIVERY_BLOCKING_WXT% are deprecated and now part of the unified caller ID config section as tag <services><calls><caller-id><outgoing-calls><clid-delivery-blocking>, using the new custom tag %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%.
- Added <proxy-discovery> tag in section <config><protocols><xsi>.

```
<config>
<protocols><xsi>
   <event-channel enabled="%ENABLE_XSI_EVENT_CHANNEL_WXT%">
      <proxy-discovery mode="%XSI_PROXY_DISCOVERY_MODE_WXT%"/>
```

- Added <inactivity-timeout> tag in section <protocols><xsi><event-channel>

```
<config>
<protocols><xsi>
   <event-channel enabled="%ENABLE_XSI_EVENT_CHANNEL_WXT%">
      <heartbeat-interval>%CHANNEL_HEARTBEAT_WXT%</heartbeat-interval>
      <inactivity-timeout>%CHANNEL_INACTIVITY_TIMEOUT_WXT%</inactivity-
timeout>
```

The following %TAG% were added:

- %ENABLE_CLID_OUTGOING_CALLS_MOBILITY_WXT%
- %CHANNEL_INACTIVITY_TIMEOUT_WXT%

The following %TAG%s were deprecated:

- %ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT%
- %ENABLE_CLID_DELIVERY_BLOCKING_WXT%

2.2 Changes for Configuration Files for Release 45.10

- [Webex Calling only]
  The <drop-two-party-conference> tag in section <services><calls><conference> now controls an official feature.

```
<config>
<services><calls>
   <conference>
      <drop-two-party-conference
enabled="%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%"/>
```


Cisco Confidential

- The *mode* and *default-active-move-option* (Desktop only) attributes in tag <services><calls><call-pull> now control an official feature.

```
<config>
<services><calls>
   <call-pull enabled="%ENABLE_CALL_PULL_WXT%" mode="%CALL_PULL_MODE_WXT%"
default-active-move-option="%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%"/>
```

- [**Important**] [BETA feature] [Desktop and Tablet only]
  Added section <emergency-location> under <services><emergency-dialing>, deprecating the <services><emergency-dialing><redsky> section.

```
<config><services>
<emergency-dialing enabled="%ENABLE_EMERGENCY_DIALING_WXT%">
   <redsky enabled="%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%"> <!-- DEPRECATED
by <emergency-location> -->
      <held-url>%BWE911-PRIMARY-HELDURL%</held-url>
      <held-org-id>%BWE911-CUSTOMERID%</held-org-id>
      <secret>%BWE911-SECRETKEY%</secret>
      <number-list>%BWE911-EMERGENCY-NUMBER-LIST%</number-list>
      <user-reminder-
timeout>%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%</user-reminder-timeout>
      <user-mandatory-
location>%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%</user-mandatory-
location>
      <user-location-
prompting>%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%</user-location-
prompting>
   </redsky>
   <emergency-location enabled="%ENABLE_EMERGENCY_LOCATION_WXT%"
               provider="%EMERGENCY_LOCATION_PROVIDER_NAME_WXT%">
      <held-url>%BWE911-PRIMARY-HELDURL%</held-url>
      <held-org-id>%BWE911-CUSTOMERID%</held-org-id>
      <secret>%BWE911-SECRETKEY%</secret>
      <number-list>%BWE911-EMERGENCY-NUMBER-LIST%</number-list>
      <user-reminder-
timeout>%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%</user-reminder-
timeout>
      <user-mandatory-
location>%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%</user-mandatory-
location>
      <user-location-
prompting>%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%</user-location-
prompting>
   </emergency-location>
</emergency-dialing>
```

- [Webex Calling only]
  Added tag <e2ee> in section <services><calls>.

```
<config>
<services><calls>
   <e2ee enabled="%ENABLE_CALLS_E2EE_WXT%"/>
```

The following %TAG%s were added:

- %ENABLE_EMERGENCY_LOCATION_WXT%
- %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%

Cisco Confidential

- %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%
- %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%
- %ENABLE_CALLS_E2EE_WXT%

The following %TAG%s were deprecated:

- %EMERGENCY_DIALING_ENABLE_REDSKY_WXT%
- %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%
- %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%
- %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%

For more information check *Emergency (911) Calling - Cisco Emergency Location Information Service (Webex Calling only) and Configuration Cleanup*.

2.3 Changes for Configuration Files for Release 45.9

There were no updates in the configuration files for this version.

2.4 Changes for Configuration Files for Release 45.8

- [Desktop only] Updated the H.264 video resolution to WIDE_FULL_HD – added the resolution, framerate and bitrate attributes in the <codec> tag for H.264 codec under section <services><calls><video><codecs>.

```
<config>
<services><calls>
<video><codecs>
       <codec name="H264" resolution="WIDE_FULL_HD" framerate="30"
bitrate="4000000" priority="1.0" payload="109">
```

2.5 Changes for Configuration Files for Release 45.7

- [BETA feature] [Webex Calling only]
  Added <drop-two-party-conference> tag in section <services><calls><conference>.

```
<config>
<services><calls>
   <conference>
      <drop-two-party-conference
enabled="%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%"/>
```

- [BETA feature]
  Added mode and default-active-move-option (Desktop only) attributes in tag <services><calls><call-pull>.

```
<config>
<services><calls>
   <call-pull enabled="%ENABLE_CALL_PULL_WXT%" mode="%CALL_PULL_MODE_WXT%"
default-active-move-option="%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%"/>
```

The following %TAG%s were added:

- %ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%

Cisco Confidential

- %CALL_PULL_MODE_WXT%
- %CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%

2.6 Changes for Configuration Files for Release 45.6

There were no updates in the configuration files for this version.

2.7 Changes for Configuration Files for Release 45.5

The following sections/tags were removed:

- [D/M] <protocols><sip><credentials>
  - Deprecated with Release 42.12
  - Replaced by the <credentials> for each line under <protocols><sip><lines><line>
- [D] <protocols><sip><auth>
  - Replaced by the <auth> for each line under <protocols><sip><lines><line><credentials>
- [D/M] <protocols><sip><q-value>
  - Deprecated with Release 43.11
  - Replaced by the <q-value> in <protocols><sip><register-failover>
- [D/M] <services><calls><conference><service-uri>
  - Deprecated with Release 42.12
  - Replaced by the. <conference-service-uri> for each line under <protocols><sip><lines><line>
- [D/M] <services><calls><noise-removal>
  - Deprecated with Release 43.12
  - Replaced with the <services><calls><speech-enhancements>
- [D/M] <services><voice-mail><center-number>
  - Deprecated with Release 42.12
  - Replaced by the <voice-mail-number> for each line under <protocols><sip><lines><line>
- [D] <services><call-center-agent><outgoing-calls>
  - Deprecated with Release 44.3
  - Replaced by the <services><calls><caller-id>

The following attributes were removed:

- [D/M] *url* attribute under <services><call-center-agent>
- [D/M] *branding-enabled* attribute under <services><call-center-agent>

Cisco Confidential

The following %TAG%s were removed:

- [D] %ENABLE_CALL_CENTER_AGENT_OUTGOING_CALLS_WXT%

2.8 Changes for Configuration Files for Release 45.4

There were no updates in the configuration files for this version.

2.9 Changes for Configuration Files for Release 45.3

There were no updates in the configuration files for this version.

2.10 Changes for Configuration Files for Release 45.2

- [BETA feature]
  Added tag <enhanced-authorization> under section <protocols><sip>.

```
<config>
<protocols>
  <sip>
    <enhanced-authorization enabled="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

The following %TAG% was added:

- %ENABLE_ENHANCED_AUTHORIZATION_WXT%

2.11 Changes for Configuration Files for Release 45.1

There were no updates in the configuration files for this version.

2.12 Changes for Configuration Files for Release 44.12

There were no updates in the configuration files for this version.

2.13 Changes for Configuration Files for Release 44.11

- [BETA feature] [Mobile only] [Webex Calling only]
  Added multi-line-enabled attribute in the tag <protocols><sip><lines>.
  Added <personal> and <line> sections for the secondary lines under section <protocols><sip><lines>.

```
<config>
<protocols><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
   <personal>
      <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
   </personal>
   <line lineType="%BW-MEMBERTYPE-1%">
      …
   </line>
   <line lineType="%BW-MEMBERTYPE-2%">
      …
   </line>
   …
   <line lineType="%BW-MEMBERTYPE-10%">
```


Cisco Confidential

```
      …
   </line>
</lines>
```

2.14 Changes for Configuration Files for Release 44.10

- [BETA feature]
  Added <personal-assistant> tag under section <services>.

```
<config>
<services>
   <personal-assistant enabled="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

- [BETA feature] [Mobile only] [Webex Calling only]
  Added delivery-mode attribute under the tag <services><push-notifications-for-calls>.

```
<config>
<services>
   <push-notifications-for-calls enabled="true" connect-sip-on-
accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%" ring-timeout-
seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%" delivery-
mode="%PN_FOR_CALLS_DELIVERY_MODE_WXT%">
```

The following %TAG%s were added:

- %PERSONAL_ASSISTANT_ENABLED_WXT%
- %PN_FOR_CALLS_DELIVERY_MODE_WXT%

2.15 Changes for Configuration Files for Release 44.9

There were no updates in the configuration files for this version.

2.16 Changes for Configuration Files for Release 44.8

There were no updates in the configuration files for this version.

2.17 Changes for Configuration Files for Release 44.7

- [BETA feature]
  Added AI codec (xCodec) under section <services><calls><audio><codecs>.

```
<config>
<services><calls>
  <audio>
    <codecs>
      <codec name="opus" priority="1" payload=""/>
      <codec name="xCodec" mode="HP" priority=".99" payload=""/>
      <codec name="xCodec" mode="ULP" priority=".98" payload=""/>
      <codec name="G722" priority=".9" payload=""/>
      <codec name="PCMU" priority=".8" payload=""/>
      <codec name="PCMA" priority=".7" payload=""/>
      <codec name="G729" priority=".5" payload="" vad=""/>
      <codec name="iLBC" priority=".4" payload="" framelength="30"/>
      <codec name="telephone-event" payload="101" in-band="false"/>
```

2.18 Changes for Configuration Files for Release 44.6

There were no updates in the configuration files for this version.

Cisco Confidential

2.19 Changes for Configuration Files for Release 44.5

- [Webex Calling only]
  Added enable-ipv6-support attribute to the <protocols><rtp><ice> tag.

```
<config>
<protocols><rtp>
  <ice enabled="%ENABLE_RTP_ICE_WXT%"
       enable-ipv6-support="%ENABLE_RTP_ICE_IPV6_WXT%"
       mode="%RTP_ICE_MODE_WXT%"
       service-uri="%RTP_ICE_SERVICE_URI_WXT%"
       port="%RTP_ICE_PORT_WXT%"/>
```

- Tag <remote-name> has been added in section <services><calls><caller-id> with <machine> as a sub-tag.

```
<config>
<services><calls>
   <caller-id>
      <remote-name>
         <machine mode="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

The following %TAG%s were added:

- %ENABLE_RTP_ICE_IPV6_WXT%
- %CLID_REMOTE_NAME_MACHINE_MODE_WXT%

2.20 Changes for Configuration Files for Release 44.4

- [Desktop only] [Webex Calling only]
  Added tags <additional-numbers>, <hunt-group> and <clid-delivery-blocking> under section <caller-id><outgoing-calls>.

```
<config>
<services><calls>
  <caller-id>
    <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <additional-numbers
enabled="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
      <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
      <hunt-group enabled="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </outgoing-calls>
```

2.21 Changes for Configuration Files for Release 44.3

- [Desktop only] [Webex Calling only]
  Added <outgoing-calls> under the new <caller-id> section, with <call-center> as a sub-tag.

```
<config>
<services><calls>
  <caller-id>
    <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
    </outgoing-calls>
```


Cisco Confidential

- Added custom tags (%UDP_KEEPALIVE_ENABLED_WXT%, %TCP_KEEPALIVE_ENABLED_WXT% and %TLS_KEEPALIVE_ENABLED_WXT%) to replace the hardcoded keep-alive enabled value for each transport under <protocols><sip><transports>.

```
<config>
<protocols><sip>
<transports>
  <udp>
    <keepalive enabled="%UDP_KEEPALIVE_ENABLED_WXT%">
      …
  </udp>
  <tcp>
    <keepalive enabled="%TCP_KEEPALIVE_ENABLED_WXT%">
      …
  </tcp>
  <tls>
    <keepalive enabled="%TLS_KEEPALIVE_ENABLED_WXT%">
      …
  </tls>
```

The following %TAG%s were added:

- %UDP_KEEPALIVE_ENABLED_WXT%
- %TCP_KEEPALIVE_ENABLED_WXT%
- %TLS_KEEPALIVE_ENABLED_WXT%

2.22 Changes for Configuration Files for Release 44.2

- [Mobile only]
  Added section <caller-id> under <services><calls>. Added sub-tags <incoming-call> and <missed-call>, with new sub-tag <append-number> for both.

```
<config>
<services><calls>
  <caller-id>
    <incoming-calls>
      <append-number
enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
    </incoming-calls>
    <missed-calls>
      <append-number
enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
    </missed-calls>
```

- [Mobile only] [Webex Calling only]
  Added <outgoing-calls> under the new <caller-id> section.

```
<config>
<services><calls>
  <caller-id>
    <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
      <additional-numbers
enabled="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
      <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
      <hunt-group enabled="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
```


Cisco Confidential

```
      <clid-delivery-blocking
enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
    </outgoing-calls>
```

- Added tag <call-forwarding-info> in section <services><calls>.

```
<config>
<services><calls>
  <call-forwarding-info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```

- [Desktop only] [Webex Calling only]
  Added <group-call-pickup-notifications> section under <services><calls>, with <display-caller> and <max-timeout> as sub-tags. Also added <group-call-pickup> tag under each <line> tag in the <protocols><sip><lines> section.

```
<config>
<services><calls>
  <group-call-pickup-notifications enabled="%ENABLE_GCP_NOTIFICATIONS_WXT%">
    <display-caller enabled="%ENABLE_GCP_DISPLAY_CALLER_WXT%"/>
    <max-timeout value="%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%"/>
  </group-call-pickup-notifications>
  …
<protocols><sip>
  <lines>
    <line>
      <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
      ...
    </line>
    <line>
      <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-2%</group-call-pickup>
      ...
    </line>
    …
```

The following %TAG%s were added:

- %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%
- %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%
- %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%
- %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%
- %ENABLE_GCP_NOTIFICATIONS_WXT%
- %ENABLE_GCP_DISPLAY_CALLER_WXT%
- %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%
- %BWGROUP-CALL-PICKUP-BOOL-n%

Cisco Confidential

The following %TAG% was deprecated:

- %ENABLE_NOISE_REMOVAL_WXT%

2.23 Changes for Configuration Files for Release 44.1

There were no updates in the configuration files for this version.

Cisco Confidential

3 Introduction

The purpose of this document is to provide a description of the configuration of the Webex for Cisco BroadWorks client.

The configuration file *config-wxt.xml* is provided in two versions – one for mobile (Android and iOS) and one for desktop (Windows and MacOS).

The clients are configured using a configuration that is not visible to the end user. The *config-wxt.xml* provides server-specific information, such as server addresses and ports and runtime options for the client itself (for example, options visible in the *Settings* screen).

The configuration files are read by the client when it starts, after being retrieved from Device Management. The information from the configuration files is stored encrypted, thus making it invisible and inaccessible to the end user.

NOTE: The XML properties should not contain spaces (for example, <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%"/> instead of <transfer-call enabled = "%ENABLE_TRANSFER_CALLS_WXT%"/>).

Cisco Confidential

4 Installation

The Webex for Cisco BroadWorks clients can be installed from the following:

https://www.webex.com/webexfromserviceproviders-downloads.html

4.1 Localized Client Download

The following localized versions of the Webex for Cisco BroadWorks clients can be downloaded as follows:

https://www.webex.com/ko/webexfromserviceproviders-downloads.html
https://www.webex.com/fr/webexfromserviceproviders-downloads.html
https://www.webex.com/pt/webexfromserviceproviders-downloads.html
https://www.webex.com/zh-tw/webexfromserviceproviders-downloads.html
https://www.webex.com/zh-cn/webexfromserviceproviders-downloads.html
https://www.webex.com/ja/webexfromserviceproviders-downloads.html
https://www.webex.com/es/webexfromserviceproviders-downloads.html
https://www.webex.com/de/webexfromserviceproviders-downloads.html
https://www.webex.com/it/webexfromserviceproviders-downloads.html

4.2 Android Client

The Android client is installed as an application (Android application package [APK]), which keeps the settings- and configuration-related data inside its private area.

There is version control based on the Google Play procedures. A standard Google Play notification is provided (that is, Android automatically indicates that there is a new version of software available).

When the new version is downloaded, the old software is overwritten; however, user data is kept by default.

Note that the user is not required to select any options for installation or un-installation.

4.3 iOS Client

The iOS client is installed as an application, which keeps the settings-related data inside its “sandbox” and the configuration file data is stored encrypted.

There is version control based on the Apple App Store procedures. The App Store icon is highlighted to indicate that there is a new version of software available.

When the new version is downloaded, the old software is overwritten; however, user data is kept by default.

Note that the user is not required to select any options for installation or un-installation.

4.4 Desktop Client

Information about the installation and version control of the desktop client (Windows and MacOS) can be found on the following: https://help.webex.com/en-us/nw5p67g/Webex-Installation-and-Automatic-Upgrade.

Cisco Confidential

5 Device Management

5.1 Device Management Tags

Webex for Cisco BroadWorks uses the *Device Management Tag Sets* shown in the following figure. The *System Default* and custom tag sets are required to provision specific device/client settings. This tag set provides flexibility in managing the client's network/service connectivity settings as well as feature activation controls.

This custom tag set is provisioned by a system administrator through the *System → Resources → Device Management Tag Sets* option. The administrator must add new tag sets:

- Mobile: Connect_Tags
- Tablet: ConnectTablet_Tags
- Desktop: BroadTouch_Tags

Create each individual tag and set its value. Section references provide detailed descriptions for each tag. The custom tags are separated in groups based on the functionality and are discussed later in this document.

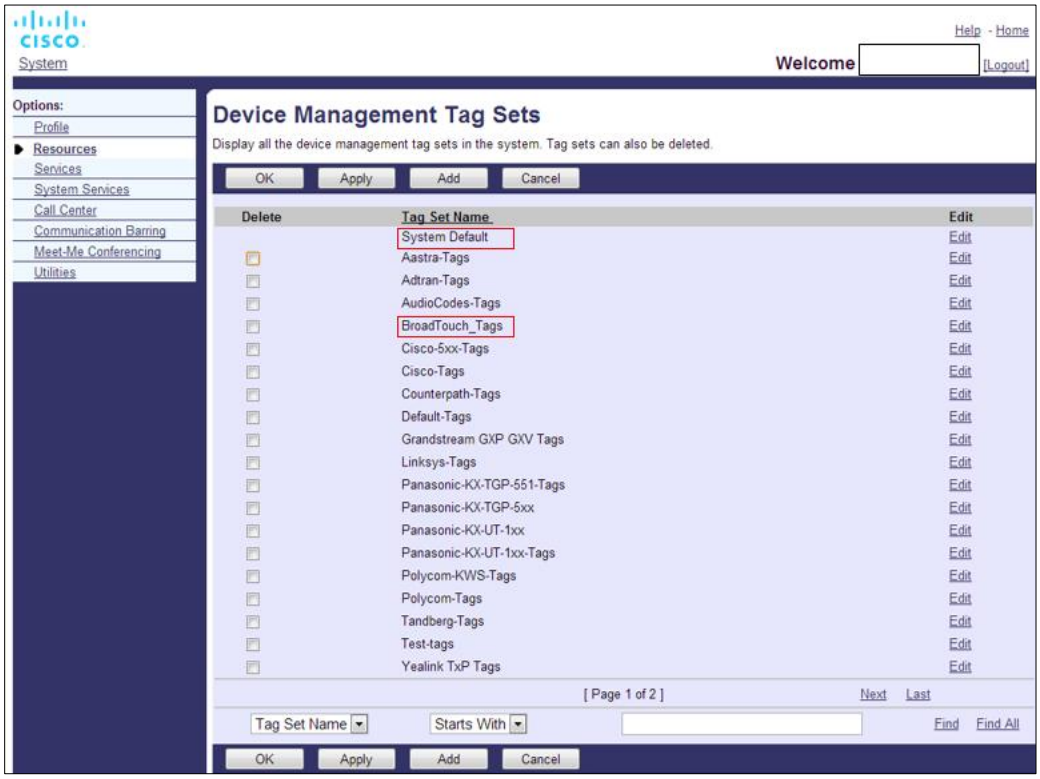


Figure 1 Desktop Device Management Tag Sets

Cisco Confidential

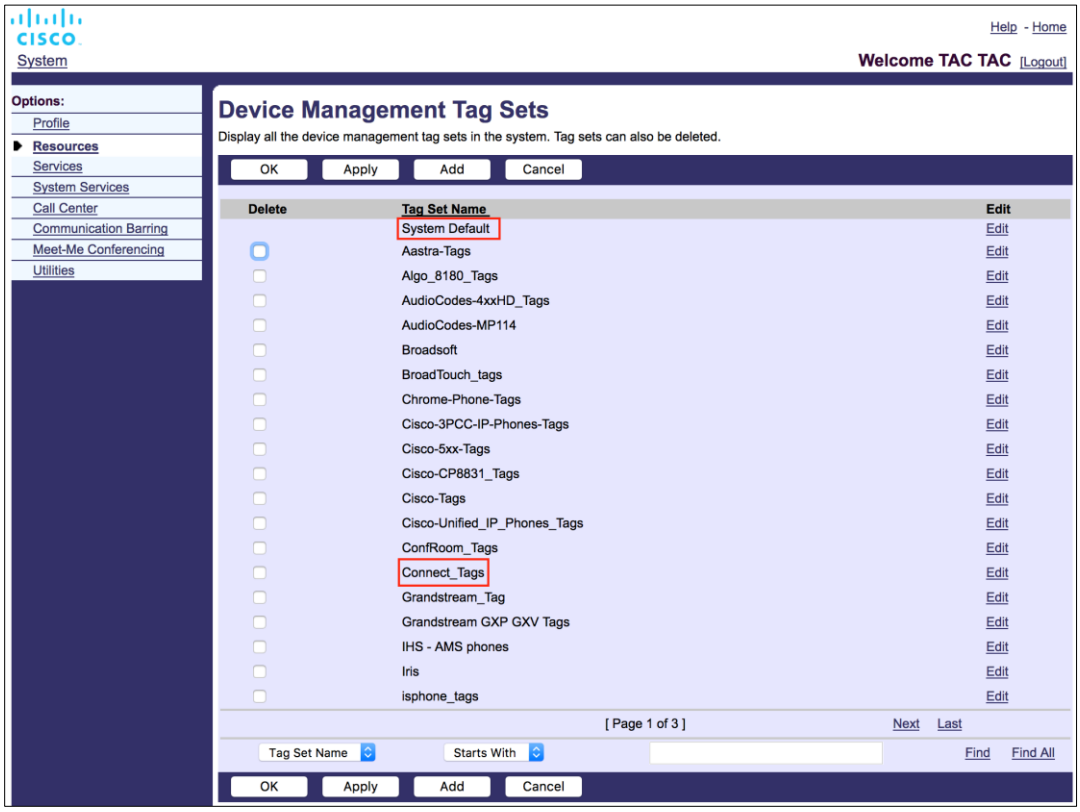


Figure 2 Mobile Device Management Tag Sets

5.2 Partial Match Enhancements for Device Type Selection

To allow increased flexibility when selecting functionality packages for user groups or individual users, the device profile type is selected based on a (first) partial match. This allows customers to use different device types.

The general Device Management procedure specifies that the Cisco BroadWorks Application Server provides a Device Profile Type. It is named “Business Communicator – PC” for desktop, “Connect - Mobile” for mobile, and “Connect – Tablet” for tablet. A Device Profile 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, the client queries the assigned device list via XSI and searches for the corresponding device type profile. The client chooses the first profile that starts with the corresponding device type name. Then the device profile configuration data (configuration file) associated with this device profile is used to enable and disable various features.

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 example, 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 changing the device profile type for them.

Cisco Confidential

Note that it is not expected to have multiple matching device profile types in the received device list XML but only one.

5.3 Client Configuration

The Webex for Cisco BroadWorks version of the client uses the *config-wxt.xml* file for configuration of its calling functionality. There is a separate configuration procedure for Webex that is not covered in this document.

5.4 Deployment of config-wxt.xml

Add the corresponding *config-wxt.xml* file to the “Connect – Mobile”, “Connect – Tablet”, and “Business Communicator – PC” device profiles. Webex for Cisco BroadWorks uses the same device profiles as UC-One so to make it easier for deployment.

> **NOTE 1**: A config file must exist for each device profile.
>
> **NOTE 2**: It is HIHGLY RECOMMENDED the templates to be kept up-to-date with the latest release of the Webex app

5.5 Configuration File (config-wxt.xml)

New custom tags, with **_WXT** suffix, are used to differentiate the new Webex for Cisco BroadWorks configuration deployment from legacy clients. However, there are still some (system) tags that are shared between UC-One and Webex.

Some of the Cisco BroadWorks System Custom Tags are also used in the *config-wxt.xml* configuration file. For more information on each of the following tags, see section *5.7 Cisco BroadWorks Dynamic Built-in* System Tags.

- %BWNETWORK-CONFERENCE-SIPURI-n%
- %BWVOICE-PORTAL-NUMBER-n%
- %BWLINEPORT-n%
- %BWAUTHUSER-n%
- %BWAUTHPASSWORD-n%
- %BWE164-n%
- %BWHOST-n%
- %BWNAME-n%
- %BWEXTENSION-n%
- %BWAPPEARANCE-LABEL-n%
- %BWDISPLAYNAMELINEPORT%
- %BWLINEPORT-PRIMARY%
- %BWE911-PRIMARY-HELDURL%
- %BWE911-CUSTOMERID%

Cisco Confidential

- %BWE911-SECRETKEY%
- %BWE911-EMERGENCY-NUMBER-LIST%
- %BW-MEMBERTYPE-n%
- %BWUSEREXTID-n%
- %BWGROUP-CALL-PICKUP-BOOL-n%" (Webex Calling only)

5.6 System Default Tags

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

Tag	Description
%SBC_ADDRESS_WXT%	This should be configured as the fully qualified domain name (FQDN) or IP address of the session border controller (SBC) deployed in the network. Example: sbc.yourdomain.com
%SBC_PORT_WXT%	If the SBC_ADDRESS_WXT is an IP address, then this parameter should be set to the SBC port. If the SBC_ADDRESS_WXT is an FQDN, then it can be left unset. Example: 5075

5.7 Cisco BroadWorks Dynamic Built-in System Tags

In addition to the default system tags and the custom tags that must be defined, there are 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. Depending on the installed solution package, not all system tags are used.

Tag	Description
%BWNETWORK-CONFERENCE-SIPURI-n%	This is the server URI used to enable N-Way conferencing.
%BWVOICE-PORTAL-NUMBER-n%	This number is used for voicemail. The client dials this number when retrieving voicemail.
%BWLINEPORT-n%	SIP username used in SIP signaling, for example, in registration.
%BWHOST-n%	This is the domain portion of the provisioned line port for the device assigned to the user. It is retrieved from the user's profile. Typically used as the SIP domain.

Cisco Confidential

Tag	Description
%BWAUTHUSER-n%	This is the authentication user name. If the subscriber has been assigned authentication, this is the provisioned user ID on the Authentication page regardless of the selected authentication mode of the device type. The SIP username, typically used in 401 and 407 signaling. Can be different from the default SIP username.
%BWAUTHPASSWORD-n%	This is the user's authentication password. If the subscriber has been assigned authentication, this is the provisioned password on the Authentication page regardless of the selected authentication mode value of the device type. The SIP password used in SIP signaling.
%BWE164-n%	This tag provides the user's phone number in international format.
%BWNAME-n%	This is the subscriber's first name and last name in the user's profile. The first and last names are concatenated together. In case of multi-line configuration, if no line label configured and if not empty, used as display name for the line in the line selector.
%BWEXTENSION-n%	The subscriber's extension is retrieved from the extension provisioned in the user's profile. If an extension has not been provisioned, the tag is replaced with the subscriber's phone number (DN).
%BWAPPEARANCE-LABEL-n%	This is the line label configured. Used as line name, if it is not empty.
%BWDISPLAYNAMELINEPORT%	This is the line/port of the first private line, as opposed to a shared line (Shared Call Appearance). This is the line port provisioned on the device assigned to the user. This is retrieved from the user's profile. Used to identify the primary line of the user.
%BWLINEPORT-PRIMARY%	The primary line port is provisioned on the device that is assigned to the user. This tag does not include the domain portion of the provisioned line port. It is retrieved from the user's profile.
%BWE911-PRIMARY-HELDURL%	Specifies the URL to the RedSky Emergency Location Platform supporting the HELD protocol.
%BWE911-CUSTOMERID%	The customer ID (HeldOrgId, CompanyID) used for the RedSky HTTPS request.
%BWE911-SECRETKEY%	The secret to authenticate the RedSky HTTPS request.

Cisco Confidential

Tag	Description
%BWE911-EMERGENCY-NUMBER-LIST%	The list of emergency numbers supported by RedSky. To use this tag, the %RESERVEDBW911-EMERGENCY-NUMBER-LIST% reserved custom tag must be added to the tag set used by the device type. The “reserved” tag must contain the emergency numbers defined on BroadWorks under AS_CLI/System/CallP/CallTypes > in a comma separated format such as 911, 0911, 933. **NOTE:** The Webex client does not support wildcards in emergency numbers; therefore, only exact emergency numbers should be added to the “reserved” custom tag. The following example shows how the reserved tag functionality is meant to be used: 1) The native tag %BWE911-EMERGENCY-NUMBER-LIST% is added to the template file of the device 2) The reserved custom tag %RESERVEDBW911-EMERGENCY-NUMBER-LIST% is added to the tag set used by the device with value 911, 0911, 933 3) When the file is rebuilt, the %RESERVEDBW911-EMERGENCY-NUMBER-LIST% native tag is resolved to 911, 0911, 933
%BW-MEMBERTYPE-n%	This is the type for each line. It can be one of "Virtual Profile", "User" or "Place".
%BWUSEREXTID-n%	This is the external ID for given line (Webex Calling only)
%BWGROUP-CALL-PICKUP-BOOL-n%"	Provides information if the corresponding line has call pickup group configured. (Webex calling only)

Cisco Confidential

6 Custom Tags

This section describes the custom tags used in Webex for Cisco BroadWorks. It lists all the custom tags used for both Desktop and Mobile/Tablet platforms.

Note, however, that some settings described in this section are supported only for the specific release of the client. To determine if a setting does not apply to an older client version, see the appropriate release-specific configuration guide.

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%ENABLE_REJECT_WITH_486_WXT%	Y	Y	true	*6.1.16 Incoming Call Rejection Behavior*
%REJECT_WITH_XSI_MODE_WXT%	N	Y	decline_false	*6.3.2 Push Notifications for Calls*
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N	Y	busy	*6.3.2 Push Notifications for Calls*
%ENABLE_TRANSFER_CALLS_WXT%	Y	Y	false	*6.1.20 Transfer*
%ENABLE_CONFERENCE_CALLS_WXT%	Y	Y	false	*6.1.21 N-Way Conference Calls*
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	Y	Y	false	*6.1.21 N-Way Conference Calls*
%MAX_CONF_PARTIES_WXT%	Y	Y	10	*6.1.21 N-Way Conference Calls*
%ENABLE_CALL_STATISTICS_WXT%	Y	Y	false	*6.1.24 Call Statistics*
%ENABLE_CALL_PULL_WXT%	Y	Y	false	*6.1.22 Call Pull*
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N	Y	false	*6.3.2 Push Notifications for Calls*
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	Y	Y	false	*6.1.28 Voicemail Transcription for Webex Calling*
%ENABLE_MWI_WXT%	Y	Y	false	*6.1.27 Voicemail, Visual Voicemail, Message Waiting Indicator*
%MWI_MODE_WXT%	Y	Y	empty	*6.1.27 Voicemail, Visual Voicemail, Message Waiting Indicator*
%ENABLE_VOICE_MAIL_WXT%	Y	Y	false	*6.1.27 Voicemail, Visual Voicemail, Message Waiting Indicator*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%ENABLE_VISUAL_VOICE_MAIL_WXT%	Y	Y	false	*6.1.27 Voicemail, Visual Voicemail, Message Waiting Indicator*
%ENABLE_FORCED_LOGOUT_WXT%	Y	N	false	*6.2.1 Forced* Logout
%FORCED_LOGOUT_APPID_WXT%	Y	N	empty	*6.2.1 Forced* Logout
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	Y	Y	false	*6.1.29.1 Call Forwarding Always*
%ENABLE_BROADWORKS_ANYWHERE_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	Y	Y	true	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	Y	Y	false	*6.1.29.3 BroadWorks Anywhere*
%ENABLE_EMERGENCY_DIALING_WXT%	N	Y	false	*6.3.1 Emergency Calling*
%EMERGENCY_DIALING_NUMBERS_WXT%	N	Y	911, 112	*6.3.1 Emergency Calling*
%ENABLE_USE_RPORT_WXT%	Y	Y	false	*6.1.14 SIP rport Management for NAT Traversal*
%RPORT_USE_LOCAL_PORT_WXT%	Y	Y	false	*6.1.14 SIP rport Management for NAT Traversal*
%USE_TLS_WXT%	Y	Y	false	*6.1.2 SIP Over TLS and Secure Real-time Transport Protocol*
%SBC_ADDRESS_WXT%	Y	Y	empty	*5.6 System Default Tags*
%SBC_PORT_WXT%	Y	Y	5060	*5.6 System Default Tags*
%USE_PROXY_DISCOVERY_WXT%	Y	Y	false	*6.1.6 Dynamic SIP Proxy Discovery*
%USE_TCP_FROM_DNS_WXT%	Y	Y	true	*6.1.6 Dynamic SIP Proxy Discovery*
%USE_UDP_FROM_DNS_WXT%	Y	Y	true	*6.1.6 Dynamic SIP Proxy Discovery*
%USE_TLS_FROM_DNS_WXT%	Y	Y	true	*6.1.6 Dynamic SIP Proxy Discovery*
%DOMAIN_OVERRIDE_WXT%	Y	Y	empty	*6.1.6 Dynamic SIP Proxy Discovery*
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	Y	Y	true	*6.1.6 Dynamic SIP Proxy Discovery*
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	Y	Y	true	*6.1.6 Dynamic SIP Proxy Discovery*
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	Y (Windows only)	N	false	*6.1.6 Dynamic SIP Proxy Discovery*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	Y	Y	5000	*6.1.5 Configurable Timeout for Opening SIP Socket*
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	Y	Y	10000	*6.1.5 Configurable Timeout for Opening SIP Socket*
%SOURCE_PORT_WXT%	Y	Y	5060	*6.1.7 Preferred-Port Usage for SIP*
%SIP_FAILBACK_ENABLED_WXT%	Y	N	true	*6.1.8.2 SIP Failback*
%SIP_FAILBACK_TIMEOUT_WXT%	Y	N	900	*6.1.8.2 SIP Failback*
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	Y	N	false	*6.1.8.2 SIP Failback*
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	Y	Y	dns	*6.1.8.3. Enforce IP Version*
%USE_ALTERNATIVE_IDENTITIES_WXT%	Y	Y	false	*6.1.10 Use P-Associated-URIs in REGISTER*
%TCP_SIZE_THRESHOLD_WXT%	Y	Y	18000	*6.1.4 Force TCP, TLS or UDP Usage and Keepalives*
%SIP_REFRESH_ON_TTL_WXT%	Y	N	false	*6.1.8.4 DNS TTL Management*
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	Y	Y	false	*6.1.12 SIP UPDATE Support*
%ENABLE_PEM_SUPPORT_WXT%	Y	Y	false	*6.1.11 SIP P-Early Media (PEM) Header*
%ENABLE_SIP_SESSION_ID_WXT%	Y	Y	false	*6.1.15 SIP Session ID*
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	Y	Y	false	*6.1.13 Legacy SIP INFO FIR*
%SRTP_ENABLED_WXT%	Y	Y	false	*6.1.2 SIP Over TLS and Secure Real-time Transport Protocol*
%SRTP_MODE_WXT%	Y	Y	false	*6.1.2 SIP Over TLS and Secure Real-time Transport Protocol*
%ENABLE_REKEYING_WXT%	Y	Y	true	*6.1.2 SIP Over TLS and Secure Real-time Transport Protocol*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%RTP_AUDIO_PORT_RANGE_START_WXT%	Y	Y	8000	*6.1.17 Real-Time Transport Protocol Port Range*
%RTP_AUDIO_PORT_RANGE_END_WXT%	Y	Y	8099	*6.1.17 Real-Time Transport Protocol Port Range*
%RTP_VIDEO_PORT_RANGE_START_WXT%	Y	Y	8100	*6.1.17 Real-Time Transport Protocol Port Range*
%RTP_VIDEO_PORT_RANGE_END_WXT%	Y	Y	8199	*6.1.17 Real-Time Transport Protocol Port Range*
%ENABLE_RTCP_MUX_WXT%	Y	Y	true	*6.1.19 RTCP MUX*

Cisco Confidential

%ENABLE_XSI_EVENT_CHANNEL_WXT%	Y	Y	true	*6.1.32.3 XSI Dynamic Proxy Discovery* The Webex App accesses the XSI (XSI-Actions & XSI-Events) and Device Management Service (DMS) services on the XSP. To find the XSI service host(s), the Webex App performs DNS SRV lookup for _xsi-client._tcp.. The SRV points to the configured URL for the XSP hosts or load balancers for the XSI service. If SRV lookup is not available, the Webex App falls back to A/AAAA lookup. The client attempts to locate the XSP nodes using the following DNS flow: ▪ Webex app initially retrieves Xsi-Actions/Xsi-Events URLs from Cisco Webex Cloud (entered when creating the associated BroadWorks Calling Cluster). The XSI hostname/domain is parsed from the URL and the client performs SRV lookup as follows: ○ Webex app performs an SRV lookup for _xsi-client._tcp.<xsi domain> ○ If the SRV lookup returns one or more targets: ▪ Webex app makes A/AAAA lookup of the XSI hostname and if it is a valid IP address, the XSI

Cisco Confidential

				hostname is added at the back of the cached list, as a backup service. ▪ The client connects to one of the targets based on the SRV priority, then weight (or at random if they're all equal). ○ If the SRV lookup does not return any targets: ▪ The Webex app makes A/AAAA lookup of the Root XSI parameter and if it is a valid IP address, this is the only address added to the cached list. This could be a load balancing edge element, or it could be the XSP server itself. ▪ The A/AAAA record must resolve to a single IP address for

Cisco Confidential

				the same reasons. ▪ Custom XSI-Actions/XSI-Events paths can be set in the DMS config file, as described in the previous section: ○ If there is a difference in the initial XSI Root or Actions paths, the client will re-initialize the XSI Actions/XSI Events connectivity. The first step in this is to perform the same DNS lookup process listed under step 1 - this time requesting a lookup for the value in the %XSI_ROOT_WXT% parameter from its configuration file. ○ Note: Make sure to create the corresponding SRV records if you use this tag to change the XSI interfaces. The Webex app also has a configurable option to control the XSI proxy discovery. The XSI proxy discovery mode can be used to control the combination of the main XSI hostname (used for the SRV lookup) and/or DNS SRV resolved XSI targets used for the XSI communication. To download the config file, the Webex app initially uses the *srv-host* mode. After the config file is downloaded, the configured proxy discovery *mode* is applied. The

Cisco Confidential

				proxy discovery *mode* can be one of: ▪ *host-only* - use only the main XSI hostname, do not trigger DNS SRV lookup ▪ *srv-only* - do not use the main XSI hostname, rely on the DNS SRV lookup only ▪ *prefer-srv* - if there are DNS SRV records found, use only them. If not, use the main XSI hostname only ▪ *srv-host* - (default) if there are DNS SRV records found, use them with priority and append the main XSI hostname at the end of the list as a backup service. If not, use the main XSI hostname After the DMS config file is downloaded: ▪ If there is an empty XSI Root or it has the same value as the main XSI hostname, and the proxy discovery mode is different than *srv-host*: ○ *host-only* - update the resulting XSI targets and leave just the main XSI hostname ○ *srv-only* - update the resulting XSI targets and leave just the SRV addresses ○ *prefer-srv* - if there is just one address, it should be the main XSI hostname. If there are more, the main XSI hostname is removed from the list

Cisco Confidential

<table>
<tr><th>Tag</th><th>Used in Desktop</th><th>Used in Mobile/ Tablet</th><th>Default Value</th><th>Section</th></tr>
<tr><td></td><td></td><td></td><td></td><td>

If the XSI Root is non-empty and its value is different than the main XSI hostname:

Perform new DNS lookup process using the XSI Root value
Order the DNS results respecting the proxy discovery mode configured
Re-initialize its XSI Actions and XSI Events connectivity

<pre>
<config>
<protocols><xsi>
<proxy-discovery
mode="%XSI_PROXY_DISCOVERY_MO
DE_WXT%"/>
</pre>
<table>
<tr><th>Tag</th><th>De
On</th></tr>
<tr><td>%XSI_PROXY_DISCOVERY
_MODE_WXT%</td><td>srv</td></tr>
</table>
XSI Event Channel
</td></tr>
</table>

Cisco Confidential

%CHANNEL_HEARTBEAT_WXT%	Y	Y	10000	*6.1.32.3 XSI Dynamic Proxy Discovery* The Webex App accesses the XSI (XSI-Actions & XSI-Events) and Device Management Service (DMS) services on the XSP. To find the XSI service host(s), the Webex App performs DNS SRV lookup for _xsi-client._tcp.. The SRV points to the configured URL for the XSP hosts or load balancers for the XSI service. If SRV lookup is not available, the Webex App falls back to A/AAAA lookup. The client attempts to locate the XSP nodes using the following DNS flow: ▪ Webex app initially retrieves Xsi-Actions/Xsi-Events URLs from Cisco Webex Cloud (entered when creating the associated BroadWorks Calling Cluster). The XSI hostname/domain is parsed from the URL and the client performs SRV lookup as follows: ○ Webex app performs an SRV lookup for _xsi-client._tcp.<xsi domain> ○ If the SRV lookup returns one or more targets: ▪ Webex app makes A/AAAA lookup of the XSI hostname and if it is a valid IP address, the XSI

Cisco Confidential

				hostname is added at the back of the cached list, as a backup service. ▪ The client connects to one of the targets based on the SRV priority, then weight (or at random if they're all equal). ○ If the SRV lookup does not return any targets: ▪ The Webex app makes A/AAAA lookup of the Root XSI parameter and if it is a valid IP address, this is the only address added to the cached list. This could be a load balancing edge element, or it could be the XSP server itself. ▪ The A/AAAA record must resolve to a single IP address for

Cisco Confidential

				the same reasons. ▪ Custom XSI-Actions/XSI-Events paths can be set in the DMS config file, as described in the previous section: ○ If there is a difference in the initial XSI Root or Actions paths, the client will re-initialize the XSI Actions/XSI Events connectivity. The first step in this is to perform the same DNS lookup process listed under step 1 - this time requesting a lookup for the value in the %XSI_ROOT_WXT% parameter from its configuration file. ○ Note: Make sure to create the corresponding SRV records if you use this tag to change the XSI interfaces. The Webex app also has a configurable option to control the XSI proxy discovery. The XSI proxy discovery mode can be used to control the combination of the main XSI hostname (used for the SRV lookup) and/or DNS SRV resolved XSI targets used for the XSI communication. To download the config file, the Webex app initially uses the *srv-host* mode. After the config file is downloaded, the configured proxy discovery *mode* is applied. The

Cisco Confidential

				proxy discovery *mode* can be one of: ▪ *host-only* - use only the main XSI hostname, do not trigger DNS SRV lookup ▪ *srv-only* - do not use the main XSI hostname, rely on the DNS SRV lookup only ▪ *prefer-srv* - if there are DNS SRV records found, use only them. If not, use the main XSI hostname only ▪ *srv-host* - (default) if there are DNS SRV records found, use them with priority and append the main XSI hostname at the end of the list as a backup service. If not, use the main XSI hostname After the DMS config file is downloaded: ▪ If there is an empty XSI Root or it has the same value as the main XSI hostname, and the proxy discovery mode is different than *srv-host*: ○ *host-only* - update the resulting XSI targets and leave just the main XSI hostname ○ *srv-only* - update the resulting XSI targets and leave just the SRV addresses ○ *prefer-srv* - if there is just one address, it should be the main XSI hostname. If there are more, the main XSI hostname is removed from the list

Cisco Confidential

<table>
<tr><th>Tag</th><th>Used in Desktop</th><th>Used in Mobile/ Tablet</th><th>Default Value</th><th>Section</th></tr>
<tr><td></td><td></td><td></td><td></td><td>
If the XSI Root is non-empty and its value is different than the main XSI hostname:
Perform new DNS lookup process using the XSI Root value
Order the DNS results respecting the proxy discovery mode configured
Re-initialize its XSI Actions and XSI Events connectivity
<pre>
<config>
<protocols><xsi>
<proxy-discovery
mode="%XSI_PROXY_DISCOVERY_MO
DE_WXT%"/>
</pre>
<table>
<tr><th>Tag</th><th>De
On</th></tr>
<tr><td>%XSI_PROXY_DISCOVERY
_MODE_WXT%</td><td>srv</td></tr>
</table>
XSI Event Channel
</td></tr>
<tr><td>%XSI_ROOT_WXT%</td><td>Y</td><td>Y</td><td>empty (uses original URL)</td><td>6.1.32.1 Xtended Services Interface (XSI)
Root and Paths</td></tr>
<tr><td>%XSI_ACTIONS_PATH_WXT%</td><td>Y</td><td>Y</td><td>/com.broadsoft.xsi-actions/</td><td>6.1.32.1 Xtended Services Interface (XSI)
Root and Paths</td></tr>
<tr><td>%XSI_EVENTS_PATH_WXT%</td><td>Y</td><td>Y</td><td>/com.broadsoft.xsi-events/</td><td>6.1.32.1 Xtended Services Interface (XSI)
Root and Paths</td></tr>
<tr><td>%ENABLE_CALLS_AUTO_RECOVERY_WXT%</td><td>Y</td><td>Y</td><td>false</td><td>6.1.25 Call Auto Recovery / Seamless Call Handover</td></tr>
</table>

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	N	Y	cs-only	*6.3.1 Emergency Calling*
%ENABLE_CALL_PICKUP_BLIND_WXT%	Y	N	false	*6.2.2 Call Pickup*
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	Y	N	false	*6.2.2 Call Pickup*
%WEB_CALL_SETTINGS_URL_WXT%	Y	Y	empty	*6.1.30 Settings Portal and Web-based Call Settings*
%USER_PORTAL_SETTINGS_URL_WXT%	Y	Y	empty	*6.1.30 Settings Portal and Web-based Call Settings*
%ENABLE_CALL_CENTER_WXT%	Y	Y	false	*6.1.31 Call Center / Call Queue Login/Logout*
%WEB_CALL_SETTINGS_TARGET_WXT%	Y	Y	external	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	Y	Y	true	*6.1.30 Settings Portal and Web-based Call Settings*
%USE_MEDIASEC_WXT%	Y	Y	false	*6.1.3 3GPP SIP Headers for SRTP*
%ENABLE_DIALING_CALL_BACK_WXT%	N	Y	false	*6.3.4 Click to Dial (Call Back)*
%DIALING_CALL_BACK_TIMER_WXT%	N	Y	10	*6.3.4 Click to Dial (Call Back)*
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	Y	N	false	*6.2.3 Boss-Admin (Executive-Assistant) Support*
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N	Y	35	*6.3.2 Push Notifications for Calls*
%ENABLE_CALL_RECORDING_WXT%	Y	Y	false	*6.1.26 Call Recording*
%ENABLE_SINGLE_ALERTING_WXT%	N	Y	false	*6.3.3 Single Alerting*
%ENABLE_CALL_PARK_WXT%	Y	Y	false	*6.1.23 Call Park/Retrieve*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	Y	Y	10	*6.1.23 Call Park/Retrieve*
%ENABLE_RTP_ICE_WXT%	Y	Y	false	*6.1.18 ICE Support (Webex Calling only)*
%RTP_ICE_MODE_WXT%	Y	Y	icestun	*6.1.18 ICE Support (Webex Calling only)*
%RTP_ICE_SERVICE_URI_WXT%	Y	Y	empty	*6.1.18 ICE Support (Webex Calling only)*
%RTP_ICE_PORT_WXT%	Y	Y	3478	*6.1.18 ICE Support (Webex Calling only)*
%ENABLE_RTP_ICE_IPV6_WXT%	Y	Y	false	*6.1.18 ICE Support (Webex Calling only)*
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	Y	N	false	*6.1.8.4 DNS TTL Management*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	Y	N	false	*6.2.4 Escalate SIP Calls to Meeting*
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	Y	N	false	*6.2.5 Desk Phone Control Calling – Auto Answer*
%ENABLE_DIALING_VOIP_WXT%	N	Y	true	*6.3.5 MNO Support* *Call with Native Dialer*
%ENABLE_DIALING_NATIVE_WXT%	N	Y	false	*6.3.5 MNO Support* *Call with Native Dialer*
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	Y	Y	true	*6.1.34 SIP-URI Dialing*
%ENABLE_SIP_VIDEOCALLS_WXT%	Y	Y	true	*6.1.36 Disable Video Calls*
%ENABLE_LOCUS_VIDEOCALLS_WXT%	Y	Y	true	*6.1.36 Disable Video Calls*
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Y	Y	Desktop - true Mobile, Tablet - false	*6.1.36 Disable Video Calls*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	Y	Mobile – N Tablet – Y	false	*6.1.37 Emergency (911) Calling - Location Reporting with E911 Provider*
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	Y	Mobile – N Tablet – Y	0	*6.1.37 Emergency (911) Calling - Location Reporting with E911 Provider*
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	Y	Mobile – N Tablet – Y	-1	*6.1.37 Emergency (911) Calling - Location Reporting with E911 Provider*
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	Y	Mobile – N Tablet – Y	once_per_login	*6.1.37 Emergency (911) Calling - Location Reporting with E911 Provider*
%ENABLE_AUTO_ANSWER_WXT%	Y	N	false	*6.2.6 Auto Answer with Tone Notification*
%ENABLE_CALLS_SPAM_INDICATION_WXT%	Y	Y	false	*6.1.40 Spam Call Indication*
%ENABLE_NOISE_REMOVAL_WXT%	Y	Y	false	*6.1.41 Noise Removal and Bandwidth Extension for PSTN/Mobile Calls*
%ENABLE_AUDIO_MARI_FEC_WXT%	Y	Y	false	*6.1.45.2 Forward Error Correction (FEC) and Packets Retransmission (RTX)*
%ENABLE_AUDIO_MARI_RTX_WXT%	Y	Y	false	*6.1.45.2 Forward Error Correction (FEC) and Packets Retransmission (RTX)*
%ENABLE_VIDEO_MARI_FEC_WXT%	Y	Y	false	*6.1.45.2 Forward Error Correction (FEC) and Packets Retransmission (RTX)*
%ENABLE_VIDEO_MARI_RTX_WXT%	Y	Y	false	*6.1.45.2 Forward Error Correction (FEC) and Packets Retransmission (RTX)*
%ENABLE_CALL_BLOCK_WXT%	Y	Y	false	*6.1.44 Block List (Webex Calling only)*
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N	Y	true	*6.3.5.6 MNO Mobility - In-call Widget*
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N	Y	true	*6.3.5.6 MNO Mobility - In-call Widget*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	Y	true	*6.3.5.6 MNO Mobility - In-call Widget*
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	Y	Y	false	*6.1.46 Simultaneous Calls with Same User*
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	Y	N	false	*6.2.11 Remote Mute Control Event Package (Webex Calling only)*
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	Y	Y	true	*6.1.29.2 Call Forwarding to Voicemail*
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	Y	Y	true	*6.1.8.1 SIP Failover*
%ENABLE_CALL_MOVE_HERE_WXT%	Y	N	false	*6.2.12 Move Call*
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	Y	Y	false	*6.1.41 Noise Removal and Bandwidth Extension for PSTN/Mobile Calls*
%DIALING_NATIVE_FAC_PREFIX_WXT%	N	Y	empty	*6.3.5.1 Call with Native Dialer*
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	Y	Y	false	*6.1.20 Transfer*
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	Y	Y	true	*6.1.47 RTCP-XR*
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N	Y	false	*6.3.6 Incoming Caller ID*
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N	Y	false	*6.3.6 Incoming Caller ID*
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N	Y	false	*6.1.49.1 Outgoing Caller ID*
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N	Y	false	*6.1.49.1 Outgoing Caller ID*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N	Y	false	*6.1.49.1 Outgoing Caller ID*
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N	Y	false	*6.1.49.1 Outgoing Caller ID*
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N	Y	false	*6.1.49.1 Outgoing Caller ID*
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	Y	Y	false	*6.1.48 Call Forwarding Info*
%ENABLE_BUSY_LAMP_FIELD_WXT%	Y	N	false	*6.2.8.1 Busy Lamp Field*
%ENABLE_BLF_DISPLAY_CALLER_WXT%	Y	N	true	*6.2.8.1 Busy Lamp Field*
%BLF_NOTIFICATION_DELAY_TIME_WXT%	Y	N	0	*6.2.8.1 Busy Lamp Field*
%ENABLE_GCP_NOTIFICATIONS_WXT%	Y	N	false	*6.2.8.2 Call Pickup Group (Webex Calling only)*
%ENABLE_GCP_DISPLAY_CALLER_WXT%	Y	N	false	*6.2.8.2 Call Pickup Group (Webex Calling only)*
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	Y	N	120	*6.2.8.2 Call Pickup Group (Webex Calling only)*
%UDP_KEEPALIVE_ENABLED_WXT%	Y	Y	true	*6.1.4 Force TCP, TLS or UDP Usage and Keepalives*
%TCP_KEEPALIVE_ENABLED_WXT%	Y	Y	false	*6.1.4 Force TCP, TLS or UDP Usage and Keepalives*
%TLS_KEEPALIVE_ENABLED_WXT%	Y	Y	false	*6.1.4 Force TCP, TLS or UDP Usage and Keepalives*
%ENABLE_MULTI_LINE_WXT%	Y	Y	false	*6.1.50 Multi-line*
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N	Y	false	*6.2.4 Escalate SIP Calls to Meeting (Webex Calling)*

Cisco Confidential

Tag	Used in Desktop	Used in Mobile/ Tablet	Default Value	Section
%ENABLE_CLID_OUTGOING_CALLS_MOBILITY_WXT%	N	Y	false	*6.3.5.3 Outgoing Calling Line Identity (CLID)*
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	Y	Y	resolved	*6.1.49.2 Remote Caller ID Name*
%PERSONAL_ASSISTANT_ENABLED_WXT%	Y	Y	false	*6.1.52 Personal Assistant (Away Presence)**Error! Reference source not found.***
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N	Y	nps	***Error! Reference source not found.*** *Delivery Mode (Webex Calling only)*
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	Y	Y	false	*6.1.51* ***Error! Reference source not found.****.*
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	Y	Y	false	*6.1.21 N-Way Conference Calls*
%CALL_PULL_MODE_WXT%	Y	Y	blind	*6.1.22 Call Pull*
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	Y	N	call_move	*6.1.22 Call Pull*
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	Y	Y	false	*6.1.35 Call History*
%ENABLE_EMERGENCY_LOCATION_WXT%	Y	Mobile – N Tablet – Y	false	*Emergency (911) Calling - Cisco Emergency Location Information Service (Webex Calling only) and Configuration Cleanup*
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	Y	Mobile – N Tablet – Y	0	*Emergency (911) Calling - Cisco Emergency Location Information Service (Webex Calling only) and Configuration Cleanup*
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	Y	Mobile – N Tablet – Y	-1	*Emergency (911) Calling - Cisco Emergency Location Information Service (Webex Calling only) and Configuration Cleanup*
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	Y	Mobile – N Tablet – Y	once_per_login	*Emergency (911) Calling - Cisco Emergency Location Information Service (Webex Calling only) and Configuration Cleanup*
%ENABLE_CALLS_E2EE_WXT %	Y	Y	false	*6.1.53 End-to-End Encryption (Webex Calling only)*

Cisco Confidential

%CHANNEL_INACTIVITY_TIMEOUT_WXT%	Y	Y	60000	*6.1.32.3 XSI Dynamic Proxy Discovery*
				The Webex App accesses the XSI (XSI-Actions & XSI-Events) and Device Management Service (DMS) services on the XSP. To find the XSI service host(s), the Webex App performs DNS SRV lookup for _xsi-client._tcp.. The SRV points to the configured URL for the XSP hosts or load balancers for the XSI service. If SRV lookup is not available, the Webex App falls back to A/AAAA lookup.
				The client attempts to locate the XSP nodes using the following DNS flow:
				▪ Webex app initially retrieves Xsi-Actions/Xsi-Events URLs from Cisco Webex Cloud (entered when creating the associated BroadWorks Calling Cluster). The XSI hostname/domain is parsed from the URL and the client performs SRV lookup as follows:
				  ○ Webex app performs an SRV lookup for _xsi-client._tcp.<xsi domain>
				  ○ If the SRV lookup returns one or more targets:
				  ▪ Webex app makes A/AAAA lookup of the XSI hostname and if it is a valid IP address, the XSI

Cisco Confidential

				hostname is added at the back of the cached list, as a backup service. ▪ The client connects to one of the targets based on the SRV priority, then weight (or at random if they're all equal). ○ If the SRV lookup does not return any targets: ▪ The Webex app makes A/AAAA lookup of the Root XSI parameter and if it is a valid IP address, this is the only address added to the cached list. This could be a load balancing edge element, or it could be the XSP server itself. ▪ The A/AAAA record must resolve to a single IP address for

Cisco Confidential

				the same reasons. ▪ Custom XSI-Actions/XSI-Events paths can be set in the DMS config file, as described in the previous section: ○ If there is a difference in the initial XSI Root or Actions paths, the client will re-initialize the XSI Actions/XSI Events connectivity. The first step in this is to perform the same DNS lookup process listed under step 1 - this time requesting a lookup for the value in the %XSI_ROOT_WXT% parameter from its configuration file. ○ Note: Make sure to create the corresponding SRV records if you use this tag to change the XSI interfaces. The Webex app also has a configurable option to control the XSI proxy discovery. The XSI proxy discovery mode can be used to control the combination of the main XSI hostname (used for the SRV lookup) and/or DNS SRV resolved XSI targets used for the XSI communication. To download the config file, the Webex app initially uses the *srv-host* mode. After the config file is downloaded, the configured proxy discovery *mode* is applied. The

Cisco Confidential

				proxy discovery *mode* can be one of: ▪ *host-only* - use only the main XSI hostname, do not trigger DNS SRV lookup ▪ *srv-only* - do not use the main XSI hostname, rely on the DNS SRV lookup only ▪ *prefer-srv* - if there are DNS SRV records found, use only them. If not, use the main XSI hostname only ▪ *srv-host* - (default) if there are DNS SRV records found, use them with priority and append the main XSI hostname at the end of the list as a backup service. If not, use the main XSI hostname After the DMS config file is downloaded: ▪ If there is an empty XSI Root or it has the same value as the main XSI hostname, and the proxy discovery mode is different than *srv-host*: ○ *host-only* - update the resulting XSI targets and leave just the main XSI hostname ○ *srv-only* - update the resulting XSI targets and leave just the SRV addresses ○ *prefer-srv* - if there is just one address, it should be the main XSI hostname. If there are more, the main XSI hostname is removed from the list

Cisco Confidential

<table>
<tr><th>Tag</th><th>Used in Desktop</th><th>Used in Mobile/ Tablet</th><th>Default Value</th><th>Section</th></tr>
<tr><td></td><td></td><td></td><td></td><td>

If the XSI Root is non-empty and its value is different than the main XSI hostname:

Perform new DNS lookup process using the XSI Root value
Order the DNS results respecting the proxy discovery mode configured
Re-initialize its XSI Actions and XSI Events connectivity

<pre>
<config>
<protocols><xsi>
  <proxy-discovery
mode="%XSI_PROXY_DISCOVERY_MO
DE_WXT%"/>
</pre>
<table>
<tr><th>Tag</th><th>De
On</th></tr>
<tr><td>%XSI_PROXY_DISCOVERY
_MODE_WXT%</td><td>srv</td></tr>
</table>
XSI Event Channel
</td></tr>
</table>

For more information about mapping the custom tags used in Webex for Cisco BroadWorks to the ones used by UC-One, see section *8 Custom Tags Mapping between Webex for Cisco BroadWorks and UC-One*.

Cisco Confidential

6.1 Common Features

6.1.1 SIP Server Settings

The client is commonly configured to use a SIP network, which is done by modifying the *config-wxt.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 remote (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 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_WXT%. Note that the DNS TTL management feature 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 must be done via separate configuration parameters. For more information on voicemail, see section *6.1.27 Voicemail, Visual Voicemail, Message Waiting Indicator*.

Note that basic SIP configuration is always needed for MWI even when SIP calls are disabled. MWI relies on SIP NOTIFYs.

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 are exposed in the configuration file (not recommended to modify them).

```
<config>
<protocols>
<sip>
   <timers>
      <T1>500</T1>
      <T2>4000</T2>
      <T4>5000</T4>
   </timers>
```

- T1 – the amount of time, in milliseconds, for a network round trip delay.
- T2 – the maximum amount of time, in milliseconds, before retransmitting non-invite requests and invite responses.

Cisco Confidential

- T4 – the maximum amount of time, in milliseconds, for a message to remain in the network.

Each line has own parameters like the voicemail number, conference URI and the domain, as well as the SIP authentication credentials. Separate credentials can be configured for 401 and 407 signaling if needed.

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

```
<config>
<protocols><sip>
<lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
       <line>
              <label>%BWAPPEARANCE-LABEL-1%</label>
              <name>%BWNAME-1%</name>
              <phone-number>%BWE164-1%</phone-number>
              <extension>%BWEXTENSION-1%</extension>
              <external-id>%BWUSEREXTID-1%</external-id>
              <voice-mail-number>%BWVOICE-PORTAL-NUMBER-1%</voice-mail-number>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
1%</conference-service-uri>
              <domain>%BWHOST-1%</domain>
              <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
              <credentials>
                     <username>%BWLINEPORT-1%</username>
                     <password>%BWAUTHPASSWORD-1%</password>
                     <auth>
                            <auth401>
                                   <default>
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </default>
                                   <realm id="%BWHOST-1%">
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </realm>
                            </auth401>
                            <auth407>
                                   <default>
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </default>
                                   <realm id="%BWHOST-1%">
                                          <username>%BWAUTHUSER-1%</username>
                                          <password>%BWAUTHPASSWORD-1%</password>
                                   </realm>
                            </auth407>
                     </auth>
              </credentials>
       </line>
       …
</lines>
<proxy address="%SBC_ADDRESS_WXT%" port="%SBC_PORT_WXT%" />
<preferred-port>%SOURCE_PORT_WXT%</preferred-port>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%BWLINEPORT-n%	empty	string	Typically SIP username. For more information, see section *5.7 Cisco BroadWorks Dynamic Built-in System Tags*. Example: johndoe
%BWAUTHPASSWORD-n%	empty	string	Typically SIP password. For more information, see section *5.7 Cisco BroadWorks Dynamic Built-in System Tags*. Example: secretpassword
%BWE164-n%	empty	phone number	Default phone number for the user in international format. For more information, see section *5.7 Cisco BroadWorks Dynamic Built-in System Tags*. Example: 12345678
%SBC_ADDRESS_WXT%	empty	string	For more information, see section *5.6 System Default Tags*. Example: sbcexample.domain.com
%SBC_PORT_WXT%	5060	number	For more information, see section *5.6 System Default Tags*. Example: 5060
%BWHOST-n%	empty	string	Typically used as the SIP domain. For more information, see section *5.7 Cisco BroadWorks Dynamic Built-in System Tags*. Example: exampledomain.com
%SOURCE_PORT_WXT%	5060	number	Typically used for the *preferred-port* parameter. For more information, see section *6.1.7 Preferred-Port Usage for SIP*. Example: 5061
%BWUSEREXTID-n%	empty	string	(Webex Calling only) Holds the external ID of the line For more information, check *6.1.50 Multi-line*. Example: 30f69bf7-710b-4cd0-ab4b-35ab393a1709

NOTE: It is strongly advisable for the SIP port to be different from 5060 (for example, 5075) due to known issues with using the standard SIP port (5060) with mobile devices.

Cisco Confidential

6.1.2 SIP Over TLS and Secure Real-time Transport Protocol

The 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 (%USE_TLS_WXT%), 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 *6.1.6 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 *Webex for Cisco BroadWorks Solution Guide*.

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, on the 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. The client 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.

Multiline SDP procedures related to SRTP is implemented, so that multiple m-lines are always used. Separate m-lines for AVP and SAVP are used.

Cisco Confidential

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 – 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>
<protocols><sip>
<secure>%USE_TLS_WXT%</secure>
```

```
<config>
<protocols><rtp>
<secure enabled="%SRTP_ENABLED_WXT%" mode="%SRTP_MODE_WXT%" rekey-
always="%ENABLE_REKEYING_WXT%"/>
```

The Secure Real-Time Control Protocol (SRTCP) is also used if SRTP is enabled.

In some deployments, re-keying for SRTP is not supported. Therefore, there is a configuration parameter for enabling/disabling SRTP re-keying. However, new keys are always taken into use when received in an updated SDP according to rfc3264. Configurability only pertains to sending new keys.

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%USE_TLS_WXT%	false	true, false	When set to “false”, SIP TLS is deactivated. When set to “true”, SIP TLS is activated. Please note that if *6.1.6 Dynamic SIP Proxy Discovery* is used, this parameter is ignored.
%SRTP_ENABLED_WXT%	false	true, false	When set to “false”, SRTP is deactivated. When set to “true”, SRTP is activated.
%SRTP_MODE_WXT%	optional	mandatory, preferred, optional, transport	Defines how preferred SRTP is at call setup. The default value is “optional”.
%ENABLE_REKEYING_WXT%	true	true, false	Enables SIP (SDP) re-keying for SRTP.

NOTE: If ICE support is enabled (see *6.1.18 ICE Support (Webex Calling* only)), re-keying will always be performed (%ENABLE_REKEYING_WXT% value from the configuration is ignored).

6.1.3 3GPP SIP Headers for SRTP

Newer 3GPP specifications require additional SIP headers to use Secure Real-time Transport Protocol (SRTP). For more information, see *3GPP TS 24.229* 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, these headers are recommended to 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.

```
<config>
<protocols><sip>
<use-mediasec enabled="%USE_MEDIASEC_WXT%"/>
```

The following tag controls this capability.

Tag	Default if Omitted	Supported Values	Description
%USE_MEDIASEC_WXT%	false	true, false	Enables 3GPP SIP headers for SRTP negotiation.

6.1.4 Force TCP, TLS or UDP Usage and Keepalives

The Webex for Cisco BroadWorks client can be configured to use either TCP, TLS or UDP for both SIP signaling and RTP media. Note that the client defaults to TCP. Note as well that without TCP keepalive, SIP TCP connections are closed after a period of inactivity.

Cisco Confidential

The following example depicts this configuration node.

```
<config>
<protocols><sip>
<transports>
   <tcp-size-threshold>%TCP_SIZE_THRESHOLD_WXT%</tcp-size-threshold>
```

The following tag, controls whether the client uses TCP or UDP.

Tag	Default if Omitted	Supported Values (Bytes)	Description
%TCP_SIZE_THRESHOLD_WXT%	0	0	Forces TCP to be used. The decision to use TCP or UDP for the client is up to the service provider; however, the recommendation is to use TCP with the default value “0”.
	0	1 - 99,000	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	Forces UDP to be used.

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

```
<config>
<protocols><sip>
<transports>
       …
       <udp>
              <keepalive enabled="%UDP_KEEPALIVE_ENABLED_WXT%">
                     <timeout>20</timeout>
                     <payload>crlf</payload>
              </keepalive>
       </udp>
       <tcp>
              <keepalive enabled="%TCP_KEEPALIVE_ENABLED_WXT%">
                     <timeout>0</timeout>
                     <payload></payload>
              </keepalive>
       </tcp>
       <tls>
              <keepalive enabled="%TLS_KEEPALIVE_ENABLED_WXT%">
                     <timeout>0</timeout>
                     <payload></payload>
              </keepalive>
       </tls>
</transports>
```

The possible parameters are:

- Enabling TCP or TLS keepalive, possible values - 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.

Cisco Confidential

- Enabling UDP keepalive, possible values - true/false, the default is “true” 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, the client 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**)

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 *6.1.6 Dynamic SIP Proxy Discovery.*

Tag	Default if Omitted	Supported Values	Description
%UDP_KEEPALIVE_ENABLED_WXT%	true	true, false	Controls if the keep-alive packets should be sent for the UDP transport.
%TCP_KEEPALIVE_ENABLED_WXT%	false	true, false	Controls if the keep-alive packets should be sent for the TCP transport.
%TLS_KEEPALIVE_ENABLED_WXT%	false	true, false	Controls if the keep-alive packets should be sent for the TLS transport.

6.1.5 Configurable Timeout for Opening SIP Socket

Previously, the timeout for opening a SIP socket was hardcoded to 5 seconds for TCP and 10 seconds for TLS. These timeouts are now configurable.

```
<config>
    <protocols>
        <sip>
            <transports>
                <udp>
                    …
                </udp>
                <tcp>
                    …
                    <connect-
timeout>%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%</connect-timeout>
                </tcp>
                <tls>
```


Cisco Confidential

```
                    <connect-
timeout>%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%</connect-timeout>
                </tcp>
            </transports>
```

The following tags control the socket connection timeout (in milliseconds).

Tag	Default if Omitted	Supported Values	Description
%SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT%	5000	<integer> - the timeout in milliseconds	The socket connection timeout when TCP transport is used.
%SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT%	10000	<integer> - the timeout in milliseconds	The socket connection timeout when TLS transport is used.

6.1.6 Dynamic SIP Proxy Discovery

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

```
<config>
<protocols><sip>
<proxy-discovery enabled="%USE_PROXY_DISCOVERY_WXT%” tcp=”%USE_TCP_FROM_DNS_WXT%"
udp="%USE_UDP_FROM_DNS_WXT%" tls="%USE_TLS_FROM_DNS_WXT%">
    <record-name>%SBC_ADDRESS_WXT%</record-name>
     <domain-override>%DOMAIN_OVERRIDE_WXT%</domain-override>
</proxy-discovery>
```

It is possible to control which transport protocols entries from DNS SRV are used when many are available following the procedures provided in this section.

Tag	Default if Omitted	Supported Values	Description
%USE_PROXY_DISCOVERY_WXT%	false	true, false	Enables dynamic SIP proxy discovery for audio and video calls. The recommended value is “true”.
%SBC_ADDRESS_WXT%	empty	String	This Cisco BroadWorks tag is typically used for the record-name parameter. It should be a valid URL – should not be an IP address. For more information, see section *5.6 System Default Tags*. Example: sbc.domain.com
%DOMAIN_OVERRIDE_WXT%	empty	String	This custom tag is used for the domain-override. For more information, see the following section. Example: other.domain.com
%USE_TCP_FROM_DNS_WXT%	true	true, false	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.

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%USE_UDP_FROM_DNS_WXT%	true	true, false	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_FROM_DNS_WXT%	true	true, false	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.
%PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT%	true, false	true	Enables/disables the DNS backup service. If enabled, then A/AAAA resolution is performed for the SIP proxy address. It is taken into account only when SRV/NAPTR service discovery is enabled.
%PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT%	true, false	true	If set to “true” and NAPTR service discovery fails or returns no results, then SRV service discovery is performed for the configured host. If set to “false”, then no SRV discovery is performed.
%PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT%	true, false	false	Allows for the bypass of the OS DNS cache.

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

DNS SRV, Naming Authority Pointer (NAPTR) and A-record queries are supported. 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.

Cisco Confidential

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, the client 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

NOTE 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.

NOTE 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.

NOTE 3: 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.

NOTE 4: The client uses operating system primitives for DNS operations and, typically, DNS responses are cached to honor the TTL of the DNS response.

NOTE 5: 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.

NOTE 6: The client supports only certain prefixes for NAPTR services. The following lists the supported prefixes:

SIP+D2U -> _sip._udp

SIP+D2T -> _sip._tcp

SIPS+D2T -> _sips._tcp

SIPS+D2T -> _sips._tls

Cisco Confidential

If the NAPTR response contains a record with prefix that does not match the service type, then this record is ignored.

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>
<protocols><sip>
<proxy address="domain.com" port="5060"/>
<proxy-discovery enabled="true" >
    <record-name>record-domain.com</record-name>
     <domain-override>override-domain.com</domain-override>
</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>
<protocols><sip
<proxy address="domain.com" port="5060"/>
<proxy-discovery enabled="true">
    <record-name>record-domain.com</record-name>
     <domain-override>override-domain.com</domain-override>
</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.

Cisco Confidential

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>
<protocols><sip>
<proxy address="domain.com" port="5060"/>
<proxy-discovery enabled="true">
   <record-name>record-domain.com</record-name>
    <domain-override>override-domain.com</domain-override>
</proxy-discovery>
<domain>sip-domain.com</domain>
```

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.

Example 4: Using DNS proxy discovery with NAPTR when service does not match service type

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

```
<config>
<protocols><sip>
<proxy address="domain.com" port="5060"/>
<proxy-discovery enabled="true" tcp="true" udp="false" tls="true">
   <record-name>record-domain.com</record-name>
    <domain-override>override-domain.com</domain-override>
</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" "SIPS+D2T" "" _sip._tls.test.sip.record-domain.com.
28591 IN NAPTR 100 10 "S" "SIP+D2T" "" _sip._tcp.test.sip.record-domain.com.
```


Cisco Confidential

```
2. For the first record we have service type "SIPS+D2T" and the prefix is
"sip._tls.". Since this prefix doesn't match the service type (see Note 6 above)
it will be ignored.

3. 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.

6.1.7 Preferred-Port Usage for SIP

There have been some cases when another software package has been running on the same machine as the client, occupying the default SIP port. To configure the client to use another port for SIP, the *preferred-port* parameter can be used. The client tries to use the configured port value specified in the *preferred-port* parameter, 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.

Tag	Default if Omitted	Supported Values	Description
%SOURCE_PORT_WXT%	5060	number	Specifies preferred local SIP port for communication. Example: 5060

6.1.8 SIP Failover and Failback

SIP failover and failback follow the Cisco BroadWorks procedures. For this, more than one proxy (typically the SBC) must be configured.

On the client side, the proxy should be resolved to multiple IP addresses. This can be achieved by either:

- SIP Proxy Discovery is enabled and the DNS server has NAPTR and/or SRV records for the SBC FQDN (see section *6.1.6 Dynamic SIP Proxy Discovery*), OR
- The SIP proxy address is provided as an FQDN and it is resolved to multiple IP addresses (see section *6.1.1 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.

At sign-in, if multiple IP addresses are resolved, they are ordered by priority. The client starts using the first available IP address.

Cisco Confidential

6.1.8.1 SIP Failover

SIP failover may be triggered by either a socket error, a request timeout error, or a definitive error response from server as follows:

- Socket error – if the socket between the client and the server gets broken or is closed, as in the case of network connectivity loss, the client reacts immediately and triggers a failover.
- Timeout (for example, when the SBC hangs) – based on the SIP T1:
  - SIP INVITE – if the INVITE request times out, the client registers to the next available SBC (IP) and retries the INVITE.
  - Another SIP request – the client tries to register to the next available SBC (IP).
- Definitive error response received from server:
  - The following SIP error responses from the server to a SIP REGISTER trigger a failover:
    - 5xx
    - 6xx
  - The following SIP *4xx* responses to SIP REGISTER do <u>not</u> 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.

When a failover is triggered, the client takes the next available IP address from the list. 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). If all IP addresses fail, then the client displays a user interface error for SIP connectivity. If a VoIP call is in progress when the failover occurs, the call is terminated.

The SIP failover logic relies on several configuration parameters:

- SIP Failover Timers – SIP timers T1, T2, and T4 are exposed in the configuration file, but it is not recommended to modify them.

```
<config><protocols><sip>
<timers>
    <T1>500</T1>
    <T2>4000</T2>
    <T4>5000</T4>
</timers>
```

  - T1 – the amount of time, in milliseconds, for a network round trip delay.
  - T2 – the maximum amount of time, in milliseconds, before retransmitting non-invite requests and invite responses.

Cisco Confidential

- T4 – the maximum amount of time, in milliseconds, for a message to remain in the network.

- SIP Proxy Address and SIP Proxy Discovery
  - See section *6.1.1 SIP Server Settings*.
  - See section *6.1.6 Dynamic SIP Proxy Discovery*.
- Register failover configuration (see below)

In case of failover, the Webex application sends SIP REGISTER with two Contact headers - one for the old session and second one with the new device information. The Contact header for the old session is included to notify the SBC to clean up the data. This header includes expires=0 and q=0.5.

The Contact header with the new device information also has q value, which is read from the *<q-value>* tag. The *<q-value>* tag value is used to indicate the preference or priority of a particular contact address. It ranges from 0 to 1.0, with 1.0 being the highest preference and 0 being the lowest. This tag does not have a custom tag to control the value - it is hardcoded to 1.0. The value can be adjusted manually, if the SBC used in the deployment has reverse logic and treats q=0.0 with maximum priority.

Starting with Release 42.11, a new *<register-failover>* section is introduced in the config template. There is a new configurable parameter *<registration-cleanup>* added to control if the application will send Contact header to clean up the old device information or not. Some SBCs clean up the old session immediately at socket disconnect, so the existence of the Contact header for the old session is not needed. By default, the registration cleanup logic is enabled.

For consistency, the *<q-value>* tag is also moved under the same *<register-failover>* section.

Example:

```
<config>
<protocols><sip>
   <q-value>1.0</q-value> <!-- DEPRECATED -->
   <register-failover>
      <registration-
cleanup>%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%</registration-cleanup>
      <q-value>1.0</q-value>
```

Tag	Default if Omitted	Supported Values	Description
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	true	true, false	Controls old device information cleanup in case of SIP failover.

Cisco Confidential

6.1.8.2 SIP Failback

If the client is connected to a proxy that is not first by priority, it tries to reconnect to the IP with the highest priority. The time for the failback is based on the DNS TTL management configuration (see section *6.1.8.4 DNS TTL Management*). If a call is in progress when the failback timer is reached, the client waits until all calls are completed and triggers the failback procedure. Note that this is only valid for desktop clients since the SIP connection is active only while on a call on mobile.

Tag	Default if Omitted	Supported Values	Description
%SIP_FAILBACK_ENABLED_WXT%	true	true, false	Enables/disables SIP failback.
%SIP_FAILBACK_TIMEOUT_WXT%	900	Over 60	The SIP failback timeout in seconds.
%SIP_FAILBACK_USE_RANDOM_FACTOR_WXT%	false	true, false	Adds a random period [0-10]% of the SIP failback.

6.1.8.3 Enforce IP Version

Webex client can be configured how to order the list of resolved hosts through the DNS and then to iterate through them in case of SIP failover. In all the modes, the priority and weight is respected.

Supported configurations are:

- dns - uses all the addresses returned by the DNS queries
- ipv4 - filters out the IPv6 addresses
- ipv6 - filters out the IPv4 addresses
- prefer-ipv4 – orders the IPv4 addresses before the IPv6 (release 42.9)
- prefer-ipv6 – orders the IPv6 addresses before the IPv4 (release 42.9)
- nat64 – ignores the IPv6 addresses, orders the IPv4 ones (release 44.2)

The default value (dns) is recommended to be used, unless environment/network configuration requires different mode.

With “dns” configuration, the IPv4 addresses are prioritized over the IPv6 ones, for given host. If there are two hosts with both IPv4 and IPv6 addresses, the order will be IPv4(host1), IPv6(host1), IPv4(host2), IPv6(host2).

In “prefer-ipv4” mode, the IPv4 addresses are ordered before the IPv6 addresses (the order within IPv4 and IPv6 groups remains)

Example: IPv4(host1), IPv4(host2), IPv6(host1), IPv6(host2).

With “prefer-ipv6” mode, the order is the opposite - the IPv6 addresses are placed before the IPv4 addresses

Example: IPv6(host1), IPv6(host2), IPv4(host1), IPv4(host2).

Cisco Confidential

With “nat64” mode - the IPv6 addresses are ignored, the IPv4 order is respected. The IPv6 prefix(es) are discovered. For each IPv4 address, a combination with each Pref64 prefix and/or suffix is created.

Example: Pref64(1)::IPv4(host1), Pref64(2)::IPv4(host1)::Suff64(2), IPv4(host1)::Suff64(3), Pref64(1)::IPv4(host2), Pref64(2)::IPv4(host2)::Suff64(2), IPv4(host2)::Suff64(3).

```
<config>
<protocols><sip><transports>
<enforce-ip-version>%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%</enforce-ip-version>
```

Tag	Default if Omitted	Supported Values	Description
%SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT%	dns	ipv4 ipv6 dns prefer-ipv4 prefer-ipv6 nat64	Controls the order of IPv4/IPv6 addresses used by the Webex client to connect the SIP session.

6.1.8.4 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 parameter in the following table, when enabled, forces the client 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 the client 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, reconnection is only done after ongoing calls have finished.

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, but rather every 15 minutes.

This parameter only works for SIP.

Note that the DNS TTL management feature cannot be used when an IP address is used in the proxy address parameter.

> **NOTE**: This is a desktop-only feature, since the mobile clients have SIP connection only while on a call.

```
<config>
<protocols><sip>
<refresh-on-ttl enabled="%SIP_REFRESH_ON_TTL_WXT%"
  use-random-factor="%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%SIP_REFRESH_ON_TTL_WXT%	false	false, true	When set to “false”, DNS TTL management is disabled for SIP. When set to “true”, DNS TTL management is enabled for SIP.
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%"	false	false, true	If enabled, adds a random period between 0-10% to the DNS TTL.

NOTE: It is highly recommended to enable the DNS TTL random factor to prevent spikes of requests to the DNS and potentially spikes of reconnection attempts to the Application Server.

6.1.9 SIP SUBCSRIBE 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).

```
<config>
<protocols><sip>
<subscription-refresh-interval>10800</subscription-refresh-interval>
<subscription-retry-interval>60</subscription-retry-interval>
<registration-refresh-interval>300</registration-refresh-interval>
<session>
       <expires-value>3600</expires-value>
</session>
```

6.1.10 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>
<protocols><sip>
<use-alternative-identities>%USE_ALTERNATIVE_IDENTITIES_WXT%</use-alternative-
identities>
```


Cisco Confidential

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.

Tag	Default if Omitted	Supported Values	Description
%USE_ALTERNATIVE_IDENTITIES_WXT%	false	true, false	Enables use of alternative identities in SIP REGISTER. If set to “true”, then the client takes its own identity from the last *P-Associated-URI* header for outgoing SIP requests. If set to “false”, then its own identity for outgoing SIP requests is taken from its own SIP URI.

6.1.11 SIP P-Early Media (PEM) Header

The SIP *P-Early Media* (PEM) header 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.

The configuration parameter enables 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.

```
<config>
<protocols><sip>
<support-p-early-media>%ENABLE_PEM_SUPPORT_WXT%</support-p-early-media>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_PEM_SUPPORT_WXT%	false	true, false	Set to “true” to enable client advertising PEM support in SIP signaling. Set to “false” to disable client advertising PEM support in SIP signaling.

6.1.12 SIP UPDATE Support

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.

Cisco Confidential

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

```
<config>
<protocols><sip>
<support-update enabled="%ENABLE_SIP_UPDATE_SUPPORT_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	false	true, false	When set to “false”, SIP UPDATE support is disabled. When set to “true”, SIP UPDATE support is enabled.

6.1.13 Legacy SIP INFO FIR

This client supports the legacy way of requesting video keyframes via SIP INFO media control request. That is needed because some of the devices have problems responding to RTCP-FB FIR and occasionally RTCP does not get thru to remote endpoint, which may lead to no-video or one-way-video. For more information, see *RFC 5168*.

```
<config>
<protocols><sip>
<force-sip-info-fir enabled="%ENABLE_FORCE_SIP_INFO_FIR_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	false	true, false	When set to “false”, SIP INFO FIR support is disabled. When set to “true”, SIP INFO FIR support is enabled.

6.1.14 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*.

For more information on SIP port and transport protocol recommendations when SIP Application Layer Gateways (ALGs) are used in the network, see the *Webex for Cisco BroadWorks 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 *6.1.7 Preferred-Port Usage for SIP*.

Cisco Confidential

There is a separate configuration parameter *use-local-port* that forces local port of the client socket to be set in the *Contact* header. This is used for some SBCs that detect the client has a real IP (from the *Contact* header) and the SBC tries to establish a separate socket to the client for its requests. In most cases, a firewall sits between the SBC and the client, and it denies the incoming connections to the client.

> **NOTE**: In IPv6 environments, all the addresses are real, and the SBC tries to establish a connection to the listening client address (from the *Contact* header).

```
<config>
<protocols><sip>
<use-rport enabled="%ENABLE_USE_RPORT_WXT%" use-local-
port="%RPORT_USE_LOCAL_PORT_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_USE_RPORT_WXT%	false	true, false	Enables rport for audio and video calls.
%RPORT_USE_LOCAL_PORT_WXT%	false	true, false	Controls whether the local port of the client's socket is to be added in the SIP *Contact* header.

6.1.15 SIP Session ID

When enabled, on initial registration, a local Session ID is generated. The Session ID is used for the lifetime of the connection/session for that device, for all out of call dialogs, REGISTER, SUBSCRIBE, NOTIFY, and so on. Same Session ID is used until the binding is lost. When the registration binding is lost (DNS lookup, connection reset, phone reset, and so on), a new local Session ID is generated.

The value of the Session ID can be used to find the full set of dialogs associated with that device.

```
<config>
<protocols><sip>
<sip-sessionid enabled="%ENABLE_SIP_SESSION_ID_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_SIP_SESSION_ID_WXT%	false	true, false	Controls usage of the SIP session ID.

6.1.16 Incoming Call Rejection Behavior

The client offers the flexibility to reject a call with *486* or *603*.

Note that if the client is configured to reject a call with *603 Decline*, then the Call Forward Busy and Call Forward No Answer services may not work as expected.

Cisco Confidential

```
<config>
<services><calls>
<reject-with-486 enabled="%ENABLE_REJECT_WITH_486_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_REJECT_WITH_486_WXT%	true	true, false	Controls the SIP error code and reason used to reject incoming SIP calls. If enabled, *486 Temporarily Unavailable* is used. Otherwise, *603 Decline* is used.

6.1.17 Real-Time Transport Protocol Port Range

The client 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>
<protocols><rtp>
<preferred-audio-port-start>%RTP_AUDIO_PORT_RANGE_START_WXT%</preferred-audio-port-start>
<preferred-audio-port-end>%RTP_AUDIO_PORT_RANGE_END_WXT%</preferred-audio-port-end>
<preferred-video-port-start>%RTP_VIDEO_PORT_RANGE_START_WXT%</preferred-video-port-start>
<preferred-video-port-end>%RTP_VIDEO_PORT_RANGE_END_WXT%</preferred-video-port-end>
```

Tag	Default if Omitted	Supported Values	Description
%RTP_AUDIO_PORT_RANGE_START_WXT%	8000	number	Start of the audio port range.
%RTP_AUDIO_PORT_RANGE_END_WXT%	8099	number	End of the audio port range.
%RTP_VIDEO_PORT_RANGE_START_WXT%	8100	number	Start of the video port range.
%RTP_VIDEO_PORT_RANGE_END_WXT%	8199	number	End of the video port range.

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

6.1.18 ICE Support (Webex Calling only)

The client supports Interactive Connectivity Establishment (ICE) negotiation that enables media path optimization between endpoints (in a peer-to-peer manner). This is done to reduce data latency, decrease packet loss, and reduce the operational costs of deploying the application.

Note that the current implementation supports STUN server, while TURN is not supported.

When ICE support is enabled, re-keying for SRTP will always be performed (see section *6.1.2 SIP Over TLS and Secure Real-time Transport Protocol*).

Cisco Confidential

Starting with Release 44.5, Webex app adds support for ICE over IPv6 using NAT64.

```
<config>
<protocols><rtp>
   <ice enabled="%ENABLE_RTP_ICE_WXT%"
        enable-ipv6-support="%ENABLE_RTP_ICE_IPV6_WXT%"
        mode="%RTP_ICE_MODE_WXT%"
        service-uri="%RTP_ICE_SERVICE_URI_WXT%"
        port="%RTP_ICE_PORT_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_RTP_ICE_WXT%	false	true, false	Enable / Disable ICE support.
%RTP_ICE_MODE_WXT%	icestun	icestun	ICE support mode. Currently the only supported value is “icestun”.
%RTP_ICE_SERVICE_URI_WXT%	(empty)	valid STUN server URI or (empty)	STUN server URI.
%RTP_ICE_PORT_WXT%	3478	Number (0-65535)	STUN server port.
%ENABLE_RTP_ICE_IPV6_WXT%	false	true, false	Enables ICE over IPv6.

6.1.19 RTCP MUX

RTCP MUX is configurable. This feature makes the client use the same port for RTP and RTCP. In SIP/SDP signaling level, the line a=rtcp-mux is added to the SDP. 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.

```
<config>
<protocols><rtp>
<mux enabled=”%ENABLE_RTCP_MUX_WXT%”/>
```

Note that RTCP MUX cannot be used with SRTP calls.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_RTCP_MUX_WXT%	true	true, false	To enable RTPC MUX, set to “true”. To disable RTCP MUX, set to “false”.

6.1.20 Transfer

The Webex for Cisco BroadWorks client supports attended (consultative), semi-consultative, and Direct (blind) call transfer.

Cisco Confidential

Semi-consultative call transfer allows the caller to complete the transfer before the call is picked up by the remote callee. The semi-consultative completion button is enabled for the caller only after the ringing is started on the callee side and the corresponding SIP notification (*180 Ringing*) is received on the caller side. Blind transfer is called “Transfer Now” in the UI.

> **NOTE**: The SIP *180 Ringing* may not be triggered in some environments, for some numbers, or in some cross-server communication scenarios.

Release 43.9 of the Webex app introduces transfer to another standalone ongoing call of the same type. Calls terminated in the Webex app can be transferred to other calls terminated in the local endpoint. And calls terminated on a remote device can be transferred to calls terminated on a remote endpoint. This feature doesn’t have configurable options.

Starting with Release 43.12, the Webex app adds configuration option to control if the current call should be placed automatically on hold when the Transfer menu item is selected. This behavior is controlled by the new *auto-hold* attribute. By default, auto-hold is disabled.

```
<config>
<services><calls>
   <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%"
                  xsi-enabled="%ENABLE_XSI_TRANSFER_CALLS_WXT%"
                  type="%TRANSFER_CALL_TYPE_WXT%"
                  auto-hold="%ENABLE_TRANSFER_AUTO_HOLD_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_TRANSFER_CALLS_WXT%	false	true, false	When set to “true”, call transfer is enabled. When set to “false”, call transfer is disabled.
%ENABLE_XSI_TRANSFER_CALLS_WXT%	false	true, false	Enables transfer option(s) for the remote (XSI) calls terminated on another location.
%TRANSFER_CALL_TYPE_WXT%	full	talk-first, blind, full	Specifies the transfer types available for the user in the BroadWorks config.
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	false	true, false	Controls if the active call will be placed on hold automatically when the user selects the Transfer option from the in-call screen menu.

6.1.21 N-Way Conference Calls

The following custom tag can be used to control the availability of the Ad Hoc (N-Way) conference call through SIP in the Webex for Cisco BroadWorks client. In addition, the N-way owner can see the full list of participants via 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.

Cisco Confidential

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 Cisco BroadWorks N-way Calling feature.

This information is retrieved from the Application Server (AS) 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 *%MAX_CONF_PARTIES_WXT%* tag should be set accordingly.

With Release 45.7, for the deployment of Webex Calling exclusively, the Webex application introduces support for the automatic transition from an N-Way ad-hoc conference call to a 1:1 call session, provided that the host and one additional participant remain in the call. A new configurable option (*drop-two-party-conference*) has been added to control the enablement of this enhancement.

```
<config>
<services><calls>
<conference enabled=”%ENABLE_CONFERENCE_CALLS_WXT%” xsi-
enabled="%ENABLE_XSI_CONFERENCE_CALLS_WXT%">
    <subscribe-conference-info enabled=”%ENABLE_NWAY_PARTICIPANT_LIST_WXT%”/>
    <max-nway-participants>%MAX_CONF_PARTIES_WXT%</max-nway-participants>
    <drop-two-party-conference enabled="%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%"/>
</conference>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CONFERENCE_CALLS_WXT%	false	true, false	Controls if the Conference option should be enabled for the user.
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	false	true, false	Set to “true” to enable N-way owner participant list. Set to “false” to disable N-way owner participant list.
%MAX_CONF_PARTIES_WXT%	10	Number between 4 and 15 (empty)	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.
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	false	true, false	Controls whether the ad-hoc conference call should be converted into a 1:1 call session, only if two participants remain in the conference call.

Cisco Confidential

6.1.22 Call Pull

The Webex app supports Call Pull, which lets users move remote calls that are terminated on their devices to the current device. There is a static (blind) Call Pull option that users can utilize even when there is no ongoing call.

Release 45.10 of the Webex app improves the feature by adding active call monitoring and offering the option to pull the remote call to the current device from the call itself. This is available only when there is a single ongoing call for the user, which is terminated on another device owned by the user.

In the Desktop app, there is a new configurable option exposed in the Webex app Call Settings, allowing different handling of the remote calls:

- Remote Call Control - this is the current behavior of the Webex app, where the remote calls are displayed with a Timer in the call list. When the Timer is selected, user can see the call control screen. With the new enhancement, user will be able to use the new "Move call to computer" option from the More menu, to initiate a call pull
- Call Move - with this option selected, the user will not be able to open the call control screen for remote calls. User will see a Move option for the call only when there is a single remote call, terminated on a device owned by the user. When the Move option is selected, user will see a confirmation dialog, before the Webex app initiates the call pull.
- Always Ask - in this type of configuration, user will see the Timer for the remote call in the call list, and when selected, user will be asked how to proceed - whether the remote call control should be displayed, the call pull to be initiated (if available) or to cancel the operation

Release 45.10 also improves the Mobile app. If the active call pull mode is enabled, it displays all remote calls for the user, enabling active call monitoring and providing the option to move calls in certain situations. If only one call is terminated on a remote device (owned by the user), the Move option will be available for that call. However, if there are multiple calls for the user, or if the call is terminated on a shared device, the calls will still be visible, but only for informational purposes – there will be no option to move or control the call remotely.

To control the feature, there are several configurable options - one to control the availability and two more - *mode* and *default-active-move-option* (Desktop only), to control the feature behavior. The *mode* may be set to one of the following options:

- blind
    - the default mode
    - Desktop – a Call pull button in the Dial pad
    - Mobile – a Call pull option in the Calling tab
- active
    - Desktop
        - no Call pull button in the Dial pad
        - allows the retrieval of an actively monitored call
        - allows configurability of the action when a call is selected

Cisco Confidential

- Mobile
    - no Call pull option in the Calling tab options
    - allows active monitoring of all the user's remote calls
    - allows the retrieval of an actively monitored call

- full – combines the blind and active mode

```
<config>
<services><calls>
<call-pull enabled="%ENABLE_CALL_PULL_WXT%"
           mode="%CALL_PULL_MODE_WXT%"
           default-active-move-option="%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_PULL_WXT%	false	true, false	Enables Call Pull.
%CALL_PULL_MODE_WXT%	blind	blind, active, full	Controls what call pull options are available for the user - it can be one of the current blind call pull, call pull based on active monitoring or both.
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	call_move	call_control, call_move, always_ask	Desktop only If the active move is available (active or full mode is configured), this setting specifies the default action enabled for the user in the call list

NOTE: This feature requires the Shared Call Appearance Call Retrieve Service to be enable for the user, by enabling the "Allow Call Retrieve from another location" check box from the Shared Call Appearance configuration page in the CommPilot portal.

6.1.23 Call Park/Retrieve

The Group Call Park feature allows ongoing VoIP calls to be transferred to a Call Park server, which allows the caller to do something else and to be retrieved by the same user or another user. An ongoing call will be parked against the first available extension within the Call Park Group.

Call retrieval can be performed by the user parking the call in the dialog for a configurable number of seconds immediately after parking the call. Or the parked call can be retrieved by the user or another user by selecting the call retrieval option and entering the number or extension.

```
<config>
<services><calls>
<call-park enabled="%ENABLE_CALL_PARK_WXT%"
timer="%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_PARK_WXT%	false	true, false	Enables Call Park/Retrieve.
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	10	Number between 5 and 30	Specifies the number of seconds the successful Call Parked dialog is visible for the user before being closed automatically.

6.1.24 Call Statistics

Reporting End-of-Call Statistics in Session Initiation Protocol (SIP) BYE message enables sending call statistics to a remote end when a call terminates. The call statistics are sent as a new header in the SIP BYE message or in the corresponding *200 OK* response to the BYE message. The statistics include Real-time Transport Protocol (RTP) packets sent or received, total bytes sent or received, total number of packets that are lost, delay jitter, round-trip delay, and call duration.

```
<config>
<services><calls>
<call-statistics enabled="%ENABLE_CALL_STATISTICS_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_STATISTICS_WXT%	false	true, false	Set to “true” to enable capturing of calling metrics. Set to “false” to disable capturing of calling metrics.

6.1.25 Call Auto Recovery / Seamless Call Handover

The client has support for call auto recovery at switching networks while the user has an ongoing VoIP call. Call auto recovery works in both directions – Cellular Data-to-WiFi and WiFi-to-Cellular Data, as well as while switching between WiFi networks. The call is tried to be recovered within a one-minute timeframe and then stops. If there are more than one ongoing VoIP calls, just the active one is recovered.

In Cellular Data-to-WiFi transition, the client will keep the ongoing VoIP calls on cellular data until terminated or cellular data network is lost.

In case of a call auto recovery because of a network change, there is a tone indication played to the user, during the call reconnect attempt.

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


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALLS_AUTO_RECOVERY_WXT%	false	true, false	Controls if the auto recovery mechanism should be enabled for the user.

NOTE: This feature depends on the Call Pull feature being enabled for the user. For more information, check section *6.1.22 Call Pull*.

6.1.26 Call Recording

The Call Recording feature is supported by the client and depends on server-side availability of the feature, as well as configuration option. The feature depends on enabled XSI event channel (see section *6.1.32.2XSI Dynamic Proxy* Discovery

The Webex App accesses the XSI (XSI-Actions & XSI-Events) and Device Management Service (DMS) services on the XSP. To find the XSI service host(s), the Webex App performs DNS SRV lookup for _xsi-client._tcp.. The SRV points to the configured URL for the XSP hosts or load balancers for the XSI service. If SRV lookup is not available, the Webex App falls back to A/AAAA lookup.

The client attempts to locate the XSP nodes using the following DNS flow:

- Webex app initially retrieves Xsi-Actions/Xsi-Events URLs from Cisco Webex Cloud (entered when creating the associated BroadWorks Calling Cluster). The XSI hostname/domain is parsed from the URL and the client performs SRV lookup as follows:
    - Webex app performs an SRV lookup for _xsi-client._tcp.<xsi domain>
    - If the SRV lookup returns one or more targets:
        - Webex app makes A/AAAA lookup of the XSI hostname and if it is a valid IP address, the XSI hostname is added at the back of the cached list, as a backup service.
        - The client connects to one of the targets based on the SRV priority, then weight (or at random if they're all equal).
    - If the SRV lookup does not return any targets:
        - The Webex app makes A/AAAA lookup of the Root XSI parameter and if it is a valid IP address, this is the only address added to the cached list. This could be a load balancing edge element, or it could be the XSP server itself.
        - The A/AAAA record must resolve to a single IP address for the same reasons.
- Custom XSI-Actions/XSI-Events paths can be set in the DMS config file, as described in the previous section:
    - If there is a difference in the initial XSI Root or Actions paths, the client will re-initialize the XSI Actions/XSI Events connectivity. The first step in this is to perform the same DNS lookup process listed under step 1 - this time requesting a lookup for the value in the %XSI_ROOT_WXT% parameter from its configuration file.

Cisco Confidential

- Note: Make sure to create the corresponding SRV records if you use this tag to change the XSI interfaces.

The Webex app also has a configurable option to control the XSI proxy discovery. The XSI proxy discovery mode can be used to control the combination of the main XSI hostname (used for the SRV lookup) and/or DNS SRV resolved XSI targets used for the XSI communication. To download the config file, the Webex app initially uses the *srv-host* mode. After the config file is downloaded, the configured proxy discovery *mode* is applied. The proxy discovery *mode* can be one of:

- *host-only* - use only the main XSI hostname, do not trigger DNS SRV lookup
- *srv-only* - do not use the main XSI hostname, rely on the DNS SRV lookup only
- *prefer-srv* - if there are DNS SRV records found, use only them. If not, use the main XSI hostname only
- *srv-host* - (default) if there are DNS SRV records found, use them with priority and append the main XSI hostname at the end of the list as a backup service. If not, use the main XSI hostname

After the DMS config file is downloaded:

- If there is an empty XSI Root or it has the same value as the main XSI hostname, and the proxy discovery mode is different than *srv-host*:
  - *host-only* - update the resulting XSI targets and leave just the main XSI hostname
  - *srv-only* - update the resulting XSI targets and leave just the SRV addresses
  - *prefer-srv* - if there is just one address, it should be the main XSI hostname. If there are more, the main XSI hostname is removed from the list
- If the XSI Root is non-empty and its value is different than the main XSI hostname:
  - Perform new DNS lookup process using the XSI Root value
  - Order the DNS results respecting the proxy discovery mode configured
  - Re-initialize its XSI Actions and XSI Events connectivity

```
<config>
<protocols><xsi>
   <proxy-discovery mode="%XSI_PROXY_DISCOVERY_MODE_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%XSI_PROXY_DISCOVERY_MODE_WXT%	srv-host	host-only, srv-only, prefer-srv, srv-host	Controls how the Webex app should build the list of XSI targets used by the application after the download of the config file. The initial discovery, before the DMS config download, always uses srv-host mode.

Cisco Confidential

XSI Event Channel) and Application Server (AS) configured to send *X-BroadWorks-Correlation-Info* SIP header (see the *Webex for Cisco BroadWorks Solution Guide*).

If the feature is disabled, there are no recording buttons and options for the user. Note that call recording operates on a per user, not per call basis – that means that if one of the participants on a call supports call recording, then the call can be recorded.

If the call recording feature is enabled, there is always a visual indication when the call is being recorded. The following call recording modes are supported by Cisco BroadWorks:

Always

- Call recording will be started automatically at call establishment.
- User is **NOT** able to stop/pause the call recording.

Always with Pause/Resume Support

- Call recording will be started automatically at call establishment but the user will be able to pause and resume the call.
- Possible user interactions:
  - Recording is in progress – **Pause** Recording action.
  - Recording is on pause – **Resume** Recording action.

On Demand

- After the call is established, call recording starts on the server.
- If the user presses the Start Recording option during the call, the call recording will be stored and it will keep the call from its startup. Otherwise, if no start recording is initiated from the user, the call recording will be deleted on the server.
- Possible user interactions:
  - No recording has started yet – **Start** Recording action.
  - Recording is in progress – **Pause** Recording action.
  - Recording is on pause – **Resume** Recording action.

On Demand with User Initiated Start

- User can start, stop, pause, and resume call recording at any time, several times during a call.
- There will be separate call recordings for each call recording startup.
- Possible user interactions:
  - No recording has started yet – **Start** Recording action.
  - Recording is in progress – **Stop** and **Pause** Recording action.
  - Recording is on pause – **Stop** and **Resume** Recording action.

The call recording mode assigned to the user can be selected from the Control Hub.

```
<config>
<services><calls>
```


Cisco Confidential

```
<record enabled="%ENABLE_CALL_RECORDING_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_RECORDING_WXT%	false	true, false	Enables Call Recording controls.

6.1.27 Voicemail, Visual Voicemail, Message Waiting Indicator

The following custom tags can be used to control the availability of the Cisco BroadWorks Voicemail and Visual Voicemail in the Webex for Cisco BroadWorks client.

Visual Voicemail (VVM) is supported for audio only. Supported formats are wav, ulaw, and mov containing H264 video (played as audio only). It allows users to view incoming voicemails in a list view and individual items can be played. This feature is based on XSI, but notifications of new voicemail are provided over SIP; therefore, SIP must be enabled for the notifications to work. In addition, SIP SUBSCRIBE for Message Waiting Indicator (MWI) configuration is needed for the notifications to arrive and MWI must be enabled for Visual Voicemail to work. For more information on SIP configuration, see section *6.1.1 SIP Server Settings*.

For Cisco BroadWorks release and patch requirements for Visual Voicemail, see the *Webex for Cisco BroadWorks Solution Guide*.

Visual Voicemail must be separately enabled in the configuration.

The following settings are needed on the CommPilot portal to have Visual Voicemail:

- Voice messaging enabled
- “When message arrives, use unified messaging” option enabled
- “Use Phone Message Waiting Indicator” option enabled

Not having the Visual Voicemail service assigned on the Cisco BroadWorks side for the user automatically disables the configuration for the service.

Note that disabling SIP registration also disables MWI for new voicemails. See the table that follows for more information on enabling MWI.

To show voicemail message information in the UI, the client needs to receive SIP MWI notifications from the server (that is, the voicemail event package). See the table that follows for subscription options. Note also that MWI is needed for Visual Voicemail notifications to work.

Note that if SIP subscription to voicemail event package fails, the client keeps retrying when configured to do so. For more information on SIP SUBSCRIBE retry configuration, see section *6.1.9 SIP SUBCSRIBE and REGISTER Refresh and SUBSCRIBE Retry.*

```
<config>
<services><calls>
<mwi enabled="%ENABLE_MWI_WXT%" type="%MWI_MODE_WXT%"/>
<voice-mail enabled="%ENABLE_VOICE_MAIL_WXT%" visual-
voicemail="%ENABLE_VISUAL_VOICE_MAIL_WXT%">
    <transcription enabled="%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%"/>
    <forwarding enabled="%ENABLE_VOICE_MAIL_FORWARDING_WXT%"/>
</voice-mail>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_MWI_WXT%	false	true, false	Set to “true” to enable MWI. Set to “false” to disable MWI.
%MWI_MODE_WXT%	empty	implicit, explicit	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. If left empty, MWI is disabled.
%ENABLE_VOICE_MAIL_WXT%	false	true, false	Set to “true” to enable Voicemail support. Set to “false” to disable Voicemail support.
%ENABLE_VISUAL_VOICE_MAIL_WXT%	false	true, false	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.

6.1.28 Voicemail Transcription for Webex Calling

With this feature, voicemail messages are converted to text and displayed in the visual voicemail message view in the Webex Calling desktop and mobile apps.

The feature should be enabled for a user only if:

1. The app is running in Webex Calling deployment.
2. The Visual Voicemail feature is enabled for the user.
3. The feature is enabled in the config (the enabled attribute in the <services><voice-mail><transcription> tag should be set to “true”).

Tag	Default if Omitted	Supported Values	Description
%ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT%	false	true, false	[Webex Calling Only] Controls the availability of voicemail transcription only if Visual Voicemail is enabled.

6.1.29 Call Settings

6.1.29.1 Call Forwarding Always

The following custom tag can be used to control the availability of the Cisco BroadWorks Call Forwarding Always service in the Webex for Cisco BroadWorks client.

```
<config>
<services><supplementary-services>
<call-forwarding-always enabled="%ENABLE_CALL_FORWARDING_ALWAYS_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	false	true, false	Controls the availability of the Call Forwarding Always service. By default, the feature is disabled.

NOTE: Call Forwarding Always and Call Forwarding to Voicemail (*6.1.29.2 Call Forwarding to Voicemail*) can be used together to display or hide the "Call Forward" setting in the Webex apps. When both tags are disabled, the "Call Forward" setting in the Webex apps is hidden.

6.1.29.2 Call Forwarding to Voicemail

Starting with release 43.9, Webex app provides an option to control the availability of the Forwarding to Voicemail. By default, the feature is enabled, and the following configuration option can be used to disable it.

```
<config>
<services>
   <voice-mail>
      <forwarding enabled="%ENABLE_VOICE_MAIL_FORWARDING_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_VOICE_MAIL_FORWARDING_WXT%	true	true, false	Controls the availability of the Forwarding to Voicemail. By default, the feature is enabled.

NOTE 1: This feature depends on one of the "Voice Messaging User" or "Third-Party Voice Mail Support" services to be assigned to the user.

NOTE 2: Call Forwarding to Voicemail and Call Forwarding Always (*6.1.29.1 Call Forwarding Always*) can be used together to display or hide the "Call Forward" setting in the Webex apps. When both tags are disabled, the "Call Forward" setting in the Webex apps is hidden.

6.1.29.3 BroadWorks Anywhere (Single Number Reach)

The following custom tags control the availability of the BroadWorks Anywhere and the availability of its settings in the Webex for Cisco BroadWorks client. Note that the name of this feature inside the client is *Manage My Numbers*.

```
<config>
<services><supplementary-services>
<broadworks-anywhere enabled="%ENABLE_BROADWORKS_ANYWHERE_WXT%">
       <description enabled="%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%"/>
       <alert-all-locations
enabled="%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%"
default="%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%"/>
```


Cisco Confidential

```
        <call-control enabled="%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%"
default="%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%"/>
        <diversion-inhibitor
enabled="%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%"
default="%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%"/>
        <answer-confirmation
enabled="%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%"
default="%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%"/>
</broadworks-anywhere>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_BROADWORKS_ANYWHERE_WXT%	false	true, false	Enables BroadWorks Anywhere (BWA) on configuration level.
%ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	true	true, false	Controls if the Description of the BWA location should be available for the user.
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	false	true, false	Set to "true" to make Alert All Locations for the BWA service available for the user. Set to "false" to make Alert All Locations for the BWA service unavailable for the user.
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	false	true, false	Controls if the application should enable the Alert All Locations state, at adding second or every subsequent new BWA location.
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	false	true, false	Controls if the Call Control of the BWA location should be available for the user.
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	false	true, false	Controls the default state of the Call Control for the BWA location.
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	false	true, false	Controls if the Diversion Inhibitor of the BWA location should be available for the user.
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	false	true, false	Controls the default state of the Diversion Inhibitor of the BWA location.
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	false	true, false	Controls if the Answer Confirmation of the BWA location should be available for the user.
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	false	true, false	Controls the default state of the Answer Confirmation of the BWA location.

6.1.30 Settings Portal and Web-based Call Settings

The Webex for Cisco BroadWorks client provides access to a settings (Self Care) portal, where the user can configure some of the application and service settings.

Cisco Confidential

Furthermore, the client provides the option to use the Call Settings Web View (CSWV) instead. That allows the user to control more of the server-based call settings. Separate tags can be used to control whether specific services should be visible in the web-based call settings.

> **NOTE**: It is advisable to hide the settings that are already visible in the application like Call Center (see section *6.1.31 Call Center / Call Queue Login/Logout*) and BroadWorks Anywhere (see section *6.1.29.3 BroadWorks Anywhere*). The Remote Office service is also advisable to be hidden because it has been succeeded by the BroadWorks Anywhere service.

The following custom tag can be used to configure the URL for the settings (Self Care or CSWV) portal. If the tag is empty, the link to the settings portal is not visible for the user in the application.

```
<config>
<services>
<web-call-settings target="%WEB_CALL_SETTINGS_TARGET_WXT%"
 <url>%WEB_CALL_SETTINGS_URL_WXT%</url>
<branding-enabled="%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%">
  <service-settings>
   <service name="Call Forwarding Always"
visible="%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%"/>
   <service name="Call Forwarding Busy"
visible="%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%"/>
   <service name="Call Forwarding Not Reachable"
visible="%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%"/>
   <service name="Call Forwarding No Answer"
visible="%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%"/>
   <service name="Do Not Disturb" visible="%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%"/>
   <service name="Anonymous Call Rejection"
visible="%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%"/>
   <service name="Simultaneous Ring Personal"
visible="%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%"/>
   <service name="Sequential Ring"
visible="%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%"/>
   <service name="Automatic Callback"
visible="%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%"/>
   <service name="Call Waiting" visible="%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%"/>
   <service name="Calling Line ID Delivery Blocking"
visible="%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%"/>
   <service name="Personal Assistant"
visible="%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%"/>
   <service name="Call Center - Standard"
visible="%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%"/>
   <service name="BroadWorks Anywhere"
visible="%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%"/>
   <service name="BroadWorks Mobility"
visible="%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%"/>
   <service name="Remote Office" visible="%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%"/>
   <service name="Voice Messaging User"
visible="%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%"/>
 </service-settings>
<userportal-settings> <url>%USER_PORTAL_SETTINGS_URL_WXT%</url></userportal-
settings>
</web-call-settings>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%WEB_CALL_SETTINGS_TARGET_WXT%	external	external, csw	Controls the admin portal mode. Set to “external” to open configured setting portal URL in an external browser. Set to “csw” to open the CSW portal in an embedded browser using the extra parameters section <services><web-call-settings> to form the POST request.
%WEB_CALL_SETTINGS_URL_WXT%	empty	URL string	URL for the settings portal. Example: https://settings.webex.com
%WEB_CALL_SETTINGS_CFA_VISIBLE_WXT%	true	true, false	Controls whether the Call Forwarding Always option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_DND_VISIBLE_WXT%	true	true, false	Controls whether the Do Not Disturb (DND) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_ACR_VISIBLE_WXT%	true	true, false	Controls whether the Anonymous Call Rejection (ACR) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_CFB_VISIBLE_WXT%	true	true, false	Controls whether the Call Forwarding Busy (CFB) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT%	true	true, false	Controls whether the Call Forwarding Not Reachable (CFNR) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT%	true	true, false	Controls whether the Call Forwarding No Answer (CFNA) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT%	true	true, false	Controls whether the Simultaneous Ring Personal (SIMRING) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT%	true	true, false	Controls whether the Sequential Ring (SEQRING) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_RO_VISIBLE_WXT%	true	true, false	Controls whether the Remote Office (RO) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_ACB_VISIBLE_WXT%	true	true, false	Controls whether the Automatic Callback (ACB) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_CW_VISIBLE_WXT%	true	true, false	Controls whether the Call Waiting (CW) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT%	true	true, false	Controls whether the Calling Line ID Delivery Blocking (CLIDB) option should be visible for the user in the web-based settings.

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%WEB_CALL_SETTINGS_PA_VISIBLE_WXT%	true	true, false	Controls whether the Personal Assistant (PA) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	true	true, false	Controls whether the BroadWorks Anywhere (BWA) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	true	true, false	Controls whether the Call Center option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	true	true, false	Controls whether the BroadWorks Mobility (BWM) option should be visible for the user in the web-based settings. Currently the recommended value is "false" due to interoperability issues between Webex for Cisco BroadWorks and BroadWorks Mobility.
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	true	true, false	Controls whether the Voice Management (VM) option should be visible for the user in the web-based settings.
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	false	true, false	Controls whether to use the new Call Settings WebView branding. Enable if the server-side CSWV version is 1.8.6 or above. Otherwise, keep it false.
%WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT%	true	true, false	Controls whether email/voicemail messages options are visible in the web-based settings.
%USER_PORTAL_SETTINGS_URL_WXT%	empty	URL string	Specifies the URL to the user settings portal. To enable the feature and present the Access User Portal button in the UI, this custom tag should be not be empty. For example: https://settings.webex.com.
%USER_PORTAL_SETTINGS_TARGET_WXT%	external	external, internal	Specifies if the URL should be opened in an embedded or external browser.
%USER_PORTAL_SETTINGS_SSO_ENABLED_WXT%	false	true, false	Applicable only when embedded browser is configured (USER_PORTAL_SETTINGS_TARGET_WXT=internal). When enabled, HTTP POST request is used, and BroadWorks short-lived token is added as part of the BODY. When disabled, the URL is opened with HTTP GET.

NOTE 1: The Call Settings WebView URL should always have a trailing "/" configured. For example: http(s)://<XSP-FQDN>/<CSW-Context-Path>/

NOTE 2: The Call Settings WebView application minimum version that is supported is 1.7.5.

Cisco Confidential

For installation on Cisco BroadWorks Release 21.0, see the additional steps described in the *Webex For Cisco BroadWorks Solution Guide*.

6.1.31 Call Center / Call Queue Login/Logout

The Webex app provides access to the Call Center (Call Queue) agent settings. If a user is provisioned for Call Center, this feature enables the user to log into a call center and view the available call queues, as well as join/unjoin queues and set the Automatic Call Distribution (ACD) status.

Starting with Desktop Release 42.8 and Mobile Release 42.12, the Call Center (Call Queue) agent is no longer based on the Call Settings Web View (see section *6.1.30 Settings Portal and Web-based Call Settings*). The Call Center (Call Queue) agent configuration is accessible through footer of the Desktop and Settings of the Mobile Webex app.

```
<config>
<services>
<call-center-agent enabled="%ENABLE_CALL_CENTER_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_CENTER_WXT%	false	true, false	Enables Call Center support.

6.1.32 Xtended Services Interface (XSI)

6.1.32.1 Root and Paths

The Webex for Cisco BroadWorks client uses the following tags to control the XSI Root, Actions and Events path if they need to be configured to differ from the ones used for sign-in.

The main reason to change the XSI Root is to implement load balancing at the configuration level, although it is recommended to use load balancing at the HTTP layer instead.

The Events and Actions paths are typically changed due to branding requirements to remove the *com.broadsoft* domain reference from the URL paths of the XSI HTTP requests performed by the client.

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


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%XSI_ROOT_WXT%	Continues to use the original one used for configuration fetch.	URL string	The XSI root for all XSI operations. Example: https://domain.com/
%XSI_ACTIONS_PATH_WXT%	/com.broadsoft.xsi-actions/	string	Specifies the XSI Actions path. It should start and end with "/" and contain only the actions context. Example: /com.domain.xsi-actions/
%XSI_EVENTS_PATH_WXT%	/com.broadsoft.xsi-events/	string	Specifies the XSI Events path. It should start and end with "/" and contain only the events context. Example: /com.domain.xsi-events/

6.1.32.2 XSI Dynamic Proxy Discovery

The Webex App accesses the XSI (XSI-Actions & XSI-Events) and Device Management Service (DMS) services on the XSP. To find the XSI service host(s), the Webex App performs DNS SRV lookup for _xsi-client._tcp.. The SRV points to the configured URL for the XSP hosts or load balancers for the XSI service. If SRV lookup is not available, the Webex App falls back to A/AAAA lookup.

The client attempts to locate the XSP nodes using the following DNS flow:

- Webex app initially retrieves Xsi-Actions/Xsi-Events URLs from Cisco Webex Cloud (entered when creating the associated BroadWorks Calling Cluster). The XSI hostname/domain is parsed from the URL and the client performs SRV lookup as follows:
    - Webex app performs an SRV lookup for _xsi-client._tcp.<xsi domain>
    - If the SRV lookup returns one or more targets:
        - Webex app makes A/AAAA lookup of the XSI hostname and if it is a valid IP address, the XSI hostname is added at the back of the cached list, as a backup service.
        - The client connects to one of the targets based on the SRV priority, then weight (or at random if they're all equal).
    - If the SRV lookup does not return any targets:
        - The Webex app makes A/AAAA lookup of the Root XSI parameter and if it is a valid IP address, this is the only address added to the cached list. This could be a load balancing edge element, or it could be the XSP server itself.
        - The A/AAAA record must resolve to a single IP address for the same reasons.
- Custom XSI-Actions/XSI-Events paths can be set in the DMS config file, as described in the previous section:

Cisco Confidential

- If there is a difference in the initial XSI Root or Actions paths, the client will re-initialize the XSI Actions/XSI Events connectivity. The first step in this is to perform the same DNS lookup process listed under step 1 - this time requesting a lookup for the value in the %XSI_ROOT_WXT% parameter from its configuration file.
- Note: Make sure to create the corresponding SRV records if you use this tag to change the XSI interfaces.

The Webex app also has a configurable option to control the XSI proxy discovery. The XSI proxy discovery mode can be used to control the combination of the main XSI hostname (used for the SRV lookup) and/or DNS SRV resolved XSI targets used for the XSI communication. To download the config file, the Webex app initially uses the *srv-host* mode. After the config file is downloaded, the configured proxy discovery *mode* is applied. The proxy discovery *mode* can be one of:

- *host-only* - use only the main XSI hostname, do not trigger DNS SRV lookup
- *srv-only* - do not use the main XSI hostname, rely on the DNS SRV lookup only
- *prefer-srv* - if there are DNS SRV records found, use only them. If not, use the main XSI hostname only
- *srv-host* - (default) if there are DNS SRV records found, use them with priority and append the main XSI hostname at the end of the list as a backup service. If not, use the main XSI hostname

After the DMS config file is downloaded:

- If there is an empty XSI Root or it has the same value as the main XSI hostname, and the proxy discovery mode is different than *srv-host*:
  - *host-only* - update the resulting XSI targets and leave just the main XSI hostname
  - *srv-only* - update the resulting XSI targets and leave just the SRV addresses
  - *prefer-srv* - if there is just one address, it should be the main XSI hostname. If there are more, the main XSI hostname is removed from the list
- If the XSI Root is non-empty and its value is different than the main XSI hostname:
  - Perform new DNS lookup process using the XSI Root value
  - Order the DNS results respecting the proxy discovery mode configured
  - Re-initialize its XSI Actions and XSI Events connectivity

```
<config>
<protocols><xsi>
   <proxy-discovery mode="%XSI_PROXY_DISCOVERY_MODE_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%XSI_PROXY_DISCOVERY_MODE_WXT%	srv-host	host-only, srv-only, prefer-srv, srv-host	Controls how the Webex app should build the list of XSI targets used by the application after the download of the config file. The initial discovery, before the DMS config download, always uses srv-host mode.

6.1.32.3 XSI Event Channel

The XSI Event channel is used for various services such as:

- XSI mid-call controls
- Call Settings status notifications
- Call Recording

XSI Events heartbeat is used to keep the XSI Event channel open and the heartbeat interval can be specified using the following parameter.

Release 45.11 introduces few optimizations to the XSI event channel usage.

- A new configurable parameter to control the inactivity timeout of the XSI event channel. If no data (XSI event) or no heartbeat response is received within the configured inactivity timeout, the XSI event channel will be closed.
- If the event channel is closed
    - The given host is added to a blacklist for 10 minutes
    - Re-connect logic will be started, trying to reconnect next XSI host, following incremental timer, starting from 5 seconds, and then following Fibonacci numbers up to 150 seconds, including random factor.
    - If all the XSI hosts are blacklisted, the blacklist is cleared and the app starts immediately reconnect to the highest priority host.

```
<config>
<protocols><xsi>
<event-channel enabled="%ENABLE_XSI_EVENT_CHANNEL_WXT%">
    <heartbeat-interval>%CHANNEL_HEARTBEAT_WXT%</heartbeat-interval>
    <inactivity-timeout>%CHANNEL_INACTIVITY_TIMEOUT_WXT%</inactivity-timeout>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_XSI_EVENT_CHANNEL_WXT%	true	true, false	Controls whether the XSI Event channel is enabled. It should be set to “true” to receive, for example, mid-call control service-related events. The recommended value is “true”.
%CHANNEL_HEARTBEAT_WXT%	10000	number	This is the XSI Event channel heartbeat (in milliseconds).

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%CHANNEL_INACTIVITY_TIMEOUT_WXT%	60000	(0-120000]	Specifies the max inactivity timeout (in milliseconds) of the XSI event channel - the time it should wait to receive an event (heartbeat response or any other kind of XSI event). Should be greater than 0 and less or equal to 120000 (2 minutes)

6.1.33 Codec Configuration

Webex for Cisco BroadWorks offers a variety of audio and video codecs. The respective lists of codecs are located under *config/services/calls/* in the *audio/codecs* and *video/codecs* sections. The priority of each codec can be changed via the *XML-attribute priority*, which is a value between 0.0 (lowest) and 1.0 (highest).

The Webex app officially supports the following codecs:

- Audio
  - Opus
  - G.722
  - G.729
  - PCMU (G.711U)
  - PCMA (G.711A)
  - iLBC
  - AI Codec
- Video
  - H.264

```
<config>
<services><calls>
  <audio>
    <codecs>
      <codec name="opus" priority="1" payload=""/>
      <codec name="xCodec" mode="HP" priority=".99" payload=""/>
      <codec name="xCodec" mode="ULP" priority=".98" payload=""/>
      <codec name="G722" priority=".9" payload=""/>
      <codec name="PCMU" priority=".8" payload=""/>
      <codec name="PCMA" priority=".7" payload=""/>
      <codec name="G729" priority=".5" payload="" vad=""/>
      <codec name="iLBC" priority=".4" payload="" framelength="30"/>
      <codec name="telephone-event" payload="101" in-band="false"/>
    …
  <video>
    <codecs>
      <codec name="H264" payload="109" resolution="HD" framerate="30"
bitrate="2000000" priority="1.0">
```


Cisco Confidential

```
        <packet-mode>0</packet-mode>
```

The client supports H.264 as video codec. The video resolution attribute, indicating the maximum video resolution advertised by the app, can set to one of the following available values: SUBQCIF, QCIF, CIF, 4CIF, VGA, HD and WIDE_FULL_HD.

Starting with the Release 45.8, the maximum video resolution used by the Desktop app is updated from the default HD to WIDE_FULL_HD, and the one for the Mobile and Tablet apps remains 4CIF.

If the bit rate is not entered in the configuration, the default bit rate values are used. Default bit rate values, per resolution and frame rate, are listed in the following table.

Resolution	Video Size *	FPS (Frames Per Second)	Default Bit Rate Values per Resolution and FPS
SUBQCIF	128 x 96	15	128000
QCIF	176 x 144	30	192000
CIF	352 x 288	15	384000
CIF	352 x 288	30	768000
VGA	640 x 460	15	2000000
4CIF	704 x 576	25	2000000
HD	960 x 720	30	2000000
WIDE_FULL_HD	1920 x 1080	30	4000000

***** Maximum advertised video resolution. The actual video resolution during a call between two Webex for Cisco BroadWorks clients depends on the capabilities of both clients – it will be the lower of the two and will be the same on both clients.

Video resolution for a video call is negotiated during session setup and is based on the capabilities of the two endpoints. Video call resolution is the same on both endpoints. That is, if the Webex for Cisco BroadWorks endpoints have different capabilities (and therefore support different resolutions), then the lower resolution is negotiated for the call. Video resolution may change during a call if the network conditions deteriorate. In this case, the two mobile endpoints may be using different video resolutions.

The packetization mode can be configured to be SingleNAL (0) or Non-interleaved (1). The template uses SingleNAL by default (<packet-mode>0</packet-mode>).

Telephone event configuration, single or multiple, is also supported. During codec negotiation, the client sends all the configured codecs, including telephone event. After the audio codec is selected, it searches for telephone event in the offer. If the offer has the telephone event with the sample rate of the negotiated audio codec, then this telephone event is selected. Otherwise, the first telephone event in the list is used.

If there is at least one telephone event negotiated, the dual-tone multi-frequencies (DTMFs) are sent as RTP packets using the corresponding payload type. And if there are no telephone events negotiated at all, the DTMFs are sent as RTP packets with the payload type of the negotiated audio codec. Out-of-band mechanism to deliver DTMFs is not supported by the Webex app.

Example configured codecs:

```
<codec name="telephone-event" payload="100" in-band="false" />
```


Cisco Confidential

```
<codec name="telephone-event" payload="101" clockrate="48000" in-band="false" />
```

If an audio codec with sample rate of 48kbps is negotiated, the telephone event with payload 101 is used.

6.1.33.1 AI Codec

Starting with Release 44.8, the Webex app introduces support of a new audio codec – AI Codec (xCodec). This audio codec is used in adverse network conditions to achieve better call quality. The Webex Media Engine in the Webex app checks the device capabilities, tracks the media quality and the AI Codec can be used if it is supported and enabled through the config file.

The AI Codec works only in combination with the Opus codec. This means that both the Opus and AI Codec should be advertised and negotiated by both sides during the SDP negotiation.

6.1.34 SIP-URI Dialing

Currently SIP-URI dialing through BroadWorks is not available and by default all SIP-URI calls are routed through Locus, also known as “Free Calling”. In some environments, this is not desirable and such calls should be blocked.

> **NOTE**: This applies only if Locus calling is disabled. Only in this case will SIP URI dialing blocking work.

The following configuration provides this option.

```
<config>
    <services>
        <calls>
            <sip-uri-dialing enable-locus-
calling="%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	true	true, false	Controls whether the SIP-URI should be routed through Locus (true) or blocked (false).

6.1.35 Call History

The Webex app supports call history to track the calls for the user. For the primary line of the user, the call history is synchronized across all devices of the user. For the secondary lines (shared and virtual), the app keeps just local call history records.

Release 45.11 adds the unified call history for the secondary lines (shared and virtual) as well, to be synchronized across all the user’s devices. The current config option now controls both the unified call history for the primary and secondary lines.

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	false	true, false	For primary line only, controls if the application should use the Unified Call History or client-side (local) one.

6.1.36 Disable Video Calls

Release 41.9 added the ability to disable video calls. There are separate configuration options to control this feature for BroadWorks-backed and Locus (free) VoIP calls.

When the feature is enabled and the feature tag is set to “false”:

- the user will not see the “Accept incoming calls with my video on” setting
- all incoming video calls if accepted, will be audio ones
- the user will not be able to escalate a call to video and video escalations will be automatically rejected

When video calls are enabled, a new configuration property is added to control the default value of the “Accept incoming calls with my video on” setting. By default, this feature is turned ON for Desktop and turned OFF for Mobile and Tablet.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_SIP_VIDEOCALLS_WXT%	true	true, false	Controls the availability of SIP video calls through BroadWorks.
%ENABLE_LOCUS_VIDEOCALLS_WXT%	true	true, false	Controls the availability of Locus (free) video calls.
%VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT%	Desktop - true Mobile / Tablet - false	true, false	Controls the default value of the “Accept incoming calls with my video on” setting.

6.1.37 Emergency (911) Calling - Location Reporting with E911 Provider

The Desktop and Tablet Webex client supports E911 location reporting using RedSky, Intrado, or another E911 emergency location provider for the Webex for BroadWorks deployment. The E911 provider provides a per-device location support (for Webex desktop and tablets apps and HELD-capable MPP devices) and a network that routes emergency calls to Public Safety Answering Points (PSAPs) around the US, its territories (Guam, Puerto Rico, and Virgin Islands), and Canada only. The service is enabled on a per-location basis.

Tag	Default if Omitted	Supported Values	Description
%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	false	true, false	Enables E911 provider Emergency Location Platform.

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%BWE911-PRIMARY-HELDURL%	empty	string	Specifies the URL to the E911 provider Emergency Location Platform supporting the HELD protocol.
%BWE911-CUSTOMERID%	empty	string	The customer ID (HeldOrgId, CompanyID) used for the E911 provider HTTPS request.
%BWE911-SECRETKEY%	empty	string	The secret to authenticate the E911 provider HTTPS request.
%BWE911-EMERGENCY-NUMBER-LIST%	empty	CSV string	The list of emergency numbers supported by E911 provider.
%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	0 (user will not be prompted again)	number [0 - 43200]	The timeout in minutes that will be used to remind the user to update the emergency location if the current one is not entered or is invalid. The suggested value if decided to enable: 1440 (one day).
%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	-1 (user can cancel the dialog always)	number [-1 - 100]	The times that the user is allowed to close the location dialog before location becomes mandatory (that is, they cannot close the location window). Possible values: ▪ N = -1 (user can cancel the dialog always) ▪ N = 0 (user is not allowed to cancel the dialog - mandatory location always) ▪ N > 0 (user is allowed to cancel the dialog N times before it becomes mandatory)
%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	aggressive, once_per_login	once_per_login	Defines the E911 location prompting behavior. The “aggressive” value will show the dialog to the user on each network change to an unknown location, while the “once_per_login” value will show the dialog only once, preventing further popup and distractions for the user.

NOTE 1: BWE911-*** tags are “Dynamic Built-in System Tags”. For more information, see section *5.7 Cisco BroadWorks Dynamic Built-in System Tags*.

NOTE 2: If VOIP calling is disabled, the only meaningful value for emergency dial sequence (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) is cs-only.

Cisco Confidential

6.1.38 PAI as Identity

For **incoming calls**, this new parameter controls the priority of SIP From and P-Asserted-Identity (PAI) headers, and what should be used as a calling line identity. If there is an X-BroadWorks-Remote-Party-Info header in the incoming SIP INVITE, it is used with priority over the SIP From and PAI headers. If there is no X-BroadWorks-Remote-Party-Info header in the incoming SIP INVITE, this new parameter determines if the SIP From header is priority over the PAI header or vice versa.

If enabled attribute of the <use-pai-as-calling-identity> tag is set to “true”, the PAI header is used with priority over the From header. This calling party identity is used to resolve the contact and present it to the user.

For **outgoing calls**, this logic is not applied. In the 18X, 200 OK responses, the connected line identity is received, so the Webex application always uses the SIP PAI header with priority.

Tag	Default if Omitted	Supported Values	Description
%USE_PAI_AS_CALLING_IDENTITY_WXT%	false	true, false	Controls whether the calling identity, presented to the user should be taken from the SIP From or SIP P-Asserted-Identity headers. Set to “true” to use the PAI header with priority.

6.1.39 Disable Screen Sharing

Release 42.5 adds the ability to control the availability of the screen sharing. When the screen sharing is disabled:

- the user will not see the option to initiate screen sharing in 1-1 calls
- the incoming screen sharing requests are rejected and user will see an informative message

By default, this feature is enabled.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_SCREEN_SHARE_WXT%	true	true, false	Specifies if screen sharing should be enabled for the user.

6.1.40 Spam Call Indication

When the feature toggle (per deployment type) is enabled, and the feature is enabled in the config file, the Webex app processes the new parameter indicating the spam call verification status, if they are received as part of the NewCall Push Notification or call history records.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALLS_SPAM_INDICATION_WXT%	false	true, false	Controls the availability of the spam call indication in the incoming call screen and call history for Webex Calling only.

Cisco Confidential

6.1.41 Noise Removal and Bandwidth Extension for PSTN/Mobile Calls

Noise removal provides a better calling experience to calling users when they talk to non-Webex users on PSTN or mobile devices. With release 43.12, noise removal is turned on by default.

Release 44.2 of the Webex app introduces new incoming audio media Speech AI enhancements for narrowband PSTN calls.

- A new bandwidth extension algorithm is added to improve the audio quality by extending the bandwidth of the narrowband PSTN spectrum and removing the noise. The extended bandwidth will increase intelligibility and decrease listening fatigue.
- The already existing Noise Removal algorithm is enhanced, removing the limitations for the Music on Hold and other audio tones (e.g. beep signals).
- When this feature is enabled, users sees the “Smart audio – external“ indicator and can control the Speech AI enhancements for the incoming audio media.

By default, these speech enhancements are enabled and turned on. User can control the initial state through Smart audio settings in the Audio Preferences.

```
<config>
   <services>
      <calls>
         <speech-enhancements enabled="%ENABLE_SPEECH_ENHANCEMENTS_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	false	true, false	Enables the speech enhancements for external (incoming) media.

NOTE: The Noise Removal is now part of the additional speech enhancements, and the <noise-removal> tag has been deprecated by the new <speech-enhancements> tag. The Noise Removal custom tag %ENABLE_NOISE_REMOVAL_WXT% is also deprecated.

6.1.42 QoS DSCP Marking

QoS DSCP marking is supported with the Webex app calling media RTP packets (Audio and Video). DSCP determines traffic classification for network data. This can be used to determine which network traffic requires higher bandwidth, has a higher priority, and is more likely to drop packets.

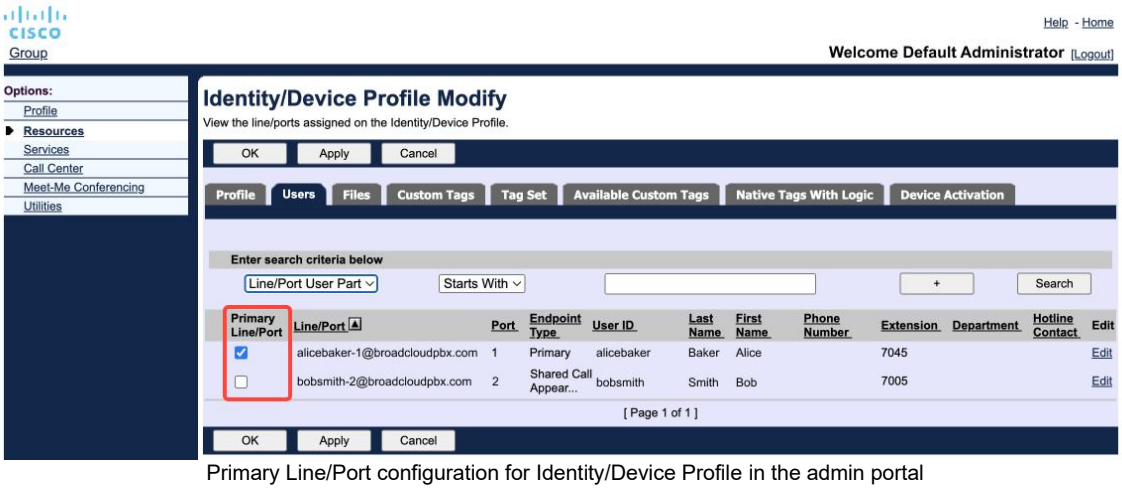
NOTE: Recent versions of the Microsoft Windows operating system do not allow applications to directly set DSCP or UP on outgoing packets, instead requiring the deployment of Group Policy Objects (GPO) to define DSCP marking policies based on UDP port ranges.

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_AUDIO_QOS_WXT%	true	true, false	Enables QoS for audio calls.
%AUDIO_QOS_VALUE_WXT%	46	0-63	Specifies the QoS value for the selected QoS type for the audio calls. Note: Default value is used, if no value is provided, or the value couldn't be parsed successfully.
%ENABLE_VIDEO_QOS_WXT%	true	true, false	Enables QoS for video calls
%VIDEO_QOS_VALUE_WXT%	34	0-63	Specifies the QoS value for the selected QoS type for the video calls. Note: Default value is used, if no value is provided, or the value couldn't be parsed successfully.

6.1.43 Primary Profile

With the integration of the Shared lines (*6.1.50.1 Desktop - Shared-Line Appearance***Error! Reference source not found.**), if user's line is shared with another user, there may be multiple profiles of the same type configured for the user. To select the correct profile to sign in the Phone services, the Cisco BroadWorks has been enhanced to indicate whether a user owns a device i.e. it is assigned the Primary Line/Port for a device - for more information about the Cisco BroadWorks update, check Owner Flag In Device List To Support Webex Client Shared Lines.



Primary Line/Port configuration for Identity/Device Profile in the admin portal

Cisco Confidential

Starting with Release 43.2, a new configuration option (*device-owner-restriction*) is added to control whether the primary profile restriction should be applied. It can be used to allow the Webex application to use a non-primary Line/Port profile to sign in the Phone services. This config option is applied for all the configurations, regardless the number of profiles configured for the user (**If the device ownership restriction is enabled and there is no device with Primary Line/Port for the corresponding platform, Phone services will not connect**).

Same restriction applies to the devices user can pair with in the Desktop Webex app. User can see and pair only with devices he is owning. This prevents pairing with devices of another user that has shared or virtual line assigned. The value of the same configuration parameter applies to this restriction too.

```
<config>
<services><calls>
<device-owner-restriction enabled="%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	true	true, false	Controls the device owner restriction – if the Phone Services should use the primary profile for the given device

NOTE: It is recommended owner's restriction to be enabled. If disabled, the Phone services will use the first profile found to sign in and some problems may occur if there are multiple profiles configured for the user of the same type.

6.1.44 Block List (Webex Calling only)

Starting with 43.5 the Webex app introduces user defined block list of phone numbers. If the feature is enabled, user can specify incoming calls from specific numbers to be blocked on the server side and not delivered on any of the user's devices. User can see these blocked calls in the call history.

User can configure the block list from two places - Calling Preferences and Call History. In the Preferences, user can see the list of blocked numbers and edit it. In the Call History, user can see the call history records for the calls blocked by the user defined block list. These records have Blocked indication if the number is in the user defined block list and user will have the option to unblock the number directly for given record. Block option is also available.

Rules for the numbers added to the user-defined block list:

Number format

- Blocking from the Calling Preferences apply E.164 format restriction locally in the Webex app
- Blocking from the Call History is allowed for all the Webex Calling records
- The Cisco BroadWorks may allow or reject requests for new numbers added in the block list based on the number format

Internal numbers - incoming calls from internal numbers will be delivered to the user, even if they are part of the user-defined block list

Cisco Confidential

The user defined block list is configured on the Cisco BroadWorks and is applied to all the WxC devices for the user.This feature works together with the admin defined block list, which is not configurable by the user and can be controlled only by the administrators through the Control Hub. There are NO call history records for the incoming calls blocked by the admin defined block list.

The user defined block list is applied after the STIR/SHAKEN, admin defined block list and the anonymous call rejection policies.

```
<config>
<services><calls>
<call-block enabled="%ENABLE_CALL_BLOCK_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_BLOCK_WXT%	true	true, false	Enables the user defined block list Set to “true”, to see the block list in the Calling Preferences and Call History

NOTE: This feature depends on the Cisco BroadWorks Call Block service being assigned to the user.

6.1.45 Media Adaptation and Resilience Implementation (MARI)

6.1.45.1 Rate Adaptation

The Webex application has already integrated adaptive media quality techniques to ensure that audio is not affected by any video packet loss, and to ensure that video can leverage video rate adaptation to manage the amount of bandwidth used during times of congestion.

Rate adaptation or dynamic bit rate adjustments adapt the call rate to the variable bandwidth available, down-speeding or up-speeding the video bit rate based on the packet loss condition. An endpoint will reduce bit rate when it receives messages from the receiver indicating there is packet loss; and once the packet loss has decreased, up-speeding of the bit rate will occur.

There are no configurable settings to control the usage of the rate adaptation mechanism.

6.1.45.2 Forward Error Correction (FEC) and Packets Retransmission (RTX)

Starting with Release 43.4, the Webex App adds to the media adaptation mechanism the support for Forward Error Correction (FEC) and Packets Retransmission (RTX) for both audio and video media.

FEC provides redundancy to the transmitted information by using a predetermined algorithm. The redundancy allows the receiver to detect and correct a limited number of errors, without the need to ask the sender for additional data. FEC gives the receiver an ability to correct errors without needing a reverse channel (such as RTCP) to request retransmission of data, but this advantage is at the cost of a fixed higher forward channel bandwidth (more packets sent).

Cisco Confidential

The endpoints do not use FEC on bandwidths lower than 768 kbps. Also, there must also be at least 1.5% packet loss before FEC is introduced. Endpoints typically monitor the effectiveness of FEC and if FEC is not efficient, it is not used.

FEC consumes more bandwidth than retransmission but has less delay. RTX is used when small delay is allowed and there are bandwidth constraints. In case of large delay and enough bandwidth, FEC is preferable.

The Webex App dynamically selects RTX or FEC depending on negotiated bandwidth and delay tolerance for a given media stream. FEC results in higher bandwidth utilization due to redundant video data, but it doesn't introduce additional delay to recover lost packets. Whereas RTX doesn't contribute to higher bandwidth utilization, because the RTP packets are retransmitted only when the receiver indicates packet loss in RTCP feedback channel. RTX introduces packet recovery delay due to the time it takes for the RTCP packet to reach the receiver from the sender and for the retransmitted packet to reach the receiver from the sender.

FEC is required to be enabled to have RTX enabled.

```
<config><services><calls>
<audio>
       <audio-quality-enhancements>
              <mari>
                     <fec enabled="%ENABLE_AUDIO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                            <payload>111</payload>
                            <max_esel>1400</max_esel>
                            <max_n>255</max_n>
                            <m>8</m>
                            <multi_ssrc>1</multi_ssrc>
                            <non_seq>1</non_seq>
                            <feedback>0</feedback>
                            <order>FEC_SRTP</order>
                     </fec>
                     <rtx enabled="%ENABLE_AUDIO_MARI_RTX_WXT%">
                            <mari-rtx>90000</mari-rtx>
                            <payload>112</payload>
                            <time>180</time>
                            <data-flow>1</data-flow>
                            <order>RTX_SRTP</order>
                     </rtx>
              </mari>
...
<video>
       <video-quality-enhancements>
              <mari>
                     <fec enabled="%ENABLE_VIDEO_MARI_FEC_WXT%">
                            <x-ulpfecuc>8000</x-ulpfecuc>
                            <payload>111</payload>
                            <max_esel>1400</max_esel>
                            <max_n>255</max_n>
                            <m>8</m>
                            <multi_ssrc>1</multi_ssrc>
                            <non_seq>1</non_seq>
                            <feedback>0</feedback>
                            <order>FEC_SRTP</order>
                     </fec>
                     <rtx enabled="%ENABLE_VIDEO_MARI_RTX_WXT%">
                            <mari-rtx>90000</mari-rtx>
                            <payload>112</payload>
```


Cisco Confidential

```
                        <time>180</time>
                        <data-flow>1</data-flow>
                        <order>RTX_SRTP</order>
                    </rtx>
                </mari>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_AUDIO_MARI_FEC_WXT%	false	true, false	Enables FEC for Audio calls
%ENABLE_AUDIO_MARI_RTX_WXT%	false	true, false	Enables RTX for Audio calls (requires enabled audio FEC)
%ENABLE_VIDEO_MARI_FEC_WXT%	false	true, false	Enables FEC for Video calls
%ENABLE_VIDEO_MARI_RTX_WXT%	false	true, false	Enables RTX for Video calls (requires enabled video FEC)

6.1.46 Simultaneous Calls with Same User

Adding support for simultaneous calls with the same user on single device.

This feature is useful for some deployments, where the presented identity of the call is not the same as the connected identity. This leads to the inability to initiate an attended transfer back to the original party. By enabling this feature, user will be able to handle multiple simultaneous calls with the same remote party.

```
<config>
   <services>
      <calls>
         <simultaneous-calls-with-same-user
enabled="%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	false	true, false	Specifies if the Webex app can have just a single or multiple WxC calls with the same user.

6.1.47 RTCP-XR

Starting with Release 43.8, Webex App adds negotiation for RTCP-XR packets exchange during a call. Negotiation happens during the SIP INVITE session establishment. If both endpoints support RTCP-XR packets, the Webex Media Engine will start exchanging these packets and help the adaptive call quality mechanism. This feature is enabled by default.

Additionally, for Webex Calling only, these additional metrics will be sent through the SIP BYE and in this way exposed in Control Hub.

```
<config>
<protocols><sip>
```


Cisco Confidential

```
<rtcp-xr>
   <negotiation enabled="%ENABLE_RTCP_XR_NEGOTIATION_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	true	true, false	Enables RTCP-XR negotiation and packets exchange for better call quality. Enabled by default.

6.1.48 Call Forwarding Info

Release 44.2 of the Webex App introduces configurable option to control the visibility of the call forwarding and redirection information in the call related screens and call history.

```
<config>
<services><calls>
<call-forwarding-info enabled="%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	true	true, false	Controls the visibility of the call forwarding and redirection info. Set to “true”, to see the info in the call related screens and call history.

6.1.49 Caller ID

6.1.49.1 Outgoing Caller ID

Webex Mobile (Release 44.2) and Desktop (Release 44.3) apps introduce a new capability for the user to choose the preferred external caller ID for outgoing calls. The list of available options includes:

- Direct line (default)
- Location number
- Custom number from the same organization
- Call Queues the user is part of, which enables agents to use their caller ID number
    - If any DNIS options are configured, they will be available for selection
- Hunt Groups the user is part of, which enables agents to use their caller ID number
- Hide Caller ID

Notes:

- List of options depend on the line:
    - Primary line – full set of options
    - Shared lines – not available

Cisco Confidential

- Virtual lines – only Call Queue options
- If the already selected identity is no longer available, user's default caller ID is used
- Emergency calls always use user's Emergency Callback Number
- Deprecates <outgoing-calls> tag under section <services><call-center-agent>

The list of the available options is configurable through the admin portal. There are also separate DMS custom tags to control the availability of these enhancements in the Webex app.

```
<config>
<services><calls>
   <caller-id>
      <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
         <additional-numbers enabled="%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%"/>
         <call-center enabled="%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%"/>
         <hunt-group enabled="%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%"/>
         <clid-delivery-blocking enabled="%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%"/>
      </outgoing-calls>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CLID_OUTGOING_CALLS_WXT%	false	true, false	Enables calling line id number selection for outgoing calls.
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	false	true, false	Controls the availability of the additional numbers configured for the user.
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	false	true, false	Controls the availability of the call center (DNIS) numbers configured for the user.
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	false	true, false	Controls the availability of the hunt group numbers configured for the user.
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	false	true, false	Enables caller id delivery blocking as selection for outgoing calls.

NOTE: Desktop app version 44.3 supports just Call Center CLID and 44.4 adds support for the rest of the options.

6.1.49.2 Remote Caller ID Name

At receiving/initiating a call, Cisco BroadWorks sends the display name of the remote party in the SIP INVITE. It is used by default by the Webex app. At the same time, the Webex app starts contact resolution against several sources, with the following priority:

- Common Identity (CI)
- Contact service (custom contacts)
- Outlook contacts (Desktop)

Cisco Confidential

- Local Address Book (Mobile)

In case of a successful contact resolution against any of the search sources the display name of the remote party is updated. Also, if the contact is found in CI, the call session is linked to the Webex cloud services of the same user, providing the option to see the avatar and presence of the remote party, have a chat, screen share, option to escalate to a Webex cloud meeting, etc.

Release 44.5 of the Webex app adds configurable option to ignore the contact resolution and always keep the Cisco BroadWorks display name for calls with Workspaces or a RoomOS devices used for 1:1 Cisco BroadWorks call.

```
<config>
<services><calls>
   <caller-id>
      <remote-name>
         <machine mode="%CLID_REMOTE_NAME_MACHINE_MODE_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%CLID_REMOTE_NAME_MACHINE_MODE_WXT%	resolved	resolved, sip	Controls the remote party display name for workspaces and RoomOS devices. Use “sip” to ignore the contact resolution and use the display name received in the SIP INVITE session.

Cisco Confidential

6.1.50 Multi-line

The Webex user can have a primary line and up to 9 secondary lines. Secondary lines can be Shared or Virtual (Webex Calling only). For Webex for BroadWorks deployment, the Desktop app works only with Shared lines, and the feature is not supported in the Mobile app.

Webex app gets the line configuration through the DMS config file which is downloaded at sign in and every 12h timeframe. In case of line configuration update is detected, the user is requested to restart the application to apply the changes. Re-login of the user will detect and apply any line configuration updates immediately.

The following depicts the section of the DMS config template related to the multi-line support for both Desktop and Mobile.

```
<config>
<protocols>
   <sip>
       <lines multi-line-enabled="%ENABLE_MULTI_LINE_WXT%">
          <personal>
              <line-port>%BWDISPLAYNAMELINEPORT%</line-port>
          </personal>
          <line lineType="%BW-MEMBERTYPE-1%">
              <external-id>%BWUSEREXTID-1%</external-id>
              <voice-mail-number>%BWVOICE-PORTAL-NUMBER-1%</voice-mail-number>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
1%</conference-service-uri>
              <domain>%BWHOST-1%</domain>
              <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
             ...
          </line>
          <line lineType="%BW-MEMBERTYPE-2%">
              <external-id>%BWUSEREXTID-2%</external-id>
              <voice-mail-number>%BWVOICE-PORTAL-NUMBER-2%</voice-mail-number>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
2%</conference-service-uri>
              <domain>%BWHOST-2%</domain>
              <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-2%</group-call-pickup>

             ...
          </line>
          ...
          <line lineType="%BW-MEMBERTYPE-10%">
              <external-id>%BWUSEREXTID-10%</external-id>
              <voice-mail-number>%BWVOICE-PORTAL-NUMBER-10%</voice-mail-number>
              <conference-service-uri>sip:%BWNETWORK-CONFERENCE-SIPURI-
10%</conference-service-uri>
              <domain>%BWHOST-10%</domain>
              <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-10%</group-call-pickup>
             ...
          </line>
```

To control the multi-line feature, use the dedicated custom tag.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_MULTI_LINE_WXT%	false	true, false	Enables multiple lines support (if configured). If disabled (set to "false"), just the first line configured will be used by the application.

Cisco Confidential

NOTE 1: The feature Boss-Admin (Executive-Assistant) support is not available in combination with multi-line configuration.

NOTE 2: See 'Shared line appearance' in the Webex-for-Cisco-BroadWorks-Solution-Guide for additional BroadWorks requirements.

6.1.50.1 Desktop - Shared-Line Appearance

Starting with Release 42.12, Webex application adds support for Shared lines. Administrator should set up the Shared Call Appearances for each shared line.

Release 43.12, the Webex app is enhanced to allow moving (locally resume) a held call on a Shared or Virtual line, handled by another user or by the same user on another device. For more information, check *6.2.12 Move Call*.

6.1.50.2 Desktop - Virtual Lines (Webex Calling only)

For Webex Calling deployment only, Webex App supports multi-line configuration using Virtual lines. Functionally, the configuration with Virtual lines matches the multi-line using shared lines – having the ability to see the virtual lines configured for the user and to use them for incoming and outgoing calls.

Release 43.4 extends the Virtual lines support, adding the Group Call Park and Call Park Retrieve.

Release 43.12, the Webex app is enhanced to allow moving (locally resume) a held call on a Shared or Virtual line, handled by another user or by the same user on another device. For more information, check *6.2.12 Move Call*.

6.1.50.3 Mobile (Webex Calling only)

For Webex Calling deployment only, Release 45.4 adds support for multiple lines (shared and virtual) in the Mobile version of the Webex app. The line assignment is applicable to both Desktop and Mobile Webex app.

Due to the specifics of the Mobile platform, user can have up to two simultaneous calls at the same time on any of the lines.

NOTE 1: If Calling with native dialer is enabled (see *6.3.5.1 Call with Native Dialer*), multi-line is disabled.

NOTE 2: Multi-line for Tablet version is not supported.

6.1.51 Enhanced SIP Authorization

Release 45.4 of the Webex app provides configurable option to optimize the SIP communication, by sharing the authorization between all the SIP sessions. The app will store the authorization and re-use it until it is still valid.

Cisco Confidential

This feature speeds up the SIP communication between the server and the Webex app, reduces the traffic, lowers the call connect time and improves the overall performance of the Webex app.

```
<config>
<protocols>
  <sip>
    <enhanced-authorization enabled="%ENABLE_ENHANCED_AUTHORIZATION_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	false	true, false	When set to “true”, the SIP authorization enhancement is enabled.

NOTE 1: Some SBCs may require new SIP authorization on every session, so this feature should be used according to the deployment specifics.

NOTE 2: Even if this feature is enabled, if the Webex app receives 401 Unauthorized, new authorization will be used in the next SIP request.

6.1.52 Personal Assistant (Away Presence)

With Release 44.11, the Mobile Webex app and Release 45.3, the Desktop Webex app, adds integration with the Cisco BroadWorks Personal Assistant (PA) service. It works in combination with the user’s Away presence and requires synchronization of the PA status with the Webex Cloud presence.

The PA service provides to the user an option to inform the callers of the reason the called party is not available, optionally providing information on when the called party will return and whether there is an attendant to handle the call.

If the PA is enabled, the Away presence option will be available for the user. It can be used to configure the PA on the Cisco BroadWorks side. When the feature is activated, users will see the user’s Away presence in combination with the PA status and the duration configured.

User can configure just the manual PA configuration. If there are any schedules affecting the PA service, the presence will be updated through the Personal Assistant Status Sync. However, the Webex app does not expose the schedules configuration and the schedules that are affecting the PA.

```
<config>
<services>
  <personal-assistant enabled="%PERSONAL_ASSISTANT_ENABLED_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%PERSONAL_ASSISTANT_ENABLED_WXT%	false	true, false	Controls whether the Away presence feature is available for the user.

Cisco Confidential

NOTE 1: This feature requires the Personal Assistant Status Sync to be enabled from the Partner Hub.

NOTE 2: The standard Personal Assistant call routing won't take effect while DND, Call Forwarding Always or Call Forwarding Selective services are active.

NOTE 3: The manual Do Not Disturb and Busy presence states have higher priority compared to Away. When user manual activates one of these presence statuses, enabling the Personal Assistant does not result in your presence status changing to Away.

6.1.53 End-to-End Encryption (Webex Calling only)

Starting with Release 45.11, for the Webex Calling deployment only, that Webex app adds audio and video media end-to-end encryption (E2EE) support for the 1-on-1 calls within the same organization. The E2EE guarantees only the participants in the communication can decrypt the content.

That calls start with the standard SRTP encryption, with keys exchanged during the SDP negotiation. If the two parties support E2EE, new set of keys, available only to the two participants, are exchanged and used to encrypt the media.

```
<config><services>
<calls>
     <e2ee enabled="%ENABLE_CALLS_E2EE_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALLS_E2EE_WXT%	false	true, false	Controls whether the E2EE should be enabled for the 1:1 calls.

Cisco Confidential

6.2 Desktop Only Features

6.2.1 Forced Logout

This feature allows Cisco BroadWorks to track online client instances with the same device type and only allow one of them to be online at any one time. When Cisco BroadWorks notifies the client to log out, the SIP connection is terminated, and the client indicates that calling is not connected.

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 to use forced logout, the SIP *Call-Info* subscription must be enabled.

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

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

```
<config>
<services>
<forced-logout enabled="%ENABLE_FORCED_LOGOUT_WXT%" control-protocol="SIP"
appid="%FORCED_LOGOUT_APPID_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_FORCED_LOGOUT_WXT%	false	true, false	Enables forced logout.
%FORCED_LOGOUT_APPID_WXT%	empty	string	Appid used on the server side for correlation. This can be any string. Example: “123abc”

6.2.2 Call Pickup

Call Pickup is a multiuser service that allows selected users to answer any ringing line within their call pickup group. A call pickup group is defined by the administrator and is a subset of the users in the group who can pick up each other’s calls.

The following pickup cases are supported:

- Blind call pickup

Cisco Confidential

- Directed call pickup (which enables a user to answer a call directed to another phone in their group by dialing the respective feature access code followed by the extension of the ringing phone).

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

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_PICKUP_BLIND_WXT%	false	true, false	Set to “true” to enable Blind Call Pickup.
%ENABLE_CALL_PICKUP_DIRECTED_WXT%	false	true, false	Set to “true” to enable Directed Call Pickup.

6.2.3 Boss-Admin (Executive-Assistant) Support

The Boss-Admin, known as Executive-Assistant feature on Cisco BroadWorks, allows an assistant to operate on behalf of an executive to screen, answer, and place calls as the “executive”. One assistant can have many executives and it is possible to:

- Select the desired role when making a call.
- Answer an incoming call on behalf of an executive and then push the call to the executive. In addition to that, all usual call management options are available.
- See that an incoming call is actually for the executive.

Executive and Executive-Assistant are two interrelated Cisco BroadWorks services that together deliver the following functionality:

- A user with the Executive service can define a pool of assistants who manage their calls. The assistants have to be selected among the users in the same group or enterprise who have the Executive-Assistant service assigned.
- A user with the Executive-Assistant service can answer and initiate calls on behalf of their executives.
- Both the executive and their assistants can specify which calls should be forwarded to the assistants, how assistants should be alerted about incoming calls, and which of the calls forwarded to the assistants should be presented to the executive for screening.

```
<config>
<services>
<executive-assistant enabled="%ENABLE_EXECUTIVE_ASSISTANT_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	false	true, false	Set to “true” to enable the Boss-Admin feature.

Cisco Confidential

NOTE: The feature Boss-Admin (Executive-Assistant) support is not available in combination with Shared-Lines.

6.2.4 Escalate SIP Calls to Meeting (Webex Calling only)

The client provides the functionality to escalate an ongoing SIP call to a meeting via Webex Calling. By using this functionality instead of a standard ad-hoc conference, the user will be able to use video as well as screen sharing during the meeting.

```
<config>
<services><calls>
       <escalate-to-webex-meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	true, false	Set to “true” to enable the Escalate to Webex Meeting menu option.

6.2.5 Desk Phone Control Calling – Auto Answer

Auto answer enables the user to use Desk Phone Control (DPC) for outgoing calls on the client to manage MPP phones with zero touch answer.

The selected MPP phone will carry the audio/video for the outgoing DPC call.

Auto answer can work on the primary and non-primary provisioned devices. If the user has more than one registered desk phone that can be paired with, only the selected/paired device shall auto-answer.

```
<config>
<services><calls>
<deskphone-control auto-answer="%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	true	true, false	When set to “true”, enables desk phone control auto answer.

NOTE: Auto answer will not affect incoming calls while in DPC mode, so that the desk phone rings for incoming calls.

Cisco Confidential

6.2.6 Auto Answer with Tone Notification

This feature enables automatic incoming call answer support for local devices, if this is indicated in the incoming call request.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_AUTO_ANSWER_WXT%	false	true, false	When set to “true”, enables automatic incoming call answer if this is requested from the backend.

6.2.7 Desk Phone Control – Mid Call Controls – Conference

This feature enables Conference and Merge options for remote (XSI) calls, terminated on another location.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_XSI_CONFERENCE_CALLS_WXT%	false	true, false	When set to “true”, enables Conference and Merge options for remote (XSI) calls, terminated on another location.

6.2.8 Call Pickup Notifications

Call pickup notifications provide the ability for the user to know when there is an incoming call to a user he is configured to monitor. Call pickup notifications can be received for watchlists configured through the Call Pickup group and Busy Lamp Field services.

Call Pickup notifications are useful when the monitored users are not physically close to each other and cannot hear the ringing of their colleague's phone.

6.2.8.1 Busy Lamp Field

The desktop Webex application displays a notification if a member in their Busy Lamp Field (BLF) watchlist has an incoming call in alerting state. The notification has information about the caller and the user that received the incoming call, with the options to pick up the call, silence or ignore the notification. Answering the incoming call by the user initiates directed call pickup.

Starting with Release 43.4, the list of BLF-monitored users is available in the Multi Call Window (MCW) for Calling (available only for Windows). Integration of the BLF list in the MCW includes:

Monitor the incoming calls with option to pick-up the call or ignore the alert.

See the full list of the BLF users.

Monitor the presence of the users – rich presence is available only for the users with Webex Cloud entitlement. Basic (telephony) presence is available only for the BroadWorks-only users.

Start a call with a BLF user.

Start a chat with a BLF user – available only for users with Webex Cloud entitlement.

Add a BLF user as a contact.

```
<config>
```


Cisco Confidential

```
<services>
  <calls>
    <busy-lamp-field enabled="%ENABLE_BUSY_LAMP_FIELD_WXT%">
      <display-caller enabled="%ENABLE_BLF_DISPLAY_CALLER_WXT%"/>
      <notification-delay time="%BLF_NOTIFICATION_DELAY_TIME_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_BUSY_LAMP_FIELD_WXT%	false	true, false	Enables the Busy Lamp Field monitoring and ringing notification for other users with ability to pick up the calls.
%ENABLE_BLF_DISPLAY_CALLER_WXT%	true	true, false	Enables displaying the caller display name/number in the ringing notification.
%BLF_NOTIFICATION_DELAY_TIME_WXT%	0	0-60	Controls how many seconds the ringing notification should be delayed before it is displayed to the user.

NOTE: This feature depends on the Directed Call Pickup service.

6.2.8.2 Call Pickup Group (Webex Calling only)

Starting with Release 44.2, Webex application adds support for Group Call Pickup (GCP) Notifications for the Webex Calling deployment. It allows users to be notified for incoming calls for any of the users monitored through the Call Pickup group.

In case of an incoming call for a user part of a Call Pickup group, it is given a chance the callee to answer the call. There is a GCP notification delay configurable through Control Hub. If the callee does not process the call within the configured time, a GCP notification is sent to the group.

In the event of multiple calls within the same Call Pickup group, they are processed sequentially based on the time they are received. The notification of the oldest call is initially delivered to the group and once it is processed, the next notification in line is delivered to the group.

Notifications may be audio-only, visual-only or audio and visual depending on the configuration in the Control Hub admin portal. If there is a visual GCP notification, user can pick up the call using the Call Pickup feature. If audio only notification is configured, user will not see a visual notification for the incoming call, will hear a specific ringtone and he can pick up the call from the Call pick up menu available in the Webex app, or by dialing the FAC code (*98) and the extension manually.

User can mute the GCP notification through the application settings. This setting applies to all the Call Pickup notifications (BLF and GCP) and by default notifications are muted.

The feature works for the primary lines, and for shared or virtual lines assigned to the user.

Cisco Confidential

```
<config>
<services><calls>
    <group-call-pickup-notifications enabled="%ENABLE_GCP_NOTIFICATIONS_WXT%">
        <display-caller enabled="%ENABLE_GCP_DISPLAY_CALLER_WXT%"/>
        <max-timeout value="%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%"/>
    </group-call-pickup-notifications>
...
<protocols><sip>
    <lines>
        <line>
            <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-1%</group-call-pickup>
            ...
        </line>
        <line>
            <group-call-pickup>%BWGROUP-CALL-PICKUP-BOOL-2%</group-call-pickup>
            ...
        </line>
        ...
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_GCP_NOTIFICATIONS_WXT%	false	true, false	Enables the Group Call Pickup Notifications
%ENABLE_GCP_DISPLAY_CALLER_WXT%	true	true, false	Enables displaying the caller display name/number in the ringing notification
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	120	5-120	Defines the maximum time a GCP notification is available for the user
%BWGROUP-CALL-PICKUP-BOOL-n%	false	true, false	Indicates if corresponding line has Call Pickup Group configured

NOTE 1: This is a Webex Calling only feature.

NOTE 2: This feature depends on the Call Pickup group being configured for the user.

6.2.9 Remote Control Event Package

For Click to Dial clients like the BroadWorks Receptionist thin client and Go integrator where the Webex app is the calling device, when receiving a call or handling hold/resume the Webex app now honors the remote control event package.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_REMOTE_CONTROL_EVENTS_WXT%	false	true, false	When set to “true”, specifies that the remote control should be enabled for the user.

Cisco Confidential

6.2.10 Survivability Gateway (Webex Calling only)

Starting with Release 43.2, Webex application adds support for Survivability call mode. if the feature is enabled and there is no Webex Cloud connectivity, the Webex application can run in survivability mode. In this mode there is limited calling functionality available for the user.

Local Survivability Gateway is deployed by the customer.

```
<config>
<protocols>
<sip>
<survivability-gateway enabled="%ENABLE_SURVIVABILITY_GATEWAY_WXT%" fallback-
time="%SURVIVABILITY_FALLBACK_TIME_WXT%">%BWSURVIVABILITYGATEWAY%</survivability-
gateway>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_SURVIVABILITY_GATEWAY_WXT%	false	true, false	Enables the survivability mode support.
%SURVIVABILITY_FALLBACK_TIME_WXT%	30	>=30	Specifies the fallback time (survivability gateway to SSE)

NOTE: This feature provides confidence in migration from On-premises to Cloud calling solutions.

6.2.11 Remote Mute Control Event Package (Webex Calling only)

Starting with Release 43.9, the Webex app adds support for remote mute call control of the audio media stream. This allows mute/unmute of an ongoing call to be triggered from another location like BroadWorks Receptionist thin client, where the Webex app is the calling device.

The feature depends on the new SIP *x-cisco-mute-status* info package. If the *Recv-Info:x-cisco-mute-status* header is received during the call SIP INVITE session establishment, then whenever there is an update (local or remote) to the mute state of the audio call session, the Webex app sends back SIP INFO with the *Info-Package:x-cisco-mute-status;muted=true* (or *muted=false*), where the muted parameter represents the updated state of the audio media stream.

Mute or unmute can be triggered locally or from a remote location. Remote update triggers a SIP NOTIFY with *Event: mute* (or *unmute*) to be sent to the Webex app from the Application Server. The Webex app honors the remote request and after the update of the audio media stream state, sends back a SIP NOTIFY with the *Info-Package:x-cisco-mute-status;muted=true* (or *muted=false*).

```
<config>
<services>
   <calls>
       <remote-mute-control enabled="%ENABLE_REMOTE_MUTE_CONTROL_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_REMOTE_MUTE_CONTROL_WXT%	false	true, false	When set to “true”, the remote mute call control is enabled for the user.

6.2.12 Move Call

Webex app provides call monitoring and call control of VoIP calls terminated on another location. This is currently available only for the primary line of the user.

Starting with Release 43.12, the Webex app is enhanced to show calls terminated on another location also for the shared and virtual lines. Such calls are visible in the ongoing calls area for information purposes and without the option to control them. Only if such a call is placed on hold, user will be able to move it to the local device by selecting it and resume it from the call screen. This mechanism is useful if the call was handled by the same user on another location or by another user using the same line.

Note that it is not possible the Webex app to move a held call to a paired device. If the user is paired with a device, he needs to disconnect first and then he can resume the held call locally.

Call monitoring for shared and virtual line depends on the SIP call-info event package.

The monitoring of the calls for the primary line of the user depends on the XSI events (Advanced Call event package) and moving a call to the local device is not available for these calls. For this type of calls, user can use the Call Pull (*6.1.22 Call Pull*) feature. Call pull works only for the last active calls of the user, while the mechanism for shared and virtual lines works for all the calls of the user that are placed on hold.

- Use case 1:
    a. Alice has Bob’s line assigned for the Desktop and Desk phone profiles.
    b. Alice has a call with Charlie through the Desk phone – Alice can see the ongoing call in the Desktop app.
    c. Alice places the call on hold form the Desk phone – the call can be resumed by Alice from the Desktop app.
- Use case 2:
    a. Alice has Bob’s line assigned for the Desktop and Desk phone profiles.
    b. Bob has a call with Charlie – Alice can see the ongoing call in the Desktop app.
    c. Bob places the call with Charlie on hold – Alice can resume the call with Charlie from the Desktop app.
- Use case 3:
    a. Alice has Bob’s line assigned for the Desktop and Desk phone profiles.
    b. Alice is paired with his Desk phone from the Desktop app.
    c. Bob has a call with Charlie – Alice can see the ongoing call in the Desktop app.
    d. Bob places the call with Charlie on hold – Alice can not resume the call with Charlie from the Desktop app.

Cisco Confidential

e. Alice disconnects the Desktop app from the Desk phone – Alice can resume the call with Charlie from the Desktop app.

```
<config>
<services><calls>
    <call-move>
         <move-here enabled="%ENABLE_CALL_MOVE_HERE_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALL_MOVE_HERE_WXT%	false	true, false	Enables call move on local device. Used for hold/resume across locations/users in the multi-line use-case.

Cisco Confidential

6.3 Mobile Only Features

6.3.1 Emergency Calling

Webex for Cisco BroadWorks supports Native Emergency Calling.

When the feature is enabled, at initiating an outgoing VoIP call, the application analyzes the dialed number and compares it against the list of emergency numbers configured. If the number is identified as an emergency one, the application executes the configured dial behavior. It is configurable using the *dial-sequence* tag.

Supported modes are:

- cs-only – The client places emergency calls only through the cellular network if the network is available.
- cs-first – Upon initiating an emergency call, the client checks the network type to which the current device is connected. If the cellular network is available, the client places that call over the cellular network. If the cellular network is not available but a cellular data/WiFi network is available, the client places the call over the cellular data/WiFi network as a VoIP call. Also, if the emergency call is placed through the cellular network, the client suggests to the user to retry the emergency call as VoIP.
- voip-only – The client places emergency calls only as VoIP if the cellular data/WiFi network is available.
- cs-voip – The client analyzes if the device can initiate it as native circuit-switched (CS) call (without taking into account if the CS network is available or not). If the device can start a native call, the emergency number is dialed as an emergency CS call. Otherwise, the call is dialed as VoIP.

> **NOTE**: If VOIP calling is disabled, the only meaningful value for emergency dial sequence (%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%) is cs-only.

There is an emergency calls disclaimer message displayed to the user at sign in. It is not controlled through the configuration options.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_EMERGENCY_DIALING_WXT%	false	true, false	Set to “true” to enable emergency calls detection. The default value is empty.
%EMERGENCY_CALL_DIAL_SEQUENCE_WXT%	cs-only	cs-only, cs-first, voip-only, cs-voip	Controls the dial-sequence mode for emergency calls.
%EMERGENCY_DIALING_NUMBERS_WXT%	“911,112”	CSV list	CSV list of emergency numbers. Example: 911,112

Cisco Confidential

6.3.2 Push Notifications for Calls

When an incoming call is received, the mobile client receives a push notification (PN) first. There is a config parameter that can be used to control when the SIP REGISTER session to be established:

1. When the push notification is received, OR
2. When the call is accepted by the user.

The second approach is recommended. However, compared to first case, it adds some delay before the call is established.

According to the iOS 13 requirements, the VoIP PNs should be used only for incoming calls. The rest of the call-related events should use regular PNs.

To meet this requirement, new PN registration API is introduced and it requires corresponding patch to be applied on the Application Server. If the backend is not configured to support the iOS 13 PNs, the configuration parameter can be used to enforce usage of the legacy push notifications, where all the call related events are delivered through VoIP PNs.

There is a Push Notification sent by the Application Server (AS) when a ringing call is accepted by the callee on another location, closed by the caller, or, for example, redirected to Voicemail. With the iOS 13, this type of Push Notification is now a regular one and it has some restrictions. It may be delayed by the Apple Push Notification Service (APNS) or even not delivered at all. To handle missing or delayed Call Update PNs, a configurable ringing timeout is added to control the maximum ringing time. If the maximum ringing time is reached, the ringing is stopped for the callee and the call is treated as missed. On the caller side, the call may remain in ringing state until the ring-no-answer policy configured on the Application Server (AS) is executed.

To keep the application behavior consistent, the configurable ringing timer applies to both Android and iOS.

A separate configuration option is added to specify the call decline behavior when an incoming call is received as a Push Notification. The client can be configured to ignore the call or to respond to the server through XSI with decline set to “true” or “false”, in which case, the assigned Cisco BroadWorks call treatment services will be applied. If “decline_false” is configured, the call continues ringing until the originator abandons or the no-answer timer expires, and the associated call treatment services start. If “decline_true” is configured, the decline reason specifies the call processing. If the decline reason is set to “busy”, the server immediately forces the busy treatment service. If “temp_unavailable” is configured, the temporary unavailable treatment service is applied.

```
<config>
<services>
    <push-notifications-for-calls enabled="true"
    connect-sip-on-accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%"
    ring-timeout-seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%"/>
    <calls>
        <reject-with-xsi mode="%REJECT_WITH_XSI_MODE_WXT%"
        declineReason="%REJECT_WITH_XSI_DECLINE_REASON_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	false	true, false	Controls when the SIP REGSITER session is established – upon receiving a Push Notification for incoming call or upon accepting it.
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	35	[0-180]	Controls the maximum incoming call ringing time for calls received through PN. If no CallUpd PN is received within the given period, the call will be treated as missed.
%REJECT_WITH_XSI_MODE_WXT%	decline_false	ignore, decline_true, decline_false	Specifies the call decline behavior.
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	busy	busy, temp_unavailable	Specifies the call decline reason, if the reject mode is set to “decline_true”.

6.3.2.1 MWI

With the MWI feature enabled, the Mobile Webex client subscribes for the MWI Push Notification to receive updates with the voicemail of the user and notify him.

To reduce the number of notifications and to avoid unnecessary distraction, the MWI Push Notifications are suppressed in some cases. For instance, when the user is listening to the Voicemail messages or is marking them as read from within the Mobile Webex client (unread number is decreasing). There is no configurable option to control this.

For more information about MWI, check section *6.1.27 Voicemail, Visual Voicemail, Message Waiting Indicator*.

6.3.2.2 Ring Splash

BroadWorks services (like DND) can send ring reminders when incoming is redirected. The Webex Mobile client can be configured to enable the Ring Splash Push Notifications and present them to the user when they are triggered by the BroadWorks.

```
config>
<services>
<ring-splash enabled="%ENABLE_RING_SPLASH_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_RING_SPLASH_WXT%	false	true, false	Enables Ring Splash in the BroadWorks config.

6.3.2.3 Delivery Mode (Webex Calling only)

The Webex app utilizes the Notification Push Server (NPS) to deliver the push notifications for calls to APNS/FCM. Release 45.2 of the Webex app now supports three different delivery modes to configure how the call-related push notifications should be delivered to APNS/FCM:

- nps - current mechanism, using the NPS
- cloud - enhanced mechanism, using Cisco Webex Cloud microservice

Cisco Confidential

- external - a mechanism that uses third-party system. It requires integration of the third-party system with the Cisco WebHooks engine

```
<config>
<services><calls>
<push-notifications-for-calls enabled="true"
      connect-sip-on-accept="%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%"
      ring-timeout-seconds="%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%"
      delivery-mode="%PN_FOR_CALLS_DELIVERY_MODE_WXT%">
```

Tag	Default if Omitted	Supported Values	Description
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	nps	nps, cloud, external	Specifies delivery mode of the push notifications for calls.

6.3.3 Single Alerting

The Mobile Single Alert feature is intended for fixed-mobile convergence (FMC) / Mobile Network Operator (MNO) deployments leveraging the BroadWorks Mobility service. Without it, when logged into the Webex client and receiving an incoming call, the user will receive concurrently two calls – a native one and a Push Notification (VoIP) call. When the feature is enabled, the application will disable Mobility alerting on the user's BroadWorks Mobility location when logging in and enable the alerting when logging out. An important precondition for using this feature is for the user to have the BroadWorks Mobility service assigned and exactly one location configured.

```
<config>
<services><calls>
<single-alerting enabled="%ENABLE_SINGLE_ALERTING_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_SINGLE_ALERTING_WXT%	false	true, false	Set to “true” to enable Single Alerting.

6.3.4 Click to Dial (Call Back)

The outbound Click to Dial ensures that the end user can have a call on their personal Circuit Switched mobile phone and deliver their business DN as the calling line ID.

The Mobile Webex client supports Click to Dial (Call Back) calls using the BroadWorks Anywhere service. The BroadWorks Anywhere locations in the Webex application are called Single Number Reach (SNR) locations.

When the feature is enabled, users can select the SNR location from the device pairing menu. When paired with SNR location, all outgoing calls are initiated using Click to Dial (Call Back) calls. To prevent double alerting, Push Notifications for incoming calls are disabled.

When a user initiates a Click to Dial call, they will see the outgoing call screen with information to expect incoming call on the selected SNR location. This screen is closed automatically based on configurable timer.

Cisco Confidential

At disconnecting from an SNR location, the application registers again for Push Notifications for incoming calls.

```
<config>
<services>
  <dialing>
    <call-back enabled="%ENABLE_DIALING_CALL_BACK_WXT%"
timer="%DIALING_CALL_BACK_TIMER_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_DIALING_CALL_BACK_WXT%	false	true, false	Set to “true” to enable Click to Dial (Call Back) calls.
%DIALING_CALL_BACK_TIMER_WXT%	10	[3-20]	Controls the number of seconds before the Call Back screen is automatically closed.

6.3.5 MNO Support

6.3.5.1 Call with Native Dialer

This feature adds support for Mobile Network Operator (MNO) deployments leveraging the BroadWorks Mobility (BWM) service. It is assumed that the user has the BroadWorks Mobility service assigned to them and has at least one location configured.

The user’s ability to initiate calls through the native dialer is controlled by the **native** configuration tag. If enabled, the application will launch the native dialer and make the call. Furthermore, the availability of VoIP calling is controlled by the **voip** tag – based on the deployment requirements VoIP calls may be enabled or disabled.

If VoIP and Native calling are enabled, the user will be able to choose which option to use.

The <dialing-mode> tag controls if users can select how incoming and outgoing calls are to be started/received. Requires both the native and VoIP calling to be enabled.

Starting with Release 43.12, native dialing configuration is extended, providing the ability a custom prefix to be pre-pended to the outgoing call number. This applies to the cellular calls initiated from the Webex app, only if the number dialed starts with a FAC code.

This feature is helpful for customers using MNO deployments, where calls instead of being redirected to the integrated Cisco BroadWorks Application Server, the FAC codes may be handled by the Telecom backend. New <fac-prefix> tag is added under section <dialing><native> and the Telecoms can use it to resolve this problem.

```
<config>
<services>
  <dialing>
    <voip enabled="%ENABLE_DIALING_VOIP_WXT%"/>
    <native enabled="%ENABLE_DIALING_NATIVE_WXT%" enable-bwks-mobility-
dependency="%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%">
      <fac-prefix value="%DIALING_NATIVE_FAC_PREFIX_WXT%"/>
    </native>
    <dialing-mode enabled="%ENABLE_DIALING_MODE_WXT%" default="%DIALING_MODE_DEFAULT_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_DIALING_VOIP_WXT%	true	true, false	Set to “true” to enable VoIP call option.
%ENABLE_DIALING_NATIVE_WXT%	false	true, false	Set to “true” to enable Native call option.
%ENABLE_DIALING_MODE_WXT%	false	true, false	Enables the calling mode selection by the user, through the Call Settings in Preferences.
%DIALING_MODE_DEFAULT_WXT%	voip	voip, native	Specifies the default calling mode selected.
%DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT%	false	true, false	Controls whether the availability of the Native calling should depend on the BroadWorks Mobility service assignment and Mobility Location being configured for the user.
%DIALING_NATIVE_FAC_PREFIX_WXT%	*empty*	string	Specifies a prefix that should be prepended, if outgoing call to a number starting with a FAC code is initiated as a cellular call. By default, no FAC prefix is defined and the tag is empty.

NOTE 1: At least one of the **voip** and **native** calling should be enabled.

NOTE 2: If just the **native** calling is enabled, in MNO deployments, it is recommended to disable the single-alerting to prevent the client from disabling the BWM alerting.

NOTE 3: If both **native** and **voip** callings are enabled, in MNO deployments, it is recommended to enable the single-alerting to prevent double alerting.

6.3.5.2 Mid-Call Controls

This feature allows the Mobile Webex client to control via XSI native calls on the mobile device that are anchored on Cisco BroadWorks. The XSI Call Controls is available only if:

- BroadWorks Mobility (BWM) service is assigned to the user,
- There is just a single BMW Mobile Identity configured,
- Native calling mode is selected by the user (for more information check section *6.3.5.1 Call with Native Dialer),*
- There is a call anchored on BroadWorks, going through the BMW service,
- There is ongoing cellular call on the mobile device.

Cisco Confidential

Release 43.10 adds better handling of the consultative transfer, creating association between the two cellular calls presented in the Webex app and providing an option for the user to complete the transfer. Also, if user has two independent cellular calls on the same device, the transfer menu is enhanced to allow transferring one to the other even if there is no association created between them.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_XSI_CALL_CONTROL_WXT%	false	true, false	Enables XSI call control for MNO environment.
%XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT%	MNO_Access	MNO_Access, MNO_Network	Controls the XSI MNO deployment type used by the application. The possible values are: ▪ MNO_Access – shows all remote (XSI) calls with the device types defined in the node below. ▪ MNO_Network - shows all remote (XSI) calls.
%DEPLOYMENT_DEVICE_TYPE_1_WXT%, %DEPLOYMENT_DEVICE_TYPE_2_WXT%, %DEPLOYMENT_DEVICE_TYPE_3_WXT%	“”	string	The device type name(s) that should be used in the MNO_Access deployment type.
%ENABLE_XSI_HOLD_CALLS_WXT%	true	true, false	Controls if the Call Hold action should be available for the user for XSI mobile calls.

6.3.5.3 Outgoing Calling Line Identity (CLID) – Dual Persona

With Mobile Release 42.12, the Webex app allows users to select their Calling Line Identity (CLID) presented to the remote party upon initiating an outgoing call.

If user is configured with Cisco BroadWorks Mobility, typical configuration for Mobile Network Operator (MNO) deployments, and Native calling is enabled, user can select which identity to be presented to the people they are calling. User can choose their business or personal identity. There is also an option to hide own identity and the call to be presented as Anonymous.

```
<config>
<services><calls>
   <caller-id>
      <outgoing-calls enabled="%ENABLE_CLID_OUTGOING_CALLS_WXT%">
         <mobility enabled="%ENABLE_CLID_OUTGOING_CALLS_MOBILITY_WXT%"/>
```


Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CLID_OUTGOING_CALLS_MOBILITY_WXT%	false	true, false	Enables the personal management for Native calls when the deployment type configured as MNO_Access or MNO_Network. (BroadWorks Mobility is used for the native calls and all the native calls are anchored on BroadWorks)

6.3.5.4 Notification for Native Calls

For users deployed with MNO, this feature adds a notification banner for native calls, which can be controlled through the Webex app. This notification relies on push notification, send by the Application Server once the call is established.

Tag	Default if Omitted	Supported Values	Description
%ENABLE_PN_MOBILE_CALL_INFO_WXT%	true	true, false	Enables the subscription for the MOBILE_CALL_INFO push notification.

6.3.5.5 Move Native Call to Converged Meeting

For users deployed with MNO, this feature allows for a native voice call to be escalated to a meeting for both parties of a 1:1 call (even if the other party is not a Webex user). If the remote user is a Webex user, once in a meeting, the parties will have the ability to:

- Initiate Webex in Meeting Chat
- Add Video (note that audio will continue in the native call)
- Share screen / content
- Trigger Meetings recording

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	false	true, false	Enables Power Up (Invite and Meet, Video Meet actions).

6.3.5.6 MNO Mobility - In-call Widget

Release 43.7 of the Android Webex app (Mobile and Tablet) officially introduces a new call control widget (bubble), providing additional call control for native calls anchored on Cisco BroadWorks, using the Mobility service. The widget will be displayed on top of the Native UI and will allow the user the following actions:

- Hold/Resume

Cisco Confidential

- Blind/Consultative Transfer– places the user in the transfer dialog in the Webex app.
- Complete Transfer – provides the option to complete consultative transfer (Release 43.10)
- Video Meeting – moves the parties into a Webex Meeting.
- End call

```
<config>
<services><calls>
       <hold xsi-enabled="%ENABLE_XSI_HOLD_CALLS_WXT%" widget-
enabled="%ENABLE_WIDGET_HOLD_CALLS_WXT%"/>
       <transfer-call enabled="%ENABLE_TRANSFER_CALLS_WXT%" xsi-
enabled="%ENABLE_XSI_TRANSFER_CALLS_WXT%" widget-
enabled="%ENABLE_WIDGET_TRANSFER_CALLS_WXT%" type="%TRANSFER_CALL_TYPE_WXT%"/>
       <escalate-to-webex-meeting
enabled="%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%" widget-
enabled="%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%"/>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_WIDGET_HOLD_CALLS_WXT%	true	true, false	Controls the availability of the Hold action in the Call Widget.
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	true	true, false	Controls the availability of the Transfer and Complete Transfer actions in the Call Widget.
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	true	true, false	Controls the availability of the Video Meeting action in the Call Widget.

6.3.6 Incoming Caller ID

Release 44.2 adds the ability to control the contact information presented to the user based on the name and number. There are two configuration options added to control the information presented to the user in the incoming call screen and incoming call notification, and the missed call notifications.

6.3.6.1 Incoming Call Screen

There are platform differences between Android and iOS when it comes to displaying data in the incoming call screen. Native experience displaying information for incoming call is as follows:

Android - there are two separate fields in the incoming call screen to show both the name and number

iOS - there is only one field to show either the name or the number - if both are available, the name takes priority

Cisco Confidential

The new config option for the incoming calls can be used to make sure that the iOS Webex app will show the number in the call screen next to the name (format: *Name (Number)*). Android Webex app behavior is not affected.

6.3.6.2 Incoming Call Notification

In some cases, the incoming call is presented to the user as a notification. Due to the limited space, the number is not always displayed there.

The new config option for the incoming calls controls also the information displayed in the incoming call notifications. If enabled and both the name and the number are available, the Webex app will append the number next to the name (format: *Name (Number)*). This is behavior of the Webex app is applicable to both Android and iOS.

6.3.6.3 Missed Call Notification

There is an additional configuration parameter added for the missed call notifications. It can be used to control the remote party information, similar to the incoming call notifications, allowing the number to be appended to the display name of the remote user and presented in the missed call notification. This is behavior of the Webex app is applicable to both Android and iOS.

```
<config>
<services><calls>
   <caller-id>
      <incoming-calls>
         <append-number enabled="%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%"/>
      </incoming-calls>
      <missed-calls>
         <append-number enabled="%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%"/>
      </missed-calls>
```

Tag	Default if Omitted	Supported Values	Description
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	false	true, false	Controls whether the number should be appended to the name in the incoming call screen (iOS only) and notifications.
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	false	true, false	Controls whether the number should be appended to the name in the missed call notification.

NOTE: If the number is delivered as a display name or the display name ends with the number, the Webex app will avoid duplication and will show the number just once.

Cisco Confidential

7 Early Field Trial (BETA) Features

7.1 Emergency (911) Calling - Cisco Emergency Location Information Service (Webex Calling only) and Configuration Cleanup

The Webex app already supports Emergency location for Emergency calls, using third-party providers, as documented in *6.1.37 Emergency (911) Calling - Location Reporting with E911 Provider*. The feature is applicable to emergency calls to the Public Safety Answering Points (PSAPs) around the US, its territories (Guam, Puerto Rico, and Virgin Islands), and Canada only.

For the Webex Calling deployment exclusively, Cisco has added own Emergency Location Information Service to handle and store HELD/HELD+ interactions, maintain company and user-created wire maps, store addresses with their PIDF-LO attributes and send the location information for the emergency calls.

Release 45.10 of the Webex app adds integration with the Cisco emergency location service. The DMS config template is updated up, to add support for different emergency location providers:

- The current <*redsky*> section under <*emergency-dialing*> of the DMS config template is deprecated. A new section <*emergency-location*> is added instead and will be used by the Webex app going forward.
- A new *provider* option is now available in the new section, allowing for the control of the Emergency Location provider that the Webex app should utilize. The available options include *redsky*, *intrado*, *9line*, and *webex*. The first three options are available for the Webex for BroadWorks deployment, and are primarily employed for tracking purposes, utilizing the HELD+ protocol for communication with third-party providers. The *webex* option is available only for the Webex calling deployment and permits the app to utilize the Cisco Emergency Location Information Service, featuring enhanced wire map and PIDF-LO support for emergency calls.
- There are new custom tags added which require their manual setup, to match the current configuration (if the feature is already in use). Without being set, the default values will be used, which may disable the feature or change the behavior
- There are no updates in the system tags used for <held-url>, <held-org-id>, <secret> and <number-list>.
- [**Important**] To prevent the emergency location feature from being disabled due to misconfiguration, ensure that the new custom tag controlling the availability of the Emergency location feature (%ENABLE_EMERGENCY_LOCATION_WXT%) is set in the same manner as the legacy tag (%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%).
- [**Important**] To avoid losing this critical functionality because of misconfiguration, the Webex app has a backwards compatibility logic added. If the new configuration section <*emergency-location*> is missing in the template or if the new custom tag (%ENABLE_EMERGENCY_LOCATION_WXT%) is not configured, resulting in *enabled* attribute to be set to "false", the Webex app will try to read the legacy configuration section (<*redsky*>) and apply its values.

Cisco Confidential

- If the feature is disabled, the emergency calls will be routed for triage by the ERC (Emergency Relay Center) to validate the caller's location before routing to an appropriate PSAP, which may lead to additional charges.

The following snippet displays the changes in the DMS config template:

```
<config><services>
<emergency-dialing enabled="%ENABLE_EMERGENCY_DIALING_WXT%">
   <redsky enabled="%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%">  <!-- DEPRECATED by <emergency-
location> -->
      <held-url>%BWE911-PRIMARY-HELDURL%</held-url>
      <held-org-id>%BWE911-CUSTOMERID%</held-org-id>
      <secret>%BWE911-SECRETKEY%</secret>
      <number-list>%BWE911-EMERGENCY-NUMBER-LIST%</number-list>
      <user-reminder-timeout>%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%</user-reminder-
timeout>
      <user-mandatory-location>%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%</user-
mandatory-location>
      <user-location-prompting>%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%</user-location-
prompting>
   </redsky>
   <emergency-location enabled="%ENABLE_EMERGENCY_LOCATION_WXT%"
                       provider="%EMERGENCY_LOCATION_PROVIDER_NAME_WXT%">
      <held-url>%BWE911-PRIMARY-HELDURL%</held-url>
      <held-org-id>%BWE911-CUSTOMERID%</held-org-id>
      <secret>%BWE911-SECRETKEY%</secret>
      <number-list>%BWE911-EMERGENCY-NUMBER-LIST%</number-list>
      <user-reminder-timeout>%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%</user-reminder-
timeout>
      <user-mandatory-location>%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%</user-
mandatory-location>
      <user-location-prompting>%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%</user-
location-prompting>
   </emergency-location>
</emergency-dialing>
```

The following table lists the mapping between the new and the legacy custom tags:

Config option	Deprecated custom tag	New custom tag
The *enabled* attribute in the <emergency-location> tag vs. the same in the legacy <redsky> tag	%EMERGENCY_DIALING_ENABLE_REDSKY_WXT%	%ENABLE_EMERGENCY_LOCATION_WXT%
Tag <user-reminder-timeout>	%EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT%	%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%
Tag <user-mandatory-location>	%EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT%	%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%
Tag <user-location-prompting>	%EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%	%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%ENABLE_EMERGENCY_LOCATION_WXT%	false	true, false	Enables the Emergency Location Platform usage.
%EMERGENCY_LOCATION_PROVIDER_NAME_WXT%	redsky	redsky, intrado, 9line, webex	Specifies what Emergency Location Provider should be used. “webex" is applicable solely to the Webex Calling deployment and should be configured to utilize the Cisco Emergency Location Information Service.
%BWE911-PRIMARY-HELDURL%	empty	string	Specifies the URL to the E911 provider supporting the HELD protocol.
%BWE911-CUSTOMERID%	empty	string	The customer ID (HeldOrgId, CompanyID) used for the E911 provider HTTPS request.
%BWE911-SECRETKEY%	empty	string	The secret to authenticate the E911 provider HTTPS request. Not used (empty) with “webex” as E911 provider
%BWE911-EMERGENCY-NUMBER-LIST%	empty	CSV string	The list of emergency numbers supported by E911 provider.
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	0 (user will not be prompted again)	number [0 - 43200]	The timeout in minutes that will be used to remind the user to update the emergency location if the current one is not entered or is invalid. The suggested value if decided to enable: 1440 (one day).
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	-1 (user can cancel the dialog always)	number [-1 - 100]	The times that the user is allowed to close the location dialog before location becomes mandatory (that is, they cannot close the location window). Possible values: ▪ N = -1 (user can cancel the dialog always) ▪ N = 0 (user is not allowed to cancel the dialog - mandatory location always) N > 0 (user is allowed to cancel the dialog N times before it becomes mandatory)

Cisco Confidential

Tag	Default if Omitted	Supported Values	Description
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	once_per_login	aggressive, once_per_login	▪ Defines the E911 location prompting behavior. The “aggressive” value will show the dialog to the user on each network change to an unknown location, while the “once_per_login” value will show the dialog only once, preventing further popup and distractions for the user.

Cisco Confidential

8 Custom Tags Mapping between Webex for Cisco BroadWorks and UC-One

The following table lists the Webex for Cisco BroadWorks custom tags, matching their legacy custom tags for UC-One.

Webex for Cisco BroadWorks Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENABLE_REJECT_WITH_486_WXT%	%ENABLE_REJECT_WITH_486_DESKTOP%	%ENABLE_REJECT_WITH_486_MOBILE%
%REJECT_WITH_XSI_MODE_WXT%	N/A	%REJECT_WITH_XSI_MODE_MOBILE%
%REJECT_WITH_XSI_DECLINE_REASON_WXT%	N/A	%REJECT_WITH_XSI_DECLINE_REASON_MOBILE%
%ENABLE_TRANSFER_CALLS_WXT%	%ENABLE_TRANSFER_CALLS%	%ENABLE_TRANSFER_CALLS_MOBILE%
%ENABLE_CONFERENCE_CALLS_WXT%	N/A	%ENABLE_CONFERENCE_CALLS_MOBILE%
%ENABLE_NWAY_PARTICIPANT_LIST_WXT%	%ENABLE_NWAY_PARTICIPANT_LIST_DESKTOP%	N/A
%MAX_CONF_PARTIES_WXT%	%MAX_CONF_PARTIES%	N/A
%ENABLE_CALL_STATISTICS_WXT%	N/A	N/A
%ENABLE_CALL_PULL_WXT%	%ENABLE_CALL_PULL_DESKTOP%	%ENABLE_CALL_PULL_MOBILE%
%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT%	N/A	%PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%ENABLE_MWI_WXT%	%DESKTOP_MWI_ENABLE%	%ENABLE_MWI_MOBILE%
%MWI_MODE_WXT%	%DESKTOP_MWI_MODE%	%MWI_MODE_MOBILE%
%ENABLE_VOICE_MAIL_WXT%	N/A	N/A
%ENABLE_VISUAL_VOICE_MAIL_WXT%	%ENABLE_VISUAL_VOICE_MAIL%	N/A
%ENABLE_FORCED_LOGOUT_WXT%	%ENABLE_FORCED_LOGOUT%	N/A
%FORCED_LOGOUT_APPID_WXT%	%FORCED_LOGOUT_APPID%	N/A
%ENABLE_CALL_FORWARDING_ALWAYS_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_WXT%	N/A	N/A

Cisco Confidential

Webex for Cisco BroadWorks Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENBLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%	N/A	N/A
%ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%	N/A	N/A
%BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%	N/A	N/A
%ENABLE_EMERGENCY_DIALING_WXT%	N/A	N/A
%EMERGENCY_DIALING_NUMBERS_WXT%	N/A	N/A
%ENABLE_USE_RPORT_WXT%	%USE_RPORT_IP%	%ENABLE_USE_RPORT_MOBILE%
%RPORT_USE_LOCAL_PORT_WXT%	N/A	%RPORT_USE_LOCAL_PORT_MOBILE%
%USE_TLS_WXT%	%USE_TLS%	N/A
%SBC_ADDRESS_WXT%	%SBC_ADDRESS%	%SBC_ADDRESS%
%SBC_PORT_WXT%	%SBC_PORT%	%SBC_PORT%
%USE_PROXY_DISCOVERY_WXT%	%USE_PROXY_DISCOVERY%	%USE_PROXY_DISCOVERY_MOBILE%
%USE_TCP_FROM_DNS_WXT%	%USE_TCP_FROM_DNS%	N/A
%USE_UDP_FROM_DNS_WXT%	%USE_UDP_FROM_DNS%	N/A

Cisco Confidential

Webex for Cisco BroadWorks Tag	Desktop Legacy Tag	Mobile Legacy Tag
%USE_TLS_FROM_DNS_WXT%	%USE_TLS_FROM_DNS%	N/A
%DOMAIN_OVERRIDE_WXT%	%DOMAIN_OVERRIDE%	%DOMAIN_OVERRIDE%
%SOURCE_PORT_WXT%	%SOURCE_PORT%	%SOURCE_PORT%
%USE_ALTERNATIVE_IDENTITIES_WXT%	%USE_ALTERNATIVE_IDENTITIES%	N/A
%TCP_SIZE_THRESHOLD_WXT%	%TCP_SIZE_THRESHOLD%	N/A
%SIP_REFRESH_ON_TTL_WXT%	%SIP_REFRESH_ON_TTL%	N/A
%ENABLE_SIP_UPDATE_SUPPORT_WXT%	%ENABLE_SIP_UPDATE_SUPPORT_DESKTOP%	%ENABLE_SIP_UPDATE_SUPPORT_MOBILE%
%ENABLE_PEM_SUPPORT_WXT%	%ENABLE_PEM_SUPPORT_DESKTOP%	N/A
%ENABLE_SIP_SESSION_ID_WXT%	N/A	N/A
%ENABLE_FORCE_SIP_INFO_FIR_WXT%	N/A	N/A
%SRTP_ENABLED_WXT%	%USE_SRTP%	%SRTP_ENABLED_MOBILE%
%SRTP_MODE_WXT%	%SRTP_PREFERENCE%	%SRTP_MODE_MOBILE%
%ENABLE_REKEYING_WXT%	%ENABLE_RE_KEYING_DESKTOP%	%ENABLE_RE-KEYING_MOBILE%
%RTP_AUDIO_PORT_RANGE_START_WXT%	%RTP_AUDIO_PORT_RANGE_START%	%RTP_AUDIO_PORT_RANGE_START%
%RTP_AUDIO_PORT_RANGE_END_WXT%	%RTP_AUDIO_PORT_RANGE_END%	%RTP_AUDIO_PORT_RANGE_END%
%RTP_VIDEO_PORT_RANGE_START_WXT%	%RTP_VIDEO_PORT_RANGE_START%	%RTP_VIDEO_PORT_RANGE_START%
%RTP_VIDEO_PORT_RANGE_END_WXT%	%RTP_VIDEO_PORT_RANGE_END%	%RTP_VIDEO_PORT_RANGE_END%
%ENABLE_RTCP_MUX_WXT%	%ENABLE_RTCP_MUX%	%ENABLE_RTCP_MUX%
%ENABLE_XSI_EVENT_CHANNEL_WXT%	%ENABLE_XSI_EVENT_CHANNEL%	N/A
%CHANNEL_HEARTBEAT_WXT%	%CHANNEL_HEARTBEAT%	%CHANNEL_HEARTBEAT_MOBILE%
%XSI_ROOT_WXT%	%XSI_ROOT%	%XSI_ROOT%
%XSI_ACTIONS_PATH_WXT%	N/A	%XSI_ACTIONS_PATH_MOBILE%
%XSI_EVENTS_PATH_WXT%	N/A	%XSI_EVENTS_PATH_MOBILE%

Cisco Confidential

Webex for Cisco BroadWorks Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENABLE_CALLS_AUTO_ RECOVERY_WXT%	N/A	%ENABLE_CALLS_AUTO_ RECOVERY_MOBILE%
%EMERGENCY_CALL_DIAL_ SEQUENCE_WXT%	N/A	%EMERGENCY_CALL_DIAL_ SEQUENCE_MOBILE%
%ENABLE_CALL_PICKUP_BLI ND_WXT%	N/A	N/A
%ENABLE_CALL_PICKUP_ DIRECTED_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_URL _WXT%	N/A	%WEB_CALL_SETTINGS_URL %
%USE_MEDIASEC_WXT%	%USE_MEDIASEC_MOBILE%	%USE_MEDIASEC_DESKTOP %
%ENABLE_CALL_CENTER_ WXT%	%ENABLE_CALL_CENTER_ DESKTOP%"	N/A
%WEB_CALL_SETTINGS_TAR GET_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_CFA _ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFA _VISIBLE%
%WEB_CALL_SETTINGS_DN D_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_DN D_VISIBLE%
%WEB_CALL_SETTINGS_AC R_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_AC R_VISIBLE%
%WEB_CALL_SETTINGS_CFB _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFB _VISIBLE%
%WEB_CALL_SETTINGS_CFN R_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFN R_VISIBLE%
%WEB_CALL_SETTINGS_CFN A_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CFN A_VISIBLE%
%WEB_CALL_SETTINGS_SIM RING_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_SIM RING_VISIBLE%
%WEB_CALL_SETTINGS_ SEQRING_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_SE QRING_VISIBLE%
%WEB_CALL_SETTINGS_RO_ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_RO_ VISIBLE%
%WEB_CALL_SETTINGS_ACB _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_ACB _VISIBLE%
%WEB_CALL_SETTINGS_CW _VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CW _VISIBLE%
%WEB_CALL_SETTINGS_CLI DB_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_CLI DB_VISIBLE%
%WEB_CALL_SETTINGS_PA_ VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_PA_ VISIBLE%

Cisco Confidential

Webex for Cisco BroadWorks Tag	Desktop Legacy Tag	Mobile Legacy Tag
%WEB_CALL_SETTINGS_BWA_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_BWA_VISIBLE%
%WEB_CALL_SETTINGS_CC_VISIBLE_WXT%	N/A	%WEB_CALL_STANDARD_SETTINGS_CC_VISIBLE%
%WEB_CALL_SETTINGS_BWM_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_BWM_VISIBLE%
%WEB_CALL_SETTINGS_VM_VISIBLE_WXT%	N/A	%WEB_CALL_SETTINGS_VM_VISIBLE%
%ENABLE_DIALING_CALL_BACK_WXT%	N/A	N/A
%DIALING_CALL_BACK_TIMER_WXT%	N/A	N/A
%ENABLE_EXECUTIVE_ASSISTANT_WXT%	%ENABLE_EXECUTIVE_ASSISTANT_DESKTOP%	N/A
%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT%	N/A	%PN_FOR_CALLS_RING_TIMEOUT_SECONDS_MOBILE%
%ENABLE_CALL_RECORDING_WXT%	%ENABLE_CALL_RECORDING_DESKTOP%	%CALL_RECORDING_MOBILE%
%ENABLE_SINGLE_ALERTING_WXT%	N/A	%ENABLE_SINGLE_ALERTING%
%ENABLE_CALL_PARK_WXT%	%ENABLE_CALL_PARK_DESKTOP%	N/A
%CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT%	N/A	N/A
%ENABLE_RTP_ICE_WXT%	N/A	N/A
%RTP_ICE_MODE_WXT%	N/A	N/A
%RTP_ICE_SERVICE_URI_WXT%	N/A	N/A
%RTP_ICE_PORT_WXT%	N/A	N/A
%SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT%	N/A	N/A
%ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N/A	N/A
%ENABLE_DIALING_VOIP_WXT%	N/A	N/A
%ENABLE_DIALING_NATIVE_WXT%	N/A	N/A
%ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT%	N/A	N/A
%SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT%	N/A	N/A

Cisco Confidential

Webex for Cisco BroadWorks Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENABLE_UNIFIED_CALL_HISTORY_WXT%	N/A	N/A
%WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT%	N/A	N/A
%USER_PORTAL_SETTINGS_URL_WXT%	N/A	N/A
%ENABLE_DEVICE_OWNER_RESTRICTION_WXT%	N/A	N/A
%ENABLE_AUDIO_MARI_FEC_WXT%	N/A	N/A
%ENABLE_AUDIO_MARI_RTX_WXT%	N/A	N/A
%ENABLE_VIDEO_MARI_FEC_WXT%	N/A	N/A
%ENABLE_VIDEO_MARI_RTX_WXT%	N/A	N/A
%ENABLE_CALL_BLOCK_WXT%	N/A	N/A
%ENABLE_WIDGET_HOLD_CALLS_WXT%	N/A	N/A
%ENABLE_WIDGET_TRANSFER_CALLS_WXT%	N/A	N/A
%ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT%	N/A	N/A
%ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT%	N/A	N/A
%SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT%	N/A	N/A
%ENABLE_CALL_MOVE_HERE_WXT%	N/A	N/A
%ENABLE_SPEECH_ENHANCEMENTS_WXT%	N/A	N/A
%DIALING_NATIVE_FAC_PREFIX_WXT%	N/A	N/A
%ENABLE_TRANSFER_AUTO_HOLD_WXT%	N/A	N/A
%ENABLE_RTCP_XR_NEGOTIATION_WXT%	N/A	N/A
%ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT%	N/A	N/A

Cisco Confidential

Webex for Cisco BroadWorks Tag	Desktop Legacy Tag	Mobile Legacy Tag
%ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT%	N/A	N/A
%ENABLE_CALL_FORWARDING_INFO_CALLS_WXT%	N/A	N/A
%ENABLE_BUSY_LAMP_FIELD_WXT%	%ENABLE_BUSY_LAMP_FIELD_DESKTOP%	N/A
%ENABLE_BLF_DISPLAY_CALLER_WXT%	%ENABLE_BLF_DISPLAY_CALLER_DESKTOP%	N/A
%BLF_NOTIFICATION_DELAY_TIME_WXT%	N/A	N/A
%ENABLE_GCP_NOTIFICATIONS_WXT%	N/A	N/A
%ENABLE_GCP_DISPLAY_CALLER_WXT%	N/A	N/A
%GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT%	N/A	N/A
%UDP_KEEPALIVE_ENABLED_WXT%	N/A	N/A
%TCP_KEEPALIVE_ENABLED_WXT%	N/A	N/A
%TLS_KEEPALIVE_ENABLED_WXT%	N/A	N/A
%PERSONAL_ASSISTANT_ENABLED_WXT%	%DESKTOP_PERSONAL_ASSISTANT_ENABLED%	%ENABLE_PERSONAL_ASSISTANT_PRESENCE%
%PN_FOR_CALLS_DELIVERY_MODE_WXT%	N/A	N/A
%ENABLE_ENHANCED_AUTHORIZATION_WXT%	N/A	N/A
%ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT%	N/A	N/A

Cisco Confidential

Webex for Cisco BroadWorks Tag	Desktop Legacy Tag	Mobile Legacy Tag
%CALL_PULL_MODE_WXT%	N/A	N/A
%CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT%	N/A	N/A
%ENABLE_EMERGENCY_LOCATION_WXT%	N/A	N/A
%EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT%	N/A	N/A
%EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT%	N/A	N/A
%EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%	N/A	N/A
%ENABLE_CALLS_E2EE_WXT%	N/A	N/A
%ENABLE_CLID_OUTGOING_CALLS_MOBILITY_WXT%	N/A	N/A
%CHANNEL_INACTIVITY_TIMEOUT_WXT%	N/A	N/A

NOTE: N/A indicates that there was no corresponding custom tag controlling the feature in UC-One. Having N/A for both Desktop and Mobile Legacy tags indicates that the Webex for Cisco BroadWorks tag is new and controls either new functionality or an existing feature, that was not controlled through a custom tag in UC-One.

Cisco Confidential

9 Appendix A: TLS Ciphers

The Webex for BroadWorks client uses CiscoSSL, which is based on OpenSSL with additional security hardening.

Cisco Confidential

10 Appendix B: DM Tag Provisioning Script

The number of custom DM tags has increased with each release, as many customers prefer tags for the new configuration parameters. To offer mechanisms for provisioning those custom DM tags more easily, this section contains a script that can be run on the Application Server (AS) side to assign values to the custom DM tags. This script is especially intended 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. 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). Note that the following example is for mobile. For desktop, use the BroadTouch_tags tag set instead of Connect_Tags. For tablet, use the ConnectTablet_Tags tag set instead of Connect_Tags.

```
%% ********************************** Connect_Tags - read file **********************************
%%
%% Instructions:
%% -------------------
%% - This read file can be used to create, add and set Webex for BroadWorks
%% 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. WxT_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/ WxT_Tags.txt
%% - Verify results
%%
%% ----------------------------------------------------------------------------------------------------------------
%% Step 1: Create Connect tag set label - Connect_Tags
%% ----------------------------------------------------------------------------------------------------------------
quit all;System;DeviceTagSet
add Connect_Tags
%% ----------------------------------------------------------------------------------------------------------------
%% Step 2: Add WxT for BWKS custom tags
%% EXAMPLE – for all mobile tags see the list below-----------------------------------------------------
quit all;System;DeviceTagSet;Tags
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% true
%% ----------------------------------------------------------------------------------------------------------------
%% Step 3: Set Connect custom tags (if tag already exists)
%% EXAMPLE – for all mobile tags see the list below
set tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% isOverridable true
tagvalue false
%% ----------------------------------------------------------------------------------------------------------------
%% Step 4: Verify custom tags have been correctly defined and set
%% ----------------------------------------------------------------------------------------------------------------
quit all;System;DeviceTagSet;Tags
get tagSetName Connect_Tags
quit all
```


Cisco Confidential

The following lists all custom tags used by Webex for Cisco BroadWorks, with example (default or recommended) values. Note that some of the tags require values specific to the corresponding deployment (like server addresses). That is why these tags are added at the end of the script but left empty, and additional set commands should be added to specify them.

10.1 Desktop

```
add tagSetName BroadTouch_tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_XSI_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BUSY_LAMP_FIELD_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BLF_DISPLAY_CALLER_WXT% true
add tagSetName BroadTouch_tags %BLF_NOTIFICATION_DELAY_TIME_WXT% 0
add tagSetName BroadTouch_tags %ENABLE_REMOTE_CONTROL_EVENTS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName BroadTouch_tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName BroadTouch_tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName BroadTouch_tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName BroadTouch_tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PULL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MWI_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%
false
add tagSetName BroadTouch_tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%
false
add tagSetName BroadTouch_tags %ENABLE_USE_RPORT_WXT% false
add tagSetName BroadTouch_tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName BroadTouch_tags %USE_TLS_WXT% false
add tagSetName BroadTouch_tags %SBC_PORT_WXT% 5075
add tagSetName BroadTouch_tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName BroadTouch_tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName BroadTouch_tags %PROXY_DISCOVERY_BYPASS_OS_CACHE_WXT% false
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName BroadTouch_tags %SOURCE_PORT_WXT% 5060
add tagSetName BroadTouch_tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName BroadTouch_tags %SIP_FAILBACK_ENABLED_WXT% true
add tagSetName BroadTouch_tags %SIP_FAILBACK_TIMEOUT_WXT% 900
add tagSetName BroadTouch_tags %SIP_FAILBACK_USE_RANDOM_FACTOR_WXT% false
add tagSetName BroadTouch_tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName BroadTouch_tags %TCP_SIZE_THRESHOLD_WXT% 18000
```


Cisco Confidential

```
add tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL_WXT% false
add tagSetName BroadTouch_tags %SIP_REFRESH_ON_TTL_USE_RANDOM_FACTOR_WXT% true
add tagSetName BroadTouch_tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName BroadTouch_tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName BroadTouch_tags %SRTP_ENABLED_WXT% false
add tagSetName BroadTouch_tags %SRTP_MODE_WXT% false
add tagSetName BroadTouch_tags %ENABLE_REKEYING_WXT% true
add tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName BroadTouch_tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName BroadTouch_tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
add tagSetName BroadTouch_tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName BroadTouch_tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName BroadTouch_tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName BroadTouch_tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName BroadTouch_tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName BroadTouch_tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName BroadTouch_tags %USE_MEDIASEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_URL_WXT%
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName BroadTouch_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_BLIND_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PICKUP_DIRECTED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIP_VIDEOCALLS_WXT% true
add tagSetName BroadTouch_tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName BroadTouch_tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% true
add tagSetName BroadTouch_tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName BroadTouch_tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName BroadTouch_tags %ENABLE_FORCED_LOGOUT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_EXECUTIVE_ASSISTANT_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_PARK_WXT% false
add tagSetName BroadTouch_tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
```


Cisco Confidential

```
add tagSetName BroadTouch_tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_DESKPHONE_CONTROL_AUTO_ANSWER_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_MODE_WXT% icestun
add tagSetName BroadTouch_tags %RTP_ICE_PORT_WXT% 3478
add tagSetName BroadTouch_tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName BroadTouch_tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName BroadTouch_tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName BroadTouch_tags %FORCED_LOGOUT_APPID_WXT% true
add tagSetName BroadTouch_tags %XSI_ROOT_WXT% true
add tagSetName BroadTouch_tags %SBC_ADDRESS_WXT% true
add tagSetName BroadTouch_tags %SBC_PORT_WXT% true
add tagSetName BroadTouch_tags %MWI_MODE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName BroadTouch_tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName BroadTouch_tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUTO_ANSWER_WXT% false
add tagSetName BroadTouch_tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName BroadTouch_tags %ENABLE_MULTI_LINE_WXT% false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName BroadTouch_tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName BroadTouch_tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName BroadTouch_tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName BroadTouch_tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName BroadTouch_tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName BroadTouch_tags %ENABLE_REMOTE_MUTE_CONTROL_WXT% false
add tagSetName BroadTouch_tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName BroadTouch_tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CALL_MOVE_HERE_WXT% true
add tagSetName BroadTouch_tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName BroadTouch_tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName BroadTouch_tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName BroadTouch_tags %ENABLE_CLID_OUTGOING_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_GCP_NOTIFICATIONS_WXT% false
add tagSetName BroadTouch_tags %ENABLE_GCP_DISPLAY_CALLER_WXT% false
add tagSetName BroadTouch_tags %GCP_NOTIFICATION_MAX_TIMEOUT_VALUE_WXT% 120
add tagSetName BroadTouch_tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName BroadTouch_tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName BroadTouch_tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
add tagSetName BroadTouch_tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName BroadTouch_tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
add tagSetName BroadTouch_tags %ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT% false
add tagSetName BroadTouch_tags %CALL_PULL_MODE_WXT% false
add tagSetName BroadTouch_tags %CALL_PULL_DEFAULT_ACTIVE_MOVE_OPTION_WXT% call_move
add tagSetName BroadTouch_tags %ENABLE_EMERGENCY_LOCATION_WXT% false
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_PROVIDER_NAME_WXT% redsky
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT% -1
```


Cisco Confidential

```
add tagSetName BroadTouch_tags %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName BroadTouch_tags %ENABLE_CALLS_E2EE_WXT% false
add tagSetName BroadTouch_tags %CHANNEL_INACTIVITY_TIMEOUT_WXT% 60000
add tagSetName BroadTouch_tags %XSI_PROXY_DISCOVERY_MODE_WXT% srv-host
```

10.2 Mobile

```
add tagSetName Connect_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName Connect_Tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName Connect_Tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName Connect_Tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName Connect_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName Connect_Tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName Connect_Tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PULL_WXT% false
add tagSetName Connect_Tags %ENABLE_MWI_WXT% false
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName Connect_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT% false
add tagSetName Connect_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT% false
add tagSetName Connect_Tags %ENABLE_USE_RPORT_WXT% false
add tagSetName Connect_Tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName Connect_Tags %USE_TLS_WXT% false
add tagSetName Connect_Tags %SBC_PORT_WXT% 5075
add tagSetName Connect_Tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName Connect_Tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName Connect_Tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName Connect_Tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName Connect_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName Connect_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName Connect_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName Connect_Tags %SOURCE_PORT_WXT% 5060
add tagSetName Connect_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName Connect_Tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName Connect_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName Connect_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
add tagSetName Connect_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName Connect_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName Connect_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName Connect_Tags %SRTP_ENABLED_WXT% false
add tagSetName Connect_Tags %SRTP_MODE_WXT% false
add tagSetName Connect_Tags %ENABLE_REKEYING_WXT% true
add tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName Connect_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName Connect_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
```


Cisco Confidential

```
add tagSetName Connect_Tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName Connect_Tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName Connect_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName Connect_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName Connect_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName Connect_Tags %USE_MEDIASEC_WXT% false
add tagSetName Connect_Tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName Connect_Tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName Connect_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
add tagSetName Connect_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName Connect_tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName Connect_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
add tagSetName Connect_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% cs-only
add tagSetName Connect_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName Connect_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
add tagSetName Connect_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
add tagSetName Connect_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% busy
add tagSetName Connect_Tags %ENABLE_DIALING_CALL_BACK_WXT% false
add tagSetName Connect_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName Connect_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
add tagSetName Connect_Tags %ENABLE_SINGLE_ALERTING_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_PARK_WXT% false
add tagSetName Connect_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName Connect_Tags %ENABLE_RTP_ICE_WXT% false
add tagSetName Connect_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName Connect_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName Connect_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName Connect_Tags %ENABLE_DIALING_VOIP_WXT% true
add tagSetName Connect_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName Connect_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName Connect_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName Connect_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName Connect_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName Connect_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName Connect_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName Connect_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
```


Cisco Confidential

```
add tagSetName Connect_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName Connect_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName Connect_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName Connect_Tags %XSI_ROOT_WXT% true
add tagSetName Connect_Tags %SBC_ADDRESS_WXT% true
add tagSetName Connect_Tags %SBC_PORT_WXT% true
add tagSetName Connect_Tags %MWI_MODE_WXT% true
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName Connect_Tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName Connect_Tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName Connect_Tags %ENABLE_SIP_VIDEOCALLS_WXT% true
add tagSetName Connect_Tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName Connect_Tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% false
add tagSetName Connect_Tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName Connect_Tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName Connect_Tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName Connect_Tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT% once_per_login
add tagSetName Connect_Tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_DELIVERY_BLOCKING_WXT% false
add tagSetName Connect_Tags %ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT% false
add tagSetName Connect_Tags %ENABLE_RING_SPLASH_WXT% false
add tagSetName Connect_Tags %ENABLE_PN_MOBILE_CALL_INFO_WXT% true
add tagSetName Connect_Tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName Connect_Tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName Connect_Tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName Connect_Tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName Connect_Tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName Connect_Tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName Connect_Tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName Connect_Tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName Connect_Tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName Connect_Tags %ENABLE_WIDGET_HOLD_CALLS_WXT% true
add tagSetName Connect_Tags %ENABLE_WIDGET_TRANSFER_CALLS_WXT% true
add tagSetName Connect_Tags %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% true
add tagSetName Connect_Tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName Connect_Tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName Connect_Tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName Connect_Tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName Connect_Tags %DIALING_NATIVE_FAC_PREFIX_WXT%
add tagSetName Connect_Tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName Connect_Tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName Connect_Tags %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% false
add tagSetName Connect_Tags %ENABLE_CLID_OUTGOING_CALLS_MOBILITY_WXT% false
add tagSetName Connect_Tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName Connect_Tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName Connect_Tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName Connect_Tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName Connect_Tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName Connect_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
add tagSetName Connect_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName Connect_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% false
add tagSetName Connect_Tags %ENABLE_MULTI_LINE_WXT% false
add tagSetName Connect_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
```


Cisco Confidential

```
add tagSetName Connect_Tags %ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT% false
add tagSetName Connect_Tags %CALL_PULL_MODE_WXT% blind
add tagSetName Connect_Tags %ENABLE_EMERGENCY_LOCATION_WXT% false
add tagSetName Connect_Tags %EMERGENCY_LOCATION_PROVIDER_NAME_WXT% redsky
add tagSetName Connect_Tags %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName Connect_Tags %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName Connect_Tags %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT% once_per_login
add tagSetName Connect_Tags %ENABLE_CALLS_E2EE_WXT% false
add tagSetName Connect_Tags %CHANNEL_INACTIVITY_TIMEOUT_WXT% 60000
add tagSetName Connect_Tags %XSI_PROXY_DISCOVERY_MODE_WXT% srv-host
```

10.3 Tablet

```
add tagSetName ConnectTablet_Tags %ENABLE_REJECT_WITH_486_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %TRANSFER_CALL_TYPE_WXT% full
add tagSetName ConnectTablet_Tags %ENABLE_XSI_TRANSFER_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_SPAM_INDICATION_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_NOISE_REMOVAL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CONFERENCE_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_NWAY_PARTICIPANT_LIST_WXT% false
add tagSetName ConnectTablet_Tags %MAX_CONF_PARTIES_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_CALL_STATISTICS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_PULL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_MWI_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VISUAL_VOICE_MAIL_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_ALWAYS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_DESCRIPTION_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_WXT%
false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_ALERT_ALL_LOCATIONS_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_CALL_CONTROL_WXT% false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_CALL_CONTROL_DEFAULT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_WXT% false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_DIVERSION_INHIBITOR_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_WXT%
false
add tagSetName ConnectTablet_Tags %BROADWORKS_ANYWHERE_ANSWER_CONFIRMATION_DEFAULT_WXT%
false
add tagSetName ConnectTablet_Tags %ENABLE_USE_RPORT_WXT% false
add tagSetName ConnectTablet_Tags %RPORT_USE_LOCAL_PORT_WXT% false
add tagSetName ConnectTablet_Tags %USE_TLS_WXT% false
add tagSetName ConnectTablet_Tags %SBC_PORT_WXT% 5075
add tagSetName ConnectTablet_Tags %USE_PROXY_DISCOVERY_WXT% false
add tagSetName ConnectTablet_Tags %USE_TCP_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %USE_UDP_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %USE_TLS_FROM_DNS_WXT% true
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_TCP_CONNECT_TIMEOUT_WXT% 5000
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_TLS_CONNECT_TIMEOUT_WXT% 10000
add tagSetName ConnectTablet_Tags %PROXY_DISCOVERY_ENABLE_BACKUP_SERVICE_WXT% true
add tagSetName ConnectTablet_Tags %PROXY_DISCOVERY_ENABLE_SRV_BACKUP_WXT% true
add tagSetName ConnectTablet_Tags %SOURCE_PORT_WXT% 5060
add tagSetName ConnectTablet_Tags %USE_ALTERNATIVE_IDENTITIES_WXT% false
add tagSetName ConnectTablet_Tags %SIP_TRANSPORTS_ENFORCE_IP_VERSION_WXT% dns
add tagSetName ConnectTablet_Tags %TCP_SIZE_THRESHOLD_WXT% 18000
add tagSetName ConnectTablet_Tags %ENABLE_SIP_UPDATE_SUPPORT_WXT% false
```


Cisco Confidential

```
add tagSetName ConnectTablet_Tags %ENABLE_PEM_SUPPORT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_SIP_SESSION_ID_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_FORCE_SIP_INFO_FIR_WXT% false
add tagSetName ConnectTablet_Tags %SRTP_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %SRTP_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_REKEYING_WXT% true
add tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_START_WXT% 8000
add tagSetName ConnectTablet_Tags %RTP_AUDIO_PORT_RANGE_END_WXT% 8099
add tagSetName ConnectTablet_Tags %RTP_VIDEO_PORT_RANGE_START_WXT% 8100
add tagSetName ConnectTablet_Tags %RTP_VIDEO_PORT_RANGE_END_WXT% 8199
add tagSetName ConnectTablet_Tags %ENABLE_RTCP_MUX_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_XSI_EVENT_CHANNEL_WXT% true
add tagSetName ConnectTablet_Tags %CHANNEL_HEARTBEAT_WXT% 10000
add tagSetName ConnectTablet_Tags %XSI_ACTIONS_PATH_WXT% /com.broadsoft.xsi-actions/
add tagSetName ConnectTablet_Tags %XSI_EVENTS_PATH_WXT% /com.broadsoft.xsi-events/
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_AUTO_RECOVERY_WXT% true
add tagSetName ConnectTablet_Tags %USE_MEDIASEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_SCREEN_SHARE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CALL_CENTER_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_TARGET_WXT% external
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFA_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFNR_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CFNA_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_DND_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_ACR_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_SIMRING_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_SEQRING_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_ACB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CW_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CLIDB_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_PA_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_CC_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BWA_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BWM_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_RO_VISIBLE_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_VM_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_BRANDING_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_EMAIL_VM_VISIBLE_WXT% true
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_URL_WXT% true
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_TARGET_WXT% external
add tagSetName ConnectTablet_Tags %USER_PORTAL_SETTINGS_SSO_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_EMERGENCY_DIALING_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_CALL_DIAL_SEQUENCE_WXT% cs-only
add tagSetName ConnectTablet_Tags %EMERGENCY_DIALING_NUMBERS_WXT% 911,112
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_CONNECT_SIP_ON_ACCEPT_WXT% false
add tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_MODE_WXT% decline_false
add tagSetName ConnectTablet_Tags %REJECT_WITH_XSI_DECLINE_REASON_WXT% busy
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_CALL_BACK_WXT% false
add tagSetName ConnectTablet_Tags %DIALING_CALL_BACK_TIMER_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_CALL_RECORDING_WXT% false
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_RING_TIMEOUT_SECONDS_WXT% 35
add tagSetName ConnectTablet_Tags %ENABLE_SINGLE_ALERTING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_PARK_WXT% false
add tagSetName ConnectTablet_Tags %CALL_PARK_AUTO_CLOSE_DIALOG_TIMER_WXT% 10
add tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_WXT% false
add tagSetName ConnectTablet_Tags %RTP_ICE_MODE_WXT% icestun
add tagSetName ConnectTablet_Tags %SIP_URI_DIALING_ENABLE_LOCUS_CALLING_WXT% true
add tagSetName ConnectTablet_Tags %RTP_ICE_PORT_WXT% 3478
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_VOIP_WXT% true
```


Cisco Confidential

```
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_NATIVE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_DIALING_MODE_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_MODE_DEFAULT_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_ENABLE_BWKS_MOBILITY_DEPENDENCY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_XSI_CALL_CONTROL_WXT% false
add tagSetName ConnectTablet_Tags %XSI_CALL_CONTROL_DEPLOYMENT_TYPE_WXT% MNO_Access
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_1_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_2_WXT% true
add tagSetName ConnectTablet_Tags %DEPLOYMENT_DEVICE_TYPE_3_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_XSI_HOLD_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_UNIFIED_CALL_HISTORY_WXT% false
add tagSetName ConnectTablet_Tags %RTP_ICE_SERVICE_URI_WXT% true
add tagSetName ConnectTablet_Tags %XSI_ROOT_WXT% true
add tagSetName ConnectTablet_Tags %SBC_ADDRESS_WXT% true
add tagSetName ConnectTablet_Tags %SBC_PORT_WXT% true
add tagSetName ConnectTablet_Tags %MWI_MODE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_TRANSCRIPTION_WXT% false
add tagSetName ConnectTablet_Tags %WEB_CALL_SETTINGS_URL_WXT% true
add tagSetName ConnectTablet_Tags %DOMAIN_OVERRIDE_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SIP_VIDEOCALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_LOCUS_VIDEOCALLS_WXT% true
add tagSetName ConnectTablet_Tags %VIDEOCALLS_ANSWER_WITH_VIDEO_ON_DEFAULT_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_DIALING_ENABLE_REDSKY_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName ConnectTablet_Tags %EMERGENCY_REDSKY_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName ConnectTablet_Tags %USE_PAI_AS_CALLING_IDENTITY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_DELIVERY_BLOCKING_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_MOBILITY_PERSONA_MANAGEMENT_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_RING_SPLASH_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_PN_MOBILE_CALL_INFO_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_QOS_WXT% true
add tagSetName ConnectTablet_Tags %AUDIO_QOS_VALUE_WXT% 46
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_QOS_WXT% true
add tagSetName ConnectTablet_Tags %VIDEO_QOS_VALUE_WXT% 34
add tagSetName ConnectTablet_Tags %ENABLE_DEVICE_OWNER_RESTRICTION_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_MARI_FEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_AUDIO_MARI_RTX_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_MARI_FEC_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VIDEO_MARI_RTX_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_BLOCK_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_HOLD_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_TRANSFER_CALLS_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_WIDGET_CALLS_ESCALATE_TO_WEBEX_MEETING_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SIMULTANEOUS_CALLS_WITH_SAME_USER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_VOICE_MAIL_FORWARDING_WXT% true
add tagSetName ConnectTablet_Tags %SIP_REGISTER_FAILOVER_REGISTRATION_CLEANUP_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_SPEECH_ENHANCEMENTS_WXT% true
add tagSetName ConnectTablet_Tags %DIALING_NATIVE_FAC_PREFIX_WXT%
add tagSetName ConnectTablet_Tags %ENABLE_TRANSFER_AUTO_HOLD_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_RTCP_XR_NEGOTIATION_WXT% true
add tagSetName ConnectTablet_Tags %ENABLE_CLID_INCOMING_CALLS_APPEND_NUMBER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_MISSED_CALLS_APPEND_NUMBER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_ADDITIONAL_NUMBERS_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_CALL_CENTER_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_HUNT_GROUP_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_DELIVERY_BLOCKING_WXT% false
```


Cisco Confidential

```
add tagSetName ConnectTablet_Tags %ENABLE_CLID_OUTGOING_CALLS_MOBILITY_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CALL_FORWARDING_INFO_CALLS_WXT% false
add tagSetName ConnectTablet_Tags %UDP_KEEPALIVE_ENABLED_WXT% true
add tagSetName ConnectTablet_Tags %TCP_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %TLS_KEEPALIVE_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_RTP_ICE_IPV6_WXT% false
add tagSetName ConnectTablet_Tags %CLID_REMOTE_NAME_MACHINE_MODE_WXT% resolved
add tagSetName ConnectTablet_Tags %PERSONAL_ASSISTANT_ENABLED_WXT% false
add tagSetName ConnectTablet_Tags %PN_FOR_CALLS_DELIVERY_MODE_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_ENHANCED_AUTHORIZATION_WXT% false
add tagSetName ConnectTablet_Tags %ENABLE_CONFERENCE_DROP_TWO_PARTY_CONFERENCE_WXT% false
add tagSetName ConnectTablet_Tags %CALL_PULL_MODE_WXT% blind
add tagSetName ConnectTablet_Tags %ENABLE_EMERGENCY_LOCATION_WXT% false
add tagSetName ConnectTablet_Tags %EMERGENCY_LOCATION_PROVIDER_NAME_WXT% redsky
add tagSetName ConnectTablet_Tags %EMERGENCY_LOCATION_USER_REMINDER_TIMEOUT_WXT% 0
add tagSetName ConnectTablet_Tags %EMERGENCY_LOCATION_USER_MANDATORY_LOCATION_WXT% -1
add tagSetName ConnectTablet_Tags %EMERGENCY_LOCATION_USER_LOCATION_PROMPTING_WXT%
once_per_login
add tagSetName ConnectTablet_Tags %ENABLE_CALLS_E2EE_WXT% false
add tagSetName ConnectTablet_Tags %CHANNEL_INACTIVITY_TIMEOUT_WXT% 60000
add tagSetName ConnectTablet_Tags %XSI_PROXY_DISCOVERY_MODE_WXT% srv-host
```

10.4 System Tags

The following lists the system tags used by Webex for BroadWorks.

```
%BWNETWORK-CONFERENCE-SIPURI-n%
%BWVOICE-PORTAL-NUMBER-n%
%BWLINEPORT-n%
%BWHOST-n%
%BWAUTHUSER-n%
%BWAUTHPASSWORD-n%
%BWE164-n%
%BWNAME-n%
%BWEXTENSION-n%
%BWAPPEARANCE-LABEL-n%
%BWDISPLAYNAMELINEPORT%
%BWLINEPORT-PRIMARY%
%BWE911-PRIMARY-HELDURL%
%BWE911-CUSTOMERID%
%BWE911-SECRETKEY%
%BWE911-EMERGENCY-NUMBER-LIST%
%BW-MEMBERTYPE-n%
%BWUSEREXTID-n%
```


Cisco Confidential

11 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.

ACB	Automatic Callback
ACD	Automatic Call Distribution
ACR	Anonymous Call Rejection
AES	Advanced Encryption Standard
ALG	Application Layer Gateway
API	Application Programming Interface
APK	Application Package
APNS	Apple Push Notification Service
ARS	Automatic bit Rate Selection
AS	Application Server (Cisco BroadWorks)
AVP	Audio Visual Profile
BW	BroadWorks
BWA	BroadWorks Anywhere
BWKS	BroadWorks
BWM	BroadWorks Mobility
BYOD	Bring Your Own Device
CC	Call Center
CFB	Call Forwarding Busy
CFNA	Call Forwarding No Answer
CFNR	Call Forwarding Not Reachable
CIF	Common Intermediate Format
CLI	Command Line Interface
CLID	Calling Line Identity
CLIDB	Calling Line ID Delivery Blocking
CRLF	Carriage Return Line Feed
CS	Circuit-Switched
CSWV	Call Settings Web View
CW	Call Waiting
DB	Database
DM	Device Management
DND	Do Not Disturb
DNS	Domain Name System

Cisco Confidential

DPC	Desk Phone Control
DTAF	Device Type Archive File
ECACS	Emergency Call Address Change Service
FMC	Fixed-Mobile Convergence
FQDN	Fully Qualified Domain Name
HMAC	Hash Message Authentication Code
ICE	Interactive Connectivity Establishment
iLBC	internet Low Bitrate Codec
IM	Instant Messaging
IM&P	Instant Messaging and Presence
IOT	Interoperability Testing
IP	Internet Protocol
JID	Jabber Identifier
M/O	Mandatory/Optional
MNO	Mobile Network Operator
MTU	Maximum Transmission Unit
MUC	Multi-User Chat
MWI	Message Waiting Indicator
NAL	Network Abstraction Layer
NAPTR	Naming Authority Pointer
NAT	Network Address Translation
OTT	Over The Top
PA	Personal Assistant
PAI	P-Asserted-Identity
PEM	P-Early Media
PLI	Picture Loss Indication
PLMN	Public Land Mobile Network
PN	Push Notification
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service
RO	Remote Office
RTCP	Real-Time Control Protocol
RTP	Real Time Protocol
SaaS	Software as a Service
SAN	Subject Alternative Name
SASL	Simple Authentication and Security Layer

Cisco Confidential

SAVP	Secure Audio Video Profile
SBC	Session Border Controller
SCA	Shared Call Appearance
SCF	Session Continuity Function
SCTP	Stream Control Transmission Protocol
SDP	Session Definition Protocol
SEQRING	Sequential Ring
SIMRING	Simultaneous Ring
SIP	Session Initiation Protocol
SNR	Signal to Noise Ratio
SNR	Single Number Reach
SRTCP	Secure Real-Time Control Protocol
SRTP	Secure Real-time Transport Protocol
SSL	Secure Sockets Layer
STUN	Session Traversal Utilities for NAT
SUBQCIF	Sub Quarter CIF
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
TURN	Traversal Using Relay NAT
UDP	User Datagram Protocol
UI	User Interface
UMS	Messaging Server (Cisco BroadWorks)
URI	Uniform Resource Identifier
UVS	Video Server (Cisco BroadWorks)
VGA	Video Graphics Array
VoIP	Voice Over IP
VVM	Visual Voicemail
WXT	Webex
XMPP	Extensible Messaging and Presence Protocol
XR	Extended Report
Xsp	Xtended Services Platform
Xsi	Xtended Services Interface

Cisco Confidential