



Cisco BroadWorks

Partner Configuration Guide

Polycom UC Software VVX Phones

April 2020

Document Version 4.7

Cisco® Guide

Notification

BroadSoft BroadWorks has been renamed to Cisco BroadWorks. You will begin to see the Cisco name and company logo, along with the new product name on the software, documentation, and packaging. During the transition process, you may see both BroadSoft and Cisco brands and former product names. These products meet the same high standards and quality that both BroadSoft and Cisco are known for in the industry.

Copyright Notice

Copyright© 2020 Cisco Systems, Inc. All rights reserved.

Trademarks

Any product names mentioned in this document may be trademarks or registered trademarks of Cisco or their respective companies and are hereby acknowledged.

Document Revision History

Version	Reason for Change
1.1	Introduced document for Polycom VVX 300/400 Phones version 4.1.4 validation with BroadWorks Release 18.sp1.
1.2	Updated document for Polycom VVX 500/600 Phones version 4.1.3 validation with BroadWorks Release 19.sp1.
1.3	Edited and published document.
1.4	Updated document to include support for new Polycom VVX 310 and VVX 410 Phones version 4.1.4.
1.5	Edited changes and published document.
1.6	Added information in section 2.1 Verified Versions to indicate that Polycom VVX 500/600 Phones version 4.1.3 was verified in both interoperability testing and access solution testing with BroadWorks Release 19.sp1.
1.7	Edited changes and published document.
1.8	Modified <i>DeviceManagementDefaults</i> device profile type is to use BroadWorks tags for reducing deployment overhead.
1.9	Edited changes and published document.
1.10	Updated document to include provisioning steps to enable Polycom VVX500/600 phones at version 4.1.3G supporting the BroadSoft UC-One application. Added validated version of 4.1.3 with BroadWorks Release 18.sp1.
1.11	Edited changes and published document.
1.12	Revised UC-One Integration section to incorporate the BroadWorks Enterprise Directory feature.
1.13	Edited changes and published document.
1.14	Updated document for VVX phones version 5.0.0 validation with BroadWorks Release 18.sp1.
1.15	Edited changes and published document.
1.16	Modified Device Management (DM) section to support Flexible Seating in Release 20.
1.17	Edited changes and published document.
1.18	Updated document with Polycom VVX phones version 5.0.1 validation with BroadWorks Release 20.sp1. Other changes include Hybrid Keys provisioning instructions for SCA support and Device Management Extended File Capture provisioning instructions to support repository of multiple log files instances.
1.19	Updated configuration file template in Appendix A.
1.20	Edited changes and published document.
1.21	Updated document.
1.22	Edited changes and published document.
1.23	Updated document with Polycom VVX phones version 5.1.1 validation with BroadWorks Release 19.sp1. Support for call recording and security classification features are also added.
1.24	Edited changes and published document.
1.25	Update document with Polycom VVX phones version 5.2.0 validation with BroadWorks Release 20.sp1. Additionally, documented for Flexible Seating configuration for device to properly differentiate with the Hoteling feature.
1.26	Edited changes and published document.

Version	Reason for Change
1.27	Revised ACD/Hoteling/Flexible Seating section for clarification.
1.28	Minor updates to provide clarification on BLF and the use of FKS with SCA.
1.29	Edited changes and published document.
1.30	Update document with Polycom VVX phones version 5.3.0 validation with BroadWorks Release 21.sp1.
1.31	Edited changes and published document.
2.0	Updated document with Polycom VVX phones version 5.4.0 validation with BroadWorks Release 20.sp1. Added VVX 101/201 models.
2.1	Edited changes and published document.
2.2	Updated document for content standardization.
2.3	Updated to extend Xtended Services Interface support to all models.
2.4	Edited changes and published document.
2.5	Updated document with Polycom Real Presence Trio 8800 version 5.4.0 and Polycom VVX Phones version 5.4.1 validation with BroadWorks Release 20.sp1.
2.6	Edited changes and published document.
2.7	Updated document with ZTP test results of Polycom VVX phones version 5.4.2 and BroadWorks Release 21.sp1
2.8	Edited changes and published document.
2.9	Updated document with the support of D60 wireless handset for VVX 3xx, 4xx, 5xx and 6xx phones at version 5.4.3 and BroadWorks Release 21.sp1.
3.0	Edited changes and published document.
3.1	Updated document with the support of Flexible Seating, Executive and Assistant, Call Decline Policy and IPv6 for VVX 3xx, 4xx, 5xx and 6xx phones at version 5.5.0 and BroadWorks Release 21.sp1.
3.2	Edited changes and published document.
3.3	Made modifications in section 4.4.3 Feature Key Synchronization to rectify false references of CF not supported under SCA configuration.
3.4	Edited changes and published document.
3.5	Updated document with Polycom VVX phones version 5.5.1 validation with BroadWorks Release 22.0. Support for client certificate mutual authentication with MAC address from CN field is added.
3.6	Edited changes and published document.
3.7	Updated the <i>SIP Interface Capabilities</i> table and <i>Device Management Capabilities</i> table.
3.8	Edited changes and published document.
3.9	Updated document with Polycom VVX phones version 5.6.0 validation with BroadWorks Release 21.sp1.
3.10	Edited changes and published document.
3.11	Updated document with Polycom VVX phones version 5.7.0 validation with BroadWorks Release 22.0. Support of Trio has been moved to its standalone Trio PCG.
3.12	Edited changes and published document.

Version	Reason for Change
4.0	Updated document with Polycom VVX phones version 5.8.0 validation with BroadWorks Release 22.0. Support for VVX 150/250/350/450 models are add.
4.1	Edited changes and published document.
4.2	Updated document with Polycom VVX phones version 5.9.0 validation with BroadWorks Release 22.0.
4.3	Edited changes and published document.
4.4	Added Test Plan Packages items to section 2.2.1 SIP Interface Capabilities .
4.5	Edited changes, rebranded and published document.
4.6	Updated document with Polycom VVX phones version 6.1.0 validation with Cisco BroadWorks Release 22.0.
4.7	Edited changes and published document.

Table of Contents

1	Overview	9
2	Interoperability Status	10
2.1	Verified Versions	10
2.2	Interface Capabilities Supported	11
2.2.1	SIP Interface Capabilities	11
2.2.2	Other Interface Capabilities	17
2.3	Known Issues	19
3	Cisco BroadWorks Configuration	21
3.1	Cisco BroadWorks Device Profile Type Configuration	21
3.2	Cisco BroadWorks Configuration Steps	22
4	Polycom VVX Phones Configuration	23
4.1	Configuration Method	23
4.2	System Level Configuration	24
4.2.1	Configure Network Settings	24
4.2.2	Configure SIP Interface Settings	25
4.2.3	Configure Service Settings	26
4.3	Subscriber Level Configuration	29
4.3.1	Attendant Console Configuration	30
4.4	Advanced SIP Features Configuration	31
4.4.1	Shared Call Appearance Configuration	31
4.4.2	Busy Lamp Field Configuration	37
4.4.3	Feature Key Synchronization	38
4.4.4	Call Center Configuration	38
4.4.5	Hoteling and Flexible Seating Feature Configuration	40
4.4.6	Call Recording Feature Configuration	41
4.4.7	Security Classification Feature Configuration	42
4.5	Xtended Services Interface Feature Configuration	42
4.5.1	Xtended Services Interface Authentication Method	42
4.5.2	Cisco BroadWorks Directory	43
4.5.3	Cisco BroadWorks Call Logs Configuration	46
4.5.4	Cisco BroadWorks Visual Voice Mail Configuration	46
4.5.5	Xtended Services Interface Feature Configuration with Cisco BroadWorks	46
4.6	Instant Message and Presence Configuration	48
4.7	Executive and Assistant Feature Configuration (UCS 5.5.0 and Newer)	48
4.8	Call Decline Policy Configuration (UCS 5.5.0 and Newer)	49
4.9	Polycom Device Management Service for Service Providers (PDMS-SP) – Cloud Management Provisioning (UCS 5.8.1 and newer feature)	50
5	Device Management	52
5.1	Device Management Capabilities Supported	52

5.2	Device Management Configuration	54
5.2.1	Configure Cisco BroadWorks Tags	54
5.2.2	Configure Cisco BroadWorks Device Profile Type	61
5.2.3	Create Device Profile Instance	96
5.2.4	Configure Cisco BroadWorks User	97
5.2.5	Configure Edge Device	99
5.2.6	Enable HTTPS for Polycom UC Software Devices	99
5.2.7	File Authentication Using MAC Address from Client Certificate	100
5.2.8	Configure Polycom UC Software Phone.....	103
5.3	Upgrade from Previous CPE Kits	115
	Appendix A: Sample Polycom® Phone Configuration Files.....	116
	Appendix B: Server Side Configuration for Device Management Extended File Capture	126
	References	129

Table of Figures

Figure 1 Device Identity/Profile Type.....	22
Figure 2 Shared Call Appearance Configuration.....	31
Figure 3 System Default Tag Settings.....	55
Figure 4 Device-Type-Specific Tag Settings.....	60
Figure 5 Device Access FQDN.....	62
Figure 6 Device Management for Release 18.0 and Later.....	64
Figure 7 Auto Configuration Options.....	64
Figure 8 Device Management Options Settings.....	66
Figure 9 sys.cfg File.....	70
Figure 10 Bitmap Image File.....	72
Figure 11 BWMACADDRESS.cfg File.....	74
Figure 12 phoneBWMACADDRESS.cfg File.....	77
Figure 13 dect.cfg File.....	78
Figure 14 efk.cfg File.....	80
Figure 15 Enable Extended File Capture Setting.....	82
Figure 16 Rebuild All Device Profile Files.....	82
Figure 17 Extended Captured Files.....	83
Figure 18 Application Firmware File Settings.....	86
Figure 19 Language Mapping.....	89
Figure 20 BroadWorks User Language Definition.....	90
Figure 21 Enable Polycom Phone Services.....	95
Figure 22 Identity/Device Profile Add.....	97
Figure 23 Assign Device Profile to User.....	98
Figure 24 MAC Address Definition for Device Profile Instance.....	101
Figure 25 Device Profile Type Update for MAC-Based Auth using Client Certificate.....	102
Figure 26 Authentication Mode Set to MAC-Based and Sourced from Client Certificate.....	102
Figure 27 Polycom Phone Service setting for MAC Authentication Using Client Certificate.....	103
Figure 28 Provisioning Server Configuration.....	105
Figure 29 Identity/Device Type Credentials – Custom Credentials.....	106
Figure 30 Device Access FQDN.....	107
Figure 31 Default Device Profile Type.....	108
Figure 32 Configure Advanced Options.....	109
Figure 33 Device Management Options Settings.....	110
Figure 34 000000000000.cfg File.....	111
Figure 35 qsetup.cfg File.....	112
Figure 36 provisioning.cfg File.....	114
Figure 37 sip.Id File.....	115

1 Overview

This guide describes the configuration procedures required for Polycom® UC Software VVX phones to be interoperable with Cisco BroadWorks. This includes the following Polycom phone models:

- VVX 101 Phone
- VVX 150 Phone
- VVX 201 Phone
- VVX 250 Phone
- VVX 301, 311 Phones
- VVX 350 Phone
- VVX 401, 411 Phones
- VVX 450 Phone
- VVX 501 Phone
- VVX 601 Phone

The VVX phones are access devices that use the Session Initiation Protocol (SIP) to communicate with Cisco BroadWorks for call control. These devices run a common software solution referred to as Polycom UC Software.

This guide describes the specific configuration items that are important for use with Cisco BroadWorks. It does not describe the purpose and use of all configuration items on a VVX phone. For more information, see the configuration guide called *Polycom® UC Software Administrator's Guide* [1] supplied by Polycom.

2 Interoperability Status

This section provides the known interoperability status of the Polycom® VVX products that use Polycom UC Software with Cisco BroadWorks. This includes the version(s) tested, supported capabilities, and known issues.

Interoperability testing validates that the device interfaces properly with Cisco BroadWorks via the SIP interface. Qualitative aspects of the device or device capabilities not affecting the SIP interface, such as display features, performance, and audio qualities, are not covered by interoperability testing. Requests for information and/or issues regarding these aspects should be directed to Polycom.

2.1 Verified Versions

The following table identifies the verified Polycom® VVX phones versions and the month/year the testing occurred. If the software has undergone more than one test cycle, versions for each test cycle are listed, with the most recent listed first.

Compatible Versions in the following table identifies specific Polycom VVX version, which the partner has identified as compatible, and should interface properly with Cisco BroadWorks. Generally, maintenance releases of the validated version are considered compatible and may not be specifically listed here. For any questions concerning maintenance and compatible releases, contact Polycom.

NOTE: Interoperability testing is usually performed with the latest generally available (GA) device firmware/software and the latest GA Cisco BroadWorks release and service pack at the time the testing occurs. If there is a need to use a non-verified mix of Cisco BroadWorks and device software versions, customers can mitigate their risk by self-testing the combination themselves using the *BroadWorks SIP Phone Interoperability Test Plan* [4].

Verified Versions Table					
Date (MM/YYYY)	Cisco BroadWorks Release	Polycom Version	Polycom Compatible Versions	Application Layer Gateway (ALG) Version **	SBC Version **
03/2020	Release 22.0	6.1.0 VVX Phones	6.1.0 VVX Phones	----	----
04/2019	Release 22.0	5.9.0 VVX Phones	5.9.0 VVX Phones	----	----
08/2018	Release 22.0	5.8.0 VVX Phones	5.8.0 VVX Phones	----	----
03/2018	Release 22.0	5.7.0 VVX Phones	5.7.0 VVX Phones	----	----
08/2017	Release 21.sp1	5.6.0 VVX Phones	5.6.0 VVX Phones	----	----
05/2017	Release 22.0	5.5.1 VVX Phones	5.5.1 VVX Phones	ALG not utilized for TLS connection made directly to SBC.	Oracle Communications SBC 3820 Firmware 3820 SCZ7.4.0 Patch 1.

Verified Versions Table					
Date (MM/YYYY)	Cisco BroadWorks Release	Polycom Version	Polycom Compatible Versions	Application Layer Gateway (ALG) Version **	SBC Version **
08/2016	Release 21.sp1	5.5.0 VVX Phones	5.5.0 VVX Phones	----	----
01/2016	Release 20.sp1	5.4.1 VVX Phones	5.4.1 VVX Phones	----	----
07/2015	Release 20.sp1	5.4.0	5.4.0	----	----

2.2 Interface Capabilities Supported

This section identifies interface capabilities that have been verified through testing as supported by Polycom UC Software VVX phones.

The Supported column in the tables in this section identifies the Polycom UC Software VVX phones' support for each of the items covered in the test plan, with the following designations:

- Yes Test item is supported
- No Test item is not supported
- NA Test item is not applicable to the device type
- NT Test item was not tested

Caveats and clarifications are identified in the *Comments* column.

2.2.1 SIP Interface Capabilities

The Polycom UC Software VVX phones have completed interoperability testing with Cisco BroadWorks using the *BroadWorks SIP Phone Interoperability Test Plan* [4]. The results are summarized in the following table.

The Cisco BroadWorks test plan is composed of packages, each covering distinct interoperability areas, such as “Basic” call scenarios and “Redundancy” scenarios. Each package is composed of one or more test items, which in turn are composed of one or more test cases. The test plan exercises the SIP interface between the device and Cisco BroadWorks with the intent to ensure interoperability sufficient to support the Cisco BroadWorks feature set.

NOTE: *DUT* in the following table refers to the *Device Under Test*, which in this case is the Polycom UC Software VVX phones.

Cisco BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	Test Plan Package Items	Supported	Comments
Basic	Call Origination	Yes	
	Call Termination	Yes	
	Session Audit	Yes	

Cisco BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	Test Plan Package Items	Supported	Comments
	Session Timer	Yes	
	Ringback	Yes	
	Forked Dialog	Yes	
	181 Call Being Forwarded	Yes	
	Dial Plan	Yes	
	DTMF – Inband	Yes	
	DTMF – RFC 2833	Yes	
	DTMF – DTMF Relay	Yes	
	Codec Negotiation	Yes	
	Codec Renegotiation	Yes	
BroadWorks Services	Third-Party Call Control – Basic	NA	
	Third-Party Call Control – Advanced	Yes	
	Voice Message Deposit/Retrieval	Yes	
	Message Waiting Indicator – Unsolicited	Yes	
	Message Waiting Indicator – Solicited	Yes	
	Message Waiting Indicator – Detail	Yes	
	Voice Portal Outcall	Yes	
	Advanced Alerting – Ringing	Yes	
	Advanced Alerting – Call Waiting	Yes	
	Advanced Alerting – Ring Splash	Yes	
	Advanced Alerting – Silent Alerting	Yes	
	Calling Line ID	Yes	
	Calling Line ID with Unicode Characters	Yes	
	Connected Line ID	Yes	Line Restriction not supported on VVX450/601.
	Connected Line ID with Unicode Characters	Yes	
	Connected Line Restriction	Yes	
	Connected Line Presentation After Call Forward	Yes	
	Connected Line Restriction After Call Forward	Yes	
	Connected Line ID on UPDATE	Yes	
	Connected Line ID on Re-INVITE	Yes	
Diversion Header	Yes		

Cisco BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	Test Plan Package Items	Supported	Comments
	Diversion Header: Multiple Redirects	Yes	
	History-Info Header	Yes	
	History-Info Header: Multiple Redirects	Yes	
	Advice of Charge	No	
	Meet-Me Conferencing	Yes	
	Meet-Me Conferencing – G722	Yes	
	Meet-Me Conferencing – AMR-WB	No	
	Meet-Me Conferencing – Opus	Yes	
	Collaborate – Audio	Yes	
	Collaborate – Audio – G722	Yes	
	Collaborate – Audio – Opus	Yes	NT on VVX 450/601.
	Call Decline Policy	Yes	
DUT Services – Call Control Services	Call Waiting	Yes	
	Call Hold	Yes	
	Call Transfer	Yes	
	Three-Way Calling	Yes	
	Network-Based Conference	Yes	
DUT Services – Registration and Authentication	Register Authentication	Yes	
	Maximum Registration	Yes	
	Minimum Registration	Yes	
	Invite Authentication	Yes	
	Re-Invite/Update Authentication	Yes	
	Refer Authentication	Yes	
	Device Authenticating BroadWorks	Yes	
DUT Services – Emergency Call	Emergency Call; Originator Hang Up	No	
	Emergency Call; Originator Hang Up; Ringback Unanswered	No	
	Emergency Call; Originator Hang Up; Ringback Answered	No	
	Emergency Call; Howler Tone	No	
DUT Services – P-Access-Network-Info Header	REGISTER with P-Access-Network-Info Header	No	
	INVITE with P-Access-Network-Info Header	No	
	Do Not Disturb	Yes	

Cisco BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	Test Plan Package Items	Supported	Comments
DUT Services – Miscellaneous	Call Forwarding Always	Yes	
	Call Forwarding Always Diversion Inhibitor	No	
	Anonymous Call	No	
	Anonymous Call Block	No	
	Remote Restart Via Notify	Yes	
Advanced Phone Services – Busy Lamp Field	Busy Lamp Field	Yes	
	Call Park Notification	Yes	
Advanced Phone Services – Feature Key Synchronization, Private Line	Do Not Disturb	Yes	
	Do Not Disturb Ring Splash	Yes	
	Call Forwarding	Yes	
	Call Forwarding Always Ring Splash	Yes	
	Call Forwarding Always Diversion Inhibitor	Yes	
	Call Center Agent Logon/Logoff	Yes	
	Call Center Agent Unavailable Code	Yes	
	Executive – Call Filtering	No	
	Executive-Assistant – Call Filtering	No	
	Executive-Assistant – Diversion	No	
	Call Recording	Yes	
	Security Classification	Yes	
	Advanced Phone Services – Feature Key Synchronization, Shared Line	Do Not Disturb	Yes
Do Not Disturb Ring Splash		Yes	
Call Forwarding		Yes	
Call Forwarding Always Ring Splash		Yes	
Call Forwarding Always Diversion Inhibitor		Yes	
Security Classification		Yes	
Advanced Phone Services – Missed Calls Display Synchronization	Missed Calls Display Sync	Yes	
Advanced Phone Services – Shared Call Appearance using Call Info	Line-Seize	Yes	
	Call-Info/Lamp Management	Yes	
	Public Hold	Yes	
	Private Hold	Yes	
	Hybrid Key System	Yes	

Cisco BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	Test Plan Package Items	Supported	Comments
	Multiple Call Arrangement	Yes	
	Bridge Active Line	Yes	
	Bridge Active Line – Silent Monitor	No	
	Call Park Notification	Yes	
Advanced Phone Services – Call Park Notification	Call Park Notification	Yes	
Advanced Phone Services – Call Center	Hold Reminder	Yes	
	Call Information	Yes	
	Hoteling Event	Yes	
	Status Event	Yes	
	Disposition Code	Yes	
	Emergency Escalation	Yes	
	Customer Originated Trace	Yes	
Advanced Phone Services – Call Recording Controls	Pause/Resume	Yes	
	Start/Stop	Yes	
	Record Local Conference	No	
	Record Network Conference	Yes	
Advanced Phone Services – Call Recording Video	Basic During call set up	NT	
	Audio only during call set up	No	
	Basic Mid-call	Yes	
	Audio only Mid-call	No	
	Hold	No	
	Pause/Resume	Yes	
	Record Local Conference	No	
	Record Network Conference	NT	
Advanced Phone Services – Security Classification	Security Classification	Yes	
Advanced Phone Services – Conference Event	Network-Based Conference Creator	No	
	Network-Based Conference Participant	No	
	Meet-Me Conference Participant	No	
Redundancy	DNS SRV Lookup	Yes	
	Register Failover/Failback	Yes	
	Invite Failover/Failback	Yes	
	Bye Failover	Yes	

Cisco BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	Test Plan Package Items	Supported	Comments
SBC/ALG – Basic	Register	Yes	
	Outgoing Invite	Yes	
	Incoming Invite	Yes	
SBC/ALG – Failover/Failback	Register Failover/Failback	Yes	
	Invite Failover/Failback	Yes	
Video – Basic Video Calls	Call Origination	Yes	Supported only on VVX501, 601.
	Call Termination	Yes	Supported only on VVX501, 601.
	Call Hold	Yes	Supported only on VVX501, 601.
	Call Waiting	Yes	Supported only on VVX501, 601.
	Call Transfer	Yes	Supported only on VVX501, 601.
Video – Cisco BroadWorks Video Services	Auto Attendant	Yes	Supported only on VVX501, 601.
	Auto Attendant – HD	No	
	Voice Messaging	Yes	Supported only on VVX501, 601.
	Voice Messaging – HD	No	
	Custom Ringback	No	
Video – Cisco BroadWorks Video Conference	Network-based Conference	Yes	Supported only on VVX501, 601.
	Network-based Conference – HD	No	
	Collaborate – Video	Yes	Supported only on VVX501, 601.
	Collaborate – Video – HD	No	
	Collaborate – Video – Upgrade to Video	No	
Video – Cisco BroadWorks WebRTC Client	Call from WebRTC Client	Yes	Supported only on VVX501, 601.
	Call to WebRTC Client	Yes	Supported only on VVX501, 601.
TCP	Register	Yes	
	Outgoing Invite	Yes	
	Incoming Invite	Yes	
IPV6	Call Origination	Yes	
	Call Termination	Yes	
	Session Audit	Yes	

Cisco BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	Test Plan Package Items	Supported	Comments
	Ringback	Yes	
	Codec Negotiation	Yes	
	Codec Renegotiation: Attended Transfer	NT	NT on VVX450, 601.
	Voice Message Deposit/Retrieval	Yes	
	Call Control	Yes	
	Registration with Authentication	Yes	
	Busy Lamp Field	Yes	
	Redundancy	Yes	
	SBC	NT	
	Video	Yes	Supported only on VVX501, 601.
	Dual Stack with Alternate Connectivity	No	

2.2.2 Other Interface Capabilities

This section identifies whether the Polycom UC Software VVX phones have implemented support for the following:

- Cisco BroadWorks Xtended Services Interface (Xsi)
- Extensible Messaging and Presence Protocol (XMPP) (BroadCloud/Cisco BroadWorks Collaborate Instant Messaging and Presence [IM&P])

Support for these interfaces is demonstrated by completing the *BroadWorks SIP Phone Xsi and XMPP Test Plan* [9]. Support for these interfaces is summarized in the following table.

Cisco BroadWorks Xtended Services Interface (Xsi) and BroadCloud IM&P Support Table			
Interface	Feature	Supported	Comments
Xsi Features – Authentication	Authenticate with SIP Credentials	Yes	Preferred and implemented method in the CPE kit.
	Authenticate with BroadWorks User Login Credentials	Yes	
	Authenticate with BroadWorks User Directory Number	No	
Xsi Features – User Service Configuration	Remote Office	Yes	
	BroadWorks Anywhere	Yes	
	Simultaneous Ringing	Yes	
	Caller ID Blocking	Yes	
	Call Forwarding Always	No	
	Call Forwarding Busy	No	

Cisco BroadWorks Xtended Services Interface (Xsi) and BroadCloud IM&P Support Table			
Interface	Feature	Supported	Comments
	Call Forwarding No Answer	No	
	Do Not Disturb	No	
Xsi Features – Directories	Enterprise Directory	Yes	
	Enterprise Common Phone List	Yes	
	Group Directory	Yes	
	Group Common Phone List	Yes	
	Personal Phone List	Yes	
	Search All Directories	No	Only group or enterprise search is supported.
	Xsi Features – Call Logs	Placed Calls	Yes
Received Calls		Yes	
Missed Calls		Yes	Delete Missed Calls are not supported.
All Calls		Yes	Delete All calls are not supported.
Sort by Name		Yes	
Xsi Features – Visual Voice Mail	View Messages	No	
	Listen to Audio Message	No	
	Watch Video Message	No	
	Mark Message Read/Unread	No	
	Delete Message	No	
	Mark All Messages Read/Unread	No	
Xsi Features – Push Notification	Register/Deregister for Push Notifications	No	
	Incoming Call via Push Notification	No	
	Call Update via Push Notification	No	
	Incoming Call via Push Notification; Second Incoming Call	No	
	MWI via Push Notification	No	
	Ring Splash via Push Notification	No	
Xsi Features – Call Recording Configurations	Call Record Mode Get	No	
	Set Record Mode	No	
	Set Play Call Recording to Start and Stop Announcement	No	
	Set Record Voice Messaging	No	
	Set Pause and Resume Notification	No	
	Set Recording Notification	No	

Cisco BroadWorks Xtended Services Interface (Xsi) and BroadCloud IM&P Support Table			
Interface	Feature	Supported	Comments
Xsi Features – Call Recording Controls	Record Mode set to Never	No	
	Record Mode set to Always	No	
	Record Mode set to Always with Pause/Resume	No	
	Start Recording Mid-Call with Record Mode set to On Demand	No	
	Start Recording During Call Setup with Record Mode set to On Demand	No	
	Perform User Initiated Start with Record Mode set to On Demand	No	
	Perform Mid-Call Start Recording after Placing Call on Hold	No	
	Perform Mid-Call Change to Call Recording Mode	No	
	Record Local Three-Way Call	No	
	Record Network Three-Way Call	No	
XMPP Features – Contact/Buddy List	Contacts	Yes	
	Favorites	Yes	
	Groups	Yes	
	Non-XMPP Contacts	Yes	
	Conferences	No	
XMPP Features – Presence	Login Invisible	No	
	Presence State	No	
	Presence Status	No	
	Contact's Presence State	No	

2.3 Known Issues

This section lists the known interoperability issues between Cisco BroadWorks and specific partner release(s). Issues identified during interoperability testing and known issues identified in the field are listed.

The following table provides a description of each issue and, where possible, identifies a workaround. The verified partner device versions are listed with an “X” indicating that the issue occurs in the specific release. The issues identified are device deficiencies or bugs, and are typically not Cisco BroadWorks release dependent.

The *Issue Number* is a tracking number for the issue. If it is a Polycom issue, the issue number is from Polycom’s tracking system. If it is a Cisco BroadWorks issue, the issue number is from Cisco’s tracking system.

For more information on any issues related to the particular partner device release, see the partner release notes.

Issue Number	Issue Description	Partner Version							
		5.4.0/5.4.1	5.5.0	5.5.1	5.6.0	5.7.0	5.8.0	5.9.0	6.1.0
SR# 1-793886891	User's XMPP state is changed and status erased on the XMPP server by VVX. This is observed from a buddy's device when the VVX restarts.	X	X	X	X	X	X	X	X
PR-45135	Cisco BroadWorks fails to start call recording during call setup and video network conference scenarios. Work around: None.	X	X	X	X	X	X	X	X
Polycorn release noted	OPUS audio Codec is disabled when video calling is enabled on VVX phones.			X	X	X	X	X	X
EN-32261	WebRTC video session results in voice only call. Work around: None.				X	X	X	X	X

3 Cisco BroadWorks Configuration

This section identifies the required Cisco BroadWorks device profiles for the Polycom VVX phones as well as any other unique Cisco BroadWorks configuration required for interoperability with the VVX phones.

3.1 Cisco BroadWorks Device Profile Type Configuration

This section identifies the device profile to use when deploying the Polycom VVX phones with Cisco BroadWorks.

Create a device profile type for the Polycom VVX phones with settings as shown in the following example. A separate device profile type should be created for each Polycom VVX phone model. The settings shown are recommended for use when deploying the Polycom VVX phones with Cisco BroadWorks. For an explanation of the profile parameters, see the *BroadWorks Device Management Configuration Guide* [2].

The device profile type shown in the following table provides the *Number of Ports* (number of SIP lines) setting for Polycom VVX 600. For other Polycom phone models, create a new device profile type and set the *Number of Ports* to match the available number of SIP lines per model according to the following table.

Model	Number of Lines	Video Capable
VVX 101	1	Un-checked
VVX 150	2	Un-checked
VVX 201	2	Un-checked
VVX 250	4	Un-checked
VVX 301 series, (including VVX 301/311)	6	Un-checked
VVX 350	6	Un-checked
VVX 401 series, (including VVX 401/411)	12	Un-checked
VVX 450	12	Un-checked
VVX 501	12	Checked
VVX 601	16	Checked

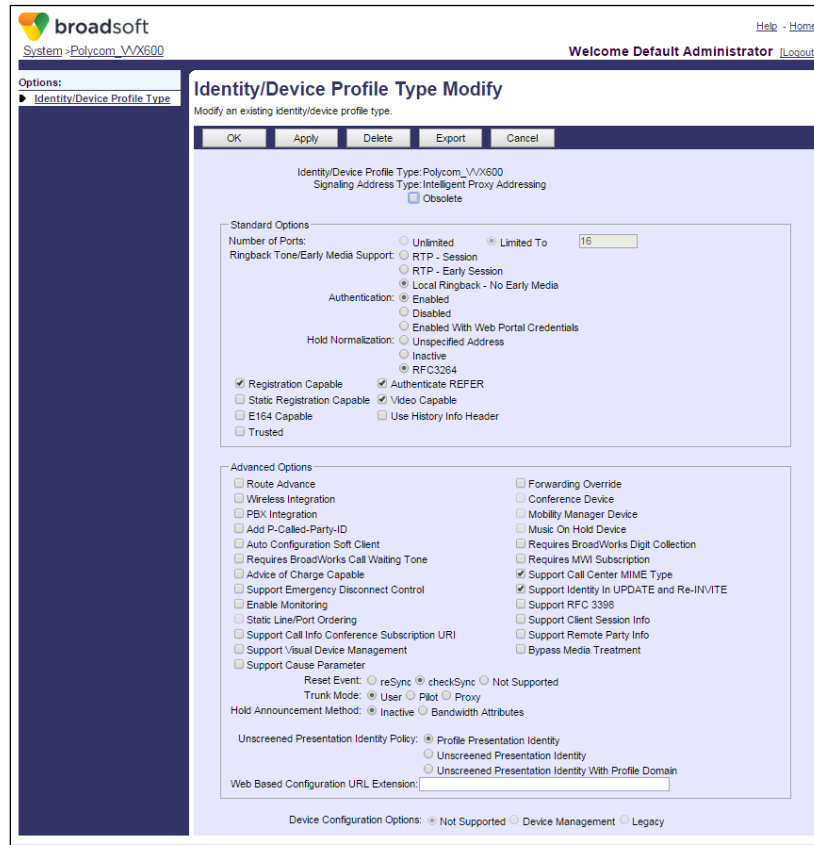


Figure 1 Device Identity/Profile Type

3.2 Cisco BroadWorks Configuration Steps

No additional Cisco BroadWorks configuration steps are required.

4 Polycom VVX Phones Configuration

This section describes the configuration settings required for the Polycom VVX phones integration with Cisco BroadWorks, primarily focusing on the SIP interface configuration. The VVX phones configuration settings identified in this section have been derived and verified through interoperability testing with Cisco BroadWorks. For configuration details not covered in this section, see the *Polycom® UC Software Administrator's Guide* [1].

4.1 Configuration Method

The Polycom VVX phones can be configured with a configuration file using the HTTP, Trivial File Transfer Protocol (TFTP) or through its embedded web server. The following examples describe how to set the parameters using a configuration file. This configuration description assumes the Polycom VVX phones use the Dynamic Host Configuration Protocol (DHCP) to get an IP address and other network settings. The VVX phones should be configured to load the configuration file each time it resets or re-synchronizes. For more information on automated provisioning, see the *Polycom® UC Software Administrator's Guide* [1].

The capabilities of the VVX phones have been verified for use with Cisco BroadWorks based on the settings described in the following table. For more information on the meaning, purposes, and applicability of the individual configuration items, see the *Polycom® UC Software Administrator's Guide* [1].

Configuration Files

Files Provided by Partner	Level	Description
sip.ld.	System	This contains the device firmware application binary.
sys.cfg	System	This contains configurable parameters in XML format. The parameters in this file are application-specific to SIP. It includes items such as proxy, register, outbound proxy, and dial plan.
phone<BWMACADDRESS>.cfg	Subscriber	This contains configurable parameters in XML format. These parameters are unique to a particular subscriber's phone. Typical parameters include the SIP registration address of record and the SIP authentication user and password. This file must be given a device specific name. It is recommended to incorporate the device's MAC address. Example: phone0004fca8a7a6.cfg

Files Provided by Partner	Level	Description
<MAC Address>.cfg	Subscriber	<p>This is the default master configuration file for the phone.</p> <p>The file must be renamed with the MAC address for the individual device (for example, 0004f200059e.cfg).</p> <p>NOTE: The hex characters must be in lowercase.</p> <p>The master configuration file for the phone identifies the file names for the application firmware, the system level, and the phone-specific configuration files.</p> <p>The listed order of the configuration files is significant. The files are processed in the order listed (from left to right).</p>

4.2 System Level Configuration

This section describes system-wide configuration items that are generally required for each VVX phone to work with Cisco BroadWorks. Subscriber-specific settings are described in the next section.

4.2.1 Configure Network Settings

Step	Command	Purpose
System Configuration File sys.cfg		
Step 1	<p>Configure the IP address on the phone.</p> <p>To use DHCP (typical and device default) set:</p> <pre>device.dhcp.enabled = "1"</pre> <p>To manually provision the IP address set:</p> <pre>device.dhcp.enabled = "0" device.net.ipAddress = "<IP address>" device.net.subnetMask = "<Network's Subnet Mask>" device.net.IPgateway = "<Default Gateway IP Address>"</pre>	To provide network configuration to the Phones.
Step 2	<p>Enter the Preferred Transport Type.</p> <p>Example:</p> <pre>voIpProt.server.1.transport="TCPP referred"</pre>	Set the Transport Protocol Type to "TCP". This is the suggested protocol to use, and prior to version 3.0.0, is required if using Busy Lamp Field (BLF).
Step 3	<p>Enter the SNTP server address.</p> <pre>device.sntp.serverName = <IP address> or <domain name string></pre> <p>Example:</p> <pre>device.sntp.serverName = "tock.usno.navy.mil"</pre>	The SNTP server from which the phone obtains the current time.
Step 4	<p>Enter the DNS server address Example:</p> <pre>device.dns.serverAddress = "8.8.8.8"</pre>	The primary server to which the phone directs DNS queries.

Step	Command	Purpose
System Configuration File sys.cfg		
Step 5	<p>Web Configuration Utility provisioning.</p> <pre>httpd.enabled = "<1 or 0>"</pre> <p>Enable or disable the complete HTTPD web client.</p> <pre>httpd.cfg.enabled = "<1 or 0>"</pre> <p>Enable or disable the Web Configuration Utility.</p> <p>*As of UCS 5.3.0, HTTPS required is the default value. Behavior can be overridden by the following parameter:</p> <pre>httpd.cfg.secureTunnelRequired="<1 or 0>"</pre> <p>HTTP is allowed if set to "0" Only HTTPS is allowed if set to "1"</p>	To enable/disable the device's web configuration Utility interface.

4.2.2 Configure SIP Interface Settings

Step	Command	Purpose
System Configuration File sys.cfg		
Step 1	<p>Enter the SIP proxy FQDN.</p> <p>Example:</p> <pre>voIpProt.server.1.address = "as.mycompany.com"</pre> <pre>voIpProt.server.1.port=""</pre>	<p>Set the SIP server to the Fully Qualified Domain Name (FQDN) of the Cisco BroadWorks Application Server cluster.</p> <p>This FQDN must match the domain configured for the Cisco BroadWorks subscriber's line/port domain.</p>
Step 2	<p>Enter the Preferred Transport Type.</p> <p>Example:</p> <pre>voIpProt.server.1.transport="TCPpREFERRED"</pre>	<p>Set the Transport Protocol Type to "TCP". This is the suggested protocol to use, and prior to version 3.0.0, is required if using Busy Lamp Field (BLF).</p>
Step 3	<p>Enter the Outbound Proxy.</p> <p>Example:</p> <pre>voIpProt.SIP.outboundProxy.address = "sbc.broadworks.com"</pre> <pre>voIpProt.SIP.outboundProxy.port = ""</pre>	<p>Set the Outbound Proxy to the Session Border Controller (SBC) if one is deployed between Polycom and Cisco BroadWorks.</p> <p>If there are redundant SBCs, set it to the FQDN for the SBC cluster.</p>

4.2.3 Configure Service Settings

Step	Command	Purpose
Step 1	Configure the dial plan. Example: <pre><dialplan> dialplan.digitmap="[2346789]11 [0-1] [2-9]11 0[#T] 00 01 [2-9]xx.[#T]*xx #xx 011x.[#T] [0-1]xxxxxxxx[#T] [0-1] [2-9]xxxxxxxx [2-9]xxxxxxxx [2-9]xxxxxxxx [2-9]xxxxxxxx [2-9]xxxxxxxx[#T] 101xxxx.[#T] 11 [2-9]x.[#T]"</pre>	Configure the dial plan as necessary for the deployment or locale. The dial plan is configured as a string compatible with the MGCP-style Digit Maps described in <i>RFC 3435</i> . When using Cisco BroadWorks Speed Dial 100 feature, include the necessary digit map pattern. The default pattern is "#xx".
Step 2	Configure the timeout for dialed digits. <pre><dialplan> dialplan.digitmap.timeOut="3"</pre>	This is the timeout (in seconds) for the "T" feature of the digit map. Make sure it is set to the default, which is "3".
Step 3	Configure the alert header information for distinctive ring/call waiting. Example: <pre><alertInfo voIpProt.SIP.alertInfo.1.value="http://127.0.0.1/Bellcore-dr2" voIpProt.SIP.alertInfo.1.class="custom1" voIpProt.SIP.alertInfo.2.value="http://127.0.0.1/Bellcore-dr3" voIpProt.SIP.alertInfo.2.class="custom2" voIpProt.SIP.alertInfo.3.value="http://127.0.0.1/Bellcore-dr4" voIpProt.SIP.alertInfo.3.class="custom3" voIpProt.SIP.alertInfo.4.value="http://127.0.0.1/Bellcore-dr5" voIpProt.SIP.alertInfo.4.class="custom1"</pre>	Configure the alert header information to enable distinctive alerting (priority alerting, alternate numbers). The <i>alertInfo.X.value</i> field must not be NULL. Do not set <i>voIpProt.SIP.alertInfo.X.value=""</i> . Cisco BroadWorks uses specific Bellcore settings for the following features: Priority Alerting: http://127.0.0.1/Bellcore-dr2 Alternate Numbers: http://127.0.0.1/Bellcore-dr3 http://127.0.0.1/Bellcore-dr4 Ring Splash: http://127.0.0.1/Bellcore-dr5
Step 4	Enable Advanced Call Control. <pre><alertInfo Add Auto-Answer: voIpProt.SIP.alertInfo.5.value="auto-answer" voIpProt.SIP.alertInfo.5.class="autoAnswer"</pre>	Configure the <i>Auto-Answer alert</i> header to enable Cisco BroadWorks Advanced Call Control features via the Cisco BroadWorks Call Manager (Click to Answer, Click to Dial).
Step 5	Enable Silent Alert. <pre>voIpProt.SIP.alertInfo.6.value=http://127.0.0.1/silent voIpProt.SIP.alertInfo.6.class="visual"</pre>	Configure the phone to turn on the call screen but not provide audible alerting ring when Cisco BroadWorks sends "Alert-Info: http://127.0.0.1/silent " in the incoming INVITE.

Step	Command	Purpose
Step 6	Configure Register. <pre><server voIpProt.server.1.expires="7200" voIpProt.server.1.register="1"</pre>	Configure the register and set the expiration to "7200" seconds, which is recommended.
Step 7	Enable phone so that it always restarts on checkSync. <pre><specialEvent voIpProt.SIP.specialEvent.checkSyn c.alwaysReboot="1"</pre>	Enable the phone so that it always restarts when the Cisco BroadWorks device reset button is selected.
Step 8	Enable RFC 3264 Hold. <pre><SIP useRFC3264HoldOnly="1"</pre> <p>For release prior to UC Software 4.1.5:</p> <pre><SIP voIpProt.SIP.useRFC2543hold="0" voIpProt.SIP.useSendOnlyHold="1"</pre>	Enable the phone to use <i>RFC 3264</i> Hold (default) and to send "sendOnly" in the hold SDP rather than "inactive".
Step 9	Enable Authentication Optimization. <pre><SIP voIpProt.SIP.authOptimizedInFailov er = "1"</pre>	Enable the phone, in failover conditions, to send INVITEs with Authentication credentials to the same Application Server that responded with the 401 challenge.
Step 10	(Optional) Configure Network-managed Conferencing URI. <pre><conference voIpProt.SIP.conference.address="c onference@mycompany.com"/></pre>	(Optional) Configure the conferencing unit to allow network-based conferences to be established from the Polycom device for Three-Way Calling.
Step 11	(Optional) Enable transfer while ringing. <pre><SIP voIpProt.SIP.allowTransferOnProcee ding = "1"</pre>	(Optional) Enable the transfer of calls while the transfer-to party is ringing.
Step 12	(Optional) Enable device authentication of SIP requests from Cisco BroadWorks. Example: <pre><requestValidation voIpProt.SIP.requestValidation.1.r equest="INVITE" voIpProt.SIP.requestValidation.1.m ethod="digest" voIpProt.SIP.requestValidation.dig est.realm="as.mycompany.com"</pre>	(Optional) Configure the device to challenge SIP requests from Cisco BroadWorks. The configuration parameters identify, which SIP requests are challenged by the phone using digest authentication. The registered authentication credentials (user/password) are used for the challenge.
Step 13	(Optional) Set SIP Session Timer Example: <pre>voIpProt.SIP.keepalive.sessionTime rs="1"</pre>	To enable the session timer, set it to "1". If it is set to "0", then the session timer is disabled, and the phone does not declare the "timer" in the <i>Support</i> header in the INVITE. Note that the phone still responds to a re-INVITE or UPDATE. However, the phone does not try to re-INVITE or do an UPDATE even if the remote end should make a request for it. The default value is "0".

Step	Command	Purpose
Step 14	(Optional) Enable Single Key Conference Example: <code>Call.singleKeyPressConference="1"</code>	If set to 1, the conference will be set up after, a user presses the Conference soft key or Conference key the first time. In addition, all sound effects (dial tone, DTMF tone while dialing and ringing back) are heard by all existing participants in the conference. This setting will enable conference before answer and n-Way call scenarios.

4.3 Subscriber Level Configuration

This section identifies the device-specific parameters, including registration and authentication. These settings must be unique across the devices to be matched with the settings for a Cisco BroadWorks subscriber.

Provisioning a subscriber to register with Cisco BroadWorks allows calls to terminate to the subscriber's line. Registration requires that a unique address of record (AoR) is provisioned on Cisco BroadWorks and the phone; provisioning an AoR on Cisco BroadWorks consists of setting the line/port parameter to a unique value in the Application Server cluster.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Configure display name. Example: <pre><reg> reg.1.displayName="Bob Smith" reg.2.displayName="Joe Brown"</pre>	The display name is used for the local user interface, as well as SIP signaling. Configure for each line ("reg.x") in use, where "x" is the line number.
Step 2	Configure the register user ID. Example: <pre><reg> reg.1.address="2405551111" reg.2.address="2405552222"</pre>	The register address must match the line/port setting on Cisco BroadWorks. Configure for each line ("reg.x") in use, where "x" is the line number.
Step 3	Enable SIP authentication for each line. Example: <pre><reg> reg.1.auth.userId="1111@as.mycompany.com" reg.1.auth.password="welcome" reg.2.auth.userId="2222@as.mycompany.com" reg.2.auth.password="welcome"</pre>	If the Authentication service is configured on Cisco BroadWorks, then these parameters must be configured to match the Cisco BroadWorks settings. Configure for each line ("reg.x") in use, where "x" is the line number.
Step 4	Configure the line label. Example: <pre><reg> reg.1.label="1111" reg.2.label="2222"</pre>	The label is shown next to the line on the phone. Configure for each line ("reg.x") in use, where "x" is the line number.
Step 5	Set the line type. <pre><reg> reg.1.type="private" reg.2.type="private"</pre>	Set the line type to "private" unless you are configuring the phone for Shared Call Appearance. See the following for Shared Call Appearance configuration requirements. Configure for each line ("reg.x") in use, where "x" is the line number.
Step 6	(Optional) Configure solicited MWI subscription. Example: <pre><msg msg.mwi.1.subscribe="2403330000"></pre>	If this is set to "non-Null", then the phone sends a SUBSCRIBE request to this contact after booting up. The default value is "Null".

4.3.1 Attendant Console Configuration

The Polycom VVX phone models can be expanded to support up to 16 registering lines. Configure lines 1 through 16 on the VVX phone models, (see the configuration instructions in section [4.3 Subscriber Level Configuration](#)). The remaining soft buttons can be configured for speed dial or other functions, such as Push To Talk or transfer to another user's voice mailbox.

To add a Push To Talk key to the phone, perform the following steps:

- 1) Make sure the user is assigned the Push To Talk feature on Cisco BroadWorks.
- 2) Click the **Directories** button on the phone.
- 3) Select the *Contact* directory.
- 4) To add a new contact, click the **Add** button.
- 5) Enter the key label parameters. The key label uses the *First* and *Last Name* fields for the display. Enter the data you wish for this key.
- 6) In the *Contact* field, enter the Push To Talk feature access code (FAC) and the user directory number (DN) or extension to dial, that is, *501212.
- 7) Click the **Save** button to store the information.
- 8) After the speed dial entry has been added, click on the speed dial entry, and then click "Add To Favorites". The favorite entry is shown on the phone's idle screen.

NOTE: The remote phone must support the auto answer functionality.

To add a Voice Mail Transfer key, perform the following steps:

- 1) Click the **Directories** button on the phone.
- 2) Select the *Contact* directory.
- 3) To add a new contact, click the **Add** button.
- 4) Enter the key label parameters. The key label uses the *First* and *Last Name* fields for the display. Enter the data you want for this key.
- 5) In the *Contact* field, enter the direct transfer to voice mail FAC code and the user DN or extension to dial, that is, *551212.
- 6) Click the **Save** button to store the information.

To add a Speed Dial key, perform the following steps:

- 1) Click the **Directories** button on the phone.
- 2) Select the *Contact* directory.
- 3) To add a new contact, click the **Add** button.
- 4) Enter the key label parameters. The key label uses the *First* and *Last Name* fields for the display. Enter the data you want for this key.
- 5) In the *Contact* field, enter the user DN to dial.
- 6) Click the **Save** button to store the information.
- 7) After the speed dial entry has been added, click on the speed dial entry, and then click "Add To Favorites". The favorite entry is shown on the phone's idle screen.

4.4 Advanced SIP Features Configuration

This section provides configuration instructions for advanced SIP features supported by the phone including but not limited to Shared Call Appearance, Busy Lamp Field, Feature Key Synchronization, Call Center, and Emergency Call.

4.4.1 Shared Call Appearance Configuration

The Shared Call Appearance (SCA) feature allows the administrator to add multiple locations to a given line. Any of the locations can be used to originate or receive calls.

When a call comes in to an idle line, all the provisioned locations for that line are alerted. The first location to answer the call is connected to the originator. If the line is already active in a call, only the active location is alerted.

A subscriber can originate calls from any of the configured locations. All other locations are unable to originate calls until all calls are released.

It is recommended that the phone number plus an index (<phoneNumber>_<index>) be used when provisioning the unique address of record (AoR) for each shared line, for example: 2405551111_2. If the phone number does not exist, then the MAC address plus an index could be used (<macAddress>_<index>).

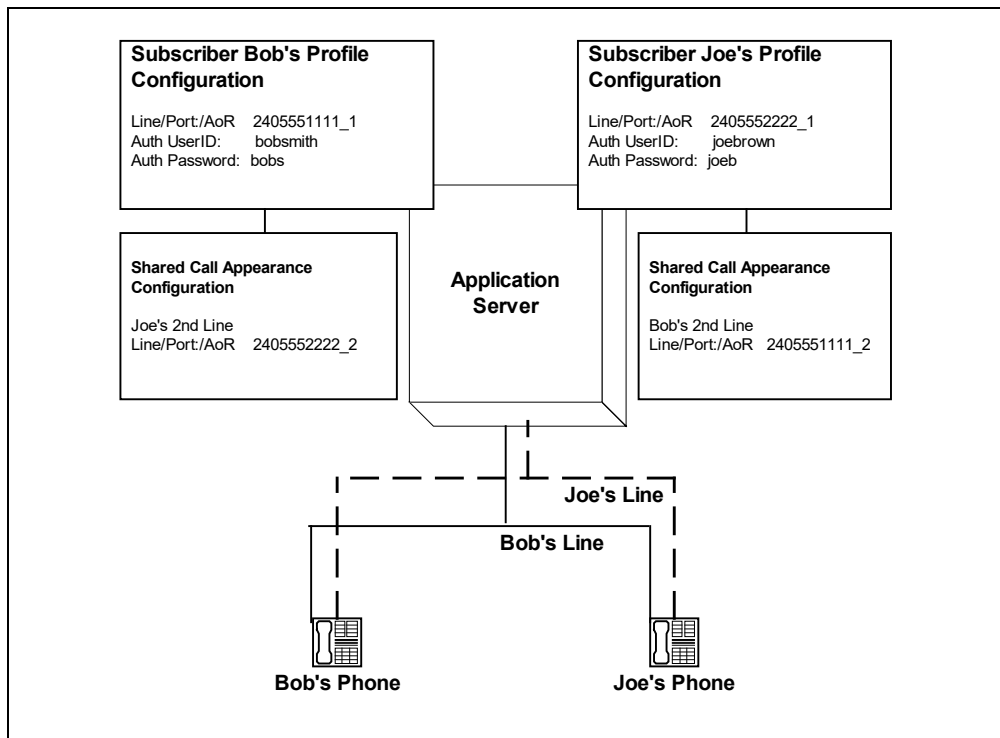


Figure 2 Shared Call Appearance Configuration

Figure 1 Shared Call Appearance Configuration shows that Bob and Joe each have two lines and that Bob shares a line with Joe and Joe shares a line with Bob. The figure also shows the applicable Subscriber Profile and Shared Call Appearance Configuration data for subscribers Bob and Joe.

When Bob is called (2405551111), Bob's first line will ring, and Joe's second line will ring. When Joe is called (2405552222), Joe's first line will ring and Bob's second line will ring.

The following steps show how to configure both phones for this Shared Call Appearance configuration.

4.4.1.1 Bob's Phone Configuration – phone<BWMACADDRESS>.cfg

The following steps are used to configure line 1 for Bob's phone. This line rings when Bob is called, so it has Bob's authentication information.

Step	Command	Purpose
Subscriber Configuration File (Bob's phone<BWMACADDRESS>.cfg)		
Step 1	Enable shared line. <code>reg.1.type="shared"</code>	Configure the line as "shared" (as opposed to "private").
Step 2	Configure the phone label. Example: <code>reg.1.label="Bob"</code>	The label is displayed on the phone next to the line key.
Step 3	Configure the register user ID. Example: <code>reg.1.address="2405551111_1"</code>	This is the register user ID, which is used to register Bob's line 1 with Cisco BroadWorks. This should match Bob's <i>line/port</i> field on the <i>Subscriber Profile</i> page.
Step 4	Enable SIP Authentication for the line. Example: <code>reg.1.auth.userid="bobsmith"</code> <code>reg.1.auth.password="bobs"</code>	If the Authentication service is configured on Cisco BroadWorks, these parameters must be configured to match the Cisco BroadWorks settings. This line rings when Bob is called, and so it has Bob's Authentication information.
Step 5	(Optional) Enable Barge-In. <code>reg.1.bargeInEnabled="1"</code>	(Optional) Enable the line for barge-in attempts on active SCA calls.
Step 6	(Optional) Enable Private Hold. <code>reg.1.enablePvtHoldSoftKey="1"</code>	(Optional) Enable the SCA lines to hold calls privately in addition to public call hold. *Available on UCS 5.3.0 or above.
Step 7	(Optional) Enable Call Forwarding on Shared Lines <code>voIpProt.SIP.serverFeatureControl.cf="1"</code> <code>divert.1.sharedDisabled="0"</code> <code>voIpProt.SIP.serverFeatureControl.localProcessing.cf="0"</code> <code>call.shared.disableDivert="0"</code>	(Optional) Enable the SCA lines to perform Call Forwarding. *Available on UCS 5.3.0 or above.

Step	Command	Purpose
Subscriber Configuration File (Bob's phone<BWMACADDRESS>.cfg)		
Step 8	(Optional) Enable Call Park Notification on Shared Lines <pre>call.parkedCallRetrieveString="<FAC for call park retrieve>" reg.1.enhancedCallPark.enabled="1" reg.1.lineAddress="<Bob's phone extension>" feature.enhancedCallPark.allowAudioN otification="1 or 0" Set to 1 for audio notification when call is parked against Bob.</pre>	(Optional) Enable the SCA lines to receive Call Park Notification. *Available on UCS 5.3.0 or above.

The following steps are used to configure line 2 for Bob's phone. This line rings when Joe is called, and so it has Joe's authentication information.

Step	Command	Purpose
Subscriber Configuration File (Bob's phone<BWMACADDRESS>.cfg)		
Step 1	Enable shared line. <pre>reg.2.type="shared"</pre>	This is a shared line, and so the type is set to "shared".
Step 2	Configure the phone label. Example: <pre>reg.2.label="Joe"</pre>	The label is displayed on the phone next to the line key.
Step 3	Configure the register user ID. Example: <pre>reg.2.address="2405551111_2"</pre>	This is the register user ID, which is used to register Bob's line 2 with Cisco BroadWorks. This should match the SCA <i>line/port</i> field on Joe's <i>Shared Call Appearance</i> page.
Step 4	Enable SIP Authentication for the line. Example: <pre>reg.2.auth.userid="joebrown" reg.2.auth.password="joeb"</pre>	If the Authentication service is configured on Cisco BroadWorks, then these parameters must be configured to match the Cisco BroadWorks settings. This line rings when Joe is called, and so it has Joe's Authentication information.
Step 5	(Optional) Enable Barge-In. <pre>reg.2.bargeInEnabled="1"</pre>	(Optional) Enable the line for barge-in attempts on active SCA calls.
Step 6	(Optional) Enable Private Hold. <pre>reg.2.enablePvtHoldSoftKey="1"</pre>	(Optional) Enable the SCA lines to hold calls privately in addition to public call hold. *Available on UCS 5.3.0 or above.

Step	Command	Purpose
Subscriber Configuration File (Bob's phone<BWMACADDRESS>.cfg)		
Step 7	(Optional) Enable Call Forwarding on Shared Lines <pre> voIpProt.SIP.serverFeatureControl.cf ="1" divert.2.sharedDisabled="0" voIpProt.SIP.serverFeatureControl.lo calProcessing.cf="0" call.shared.disableDivert="0" </pre>	(Optional) Enable the SCA lines to perform Call Forwarding. *Available on UCS 5.3.0 or above.
Step 8	(Optional) Enable Call Park Notification on Shared Lines <pre> call.parkedCallRetrieveString="<FAC for call park retrieve>" reg.2.enhancedCallPark.enabled="1" reg.2.lineAddress="<Joe's phone extension>" feature.enhancedCallPark.allowAudioN otification="1 or 0" </pre> Set to 1 for audio notification when call is parked against Joe.	(Optional) Enable the SCA lines to receive Call Park Notification. *Available on UCS 5.3.0 or above.

4.4.1.2 Joe's Phone Configuration – phone<BWMACADDRESS>.cfg

The following steps are used to configure line 1 for Joe's phone. This line rings when Joe is called, so it has Joe's authentication information.

Step	Command	Purpose
Subscriber Configuration File (Joe's phone<BWMACADDRESS>.cfg)		
Step 1	Enable shared line. <code>reg.1.type="shared"</code>	This is a shared line, and so the type is set to "shared".
Step 2	Configure the phone label. Example: <code>reg.1.label="Joe"</code>	The label is displayed on the phone next to the line key.
Step 3	Configure the register user ID. Example: <code>reg.1.address="2405552222_1"</code>	This is the register user ID, which is used to register Joe's line 1 with Cisco BroadWorks. This should match Joe's line/port field on the <i>Subscriber Profile</i> page.
Step 4	Enable SIP Authentication for the line. Example: <code>reg.1.auth.userid="joebrown"</code> <code>reg.1.auth.password="joeb"</code>	If the Authentication service is configured on Cisco BroadWorks, then these parameters must be configured to match the Cisco BroadWorks settings. This line rings when Joe is called, and so it has Joe's authentication information.
Step 5	(Optional) Enable Barge-In. <code>reg.1.bargeInEnabled="1"</code>	(Optional) Enable the line for barge-in attempts on active SCA calls.
Step 6	(Optional) Enable Private Hold. <code>reg.1.enablePvtHoldSoftKey="1"</code>	(Optional) Enable the SCA lines to hold calls privately in addition to public call hold. *Available on UCS 5.3.0 or above.
Step 7	(Optional) Enable Call Forwarding on Shared Lines. <code>voIpProt.SIP.serverFeatureControl.cf="1"</code> <code>divert.1.sharedDisabled="0"</code> <code>voIpProt.SIP.serverFeatureControl.localProcessing.cf="0"</code> <code>call.shared.disableDivert="0"</code>	(Optional) Enable the SCA lines to perform Call Forwarding. *Available on UCS 5.3.0 or above.
Step 8	(Optional) Enable Call Park Notification on Shared Lines <code>call.parkedCallRetrieveString="<FAC for call park retrieve>"</code> <code>reg.1.enhancedCallPark.enabled="1"</code> <code>reg.1.lineAddress="<Joe's phone extension>"</code> <code>feature.enhancedCallPark.allowAudioNotification="1 or 0"</code> Set to 1 for audio notification when call is parked against Joe.	(Optional) Enable the SCA lines to receive Call Park Notification. *Available on UCS 5.3.0 or above.

The following steps are used to configure line 2 for Joe's phone. This line rings when Bob is called, so it has Bob's authentication information.

Step	Command	Purpose
Subscriber Configuration File (Joe's phone<BWMACADDRESS>.cfg)		
Step 1	Enable shared line. <code>reg.2.type="shared"</code>	This is a shared line, and so the type is set to "shared".
Step 2	Configure the phone label. Example: <code>reg.2.label="Bob"</code>	The label is displayed on the phone next to the line key.
Step 3	Configure the register user ID. Example: <code>reg.2.address="2405552222_2"</code>	This is the register user ID, which is used to register Joe's line 2 with Cisco BroadWorks. This should match the SCA <i>line/port</i> field on Bob's <i>Shared Call Appearance</i> page.
Step 4	Enable SIP Authentication for the line. Example: <code>reg.2.auth.userid="bobsmith"</code> <code>reg.2.auth.password="bobs"</code>	If the Authentication service is configured on Cisco BroadWorks, then these parameters must be configured to match the Cisco BroadWorks settings. This line rings when Bob is called, and so it has Bob's authentication information.
Step 5	(Optional) Enable Barge-In. <code>2reg.2.bargeInEnabled="1"</code>	(Optional) Enable the line for barge-in attempts on active SCA calls.
Step 6	(Optional) Enable Private Hold. <code>reg.2.enablePvtHoldSoftKey="1"</code>	(Optional) Enable the SCA lines to hold calls privately in addition to public call hold. *Available on UCS 5.3.0 or above.
Step 7	(Optional) Enable Call Forwarding on Shared Lines <code>voIpProt.SIP.serverFeatureControl.cf="1"</code> <code>divert.2.sharedDisabled="0"</code> <code>voIpProt.SIP.serverFeatureControl.localProcessing.cf="0"</code> <code>call.shared.disableDivert="0"</code>	(Optional) Enable the SCA lines to perform Call Forwarding. *Available on UCS 5.3.0 or above.
Step 8	(Optional) Enable Call Park Notification on Shared Lines <code>call.parkedCallRetrieveString="<FAC for call park retrieve>"</code> <code>reg.2.enhancedCallPark.enabled="1"</code> <code>reg.2.lineAddress="<Bob's phone extension>"</code> <code>feature.enhancedCallPark.allowAudioNotification="1 or 0"</code> Set to 1 for audio notification when call is parked against Bob.	(Optional) Enable the SCA lines to receive Call Park Notification. *Available on UCS 5.3.0 or above.

4.4.1.3 Hybrid Key System Configuration

Hybrid Key System emulation requires the phone to support assignment of multiple line keys to a single registering line on the phone. It also requires the phone to limit each line key to a single call appearance or provide the configurability to roll a new call over to the next free line key. Any of the locations can be used to originate or receive calls.

Step	Command	Purpose
Subscriber Configuration File (<BWMACADDRESS>.cfg)		
Step 1	Enable hybrid keys. <pre>reg.x.lineKeys="<number of keys>"</pre> Example: <pre>reg.1.lineKeys="3"</pre> This will place 3 keys on the UI to represent line 1 of the phone.	This defines the number of line keys for a specific registration.

4.4.2 Busy Lamp Field Configuration

The Busy Lamp Field (BLF) feature allows the VVX phones to monitor the call state for one or more Cisco BroadWorks users (who are configured in the same Cisco BroadWorks group as the Polycom desktop phone).

The VVX phone sends a SIP SUBSCRIBE message to the Application Server indicating which BLF list it wants to monitor. After the Application Server completes sending the SIP NOTIFY message that includes all of the Cisco BroadWorks users who are members of the BLF list to which the VVX phone is subscribed, the Application Server then sends call state change SIP NOTIFY messages every time a Cisco BroadWorks user who is part of the BLF list changes their call state. For more information regarding to Polycom UC Software Devices' support of BLF, see Polycom's Knowledgebase Quick Tip 37381 on BLF enhancements available from Polycom.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Configure the BLF URI that the Polycom VVX phone subscribes to. <pre><attendant attendant.uri="8080blf@as.mycompany.com " attendant.reg="" /></pre>	This configures the Polycom VVX phone to subscribe to a Busy Lamp Field list, which allows the status of each Cisco BroadWorks user, who is part of the BLF list, to be monitored from this Polycom UCS phone.
Step 2	(Optional) BLF through TCP protocol override configuration. Append ";transport=TCP" to the BLF URI from "Step 1" to override the BLF network protocol. <pre><attendant attendant.uri="8080blf@as.mycompany.com;transport=TCP" attendant.reg="" /></pre>	While maintaining the general transport protocol of the SIP signaling from a Polycom UCS phone to Cisco BroadWorks, this alteration forces the Polycom UCS phone to use TCP as the transport protocol to perform BLF signaling. NOTE: This optional configuration is not applicable when Outbound Proxy (OBP) is being used. Force the use of TCP protocol for SIP signaling on the OBP if TCP is required for BLF.

4.4.3 Feature Key Synchronization

Feature Key Synchronization provides synchronization of phone services such as *Call Forwarding* and *Do Not Disturb* with the settings on Cisco BroadWorks for the analogous services. Configuration of the phone to enable Feature Key Synchronization is described as follows.

To enable feature key synchronization for Do Not Disturb, Call Forwarding Always, Call Forwarding Busy, and Call Forwarding No Answer, follow the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Configure the Feature Key Synchronization for the Polycom VVX. <pre>voIpProt.SIP.serverFeatureControl.dnd="1" voIpProt.SIP.serverFeatureControl.cf="1"</pre>	This enables the Polycom VVX phone to synchronize feature status with the Cisco BroadWorks Application Server. After successful registration, the Polycom VVX phone sends an empty body SUBSCRIBE message with the <i>Event</i> header, <i>as-feature-key</i> .
Step 2	Disable the local message processing associated with Feature Key Synchronization. <pre>reg.1.serverFeatureControl.localProcessing.dnd="0" reg.1.serverFeatureControl.localProcessing.cf="0"</pre>	This disables local message processing on the phone such that the phone would not send a response code for incoming messages to invoke splash tones. The default value is "1".
Step 3	(Optional) Enable Call Forwarding on Shared Lines <pre>voIpProt.SIP.serverFeatureControl.cf="1" divert.1.sharedDisabled="0" voIpProt.SIP.serverFeatureControl.localProcessing.cf="0" call.shared.disableDivert="0"</pre>	(Optional) Enable the SCA lines to perform Call Forwarding. *Available on UCS 5.3.0 or above.

4.4.4 Call Center Configuration

This section provides configuration instructions to configure the phone to enable integration with Cisco BroadWorks Call Center Configuration.

Cisco BroadWorks Call Center feature is supported through Polycom's Automatic Call Distribution (ACD), to enable this feature, follow the steps in the following table. ACD can only be configured on private lines; it is not supported on shared lines. Further, the VVX Phones is unable to simultaneously support Hoteling feature with the Cisco BroadWorks Call Center feature.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Set ACD signaling method to call center type. <pre>voIpProt.SIP.acd.signalingMethod="1"</pre>	The Polycom phone supports two methods for ACD functionality. For interoperability with Cisco BroadWorks, set the method to "1".
Step 2	Enable ACD Login/Logout. <pre>feature.acdLoginLogout.enabled="1"</pre>	ACD sign-in/sign-out must be enabled for basic and premium ACD feature synchronization.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 3	Enable ACD Agent availability. feature.acdAgentAvailability.enabled="1"	ACD agent availability status must be enabled for basic and premium ACD feature synchronization.
Step 4	Enable ACD service controller URI. feature.acdServiceControllerUri.enabled="1"	ACD service controller URI must be enabled for basic and premium ACD feature synchronization.
Step 5	Enable enhanced feature keys. feature.enhancedFeatureKeys.enabled="1"	Enhanced feature keys must be enabled for premium ACD feature synchronization.
Step 6	Set ACD registration line. acd.reg=<reg_index> Example: acd.reg="1"	Identifies the registration index to be used for feature synchronized ACD. If null, the default is "1".
Step 7	Set sign-in state. acd.stateAtSignIn="1"	Identifies the user's state as sign-in. "1" – sign-in state is <i>Available</i> . "0" – sign-in state is <i>Unavailable</i> .
Step 8	Enable unavailable reason code. acd.x.unavailreason.active=1 Examples: acd.1.unavailreason.active=1 acd.2.unavailreason.active=2	Enables individual unavailable reason codes for premium ACD.
Step 9	Configure unavailable reason codes. acd.x.unavailreason.codeValue=<string> acd.x.unavailreason.codeName=<string> Examples: acd.1.unavailreason.codeValue="10001" acd.1.unavailreason.codeName="Out to Lunch" acd.2.unavailreason.codeValue="10002" acd.2.unavailreason.codeName="On the Phone"	Sets the numeric and text values for unavailable reason codes.

4.4.5 Hoteling and Flexible Seating Feature Configuration

This section provides configuration instructions to configure the phone to enable integration with BroadWorks Hoteling feature or Flexible Seating feature. The BroadWorks Hoteling and Flexible Seating Feature are similar where both features allow a capable device to associate with a separate user's profile. The BroadWorks Hoteling feature has specific host-guest association signaling requirement where the device must support the SIP Subscribe and Notify "x-broadworks-hoteling" event package. The BroadWorks Flexible Seating feature is similar in concept as hoteling feature with the exception where the requirement of host-guest association requirement is reduced to the support of Cisco BroadWorks Device Management and Remote Restart. For Flexible Seating, the "x-broadworks-hoteling" event package is only required if the host-guest association is to be performed by the device. The VVX Phones provides support for both features using an alternative ACD signaling method to enable these features.

For Hoteling Feature:

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Set ACD signaling method to alternative type. <code>voIpProt.SIP.acd.signalingMethod="0"</code>	Set the method to "0" for Hoteling.
Step 2	Disable ACD Login/Logout. <code>feature.acdLoginLogout.enabled="0"</code>	The ACD sign-in/sign-out must be disabled for Hoteling.
Step 3	Disable ACD Agent availability. <code>feature.acdAgentAvailability.enabled="0"</code>	The ACD agent availability status must be enabled for basic and premium ACD feature synchronization.
Step 4	Disable ACD service controller URI. <code>feature.acdServiceControllerUri.enabled="0"</code>	The ACD service controller URI must be disabled for Hoteling.
Step 5	Enable enhanced feature keys. <code>feature.enhancedFeatureKeys.enabled="1"</code>	The enhanced feature keys must be enabled.
Step 6	Set Hoteling registration line. <code>hoteling.reg=<reg index></code> Example: <code>hoteling.reg="1"</code>	This identifies the registration index to be used for Hoteling feature synchronization. If null, the default is "1". %BWHOTELINGLINE-x% tag used.
Step 7	Enabling Hoteling <code>feature.hoteling.enabled="1"</code>	This enables the Hoteling - feature. %BWHOTELINGMODE-x% tag used. Flexible Seating and Hoteling are not compatible with each other. If Flexible Seating is enabled, then the <code>hotelingMode.type</code> parameter overrides the <code>feature.hoteling.enable</code> parameter.
Step 8	Set Hoteling Mode type <code>hotelingMode.type="1"</code>	This sets the Hoteling mode type to Hoteling feature. %BWHOTELINGMODE-x% tag used.

Flexible Seating Feature can be configured with ACD or without ACD. See the ACD section for enabling ACD (UCS 5.5.0 and newer).

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Set Hoteling Mode type <code>hotelMode.type="%BWHOTELINGMODE-x%"</code> example: <code>hotelMode.type="2"</code>	Set the method to "2" for Flexible Seating feature. %BWHOTELINGMODE-x% tag used.
Step 2	Set Flexible Seating registration line. <code>hotelMode.reg="%BWHOTELINGLINE-x%"</code> Example: <code>hotelMode.reg="1"</code>	This identifies the registration index to be used for Flexible seating guest signing/out. If null, the default is "1". %BWHOTELINGLINE-x% tag used.
Step 3	Set Unlock PIN <code>fs.unlockPhone.pin="%BWFLEXIBLESEATINGUNLOCKPIN-x%"</code>	This sets the security pin for the Flexible Seating guest line on the host phone. %BWFLEXIBLESEATINGUNLOCKPIN-x% tag used.
Step 4	Configure the Feature Key Synchronization for the Polycom VVX. <code>volpProt.SIP.serverFeatureControl.dnd="1"</code> <code>volpProt.SIP.serverFeatureControl.cf="1"</code>	This enables the Polycom VVX phone to synchronize feature status with the Cisco BroadWorks Application Server. After successful registration, the Polycom VVX phone sends an empty body SUBSCRIBE message with the Event header, as-feature-key.
Step 5	Disable the local message processing associated with Feature Key Synchronization. <code>reg.1.serverFeatureControl.localProcessing.dnd="0"</code> <code>reg.1.serverFeatureControl.localProcessing.cf="0"</code>	This disables local message processing on the phone such that the phone would not send a response code for incoming messages to invoke splash tones. The default value is "1". Flexible Seating feature is not compatible with local call forwarding.

4.4.6 Call Recording Feature Configuration

This section provides configuration instructions to configure the phone to enable integration with BroadWorks Call Recording feature.

To enable BroadWorks Call Recording feature, follow the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable Call Recording for each line. <code>reg.x.serverFeatureControl.callRecording="1"</code> Example: <code>reg.1.serverFeatureControl.callRecording="1"</code> <code>reg.2.serverFeatureControl.callRecording="1"</code>	The Polycom phone supports Call Recording feature: "1" – The call recording feature is <i>Enabled</i> . "0" – The call recording feature is <i>Disabled</i> .

4.4.7 Security Classification Feature Configuration

This section provides configuration instructions to configure the phone to enable integration with BroadWorks Security Classification feature.

To enable BroadWorks Security Classification feature, follow the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable security classification for each line. <code>reg.1.serverFeatureControl.securityClassification="1"</code> <code>reg.2.serverFeatureControl.securityClassification="1"</code>	The Polycom phone supports Security Classification feature: "1" – The security classification feature is <i>Enabled</i> . "0" – The security classification feature is <i>Disabled</i> .

4.5 Xtended Services Interface Feature Configuration

This section provides configuration instructions for configuration of Xtended Services Interface (Xsi) features supported by the phone, including but not limited to, BroadWorks Directory and Cisco BroadWorks Call Logs.

4.5.1 Xtended Services Interface Authentication Method

The phone must authenticate with the Xtended Services Interface to access the available features. This section identifies the authentication method(s) supported by the phone and the configuration required.

The VVX phones provide support Xsi Authentication using the preferred SIP credentials as well as the Xsi username/password.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	<p>For UCS release 5.3.0 or later, enable Xsi authentication using the user's SIP credential.</p> <pre>dir.broadsoft.regMap="1" (or the registration line that will be used to authenticate with XSP for XSI access) dir.broadsoft.useXspCredentials="0" reg.x.broadsoft.userId="<User's Xsi Login ID>" reg.x.auth.userId="<User's SIP authentication username>" reg.x.auth.password="<User's SIP authentication password>"</pre> <p>For enabling Xsi authentication using the non-preferred web portal login username/password.</p> <pre>dir.broadsoft.regMap="1" (or the registration line that will be used to authenticate with XSP for XSI access) dir.broadsoft.useXspCredentials="1" dir.broadsoft.xsp.username="<username>" dir.broadsoft.xsp.password="<password>"</pre>	Configure the Xsi service authentication method user either the preferred SIP credential of the user or user's web portal login username/password.

4.5.2 Cisco BroadWorks Directory

The Cisco BroadWorks Directory service makes access to the directories associated with a user account through the Cisco BroadWorks Xtended Services Interface. Using this service means that the user's credentials must be provisioned on the Xtended Services Interface. Since UCS 5.5.2, the VVX phones' Cisco BroadWorks Directory support include the Enterprise Directory, the Group Directory, and the Personal Directory.

4.5.2.1 Cisco BroadWorks Enterprise Directory

The format for the web link for the Cisco BroadWorks Enterprise Directory service is as follows: *http(s)://<XSP hostaddress:port>/com.broadsoft.xsi-actions/v2.0/user/<userid>/directories/enterprise.*

The Cisco BroadWorks Directory can only be enabled on one line (user account) for each supported VVX Phone. To enable the Cisco BroadWorks Enterprise Directory service on the phone, perform the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable the Cisco BroadWorks Enterprise Directory. <pre>feature.broadsoftdir.enabled="1"</pre> Enable QML application. <pre>feature.qml.enabled="1"</pre>	This toggles the Cisco BroadWorks Enterprise Directory service where: "1" – Enabled "0" – Disabled NOTE: BW Enterprise Directory requires Polycom release version 4.1.3G or higher.
Step 2	Additional directory options. Enable the Default Search. <pre>feature.broadsoftdir.showDefaultSearch="1"</pre> Hide Local Contact Directory <pre>directory.local.Uienabled</pre>	This toggles the default search where: "1" – Enabled "0" – Disabled This toggles the hide/show of the local directories where: "1" – Enabled (default) "0" – Disabled NOTE: Requires Polycom release version 5.5.2 or higher.
Step 3	Provision the Xtended Services Platform host address. <pre>dir.broadsoft.xsp.address=http://<XSP_ADDRESS>:<XSP_PORT>/</pre> Example: <pre>dir.broadsoft.xsp.address=http://xsp1.iopl.broadworks.net:80/</pre>	Provide the Xtended Services Platform (Xsp) server address.

4.5.2.2 Cisco BroadWorks Group Directory

The format for the web link for the Cisco BroadWorks Group Directory service is as follows: *http(s)://<XSP hostaddress:port>/com.broadsoft.xsi-actions/v2.0/user/<userid>/directories/group*.

The Cisco BroadWorks Directory can only be enabled on one line (user account) for each supported VVX Phone. To enable the Cisco BroadWorks Group Directory service on the phone, perform the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable the Cisco BroadWorks Group Directory. <pre>feature.broadsoftGroupDir.enabled="1"</pre> Enable QML application. <pre>feature.qml.enabled="1"</pre>	This toggles the Cisco BroadWorks Group Directory service where: "1" – Enabled "0" – Disabled NOTE: Group/Common/Personal Directories requires Polycom release version 5.5.2 or higher.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 2	Provision the Xtended Services Platform host address. <pre>dir.broadsoft.xsp.address=http://<XSP_ADDRESS>:<XSP_PORT>/</pre> Example: <pre>dir.broadsoft.xsp.address=http://xsp1.iopl.broadworks.net:80/</pre>	Provide the Xtended Services Platform (Xsp) server address.

4.5.2.3 Cisco BroadWorks Personal Directory

The format for the web link for the Cisco BroadWorks Personal Directory service is as follows: *http(s)://<XSP hostaddress:port>/com.broadsoft.xsi-actions/v2.0/user/<userid>/directories/Personal*.

The Cisco BroadWorks Directory can only be enabled on one line (user account) for each supported VVX Phone. To enable the Cisco BroadWorks Personal Directory service on the phone, perform the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable the Cisco BroadWorks Personal Directory. <pre>feature.broadsofPersonalDir.enabled="1"</pre> Enable QML application. <pre>feature.qml.enabled="1"</pre>	This toggles the Cisco BroadWorks Personal Directory service where: "1" – Enabled "0" – Disabled NOTE: Group/Common/Personal Directories requires Polycom release version 5.5.2 or higher.
Step 2	Provision the Xtended Services Platform host address. <pre>dir.broadsoft.xsp.address=http://<XSP_ADDRESS>:<XSP_PORT>/</pre> Example: <pre>dir.broadsoft.xsp.address=http://xsp1.iopl.broadworks.net:80/</pre>	Provide the Xtended Services Platform (Xsp) server address.

4.5.3 Cisco BroadWorks Call Logs Configuration

Integration with the Cisco BroadWorks Xtended Services Interface for Call Logs enables the phone to get call log history (missed, placed, and received calls) from Cisco BroadWorks and make them available to a user via the phone menus.

Polycom VVX devices support BroadWorks Basic Call Logs service. By enabling this service, user can perform server based Last Call Return service (LCR) from the call logs provided by Cisco BroadWorks. That is in addition to the call logs from the local phone, user can obtain and utilize the aggregated call log information among all user associated devices via the phone's user interface.

To enable the BroadWorks Basic Call Logs service and Last Call Return service on the phone, perform the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable the BroadWorks Basic Call Logs Service. <pre>feature.broadsoft.callLogs="Basic"</pre> Enable the BroadWorks Last Call Return service. <pre>feature.broadsoft.basicCallLogs.r edial.enabled="1"</pre>	This toggles the BroadWorks Basic Call Logs service where: "Basic" – Enabled "" – Disabled (null) This toggles the BroadWorks LCR service where: "1" – Enabled "0" – Disabled (null) NOTE: Requires Polycom release version 5.5.2 or higher.
Step 2	Provision the Xtended Services Platform host address. <pre>dir.broadsoft.xsp.address=http://<XSP_ADD RESS>:<XSP_PORT>/</pre> Example: <pre>dir.broadsoft.xsp.address=http://xsp1.iop1.br oadworks.net:80/</pre>	Provide the Xtended Services Platform (Xsp) server address.

4.5.4 Cisco BroadWorks Visual Voice Mail Configuration

Integration with the Cisco BroadWorks Xtended Services Interface for Visual Voice Mail enables the phone to obtain voice mail envelope details from Cisco BroadWorks and make the details available to a user via the phone menus.

This feature is not supported by the VVX devices.

4.5.5 Xtended Services Interface Feature Configuration with Cisco BroadWorks

Integration with the Cisco BroadWorks Xtended Services Interface for feature configuration enables the phone to perform configuration on selected features onto the Cisco BroadWorks via the phone menus. The supported features are:

- Anonymous Call Rejection
- Simultaneous Ring Personal
- Line ID Delivery Blocking
- BroadWorks Anywhere
- Remote Office

■ Call Waiting

To enable the features above, use the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable Anonymous Call Rejection. <code>feature.broadsoft.xsi.AnonymousCalRe ject.enabled="1"</code>	The Polycom phone supports Anonymous Call Rejection Xsi configuration in the feature menu: "1" – The Xsi feature is <i>Enabled</i> . "0" – The Xsi feature is <i>Disabled</i> .
Step 2	Enable Simultaneous Ring Personal. <code>feature.broadsoft.xsi.SimultaneousRi ng.enabled="1"</code>	The Polycom phone supports Simultaneous Ring Personal Xsi configuration in the feature menu: "1" – The Xsi feature is <i>Enabled</i> . "0" – The Xsi feature is <i>Disabled</i> .
Step 3	Enable Line ID Delivery Blocking. <code>feature.broadsoft.xsi.LineIdblock.en abled="1"</code>	The Polycom phone supports Line ID Delivery Blocking Xsi configuration in the feature menu: "1" – The Xsi feature is <i>Enabled</i> . "0" – The Xsi feature is <i>Disabled</i> .
Step 4	Enable BroadWorks Anywhere. <code>feature.broadsoft.xsi.BroadWorksAnyw here.enabled="1"</code>	The Polycom phone supports BroadWorks Anywhere Xsi configuration in the feature menu: "1" – The Xsi feature is <i>Enabled</i> . "0" – The Xsi feature is <i>Disabled</i> .
Step 5	Enable Remote Office. <code>feature.broadsoft.xsi.RemoteOffice="1"</code>	The Polycom phone supports Remote Office Xsi configuration in the feature menu: "1" – The Xsi feature is <i>Enabled</i> . "0" – The Xsi feature is <i>Disabled</i> .
Step 6	Enable Call Waiting. <code>feature.broadsoft.xsi.callWaiting.en abled="1"</code>	The Polycom phone supports BroadWorks Call Waiting Xsi configuration in the feature menu: "1" – The Xsi feature is <i>Enabled</i> . "0" – The Xsi feature is <i>Disabled</i> .

4.6 Instant Message and Presence Configuration

This section provides configuration instructions for configuration of the phone for integration with BroadCloud Instant Message and Presence.

This feature makes access to the Instant Messaging and Presence (IM&P) directory associated with a user account using the Extensible Messaging and Presence Protocol (XMPP). Hence, using this service means the user has to be provisioned with the Integrated IM&P service. Further, it can only be enabled on one line (user account) for each supported VVX device.

To enable the BroadCloud IM&P integration feature on the phone, see the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable the UC-One integration. <code>feature.broadsoftUcOne.enabled="1"</code> Enable QML application. <code>feature.qml.enabled="1"</code> Enable optional UC-One integration presence support. <code>feature.presence.enabled="1"</code>	To toggle the UC-One Integration feature: "1" – Enabled "0" – Disabled Note that this requires Polycom release version 4.1.3G or higher.
Step 2	Enable the XMPP support. <code>xmpp.1.enable="1"</code>	To toggle the XMPP protocol support: "1" – Enabled "0" – Disabled
Step 3	Provision the XMPP server address. <code>xmpp.1.server="%BW_IMP_SERVICE_NET_ADDRESS-1%"</code>	Provide the XMPP server information.
Step 4	Provision the XMPP authentication domain, user name, and password. <code>xmpp.1.auth.domain="<IMP_SERVICE_NET_ADDRESS>"</code> <code>xmpp.1.jid="<username>"</code> <code>xmpp.1.auth.password="<password>"</code>	Provide the XMPP authentication information.
Step 5	Set the dial method of XMPP to SIP. <code>xmpp.1.dialMethod="sip"</code> Turn on the BroadSoft XMPP inviter's subscription for presence. <code>xmpp.1.roster.invite.accept="prompt"</code> <code>xmpp.1.roster.invite.addMethod="h350 Person"</code> Set to toggle for the TLS certificate verification on the VVX device: <code>xmpp.1.verifyCert="0"</code>	Perform the remaining configuration.

4.7 Executive and Assistant Feature Configuration (UCS 5.5.0 and Newer)

This section provides configuration instructions for configuration of the phone for integration with BroadWorks Executive and Assistant feature. A feature on BroadWorks Release 20.0 and later servers enable a system administrator to assign users as executives or assistants for private or shared lines.

Executives and assistants can enable call filtering, which sends all executive calls directly to an assistant's phone to answer. Executives and assistants can also enable screening, which enables the executive's phone to display the incoming call notification for all filtered calls.

To enable the Executive and Assistant feature on the phone, see the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable the BroadSoft Executive-Assistant feature. <pre>feature.BSExecutiveAssistant.enabled =%FEATURE_EXEC_ADMIN%</pre> example: <pre>feature.BSExecutiveAssistant.enabled ="1"</pre> This enables the feature.	This enables the BroadSoft Executive-Assistant feature. "1" – Enabled "0" – Disabled %FEATURE_EXEC_ADMIN% tag used
Step 2	Configure the line registration assigned to the executive or assistant. <pre>feature.BSExecutiveAssistant.regIndex =%EXEC_ASSIST_LINE%</pre>	The registered line assigned to the executive or assistant for the BroadSoft Executive-Assistant feature. 1 (default) to 255 – The registered line for the Executive or Assistant. %EXEC_ASSIST_LINE% tag used
Step 3	Configure the role – Executive or Assistant. <pre>feature.BSExecutiveAssistant.userRole =%EXEC_ASSIST_ROLE%</pre>	ExecutiveRole (default) – Sets the registered line as an Executive line. AssistantRole – Sets the registered line as an Assistant line. Note that a phone can only have a line set as an Executive or an Assistant; an Executive and an Assistant line cannot be on the same phone. %EXEC_ASSIST_ROLE% tag used.
Step 4	Provision the Xsi Authentication using SIP credentials. <pre>dir.broadsoft.useXspCredentials="0" reg.x.broadsoft.userId="<User's Xsi Login ID>" reg.x.auth.userId="<User's SIP authentication username>" reg.x.auth.password="<User's SIP authentication password>" dir.broadsoft.xsp.address=http://<XSP_ADDRESS>:<XSP_PORT>/</pre>	Provide the Xsi access required for the Executive and Assistant Feature.

4.8 Call Decline Policy Configuration (UCS 5.5.0 and Newer)

This section provides configuration instructions for configuration of the phone for supporting the Call Decline Feature, a feature on the BroadWorks Release 21.0 and later server.

To enable the Call Decline Feature on the phone, use the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (phone<BWMACADDRESS>.cfg)		
Step 1	Enable the BroadSoft Executive-Assistant feature. <code>call.shared.reject="%CALL_DECLINE%"</code> example: <code>call.shared.reject="1"</code> This enables the feature.	This enables the BroadSoft Call Decline Feature. The parameter will be applicable for Calls on shared line. "1" – Enabled and offer Reject softkey "0" – Disabled %CALL_DECLINE% tag used

4.9 Polycom Device Management Service for Service Providers (PDMS-SP) – Cloud Management Provisioning (UCS 5.8.1 and newer feature)

PDMS-SP operates www.obitalk.com, a website for both VVX devices running on UCS 5.8.1 and newer SW and Polycom ATA users to manage their devices from the cloud. The site has many setup wizards to help users configure their devices for BYOD services and other user features. A user must sign-up for an PDMS-SP user account to access the portal features. A user ID and password are required to log-in. The log-in user ID must be a valid email address. Once logged-in, a user can add one or more devices to the account to be managed. Note that a device may be added to one user account only. Attempting to add a device that has already been added to another account generates an error message.

Approved Service Provider and/or API Service Activation Code API

A service provisioning model can incorporate the PDMS-SP automated service configuration APIs. PDMS-SP has two API-based provisioning models currently. One is the Approved Service Provider (ASP). The other one is the Service Activation Code (SAC).

The ASP API model allows for a new subscriber to sign-up from a choice of services (or service providers) from the PDMS-SP User Portal. This is usually the case when the subscriber already owns an VVX/ATA device and has an PDMS-SP user account. When the user logs onto PDMS-SP, he will find the option to add to one of his VVX/ATA devices a new service from an ITSP chosen from a list of ITSPs partnering with Polycom.

The SAC is a seamless BYOD subscriber activation feature available in all VVX/ATA devices. The SAC API enables a service provider to on-board customers directly from their web site or with the assistance of a trained customer service representative. The SAC API method does not require the customer to be logged-in to an PDMS-SP account like the ASP API requires. The customer can complete sign-up and activation (at any time) all from the service provider's web site or store/kiosk. The VVX/ATA device can be procured from any generic VVX/ATA devices that are sold/distributed.

With both API-based methods, the VVX/ATA device will be redirected automatically and securely to the BroadWorks Device Management service interface for further provisioning of specific parameters required to bring the subscriber's device into service.

To enable the PDMS-SP feature on the phone, see the steps in the following table.

Step	Command	Purpose
Subscriber Configuration File (Phone<BWMACADDRESS>.cfg)		
Step 1	<p>Enable the PDMS-SP feature.</p> <pre>feature.obitalk.enabled="%FEATURE_PDMS-SP%"</pre> <p>example:</p> <pre>feature.obitalk.enabled="1"</pre> <p>This enables the feature.</p>	<p>This enables the PDMS-SP feature.</p> <p>"1" – Enabled "0" – Disabled</p> <p>%FEATURE_PDMS-SP% tag used</p>
Step 2	<p>Configure the line registration assigned to the executive or assistant.</p> <pre>obitalk.accountCode="%FEATURE_PDMS-SP_ACCOUNT_CODE%"</pre> <p>example:</p> <pre>obitalk.accountCode="Mister-SP-123456"</pre>	<p>The Service API value is unique identifier that is assigned to SP to specify which SP the VVX belongs to.</p> <p>Null (default) or the Service API string.</p> <p>%FEATURE_PDMS-SP_ACCOUNT_CODE% tag used</p>
Step 3	<p>Configure the remote PCAP feature.</p> <pre>diags.pcap.enabled="%FEATURE_PCAP%"</pre>	<p>This enables the remote PCAP feature as part of the PDMS-SP service.</p> <p>"1" – Enabled "0" – Disabled</p> <p>%FEATURE_PCAP% tag used.</p>

5 Device Management

The BroadWorks Device Management feature provides the capability to automate generation of device configuration files to support mass deployment of devices. This section identifies the Device Management capabilities supported by the Polycom VVX phones. The configuration steps required are also documented in this section. For Device Management configuration details not covered here, see the *BroadWorks Device Management Configuration Guide* [2] and the *BroadWorks CPE Kit Usage Guide* [10].

5.1 Device Management Capabilities Supported

The Polycom UC Software VVX phones have completed Device Management interoperability testing with Cisco BroadWorks using the *BroadWorks Device Management Interoperability Test Plan* [5]. The results are summarized in the following table.

The Cisco BroadWorks test plan is composed of packages, each covering distinct interoperability areas. Each package is composed of one or more test items, which in turn are composed of one or more test cases. The test plan exercises the Device Management interface between the device and Cisco BroadWorks with the intent to ensure interoperability.

The *Supported* column in the following table identifies the Polycom UC Software VVX phones support for each of the items covered in the test plan packages, with the following designations:

- Yes Test item is supported
- No Test item is not supported
- NA Test item is not applicable
- NT Test item was not tested

Caveats or clarifications are identified in the *Comments* column.

NOTE: *DUT* in the following table refers to the *Device Under Test*, which in this case are the Polycom VVX phones.

Test Plan Package	Test Plan Package Items	Supported	Comments
HTTP File Download	HTTP Download Using XSP IP Address	Yes	
	HTTP Download Using XSP FQDN	Yes	
	HTTP Download Using XSP Cluster FQDN	Yes	
	HTTP Download with Double Slash	Yes	
HTTPS File Download	HTTPS Download Using XSP IP Address	NT	Not a part of Release 22.0 Test Plan.
	HTTPS Download Using XSP FQDN	Yes	
	HTTPS Download Using XSP Cluster FQDN	Yes	
HTTPS File Download with	HTTPS Download with Client Authentication Using XSP FQDN	Yes	

Cisco BroadWorks Device Management Interoperability Test Plan Support Table			
Test Plan Package	Test Plan Package Items	Supported	Comments
Client Authentication	HTTPS Download with Client Authentication Using XSP Cluster FQDN	Yes	
Time Zone Mapping	No associated test cases	Yes	
Language Mapping	No associated test cases	Yes	
File Inspection	Inspect System Config File	Yes	
	Inspect Device-Specific Config File	Yes	
	Inspect Other Config Files	Yes	
	Inspect Static Files	Yes	
Device Inspection	Inspect SIP Settings	Yes	
	Inspect Line Settings	Yes	
	Inspect Service Settings	Yes	
HTTP File Upload	HTTP Upload Using XSP IP Address	Yes	
	HTTP Upload Using XSP FQDN	Yes	
	HTTP Upload Using XSP Cluster FQDN	Yes	
Call Processing Sanity Tests	Register with Authentication	Yes	
	Call Origination	Yes	
	Call Termination	Yes	
	Remote Restart	Yes	
	Shared Line Origination	Yes	
	Shared Line Termination	Yes	
	Shared Line Status	Yes	
	Busy Lamp Field	Yes	
Flexible Seating	Association via Voice Portal	Yes	
	Association via Phone	Yes	
No Touch Provisioning	Provision via DHCP Options Field	Yes	
	No Touch Provision via DM redirect	Yes	
	No Touch Provision via Vendor redirect	Yes	

5.2 Device Management Configuration

This section identifies the steps required to enable VVX phones running Polycom UC Software for Device Management. For Device Management configuration details not covered in this guide, see the *BroadWorks Device Management Configuration Guide* [2].

Device Management configuration is performed using the steps described in the following subsections:

- [5.2.1 Configure Cisco BroadWorks Tags](#)
- [5.2.2 Configure Cisco BroadWorks Device Profile Type](#)
 - [5.2.2.1 Configuration Method 1: Import](#)
 - [5.2.2.2 Configuration Method 2: Manual](#)
- [5.2.3 Create Device Profile Instance](#)
- [5.2.4 Configure BroadWorks User](#)
- [5.2.5 Configure Edge Device](#)
- [5.2.6 Enable HTTPS for Polycom UC Software Devices](#)
- [5.2.7 Configure Polycom UC Software Phone](#)
 - [5.2.8.1 Manual Provisioning](#)
 - [5.2.8.2 No Touch Provisioning via Cisco BroadWorks Device Management](#)
 - [5.2.8.3 No Touch Provisioning via Polycom Zero Touch Provisioning](#)

5.2.1 Configure Cisco BroadWorks Tags

The template files in Device Management use tags to represent the data stored on Cisco BroadWorks. When a configuration changes for a user, Device Management parses the template files and replaces the Device Management tags with the associated data stored on Cisco BroadWorks. Default tags are defined in the Device Management software and there are custom tags that a service provider can create and define via the web portal for use by Device Management. Two types of custom tags can be defined:

- System default – These tags are common to all phones on the system.
- Device type-specific – These tags are only common to Polycom UC Software phone models.

VVX phones running Polycom UC Software make use of dynamic tags, which can be configured by a Cisco BroadWorks administrator as system default or device-type-specific tags. This section identifies the required tags.

5.2.1.1 Create System Default Tags

Browse to *System* → *Resources* → *Device Management Tag Sets* and select the *System Default* tag set. Polycom configuration templates make use of the tags in the following table. Add the tags if they do not already exist.

The Polycom system configuration file also uses the `%BWASCLUSTERFQDN%`, which is a pre-defined tag. For this tag to resolve properly, make sure that the following command line interface (CLI) parameter is set to the Application Server cluster address as follows:

```
AS_CLI/System/Device/IpDeviceMgmt> set deviceAccessAppServerClusterName  
<AS-Cluster-FQDN>
```

Tag Name	Valid Settings	Description
%SNTP_SERVER%	IP address or FQDN	This is the NTP server address.
%DNS_SERVER_1%	IP address	This is the DNS server address.
%DNS_SERVER_2%	IP address	This is the alternate DNS server address.
%SBC_ADDRESS%	IP address or FQDN	This is the SBC SIP address.
%SBC_PORT%	Port	This is the SBC SIP port. If the defined SBC address is an IP address, then the port should be set. If the SBC address is an FQDN, then the SBC port should not be set.
%XSP_ADDRESS_XSI_ACTIONS%	IP address or FQDN Example: xsp1.iop1.broadworks.net	This is the Cisco BroadWorks Xtended Services Platform (Xsp) server address, which provides the Xsi-Actions web services.

Example system default tag settings:

Figure 3 System Default Tag Settings

5.2.1.2 Create Device Type Specific Tags

Browse to *System* → *Resources* → *Device Management Tag Sets* and select *Add* to add a new tag set. Configure the tag set name as *Polycom-Tags*. Add the device type specific tags in the following table to the device tag set. If the tag set already exists, make sure that the tags in the following table have been defined.

Tag Name	Valid Settings	Description
%SBC_TRANSPORT%	DNSnaptr, TCPpreferred, UDPOnly, TCPOnly, or TLS	Set this to the transport that the phone uses when communicating with the SBC.
%DIAL_PLAN%	[2346789]11[[0-1][2-9]11 0[#T]00 01[2-9]xx.[#T]]*xx 011x.[#T] [0-1]xxxxxx[#T] [0-1][2-9]xxxxxxxxx [2-9]xxxxxxxxx [2-9]xxxxxx[#T] 101xxxx.[#T] 11 [2-9]x.[#T]	This is the default dial plan for U.S. dialing on the Polycom phones.
%APP_VERSION%	6.1.0	This is set to the currently supported version of Polycom firmware.
%APP_VERSION_VVX-101-201%	6.1.0	This is set to the latest supported version of Polycom firmware for VVX101 and VVX201 phones.
%APP_VERSION_VVX-301-401%	6.1.0	This is set to the latest supported version of Polycom firmware for VVX301/311 and VVX401/411 phones.
%APP_VERSION_VVX-501-601%	6.1.0	This is set to the latest supported version of Polycom firmware for VVX501/601 phones.
%APP_VERSION_VVX-150%	6.1.0	This is set to the latest supported version of Polycom firmware for VVX150 phones.
%APP_VERSION_VVX-250%	6.1.0	This is set to the latest supported version of Polycom firmware for VVX250 phones.
%APP_VERSION_VVX-350%	6.1.0	This is set to the latest supported version of Polycom firmware for VVX350 phones.
%APP_VERSION_VVX-450%	6.1.0	This is set to the latest supported version of Polycom firmware for VVX450 phones.
%FEATURE_SYNC_DND%	1 or 0	Setting this value to “1” activates the Do Not Disturb synchronization feature with Cisco BroadWorks for all Polycom phones on the system.
%FEATURE_SYNC_CF%	1 or 0	Setting this value to “1” activates the Call Forwarding synchronization feature with Cisco BroadWorks for all Polycom phones on the system.
%FEATURE_SYNC_ACD%	1 or 0	For all Polycom phones on the system: Setting this value to “1” activates the ACD synchronization for Call center. Setting this value to “0” will allow the phones to support Hoteling and Flexible Seating feature.
%ACD_LINE%	1 through 16	This is the register line index of the line, which synchronizes the ACD or Flexible Seating state with Cisco BroadWorks. By default, this should be the primary line or line 1.

Tag Name	Valid Settings	Description
%ACD_SIGNIN_STATE %	1 or 0	When set to "1", the sign-in state is set to <i>Available</i> . When set to "0", the sign-in state is set to <i>Unavailable</i> .
%HOTEL_FLEXSEAT%	1 or 0	This tag is deprecated from UCS 5.5.0. Replace with %FEATURE_SYNC_ACD% tag.
%VIDEO_QUALITY%	Motion or sharpness	This is the motion or sharpness. Set to "motion" for use with people or moving video. Set to "sharpness" for use with static video.
%VIDEO_CALL_RATE%	128 through 1024	Set to the maximum bandwidth to be used by a call. The recommended setting is "448" Kbps.
%VIDEO_SCREEN_MODE%	1 or 0	Set this to "1" so that the video fills the entire VVX screen.
%VIDEO_LOCAL_MODE %	null or pip	Set this to "pip" for the local camera view to be displayed as a picture-in-picture with the far-end camera view. Otherwise, leave this blank for the local camera view to appear side by side with the far-end camera view.
%VIDEO_FRAME_RATE %	5 through 30	This determines the smoothness of the video. The higher the number then the smoother the video. The recommended value is "25".
%FEATURE_BW_DIR%	1 or 0	Set to "1" to activate the BroadWorks Xsi Enterprise Directory service. NOTE: This requires the 4.1.3G or later firmware revision.
%FEATURE_BW_UC_ONE%	1 or 0	Set to "1" to enable UC-One integration. NOTE: This requires the 4.1.3G or later firmware revision.
%FEATURE_CALL_CENTER%	1 or 0	Set to "1" to enable the Call Center feature.
%FEATURE_HOTELING %	1 or 0	Set to "1" to enable the Hoteling or Flexible Seating feature.
%FEATURE_PRESENCE%	1 or 0	Set to "1" to enable the UC-One integration presence feature. NOTE: This requires the 4.1.3G or later firmware revision.
%HTTPS_CFG_REQ%	1 or 0	Set to "0" to enable device's HTTP web configuration access. NOTE: In 5.3.0 or later firmware revision HTTPS is required by default, this parameter is introduced to provide an override.
%FEATURE_ENHANCED_CP%	1 or 0	Set to "1" to enable enhanced call park notification feature. NOTE: This requires the 5.3.0 or later firmware revision.

Tag Name	Valid Settings	Description
%FEATURE_REMOTE_OFFICE%	1 or 0	Set to "1" to enable Remote Office Xsi configuration feature. NOTE: This requires the 5.3.0 or later firmware revision.
%FEATURE_BW_ANYWHERE%	1 or 0	Set to "1" to enable BW Anywhere Xsi configuration feature. NOTE: This requires the 5.3.0 or later firmware revision.
%FEATURE_SIM_RING%	1 or 0	Set to "1" to enable Simultaneous Ring Xsi configuration feature. NOTE: This requires the 5.3.0 or later firmware revision.
%FEATURE_CLID_BLOCK%	1 or 0	Set to "1" to enable Call Line ID Blocking Xsi configuration feature. NOTE: This requires the 5.3.0 or later firmware revision.
%FEATURE_ANONYMOUS_REJ%	1 or 0	Set to "1" to enable Anonymous Call Rejection Xsi configuration feature. NOTE: This requires the 5.3.0 or later firmware revision.
%DIR_LINE%	1 through 16	This is the register line index of the line, which the BroadSoft Directory will be requested through Xtended Services Interface (XSI). By default, this should be the primary line or line 1.
%FEATURE_DECT%	1 or 0	Set to "1" to enable D60 support. NOTE: This is only on VVX 3xx, 4xx, 5xx and 6xx models and requires 5.4.3 or later firmware revision.
%CALL_DECLINE%	1 or 0	Set to "1" to enable Call Decline support. NOTE: This is for UCS 5.5.0 or later firmware revision.
%FEATURE_EXEC_ASSISTANT%	0 or 1	Set to "1" to enable Executive and Assistant feature. NOTE: This is for UCS 5.5.0 or later firmware revision.
%EXEC_ASSIST_LINE%	1 to 255	This is the register line index for the Executive or Assistant. 1 (default) to 255 NOTE: This is for UCS 5.5.0 or later firmware revision.
%EXEC_ASSIST_ROLE%	ExecutiveRole or AssistantRole	Set to ExecutiveRole (default) - Sets the registered line as an Executive line. Set to AssistantRole - Sets the registered line as an Assistant line. NOTE: This is for UCS 5.5.0 or later firmware revision.
%FEATURE_BW_PERSONAL%	0 or 1	Set to "1" to enable BroadWorks Xsi Personal Directory feature. NOTE: This is for UCS 5.6.0 or later firmware revision.

Tag Name	Valid Settings	Description
%FEATURE_BW_DIR_GROUP%	0 or 1	Set to "1" to enable BroadWorks Xsi Group Directory feature. NOTE: This is for UCS 5.6.0 or later firmware revision.
%FEATURE_BW_DIR_DEFAULT_SEARCH%	0 or 1	The Enterprise Directory default search feature allows the users to view the initial list of contacts by default. Set to "1" to enable the feature. NOTE: This is for UCS 5.6.0 or later firmware revision.
%FEATURE_CALL_LOGS%	Basic or Disabled	Set to "Basic" to enable BroadWorks Basic Call Log feature. NOTE: This is for UCS 5.6.0 or later firmware revision.
%FEATURE_PDMS-SP%	0 or 1	Set to "1" to enable PDMS-SP feature. NOTE: This is for UCS 5.8.1 or later firmware revision.
%FEATURE_PDMS-SP_ACCOUNT_CODE%	SP Account Code from Polycom	Populate with the SP account code string from Polycom. NOTE: This is for UCS 5.8.1 or later firmware revision.
%FEATURE_PCAP%	0 or 1	Set to "1" to enable remote PCAP functionality that is offered through the PDMS-SP service. NOTE: This is for UCS 5.8.1 or later firmware revision.

Example device-type-specific tag settings:

System Help - Home
Welcome Default Administrator [\[Logout\]](#)

Device Management Tag Sets Modify
 Display all the device management tags defined in the tag set. Tags can be added to the set or deleted from the set.

OK Apply Add Cancel

* Tag Set Name:

Delete	Tag Name	Tag Value	Edit
<input type="checkbox"/>	%ACD_LINE%	1	Edit
<input type="checkbox"/>	%ACD_SIGNIN_STATE%	1	Edit
<input type="checkbox"/>	%APP_VERSION_VVX-300-400%	5.3.0	Edit
<input type="checkbox"/>	%APP_VERSION_VVX-500-600%	5.3.0	Edit
<input type="checkbox"/>	%APP_VERSION%	4.0.4	Edit
<input type="checkbox"/>	%APP_VERSION-320-330%	4.0.1	Edit
<input type="checkbox"/>	%APP_VERSION-VVX-1500%	5.0.1	Edit
<input type="checkbox"/>	%DIAL_PLAN%	[2346789]11[0-1][2-9]110[#T]00[01[2-9]xx. [#T]"*xx[01]x.[#T][0-1]xxxxxxxx[#T][0-1][2-9]xxxxxxxx[2-9]xxxxxxxx[2-9]xxxxxxxx[#T]101xxxx. [#T]11[2-9]x.[#T]	Edit
<input type="checkbox"/>	%FEATURE_CALL_CENTER%	1	Edit
<input type="checkbox"/>	%FEATURE_ENHANCED_CP%	1	Edit
<input type="checkbox"/>	%FEATURE_SYNC_ACD%	1	Edit
<input type="checkbox"/>	%FEATURE_SYNC_CF%	1	Edit
<input type="checkbox"/>	%FEATURE_SYNC_DND%	1	Edit
<input type="checkbox"/>	%GROUPID%		Edit
<input type="checkbox"/>	%HOTEL_FLEXSEAT%	1	Edit
<input type="checkbox"/>	%HTTPS_CFG_REQ%	0	Edit
<input type="checkbox"/>	%SBC_PORT%	5060	Edit
<input type="checkbox"/>	%SBC_TRANSPORT%	DNSnaptr	Edit
<input type="checkbox"/>	%VIDEO_CALL_RATE%	448	Edit
<input type="checkbox"/>	%VIDEO_FRAME_RATE%	25	Edit

[Page 1 of 2] [Next](#) [Last](#)

Tag Name Starts With [Find](#) [Find All](#)

OK Apply Add Cancel

Figure 4 Device-Type-Specific Tag Settings

5.2.2 Configure Cisco BroadWorks Device Profile Type

The device profile type is a system-level structure that defines how the device interfaces with Cisco BroadWorks. It also identifies the default configuration files and other files, such as firmware, which are required for the phone to operate correctly. The device profile type is created by the system administrator. Group administrators use the device profile type to create a device profile. The device profile is an instance of the device profile type that is associated with a physical device or IP phone.

There are two Cisco BroadWorks device profile configuration methods described: import and manual. The import method takes a DTAF as input and builds the Cisco BroadWorks device profile type(s) automatically. The manual method takes the administrator through the steps to manually add and configure the device profile type(s).

The import method should be used if all of the following prerequisites are met:

- The BroadWorks Release is 17.0 or later.
- The device profile type(s) being imported do not already exist on the system. (If either a previous import or manual configuration was done, the import fails.)
- There is a DTAF file available for import with a Cisco BroadWorks release level that is the same as or prior to the release to which it is being imported. If the DTAF file is at a release level later than the release being imported to, the import may fail.

Otherwise, the manual method must be used.

5.2.2.1 Configuration Method 1: Import

This section identifies the steps necessary to make use of the Device Management import feature to configure Cisco BroadWorks to add the Polycom VVX phones as Device Management-enabled device types.

The import method is available in BroadWorks Release 17.0 and later. For previous releases, use the manual configuration method described in the next section.

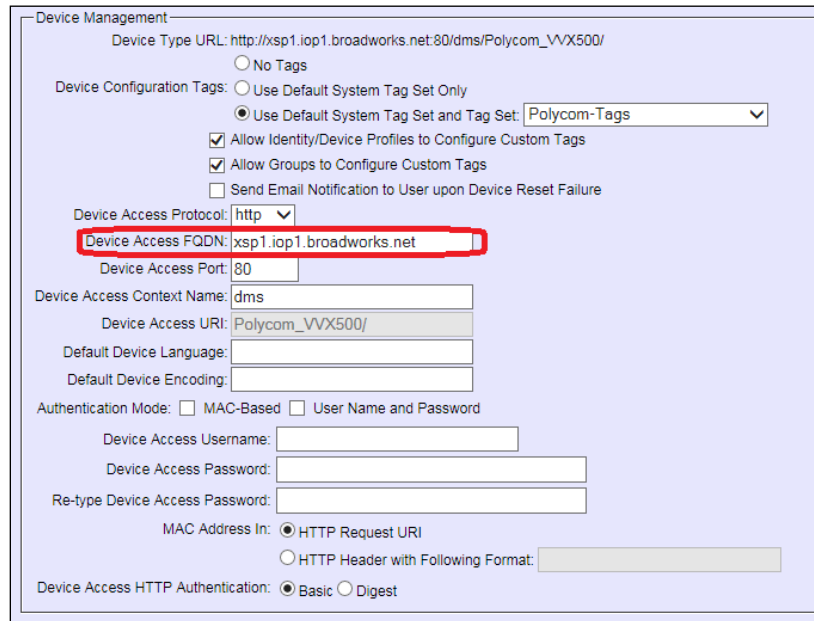
Download the Polycom UC Software device VVX CPE kit from Cisco Xchange at www.broadsoft.com/xchange. Extract the DTAF file(s) from the CPE kit. These are the import files. Repeat the following steps for each model you want to import.

Log in to Cisco BroadWorks as an administrator. Browse to *System* → *Resources* → *Identity/Device Profile Types* and select *Import*. Select *Browse* to find the extracted DTAF file for the model and click **OK** to start the import.

After the import finishes, the following post-import configuration steps must be completed.

Browse to *System* → *Resources* → *Identity/Device Profile Types* and perform a search to find the imported Polycom device profile type (for example, *Polycom_VVX500*). Browse to the *Profile* page and change the Device Management Device Access FQDN to your Xtended Services Platform or Xtended Services Platform cluster address.

Example:



Device Management

Device Type URL: `http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX500/`

Device Configuration Tags: No Tags
 Use Default System Tag Set Only
 Use Default System Tag Set and Tag Set: `Polycom-Tags`

Allow Identity/Device Profiles to Configure Custom Tags
 Allow Groups to Configure Custom Tags
 Send Email Notification to User upon Device Reset Failure

Device Access Protocol: `http`

Device Access FQDN: `xsp1.iop1.broadworks.net`

Device Access Port: `80`

Device Access Context Name: `dms`

Device Access URI: `Polycom_VVX500/`

Default Device Language:

Default Device Encoding:

Authentication Mode: MAC-Based User Name and Password

Device Access Username:

Device Access Password:

Re-type Device Access Password:

MAC Address In: HTTP Request URI
 HTTP Header with Following Format:

Device Access HTTP Authentication: Basic Digest

Figure 5 Device Access FQDN

Next, using the *Files and Authentication* link, select the option to rebuild all system files.

Firmware files must be obtained from Polycom. These files are not included in the import. Complete the steps in section [5.2.2.2.3 Static Files](#) to define the static firmware files and to upload the firmware.

The Polycom configuration features described in the following subsections are optional and are not enabled by the import:

- [5.2.2.2.1.2 Phone Branding](#)
- [5.2.2.2.2.3 *efk.cfg*](#)
- [5.2.2.2.3.3 Language Provisioning \(Optional\)](#)
- [5.2.2.2.3.4 Startup Welcome Audio File \(Optional\)](#)
- [5.2.2.2.3.6 Polycom Productivity Suite Files \(Optional\)](#)
- [5.2.2.2.3.7 Polycom Phone Service](#)

After importing the DTAFs, the Application Server must be restarted to load the *TimeZoneAlias* files.

5.2.2.2 Configuration Method 2: Manual

This section identifies the manual steps necessary to configure Cisco BroadWorks to add the VVX phones running Polycom UC Software as a Device Management-enabled device type.

The manual method must be used for Cisco BroadWorks releases prior to Release 17.0. It is an optional method in Release 17.0 and later. To determine when to use the manual method, see section [5.2.2 Configure BroadWorks Device Profile Type](#). The steps in this subsection can also be followed to update previously imported or configured device profile type(s) with new configuration files and firmware.

Device profile types can be created for each Polycom VVX device model or one generic device profile type can be created to apply to all Polycom VVX phone models (for example, *Polycom-VVX-Standard*). The steps in this section apply in either case; however, they must be repeated for each device profile type if there is one for each Polycom device model.

Manual configuration requires the steps described in the following subsections:

- [5.2.2.2.1 Modify Device Profile Type](#)
- [5.2.2.2.1.1 Configure Device Configuration Options](#)
- [5.2.2.2.1.2 Configure Device Management Options](#)
- [5.2.2.2.2 Define Device Profile Type Files](#)
- [5.2.2.2.2.1 System Files](#)
- [5.2.2.2.2.2 Device-Specific Files](#)
- [5.2.2.2.2.3 Static Files](#)

5.2.2.2.1 Modify Device Profile Type

This subsection identifies the Cisco BroadWorks device profile type settings, which are relevant to Device Management for the VVX phone running Polycom UC Software.

Browse to *System* → *Resources* → *Identity/Device Profile Types* and perform a search to find the Polycom device profile type(s) created in section [3.1 Cisco BroadWorks Device Profile Type Configuration](#) or add the device profile type for each model using the settings from section [3.1 Cisco BroadWorks Device Profile Type Configuration](#) if they do not exist.

The *Standard Options* and *Advanced Options* should already be configured as specified in section [3.1 Cisco BroadWorks Device Profile Type Configuration](#). If there are differences, update to match the settings in section [3.1 Cisco BroadWorks Device Profile Type Configuration](#).

NOTE: When using a single device profile type for all Polycom VVX models (for example, *Polycom-VVX-Standard*), the *Number of Ports* under the *Standard Options* must be set to the maximum number of lines supported by a Polycom model (16).

The following subsections identify the required settings specific to Device Management.

5.2.2.2.1.1 Configure Device Configuration Options

If Device Management has been enabled previously for the device profile type(s), go to the next section.

Device configuration is enabled differently depending on the deployed Cisco BroadWorks release.

For BroadWorks Release 18.0 and later, configure as described in the following table.

Parameter	Value	Description
Device Configuration Options	Device Management	Use BroadWorks Device Management.

The following shows Device Management enabled for BroadWorks Release 18.0 and later.

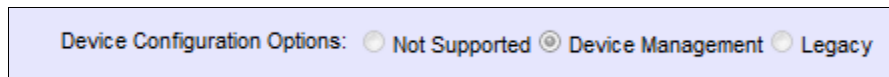


Figure 6 Device Management for Release 18.0 and Later

For BroadWorks releases prior to Release 18.0, configure as described in the following table. Note that these settings serve only to enable Device Management and are otherwise not meaningful in this context.

Parameter	Value	Description
Auto Configuration Type	2 Config File	Not meaningful other than it must be selected.
CPE System File Name	not_used	This parameter must not be blank, so set it to "not_used".
Device File Format	not_used	This parameter must not be blank, so set it to "not_used".

The following shows Device Management enabled for a BroadWorks release prior to Release 18.0.

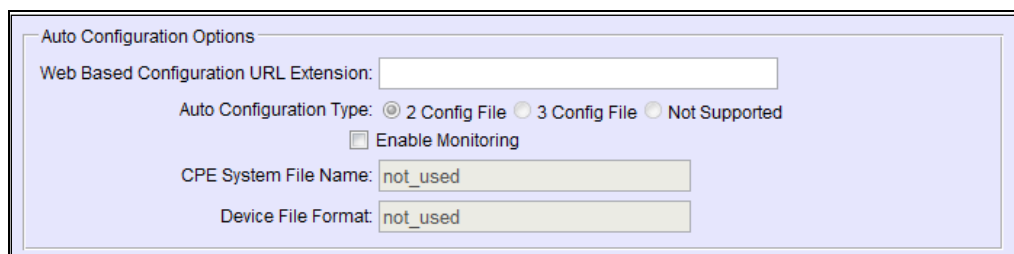


Figure 7 Auto Configuration Options

5.2.2.2.1.2 Configure Device Management Options

If Device Management has been enabled previously for the device profile type(s), make sure that the existing settings match the settings described in this subsection.

Modify the device profile type *Device Management Options* as described in the following table. These are common settings, which apply to all devices enabled for Device Management.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Configuration Tags	Use the Default System Tag Set and Tag Set. Select the device tag set created as described in section 5.2.1.2 Create Device Type Specific Tags .	
Allow Identity/Device Profiles to Configure Custom Tags	Checked	Optional
Allow Groups to Configure Custom Tags	Checked	Optional
Device Access Protocol	http or https	
Device Access FQDN	<BroadWorks-XSP-Cluster-Address> Example: xsp.iop1.broadworks.net	If using an Xtended Services Platform farm, set this to the Xtended Services Platform cluster FQDN. Otherwise, set this to the individual Xtended Services Platform FQDN or IP address.
Device Access Port	<BroadWorks-XSP-Port> Example: 80	This should be set to the listening port of the device access protocol.
Device Access Context Name	Dms	This does not need to be defined. Cisco BroadWorks defaults to the system-defined value.
Device Access URI	<device name> Example: Polycom_VVX500 Or Polycom-VVX-Standard	This defines the directory the Xtended Services Platform uses to access the configuration files. Polycom-Standard (or similar) would be used when a single device type is defined for all Polycom models.

Example *Device Management* options settings:

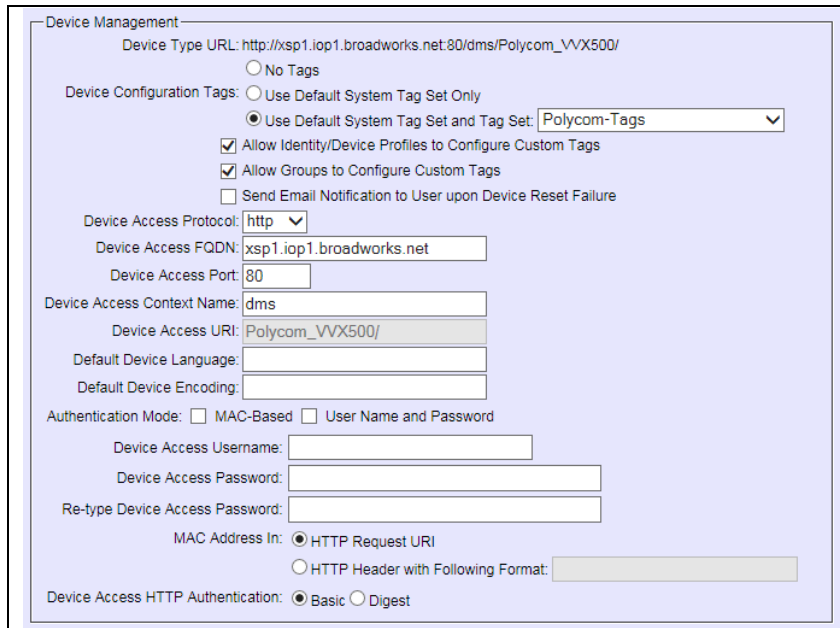


Figure 8 Device Management Options Settings

5.2.2.2.2 Define Device Profile Type Files

This section describes the Cisco BroadWorks Device Management configuration necessary to identify the configuration files and other files that the VVX phones running Polycom UC Software download.

Configuration templates, firmware, and other files applicable to devices running Polycom UC Software must be uploaded to Cisco BroadWorks. Download the Polycom VVX CPE kit from Cisco Xchange at www.broadsoft.com/xchange. Extract the configuration files from the *Configuration Files* folder of CPE kit. Get the firmware files directly from Polycom.

The following table identifies the Polycom configuration files distributed with the 5.9.0 CPE kit.

File Name	CPE Kit Template File Name	File Type	Description
BWMACADDRESS.cfg	%BWMACADDRESS%.cfg.template	Device-specific	This file contains all the configuration and firmware files that the phone has to load.
BWMACADDRESS-directory.xml	%BWMACADDRESS%-directory.xml.template	Device-specific	This is the template file is for reference only, the Polycom directory file will be created automatically by Cisco BroadWorks when Polycom Phone Service is enabled.
000000000000.cfg	000000000000.cfg.template	System-level	This file is the default file that the Polycom UC Software device request when the <i>BWMACADDRESS.cfg</i> file is not present.
efk.cfg	efk.cfg.tmpl	System-level	This file configures the soft keys on the phone to perform special functions.

File Name	CPE Kit Template File Name	File Type	Description
phoneBWDEVICE ID.cfg	phone%BWDEVICED%.cfg.template	Device-specific	This file contains data specific to a Cisco BroadWorks user. This file is created from the Polycom <i>phone1.cfg</i> file and it contains the <i>phone1.cfg</i> parameters, which have to be changed from their default values.
qsetup.cfg	qsetup.cfg.tmpl	System-level	This file contains quick setup key configuration.
sys.cfg	sys.cfg.template	System-level	This file is created from the Polycom <i>sip.cfg</i> file and it contains the <i>sip.cfg</i> parameters, which have to be changed from their default values.
TimeZoneAlias Labels_Polycom-<model>.properties	TimeZoneAliasLabels_Polycom<model>.properties	Time Zone Alias	The <i>TimeZoneAlias</i> file is a Cisco BroadWorks Device Management file used to map time zone identifiers between Cisco BroadWorks and Polycom phones. A <i>TimeZoneAlias</i> file is required for each model.
dect.cfg	dect.cfg	Device-specific	This file contains configuration parameters necessary for the VVX phones to enable the support and provision for D60 wireless hands.

The following table identifies other files that the Polycom phone downloads from the server or uploads to the server. These files are not provided in the CPE kit.

File Name	File Type	Description
BWMACADDRESS-boot.log	Device-specific	This is a log file created by the boot firmware.
BWMACADDRESS-app.log	Device-specific	This is a log file created by the application firmware.
BWMACADDRESS-license.cfg	Device-specific	This file licenses the Polycom Productivity Suite applications to a specific phone.
BWMACADDRESS-phone.cfg	Device-specific	This file documents the current settings used by the phone. If a configuration item is set at the phone then the setting is documented in this file.
000000000000-license.cfg	Static	This file licenses the Polycom Productivity Suite applications to all phones on a Cisco BroadWorks system.
VVX-dictionary.xml	System-level	This is the language file used by the phone. Each of the supported languages is added to a file with this name.
5.6.x.sip.ld or [Part_Number].5.9.0.sip.ld	Static	The <i>5.9.0.sip.ld</i> file is the generic application for the VVX models. The <i>[PART_NUMBER].5.9.0.sip.ld</i> is the VVX model-specific application.
*.jpg	Static	Any user-defined JPG files, meeting the Polycom-defined size requirements, can be uploaded.

Browse to *System* → *Resources* → *Identity/Device Profile Types* → *Files and Authentication* to add the files distributed with the CPE kit as described in the following subsections.

5.2.2.2.2.1 System Files

This section identifies the system-level files used by Polycom and provides instructions for defining the files and uploading for Device Management.

The system-level files and topics are described in the following subsections:

- [5.2.2.2.2.1.1 sys.cfg](#)
- [5.2.2.2.2.1.2 Phone Branding](#)

5.2.2.2.2.1.1 sys.cfg

The *sys.cfg* file is created from data in the *sip.cfg* file. The parameters in the *sip.cfg* file, which must be configured to support the interface to Cisco BroadWorks, are moved to the *sys.cfg* file.

Add a Cisco BroadWorks device profile type file to the Polycom UC Software VVX device profile for the *sys.cfg* file using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	sys.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	sys-%BWTIMESTAMP%.cfg	This is the file name as stored in the Device Management repository. If group customization of the system file is required, then the repository file name must contain the <i>timestamp</i> tag.
File Category	Dynamic Per-Type	This is the system file that applies to the device type.
File Customization	Administrator	This identifies who can customize the system file template.
Enable Caching	This is not set.	Caching is optional for a system file.
Assign File	Custom	
Authentication Mode	User name and password	This must be set based on what the device supports. If group customization of the system file is required, then Authentication must be set to the user name and password.
Device Access HTTP Authentication	Digest	

After defining the system file type, upload the corresponding system file template downloaded from Cisco Xchange. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

Example *sys.cfg* file settings:

Identity/Device Profile Type File Modify

Modify or delete a file type defined in an Identity/Device Profile Type.

OK
Apply
Delete
Cancel

Device Access File Format: *sys.cfg*
 Repository File Format: *sys-%BWTIMESTAMP%.cfg*
 Access File: http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX500/sys.cfg
 Repository File: [Download](#)
 Template File: [Download](#)
 File Category: Static Dynamic Per-Type Dynamic Per-Device
 File Customization: Administrator ▼
 Enable caching

Assign File

Manual
 Custom

Upload File: Browse...

Currently using configuration file: */var/broadworks/lpDeviceConfig/type/Polycom_VVX500/sys.cfg.template*

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- PlcmConversionCreatedFile version=1.2 converted=Wed Jul 28
14:33:16 2010 -->
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
  <bg>
    <bg.VVX_1500>
      <bg.VVX_1500.color bg.VVX_1500.color.selection="3,1">
        <bg.VVX_1500.color.bm bg.VVX_1500.color.bm.1.name="" />
      </bg.VVX_1500.color>
    </bg.VVX_1500>
  </bg>
</polycomConfig>

```

File Authentication

Authentication Mode: MAC-Based User Name and Password

MAC Address In: HTTP Request URI
 HTTP Header with Following Format:

Device Access HTTP Authentication: Basic Digest

Allowed Access Protocols: http https tftp

Figure 9 *sys.cfg* File

5.2.2.2.1.2 Phone Branding

The `sys.cfg` file contains configuration data to allow branding of the phone by uploading a custom bitmap to the background display of the phone and the sidecars. This section describes the steps necessary to enable custom bitmaps.

To enable the phone to look for bitmaps to download, modify the `sys.cfg` file as described in the following table.

Step	Command	Purpose
Step 1	<pre>Select the background for the VVX phone mode. Example: <bg> <bg.color bg.color.selection.VVX501="2,1"> <bg.color.bm bg.color.bm.1.name.VVX501="http://% BWDEVICEACCESSFQDN%:%BWDEVICEACCESS PORT%/ %BWDMSCONTEXT%/%BWDEVICEACCESSURI%b soft.jpg" /> </bg></pre>	<p>These parameters are used to load a custom bitmap to the VVX models.</p> <p>Modify the <code>bsoft.jpg</code> file name to the file names you are using.</p>

To load the bitmap images to Device Management, add a new Cisco BroadWorks device profile type file to the Polycom UC Software device profile using the settings described in the following table. Repeat for each bitmap image to be loaded. For the bitmap size requirements, see the *Polycom UC Software Administrator's Guide* [1].

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	<bitmap-name>.jpg Example: bsoft.jpg	This is the file name, which the phone uses to request the file.
Repository File Format	<bitmap-name>.jpg Example: bsoft.jpg	This is the file name as stored in the Device Management repository. If group customization of the system file is required, then the repository file name must contain the <i>timestamp</i> tag.
File Category	Static	
File Customization	Administrator	This identifies who can customize the system file template.
Enable Caching	This is not set.	Caching is optional.
Assign File	Custom	Use the <i>Browse</i> button to upload the background image for the phone.

Example *bitmap image file* settings:

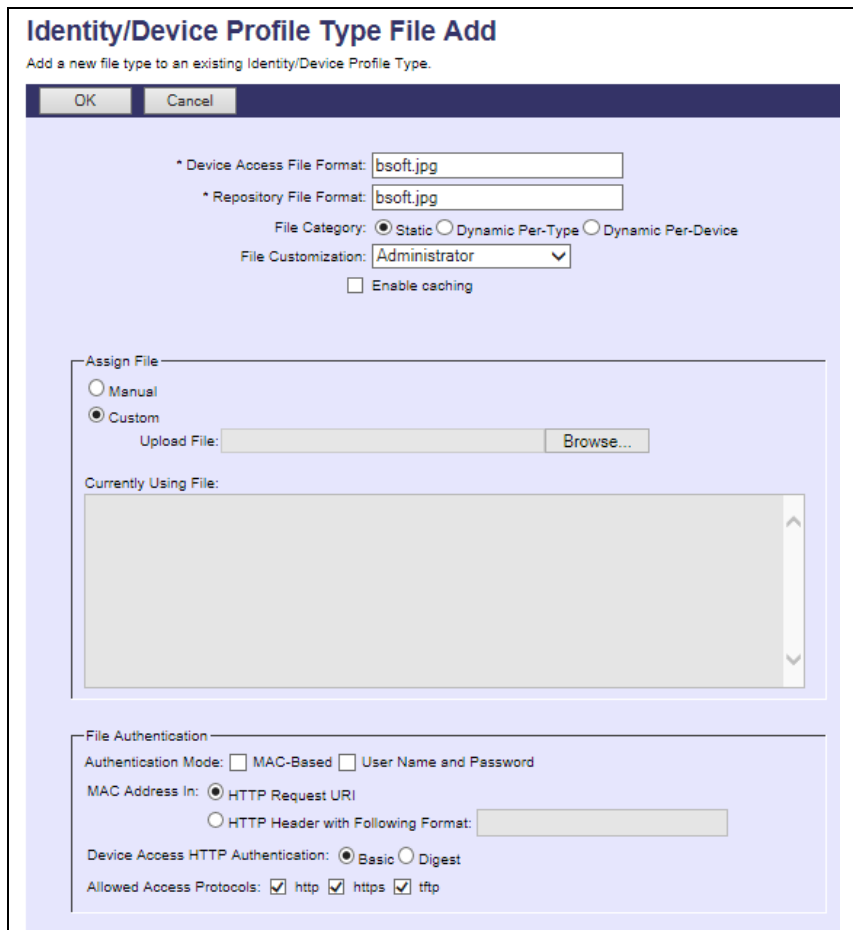


Figure 10 Bitmap Image File

Polycom phones can also load the default background images provided in the Polycom release zip file. These images are released as part of the Polycom firmware package. These files can be uploaded using the mechanism described earlier. These files include *Beach256x116.jpg*, *Beach.jpg*, *BeachEM.jpg*, *Jellyfish256x116.jpg*, *Jellyfish.jpg*, *JellyfishEM.jpg*, *Leaf256x116.jpg*, *Leaf.jpg*, *LeafEM.jpg*, *Mountain256x116.jpg*, *Mountain.jpg*, *MountainEM.jpg*, *Palm256x116.jpg*, *Palm.jpg*, *PalmEm.jpg*, *Sailboat256x116.jpg*, *Sailboat.jpg*, and *SailboatEM.jpg*.

5.2.2.2.2 Device-Specific Files

This section identifies the device-specific files used by Polycom and provides instructions for defining the files and uploading for Device Management.

The device-specific files are described in the following subsections:

- [5.2.2.2.2.1 BWMACADDRESS.cfg](#)
- [5.2.2.2.2.2 phoneBWMACADDRESS.cfg](#)
- [5.2.2.2.2.3 dect.cfg](#)
- [5.2.2.2.2.4 efk.cfg](#)
- [5.2.2.2.2.5 BWMACADDRESS-app.log, BWMACADDRESS-boot.log](#)

5.2.2.2.2.1 BWMACADDRESS.cfg

This is the first file that the phone requests from Device Management at restart. This file defines the firmware file to load, the configuration files to load, and the order in which to load these files.

If necessary, this file can be modified and customized at the group or user level to control the firmware versions and provide custom configurations. The following table describes the file content that can be modified.

Step	Parameter	Purpose
Step 1	Firmware Version Example: <i>Option 1:</i> <pre>APP_FILE_PATH="[PHONE_PART_NUMBER].%APP_VERSION%.sip.ld"</pre> <i>Option 2:</i> <pre>APP_FILE_PATH="%APP_VERSION%.sip.ld"</pre>	The phone can download a firmware file specific to a phone model or a firmware file common to all phone models. <ul style="list-style-type: none"> Option 1 defines a model-specific firmware file. It also uses a Polycom system tag to define the firmware version. Assuming the <code>%APP_VERSION%</code> tag is defined as "5.6.0", the VVX501 model would request a firmware file of 3111-44500-001.6.1.0 sip.ld from Device Management. Option 2 defines a common firmware file. Assuming the <code>%APP_VERSION%</code> tag is defined as "6.1.0", the VVX500 model would request a firmware file of 5.9.0.sip.ld from Device Management. NOTE: The CPE kit uses Option 1.
Step 2	Configuration Files Example: <pre>CONFIG_FILES="phone%BWMACADDRESS%.cfg, efk.cfg, sys.cfg, phonel.cfg, sip.cfg"</pre>	This parameter defines the configuration files to load and the order in which they are loaded. The settings in first file loaded take precedence over the settings in the files that follow. The <i>efk.cfg</i> file is an optional file. If you do not want to use this file, then it needs to be removed from this line so that the phone does not load it. For more information on this file, see section 5.2.2.2.2.3 efk.cfg .

Add a Cisco BroadWorks device profile type file to the Polycom UC Software VVX device profile for the *BWMACADDRESS.cfg* file using the settings described in the following table.

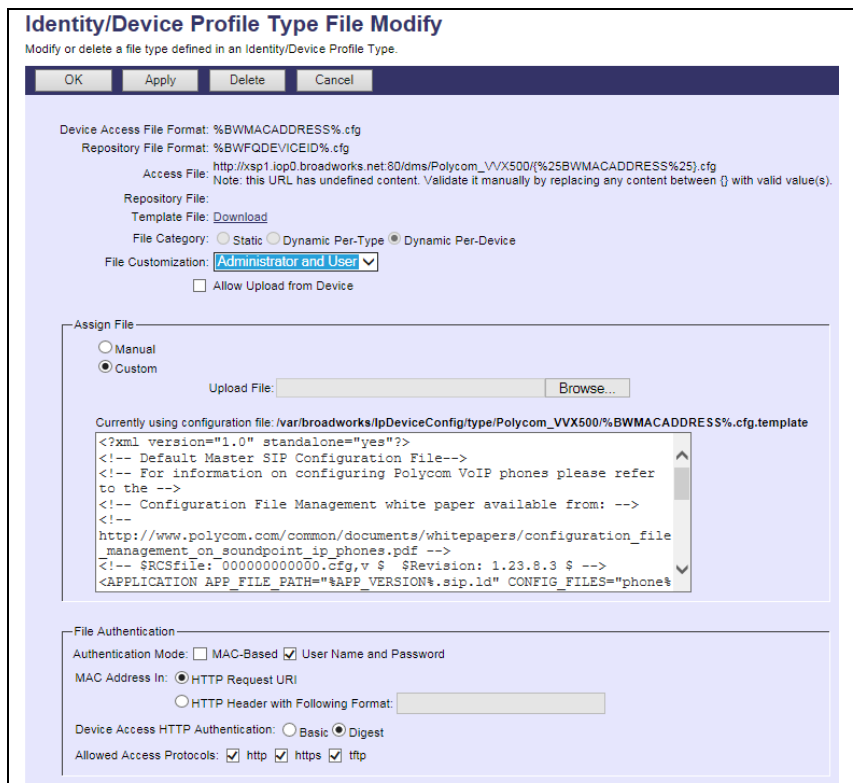
Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	%BWMACADDRESS%.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	%BWFQDEVICEID%.cfg	This is the file name, (as stored in the Device Management repository).
File Category	Dynamic Per-Device	This file is unique per device.
File Customization	Administrator and user	This identifies who can customize this file template.

Parameter	Value	Description
Enable Caching	This is not set.	Caching should not be enabled for device-specific files.
Assign File	Custom	
Authentication Mode	User name and password	This phone-specific file is authenticated with a user name and password.
Device Access HTTP Authentication	Digest	

After defining the device-specific file type, upload the corresponding device-specific file template downloaded from Cisco Xchange. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

Example *BWMACADDRESS.cfg* file settings:



Identity/Device Profile Type File Modify
Modify or delete a file type defined in an Identity/Device Profile Type.

OK Apply Delete Cancel

Device Access File Format: %BWMACADDRESS%.cfg
Repository File Format: %BWFQDEVICEID%.cfg
Access File: http://xsp1.iop0.broadworks.net:80/dms/Polycom_VVX500/(%25BWMACADDRESS%25).cfg
Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).
Repository File:
Template File: [Download](#)
File Category: Static Dynamic Per-Type Dynamic Per-Device
File Customization: [Administrator and User](#)
 Allow Upload from Device

Assign File
 Manual
 Custom
Upload File: [Browse...](#)

Currently using configuration file: /var/broadworks/lpDeviceConfig/type/Polycom_VVX500/%BWMACADDRESS%.cfg.template

```
<?xml version="1.0" standalone="yes"?>
<!-- Default Master SIP Configuration File-->
<!-- For information on configuring Polycom VoIP phones please refer
to the -->
<!-- Configuration File Management white paper available from: -->
<!--
http://www.polycom.com/common/documents/whitepapers/configuration_file
_management_on_soundpoint_ip_phones.pdf -->
<!-- $RCFile: 000000000000.Cfg,v $ $Revision: 1.23.8.3 $ -->
<APPLICATION APP_FILE_PATH="%APP_VERSION%.sip.ld" CONFIG_FILES="phone%
```

File Authentication
Authentication Mode: MAC-Based User Name and Password
MAC Address In: HTTP Request URI
 HTTP Header with Following Format:
Device Access HTTP Authentication: Basic Digest
Allowed Access Protocols: http https tftp

Figure 11 BWMACADDRESS.cfg File

5.2.2.2.2.2 phoneBWMACADDRESS.cfg

The *phoneBWMACADDRESS.cfg* template file in the Polycom CPE kit provides line provisioning of the phone. It may be necessary or desirable for the service provider to customize this file. Note that this file contains configuration data for only 12 lines. To enable configuration for more than 12 lines on the VVX601, additional line configuration items must be added to the file.

The following table describes the file content. Repeat this content structure to add additional lines.

Step	Parameter	Purpose
Step 1	Display Name Example: <code>reg.1.displayName="%BWFIRSTNAME-1% %BWLASTNAME-1%"</code>	Device Management sets this field to the first and last name of the user assigned to the device.
Step 2	Registering Address Example: <code>reg.1.address="%BWLINPORT-1%"</code>	Device Management sets this field to the user part assigned in the user's device address, defined in the <i>line/port</i> field at <i>User → Addresses</i> link.
Step 3	Line Label Example: <code>reg.1.label="%BWEXTENSION-1%"</code>	Device Management sets this field to the extension defined for the user assigned to the device.
Step 4	Line Type Example: <code>reg.1.type="%BWSHAREDLINE-1%"</code>	Device Management sets this field to "shared" if the Shared Call Appearance feature is defined and the shared device is added. Otherwise, this field is set to "private".
Step 5	User Authentication Username Example: <code>reg.1.auth.userId="%BWAUTHUSER-1%"</code>	Device Management sets this field to the authentication user ID defined for the user on Cisco BroadWorks.
Step 6	User Authentication Password Example: <code>reg.1.auth.password="%BWAUTHPASSWORD-1%"</code>	Device Management sets this field to the authentication password defined for the user on Cisco BroadWorks.
Step 7	Server Address Example: <code>reg.1.server.1.address="%BWHOST-1%"</code>	Device Management sets this file to the domain name assigned in the user's device address, defined in the <i>line/port</i> field at the <i>User → Addresses</i> link.
Step 8	Device Feature Synchronization configuration <code>reg.1.serverFeatureControl.cf="%FEAT URE_SYNC_CF%"</code> <code>reg.1.serverFeatureControl.dnd="%FEA TURE_SYNC_DND%"</code>	Device Management sets these parameters to the values defined in section 5.2.1.2 Create Device Type Specific Tags .
Step 9	Bypass Instant Message Example: <code>msg.bypassInstantMessage="1"</code>	This field configures the phone to go directly to the <i>Message Center</i> menu when the <i>Messages</i> button is pressed on the phone.
Step 10	Call Back Address Example: <code>msg.mwi.1.callBack="%BWVOICE-PORTAL- NUMBER-1%"</code>	Device Management sets this field to the group voice portal directory number (DN) assigned to the user, assigned to the device line.

Step	Parameter	Purpose
Step 11	Busy Lamp Field <code><attendant attendant.uri="%BWBLF-USER-1@%BWBLF-DOMAIN-1%" /></code>	Device Management sets this parameter to the <i>user@domain</i> address defined in the Busy Lamp Field feature on Cisco BroadWorks.
Step 12	ACD Synchronization <code><acd acd.reg="%ACD_LINE%" acd.stateAtSignIn="%ACD_SIGNIN_STATE%" /></code>	Device Management sets these parameters to the values defined in section 5.2.1.2 Create Device Type Specific Tags .
Step 13	Barge In <code>reg.1.bargeInEnabled="%BWSCA-BRIDGING-BINARY-1%"</code>	Device Management sets this to the setting for SCA bridging for the line.
Step 14	BroadWorks Enterprise Directory <code>feature.broadsoftdir.enabled="%FEATURE_BW_DIR%"</code> <code>feature.qml.enabled="1"</code> <code>dir.broadsoft.xsp.address="http://%XSP_ADDRESS_XSI_ACTIONS/"</code>	This is used to enable the BroadWorks Enterprise Directory service. NOTE: The Qt Meta Language (QML) is basis of the user interface (UI) for the BroadSoft Enterprise Directory as well as BroadCloud UC-One. This parameter must be set to "1".
Step 15	BroadCloud UC-One <code>feature.broadsoftUcOne.enabled="%FEATURE_BW_UC_ONE%"</code> <code>xmpp.1.enable="%FEATURE_BW_UC_ONE%"</code> <code>xmpp.1.server="%BW_IMP_SERVICE_NET_ADDRESS-1%"</code> <code>xmpp.1.auth.domain="%BW_IMP_SERVICE_NET_ADDRESS-1%"</code> <code>xmpp.1.auth.password="%BW_USER_IMP_PWD-1%"</code> <code>xmpp.1.jid="%BW_USER_IMP_ID-1%"</code> <code>xmpp.1.dialMethod="sip"</code>	This is used to enable the BroadCloud UC-One directory feature. NOTE: The BroadSoft Enterprise Directory must be enabled for BroadCloud UC-One to be shown on user interface.
Step 16	UC-One Presence <code>feature.presence.enabled="%FEATURE_PRESENCE%"</code>	This is used to enable the BroadCloud UC-One Presence feature.

Add a Cisco BroadWorks device profile type file to the Polycom UC Software device profile for the *phoneBWMACADDRESS.cfg* file using the settings described in the following table.

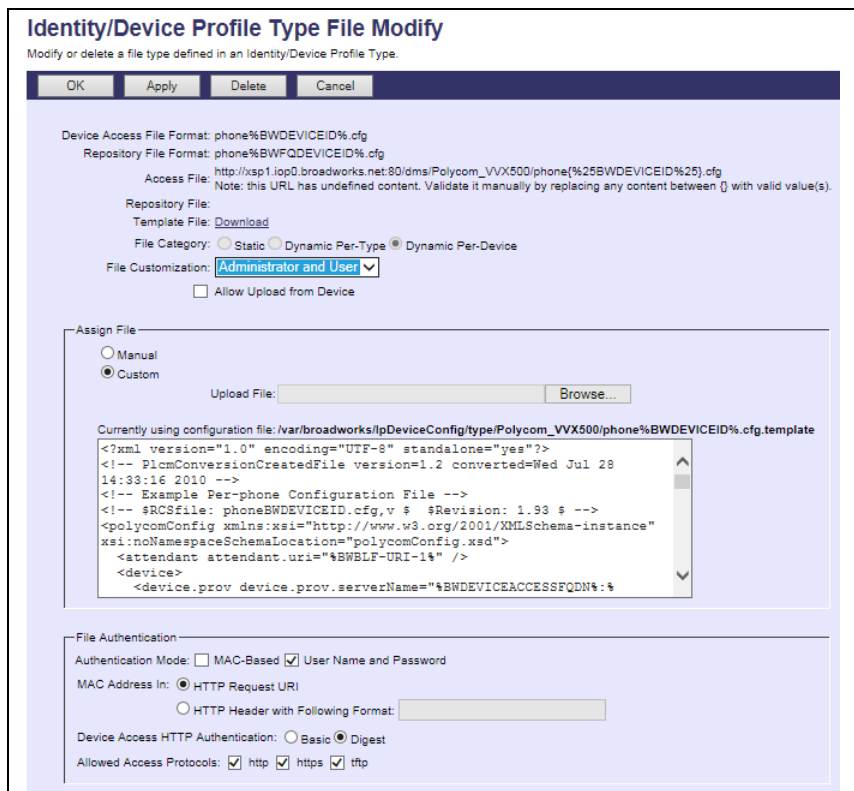
Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	phone%BWMACADDRESS%.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	phone%BWFQDEVICEID%.cfg	This is the file name, (as stored in the Device Management repository).
File Category	Dynamic Per-Device	This file is unique per device.
File Customization	Administrator and user	This identifies who can customize this file template.
Enable Caching	This is not set.	Caching should not be enabled for device-specific files.
Assign File	Custom	

Parameter	Value	Description
Authentication Mode	User name and password	The phone-specific file is authenticated with a user name and password.
Device Access HTTP Authentication	Digest	

After defining the device-specific file type, upload the corresponding device-specific file template downloaded from Cisco Xchange. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

Example *phoneBWMACADDRESS.cfg* file settings:



Identity/Device Profile Type File Modify
Modify or delete a file type defined in an Identity/Device Profile Type.

OK Apply Delete Cancel

Device Access File Format: phone%BWDEVICEID%.cfg
Repository File Format: phone%BWFQDEVICEID%.cfg
Access File: http://xsp1.iop0.broadworks.net:80/dms/Polycom_VVX500/phone(%25BWDEVICEID%25).cfg
Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).

Repository File:
Template File: [Download](#)
File Category: Static Dynamic Per-Type Dynamic Per-Device
File Customization: **Administrator and User** Allow Upload from Device

Assign File
 Manual
 Custom
Upload File: [Browse...](#)

Currently using configuration file: /var/broadworks/lpDeviceConfig/type/Polycom_VVX500/phone%BWDEVICEID%.cfg.template

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- PlcmConversionCreatedFile version=1.2 converted=Wed Jul 28
14:33:16 2010 -->
<!-- Example Per-phone Configuration File -->
<!-- $RCSfile: phoneBNDVICEID.cfg,v $ $Revision: 1.93 $ -->
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
  <attendant attendant.uri="%BWLFI-URI-1%" />
</device>
<device.prov device.prov.serverName="%BNDVICEACCESSFQDN%:"
```

File Authentication
Authentication Mode: MAC-Based User Name and Password
MAC Address In: HTTP Request URI
 HTTP Header with Following Format:
Device Access HTTP Authentication: Basic Digest
Allowed Access Protocols: http https tftp

Figure 12 phoneBWMACADDRESS.cfg File

5.2.2.2.2.3 dect.cfg

The D60 wireless base station and handsets is an optional accessory for the VVX 3x1 series, 4x1 series, 501 series, and 601 series business media phones that enables users to manage calls to their lines at any time while they are away from their desk. The *dect.cfg* file in the CPE kit provides an example of how to configure the D60 on the Polycom phones.

This file is intended as an example. It is expected that the service provider or group administrator customizes this file as appropriate for individual phones that are attached to the D60 base station. For a description and instructions to provision the D60 base station and handsets, see the *Polycom UC Software Administrator's Guide* [1].

Example *dect.cfg* file settings:



Identity/Device Profile Type File Modify
Modify or delete a file type defined in an Identity/Device Profile Type.

OK Apply Delete Cancel

Device Access File Format: dect.cfg
Repository File Format: dect-%BWFQDEVICEID%.cfg
Access File: http://xsp1.ipp1.broadworks.net:80/dms/Polycom_VVX500/dect.cfg
Repository File:
Template File: [Download](#)
File Category: Static Dynamic Per-Type Dynamic Per-Device
File Customization: Administrator and User ▾
 Allow Upload from Device
Extended File Capture
 Default Extended File Capture Mode
[Enable for All File Instances](#) [Disable for All File Instances](#)

Assign File
 Manual
 Custom
Upload File: [Choose File](#) No file chosen

Currently using configuration file: /var/broadworks/lpDeviceConfig/type/Polycom_VVX500/dect.cfg.template

```

???<?xml version="1.0" encoding="utf-8" standalone="yes">
<!-- Generated global_full.cfg Configuration File -->
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
<dect>
<dect.update dect.update.mask="0"></dect.update>
</dect>
<feature>
<feature.dect feature.dect.enabled="%FEATURE_DECT%">
</feature.dect>

```

File Authentication
Authentication Mode: MAC-Based User Name and Password
MAC Address In: HTTP Request URI
 HTTP Header
 Client Certificate
MAC Address Format:
Device Access HTTP Authentication: Basic Digest
Allowed Access Protocols: http https tftp

OK Apply Delete Cancel

Figure 13 dect.cfg File

5.2.2.2.2.4 efk.cfg

The enhanced feature and soft key (*efk.cfg*) file is an optional configuration file. The *efk.cfg* file in the CPE kit provides an example of how to configure the enhanced feature soft keys on the Polycom phones. The example file provides configuration of the following buttons on the Polycom phones:

- Conference Bridge (CnfBridge) – This feature key prompts for a bridge extension and then prompts for the passcode. Once this information is entered, the phone dials the bridge and enters the passcode. This configuration needs to be modified for your specific deployment.
- Push To Talk (PTT) – This key prompts for a user extension and then performs the Push to Talk function to the user requested.
- Call Pull – This key is defined to do a call pull from a call on a BroadWorks Anywhere number (cell phone) to the Polycom phone.
- Qsetup – This key displays the phone’s file server configuration page. The Xtended Services Platform location, user name, and password can be entered on this page.
- SendVM – This key is displayed when a call is active. When pressed, it prompts for a user extension to transfer to Voice Messaging. The call is transferred to this user’s Voice Messaging.

This file is intended as an example. It is expected that the service provider would usually customize this file as appropriate for their customer base and possibly for individual phones. For description and instructions to define the feature and soft keys, see the *Polycom UC Software Administrator’s Guide* [1]. Note that there are no Device Management tags used in this file so the file is actually a *static* Device Management file.

If this Polycom capability is not used, then the *efk.cfg* file should be removed from the *BWMACADDRESS.cfg* file described in section [5.2.2.2.2.1 BWMACADDRESS.cfg](#).

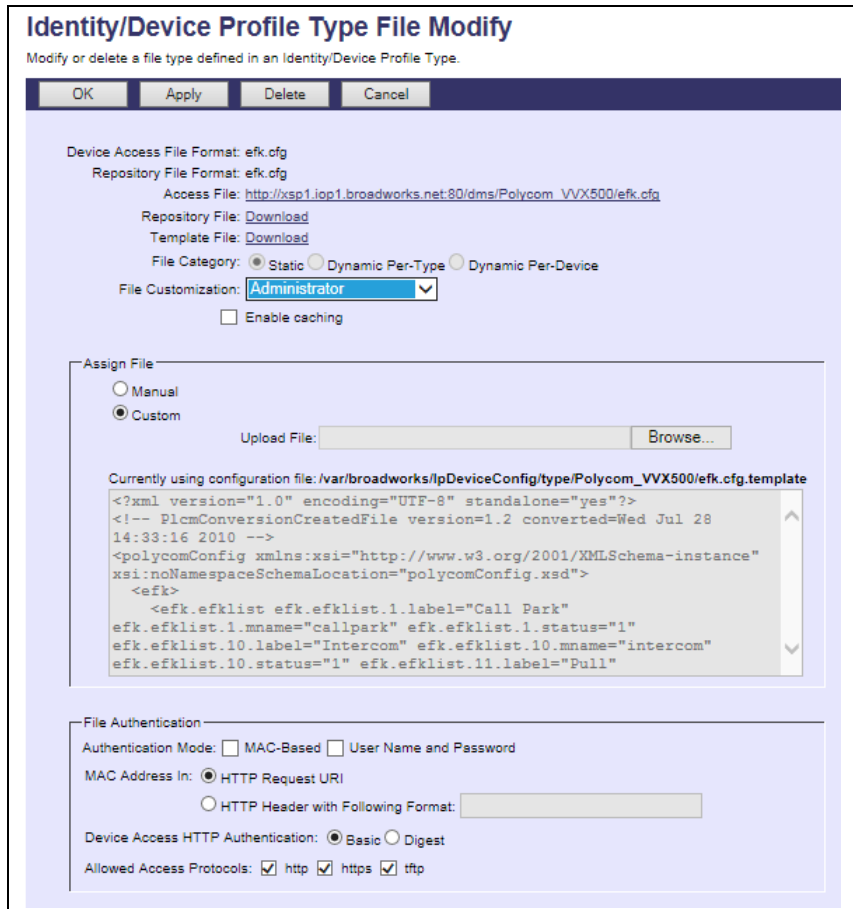
If this capability is used, add a BroadWorks device profile type file to the Polycom UC Software device profile for the *efk.cfg* file using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	efk.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	efk.cfg	This is the file name, (as stored in the Device Management repository).
File Category	Static	This file does not contain tags.
File Customization	Administrator	This identifies who can customize this file template.
Enable Caching	This is not set.	Caching is not recommended.
Assign File	Custom	

After defining the file, upload the corresponding *efk.cfg* file template downloaded from Cisco Xchange. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

Example *efk.cfg* file settings:



Identity/Device Profile Type File Modify
Modify or delete a file type defined in an Identity/Device Profile Type.

OK Apply Delete Cancel

Device Access File Format: efk.cfg
Repository File Format: efk.cfg
Access File: http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX500/efk.cfg
Repository File: [Download](#)
Template File: [Download](#)
File Category: Static Dynamic Per-Type Dynamic Per-Device
File Customization: Administrator
 Enable caching

Assign File
 Manual
 Custom
Upload File: Browse...

Currently using configuration file: /var/broadworks/lpDeviceConfig/type/Polycom_VVX500/efk.cfg.template

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- PlcmConversionCreatedFile version=1.2 converted=Wed Jul 28
14:33:16 2010 -->
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
  <efk>
    <efk.efklist efk.efklist.1.label="Call Park"
efk.efklist.1.mname="callpark" efk.efklist.1.status="1"
efk.efklist.10.label="Intercom" efk.efklist.10.mname="intercom"
efk.efklist.10.status="1" efk.efklist.11.label="Pull"
  </efk>
</polycomConfig>
```

File Authentication
Authentication Mode: MAC-Based User Name and Password
MAC Address In: HTTP Request URI
 HTTP Header with Following Format:
Device Access HTTP Authentication: Basic Digest
Allowed Access Protocols: http https ftp

Figure 14 efk.cfg File

5.2.2.2.2.5 BWMACCADDRESS-app.log, BWMACCADDRESS-boot.log with Extended File Capture

The Polycom UC Software VVX devices periodically upload the <MAC Address>-app.log and <MAC Address>-boot.log files onto the device management server for administrative review. This capability can be further enhanced with the Cisco BroadWorks Device Management's Extended File Capture feature where several iterations of the files can be kept on the Device Management server.

To enable the Extended File Capture feature, these following steps are required:

- 1) Deploy the extended file capture repository web application on the Profile Server. Then, perform the file repository provisioning on the profile server.
- 2) Perform Application Server extended capture repository configuration.
- 3) Associate a device profile type to the extended file capture repository; then, enable extended file capture on the device profile type template files.

The first two steps are one-time server-side configurations and must be performed through the BroadWorks Command Line Interface (BWCLI). For the configure procedures of the server-side configuration, see the Appendix B. Following is the last configuration step. It is device profile type specific and must be individually performed for each device profile type:

Associating Device Profile Type and Extended File Capture repository

From the Application Server Command Line Interface (AS_CLI), the device profile type needs to be associated with an extended capture file repository.

Example:

```
AS_CLI/System/Device/IpDeviceMgmt/Fileserver> set Polycom_VVX600 extendedCaptureFileReposName
PSExtended

AS_CLI/System/Device/IpDeviceMgmt/Fileserver> 0
Device Type File Repository Name Extended Capture File Repository Name Directory
=====
Polycom_VVX600 ProfileServer PSExtended Polycom_VVX600
```

Enable Extended File Capture on <MAC Address>-app.log and <MAC Address>-boot.log

The two files uploaded by the boot firmware and the application firmware respectively must be identified to Cisco BroadWorks with place holders so that the phone can upload these files to the system.

Add a Cisco BroadWorks device profile type file to the Polycom UC Software device profile for both the *BWMACADDRESS-app.log* and *BWMACADDRESS-boot.log* files using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	%BWMACADDRESS%-app.log %BWMACADDRESS%-boot.log	This is the file name, which the phone uses to request the file.
Repository File Format	%BWFQDEVICEID%-app.log %BWFQDEVICEID%-boot.log	This is the file name, (as stored in the Device Management repository).
File Category	Dynamic-Per-Device	This file does not contain tags.
File Customization	Administrator	This identifies who can customize the file.
Allow Upload from Device	X	This check box controls whether the file can be uploaded from a device.
Default Extended File Capture Mode	X	This check box controls whether the file will be kept in the extended file capture repository.
Assign File	Manual	
Authentication Mode	User name and password	The phone-specific file is authenticated with a user name and password.
Device Access HTTP Authentication	Digest	

Example *Default Extended File Capture Mode*:

Identity/Device Profile Type File Modify

Modify or delete a file type defined in an Identity/Device Profile Type.

Device Access File: %BWMACADDRESS%-app.log
 Format: %BWMACADDRESS%-app.log
 Repository File: %BWFQDEVICEID%-app.log
 Format: %BWFQDEVICEID%-app.log
 Access File: http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800(%25BWMACADDRESS%25)-app.log
 Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).
 Repository File:
 Template File:
 File Category: Static Dynamic Per-Type Dynamic Per-Device
 File Customization: Administrator

Allow Upload from Device
 Extended File Capture
 Default Extended File Capture Mode
[Enable for All File Instances](#) [Disable for All File Instances](#)

Assign File
 Manual
 Custom
 Upload File:

File Authentication
 Authentication Mode: MAC-Based User Name and Password
 MAC Address In: HTTP Request URI
 HTTP Header with Following Format:
 Device Access HTTP Authentication: Basic Digest
 Allowed Access Protocols: http https tftp

Figure 15 Enable Extended File Capture Setting

After the place holder files are created, the files must be rebuilt for the appropriate file structure to be created in the file repository. Click on the *Rebuild all device profile files* on the *Identity/Device Profile Type Files* page.

Example *Identity/Device Profile Type Files* page:

Identity/Device Profile Type Files

Displays the files defined for the Identity/Device Profile Type.

[Rebuild all device type files](#) **Rebuild all device profile files** [Reset the phones](#)
(After rebuilding the files, be sure to reload the phones to apply your changes to take effect)

File Format	Is Authenticated	Access File	Repository File	Template File	Edit
%BWMACADDRESS%.cfg	✓	http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800(%25BWMACADDRESS%25).cfg Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).		Download	Edit
%BWMACADDRESS%-app.log	✓	http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800(%25BWMACADDRESS%25)-app.log Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).			Edit
%BWMACADDRESS%-boot.log	✓	http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800(%25BWMACADDRESS%25)-boot.log Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).			Edit
%BWMACADDRESS%-directory.xml	✓	http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800(%25BWMACADDRESS%25)-directory.xml Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).		Download	Edit
000000000000.cfg		http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800/000000000000.cfg	Download		Edit
3111-44600-001.4.1.3.sip.id		http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800/3111-44600-001.4.1.3.sip.id	Download	Download	Edit
phone%BWMACADDRESS%.cfg	✓	http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800/phone(%25BWMACADDRESS%25).cfg Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).		Download	Edit
qsetup.cfg		http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800/qsetup.cfg	Download	Download	Edit
sys.cfg	✓	http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX800/sys.cfg	Download	Download	Edit

[Page 1 of 1]

Figure 16 Rebuild All Device Profile Files

Accessing Extended Captured files

The files uploaded from the Polycom UC Devices can be access by administrators from each of the device profile's Files page. Once the Download link is followed, a compressed ZIP folder containing the kept instances on the Extended File Capture Repository is downloaded.

Example of the available Extended Captures

Identity/Device Profile Modify
View or modify files used by the Identity/Device Profile.

OK

Profile | **Users** | **Files** | **Custom Tags**

Identity/Device Profile Name: polyvxx800
Identity/Device Profile Type: Polycom_VVX800

Rebuild the files *Reset the phones*
(After rebuilding the files, be sure to reset the phones for your changes to take effect)

File Format(A)	Is Authenticated	Access File	Repository File	Template File	Extended Capture	Edit
%BWMACADDRESS% cfg	✓	http://xsp1.lip1.broadworks.net:80/dms/Polycom_VVX800/0004f2807897.cfg	Download	Download	Download	Edit
%BWMACADDRESS%-app.log	✓	http://xsp1.lip1.broadworks.net:80/dms/Polycom_VVX800/0004f2807897-app.log			Download	Edit
%BWMACADDRESS%-boot.log	✓	http://xsp1.lip1.broadworks.net:80/dms/Polycom_VVX800/0004f2807897-boot.log			Download	Edit
000000000000.cfg		http://xsp1.lip1.broadworks.net:80/dms/Polycom_VVX800/000000000000.cfg	Download	Download		Edit
phone%BWMACADDRESS% cfg	✓	http://xsp1.lip1.broadworks.net:80/dms/Polycom_VVX800/phone0004f2807897.cfg	Download	Download		Edit
qsetup.cfg		http://xsp1.lip1.broadworks.net:80/dms/Polycom_VVX800/qsetup.cfg	Download	Download		Edit
sys.cfg	✓	http://xsp1.lip1.broadworks.net:80/dms/Polycom_VVX800/sys.cfg	Download	Download		Edit

[Page 1 of 1]

OK

Figure 17 Extended Captured Files

5.2.2.2.2.3 Static Files

Static files are files, such as firmware and media files, that are not configurable and/or do not make use of the dynamic Cisco BroadWorks Device Management tags.

The following sections cover the following Polycom UC Software static files and topics:

- [5.2.2.2.2.3.1 Application Firmware](#)
- [5.2.2.2.2.3.2 Time Zone Alias File](#)
- [5.2.2.2.2.3.3 Language Provisioning \(Optional\)](#)
- [5.2.2.2.2.3.4 Startup Welcome Audio File \(Optional\)](#)
- [5.2.2.2.2.3.5 Quick Setup \(Optional\)](#)
- [5.2.2.2.2.3.6 Polycom Productivity Suite Files \(Optional\)](#)
- [5.2.2.2.2.3.7 Polycom Phone Service](#)

5.2.2.2.2.3.1 Application Firmware

The application firmware is identified similarly to the boot firmware as follows:

`<part number>.<version>.sip.ld`

The *part number* is Polycom's distinct identifier mapping a model to firmware. For a complete part number mapping list, see the *Polycom UC Software Administrator's Guide* [1].

The *version* is the application firmware version as specified by the `APP_VERSION` tag in the `BWMACADDRESS.cfg` template file. Note that the `APP_VERSION` tag can be overridden at the group or user level for a controlled or phased upgrade.

Examples:

- Polycom VVX101: 3111-40250-001.6.1.0.sip.ld
- Polycom VVX150: 3111-48810-001.6.1.0.sip.ld
- Polycom VVX201: 3111-40450-001.6.1.0.sip.ld
- Polycom VVX250: 3111-48820-001.6.1.0.sip.ld
- Polycom VVX301: 3111-48300-001.6.1.0.sip.ld
- Polycom VVX311: 3111-48350-001.6.1.0.sip.ld
- Polycom VVX350: 3111-48830-001.6.1.0.sip.ld
- Polycom VVX401: 3111-48400-001.6.1.0.sip.ld
- Polycom VVX411: 3111-48450-001.6.1.0.sip.ld
- Polycom VVX450: 3111-48840-001.6.1.0.sip.ld
- Polycom VVX501: 3111-48500-001.6.1.0.sip.ld
- Polycom VVX601: 3111-48600-001.6.1.0.sip.ld

Note that during boot time, the phone requests the specific model file (`<part-number>.<version>.sip.ld`) first, and if it is not found, it requests the `<version>.sip.ld` file.

Add a Cisco BroadWorks device profile type file to the Polycom UC Software device profile for the application file using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	<part number>.<version>.sip.ld Example: 3111-48600-001.6.1.0.sip.ld	This is the file name, which the phone uses to request the file.
Repository File Format	<part number>.<version>.sip.ld Example: 3111-48600-001.6.1.0.sip.ld	This is the file name stored in the Device Management repository. Use the same name as the actual file name.
File Category	Static	This is a static file. There are no dynamic tags in the file.
File Customization	Disallow	This file must not be modified.
Enable Caching	Selected	Caching should usually be enabled for static files.
Assign File	Custom	
Authentication Mode	This is not set.	The static files are not authenticated so do not select either of the options.

After defining the application firmware file type, upload the corresponding application firmware file for the device or firmware files for the series. Application firmware files are not included in the CPE kit and must be obtained from Polycom. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

Repeat the instructions in this section for each model's application firmware.

Example application firmware file settings:

Identity/Device Profile Type File Add

Add a new file type to an existing Identity/Device Profile Type.

OK
Cancel

* Device Access File Format:

* Repository File Format:

File Category: Static Dynamic Per-Type Dynamic Per-Device

File Customization:

Enable caching

Assign File

Manual

Custom

Upload File: No file chosen

Currently Using File:

File Authentication

Authentication Mode: MAC-Based User Name and Password

MAC Address In: HTTP Request URI HTTP Header Client Certificate

MAC Address Format:

Device Access HTTP Authentication: Basic Digest

Allowed Access Protocols: http https tftp

OK
Cancel

Figure 18 Application Firmware File Settings

5.2.2.2.3.2 Time Zone Alias File

To map a Cisco BroadWorks configured user time zone properly to the Polycom UC Software devices, a mapping file must be created on the Cisco BroadWorks system. This file maps the Cisco BroadWorks user time zone settings to the phone's time zone settings. Time zone mapping for the device profile type is documented in the *BroadWorks Device Management Configuration Guide* [2].

This time zone mapping file must be added to the `/usr/local/broadworks/bw_base/conf/dms` directory on the Application Server using the following file name format:

- `TimeZoneAliasLabels_Polycom_VVX500.properties`
- `TimeZoneAliasLabels_Polycom-VVX-Standard.properties`

For example, if the device type name is `Polycom_VVX500`, the time zone mapping file name must be `TimeZoneAliasLabels_Polycom_VVX500.properties`. (Note that if there is a space in the device name, then the space must be converted to a "+" in the file name.)

If a unique device profile type is configured for each model, a separate `TimeZoneAlias` file must be created for each model. If a single device type is used for all models, a single `TimeZoneAlias` file is required (for example, `TimeZoneAliasLabels_Polycom-VVX-Standard.properties`).

The file must contain the mapping of Cisco BroadWorks time zones values to Polycom UC Software device time zone values. The following is an example of the file contents:

```
CANADA_PACIFIC_TIME=-28800
US_PACIFIC_TIME=-28800
CANADA_MOUNTAIN_TIME=-25200
US_MOUNTAIN_TIME=-25200
CANADA_CENTRAL_TIME=-21600
US_CENTRAL_TIME=-21600
CANADA_EASTERN_TIME=-18000
US_EASTERN_TIME=-18000
CANADA_ALTANTIC_TIME=-14400
CANADA_NEWFOUNDLAND=-12600
```

This file should contain all time zones supported by the service provider's Cisco BroadWorks system. The Application Server must be restarted to load this file.

The CPE kit contains the time zone properties files defined for the continental U.S. and Canadian time zones. For other time zone settings, see the *Polycom UC Software Administrator's Guide* [1]. When using the DTAF import, the `TimeZoneAlias` files are automatically copied to the system.

The Cisco BroadWorks Application Server must be restarted for the `TimeZoneAlias` files to be picked up by the system.

5.2.2.2.3.3 Language Provisioning (Optional)

There are two aspects to language provisioning. First, the Polycom phone must be enabled to download the Polycom language files. Second, a mapping is required between the Cisco BroadWorks language identifiers and Polycom's language identifiers.

5.2.2.2.3.3.1 Language Files

The Polycom VVX phone by default is preloaded with the English language. If the phone is configured to use a language other than English, then it downloads the language file from Device Management.

The phone requests the language file in the following format:

<Localization Directory>/<Language Directory>/VFX-dictionary.xml

The available Polycom VFX language files are delivered from Polycom along with the firmware. The following table defines the file paths that should be entered when uploading the files to Device Management.

Language	File Path
Chinese	VFXLocalization/Chinese_China/VFX-dictionary.xml
Danish	VFXLocalization/Danish_Denmark/VFX-dictionary.xml
Dutch	VFXLocalization/Dutch_Netherlands/VFX-dictionary.xml
English Canada	VFXLocalization/English_Canada/VFX-dictionary.xml
English United Kingdom	VFXLocalization/English_United_Kingdom/VFX-dictionary.xml
English United States	VFXLocalization/English_United_States/VFX-dictionary.xml
French	VFXLocalization/French_France/VFX-dictionary.xml
German	VFXLocalization/German_Germany/VFX-dictionary.xml
Italian	VFXLocalization/Italian_Italy/VFX-dictionary.xml
Japanese	VFXLocalization/Japanese_Japan/VFX-dictionary.xml
Korean	VFXLocalization/Korean_Korea/VFX-dictionary.xml
Norwegian	VFXLocalization/Norwegian_Norway/VFX-dictionary.xml
Polish	VFXLocalization/Polish_Poland/VFX-dictionary.xml
Portuguese	VFXLocalization/Portuguese_Portugal/VFX-dictionary.xml
Russian	VFXLocalization/Russian_Russia/VFX-dictionary.xml
Slovenian	VFXLocalization/Slovenian_Slovenia/VFX-dictionary.xml
Spanish	VFXLocalization/Spanish_Spain/VFX-dictionary.xml
Swedish	VFXLocalization/Swedish_Sweden/VFX-dictionary.xml

To enable language file download, add a Cisco BroadWorks device profile type file to the Polycom UC Software VFX device profile using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	Enter the path in the table above for the requested file format for the language file uploaded.	This is the file name, which the phone uses to request the file.
Repository File Format	Enter the path in the table above for the requested file format for the language file uploaded.	This is the file name, (as stored in the Device Management repository). Note, use the same name as the actual file name.
File Category	Static	This is a static file. There are no dynamic tags in the file.
File Customization	Disallow	This file must not be modified.

Parameter	Value	Description
Enable Caching	This is not selected.	Caching is optional for this file.
Assign File	Custom	
Authentication Mode	This is not set.	The static files are not authenticated so do not select either of the options.

After defining the language file type, upload the associated language file obtained from Polycom. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

Repeat the instructions in this section for each language to be loaded. After loading languages for this Polycom VVX device profile type, repeat this section for other models.

5.2.2.2.3.3.2 Language Mapping

To enable Device Management control of the phone language, the languages defined on the Cisco BroadWorks Application Server must be mapped to the Polycom definitions. To perform the mapping, select the Polycom device profile type and then select the *Languages* link. The defined Cisco BroadWorks languages are listed in a table. If languages other than English do not appear, they have not been defined. The supported languages and required mapping are as follows:

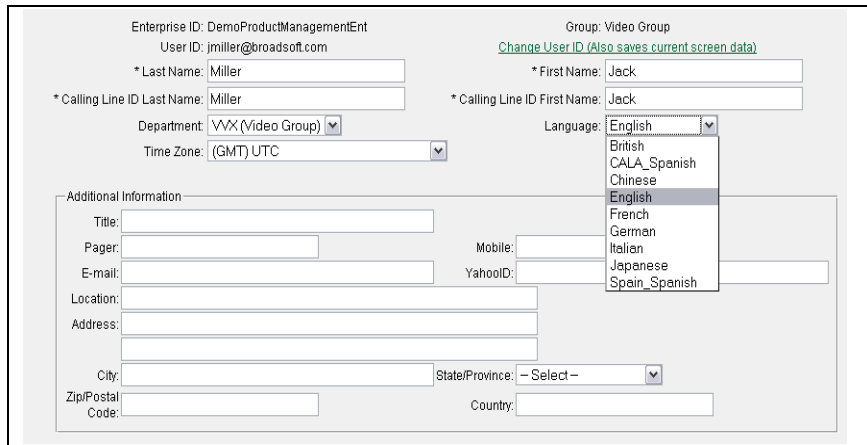
Cisco BroadWorks Language	Polycom Language Mapping
English	English_United_States or English_Canada
British	English_United_Kingdom
CALA_Spanish	Spanish_Spain
Chinese	Chinese_China
French	French_France
German	German_Germany
Italian	Italian_Italy
Japanese	Japanese_Japan
Spain_Spanish	Spanish_Spain

Example language mapping:

BroadWorks Language	Device Language
British:	English_United_Kingdom
CALA_Spanish:	Spanish_Spain
Chinese:	Chinese_China
English:	English_United_States
French:	French_France
German:	German_Germany
Italian:	Italian_Italy
Japanese:	Japanese_Japan
Spain_Spanish:	Spanish_Spain

Figure 19 Language Mapping

The language applied to an individual phone is determined by the language defined for the user on the *BroadWorks User's Profile* page (see [Figure 20 BroadWorks User Language Definition](#)).



Enterprise ID: DemoProductManagementEnt
 User ID: jmiller@broadsoft.com
 Group: Video Group
[Change User ID \(Also saves current screen data\)](#)

* Last Name: Miller * First Name: Jack
 * Calling Line ID Last Name: Miller * Calling Line ID First Name: Jack

Department: VVX (Video Group) Language: English
 Time Zone: (GMT) UTC

Additional Information

Title: _____
 Pager: _____ Mobile: _____
 E-mail: _____ YahooID: _____
 Location: _____
 Address: _____
 City: _____ State/Province: - Select -
 Zip/Postal Code: _____ Country: _____

Figure 20 BroadWorks User Language Definition

The phone can manually download Polycom-supported languages not supported by Cisco BroadWorks via the *Language Preferences* menu on the phone. To access this menu, press the *Menu* key on the phone and select *Settings* → *Basic* → *Preferences* → *Language*, and from this page select the desired language for the phone to use on the display.

5.2.2.2.3.4 Startup Welcome Audio File (Optional)

The Polycom phone can be configured to play a WAV file at startup. The WAV file must be uploaded to Device Management. Polycom provides the WAV file (*Welcome.wav*) in the Polycom release ZIP file.

To upload the WAV file, add a Cisco BroadWorks device profile type file to the Polycom UC Software device profile using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	Welcome.wav	This is the file name, which the phone uses to request the file.
Repository File Format	Welcome.wav	This is the file name, (as stored in the Device Management repository). Note, use the same name as the actual file name.
File Category	Static	This is a static file. There are no dynamic tags in the file.
File Customization	Disallow	This file must not be modified.
Enable Caching	This is not selected.	Caching is optional for this file.
Assign File	Custom	
Authentication Mode	This is not set.	The static files are not authenticated so do not select either of the options.

After defining the welcome audio file type, upload the WAV file obtained from Polycom. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

Repeat the instructions in this section for each model.

5.2.2.2.3.5 Quick Setup (Optional)

Polycom provides a quick setup feature, which enables a phone to boot up when it cannot find its *macaddress.cfg* file. It presents the user with a Quick Setup key on the phone to enter the data from the phone. This section identifies the files and configuration necessary to enable Quick Setup.

5.2.2.2.3.5.1 000000000000.cfg

Polycom devices request the default *macaddress* file (*000000000000.cfg*) from Device Management if a request for the *macaddress.cfg* file fails. The *000000000000.cfg* file provides default instructions applicable to any Polycom device. This file identifies the following files for the phone to download:

- *sip.ld* firmware file
- *qsetup.cfg* file to trigger the Quick Setup soft key and its functionality

Add a Cisco BroadWorks device profile type file to the *DeviceManagementDefaults* device profile for the *000000000000.cfg* file using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	000000000000.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	000000000000.cfg	This is the file name, (as stored in the Device Management repository).
File Category	Static	This file is unique per device type.
File Customization	Disallow	This identifies who can customize this file template.
Enable Caching	Selected	Caching is recommended for this file.
Assign File	Custom	
Authentication Mode	None	The phone-specific file is authenticated with a user name and password.

After defining the file, upload the *000000000000.cfg* file template downloaded from Cisco Xchange. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

5.2.2.2.2.3.5.2 *qsetup.cfg*

Polycom has implemented a Quick Setup (QSetup) soft key. Pressing this key at phone initialization automatically brings up the file server menu and the associated parameters on the Polycom UC Software device. By identifying this configuration file name in the *000000000000.cfg* file, the Quick Setup soft key is shown on the device.

Add a Cisco BroadWorks device profile type file to the *DeviceManagementDefaults* device profile for the *qsetup.cfg* file using the settings described in the following table.

Parameters not identified in the following table can usually be left as defaults.

Parameter	Value	Description
Device Access File Format	qsetup.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	qsetup.cfg	This is the file name, (as stored in the Device Management repository).
File Category	Static	This file is unique per device type.
File Customization	Disallow	This identifies who can customize this file template.
Enable Caching	Selected	Caching is recommended for this file.
Assign File	Custom	
Authentication Mode	None	The phone-specific file is authenticated with a user name and password.

After defining the file, upload the corresponding *qsetup.cfg* file template downloaded from Cisco Xchange. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

5.2.2.2.3.6 Polycom Productivity Suite Files (Optional)

Polycom provides a licensable UC Software Productivity Suite, which when licensed, enables additional features and capabilities on the phone. For more information on the Productivity Suite, see the *Polycom UC Software Administrator's Guide* [1]. Skip this section if not applicable.

The service provider must purchase a Productivity Suite license from Polycom. After doing so, the license can be applied to all phones or select phones using Device Management.

Polycom delivers the site license in the *000000000000-license.cfg* file and the individual user license in the *MACADDRESS-license.cfg* file, where MACADDRESS is the end user's phone MAC address. The service provider can use Device Management and the Polycom site license key to license these features to the entire system or on a per-Cisco BroadWorks group or per-Cisco BroadWorks user basis.

5.2.2.2.3.6.1 Polycom Productivity Suite License – System Wide

To assign the Productivity Suite license to all Polycom VVX phones, add a Cisco BroadWorks device profile type file to the Polycom UC Software VVX device profile using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	000000000000-license.cfg.	This is the file name, which the phone uses to request the file.
Repository File Format	000000000000-license.cfg.	This is the file name, (as stored in the Device Management repository). Note, use the same name as the actual file name.
File Category	Static.	This is a static file. There are no dynamic tags in the file.
File Customization	Disallow.	This file must not be modified.
Enable Caching	This is not selected.	Caching is optional for this file.
Assign File	Custom.	
Authentication Mode	This is not set.	The static files are not authenticated so do not select either of the options.

After defining the Productivity Suite license file type, upload the license file obtained from Polycom. Click the **Browse** button on the file definition screen and click the **Apply** button after uploading the file.

Repeat the instructions in this section for each model for which the license applies.

5.2.2.2.3.6.2 Polycom Productivity Suite License – Per Group or User

To assign the Productivity Suite license to specific groups or users, add a Cisco BroadWorks device profile type file to the Polycom UC Software VVX device profile using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	%BWMACADDRESS%-license.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	%BWFQDEVICEID%-license.cfg	This is the file name, (as stored in the Device Management repository). Note, use the same name as the actual file name.
File Category	Static	This is a static file. There are no dynamic tags in the file.
File Customization	Administrator	Allow administrator to customize the file.
Enable Caching	<i>This is not selected.</i>	Caching is optional for this file.
Assign File	Manual	
Authentication Mode	User name and password	The phone-specific file is authenticated with a user name and password.
Device Access HTTP Authentication	Digest	

At this point, the file is defined for the device profile type. Repeat the instructions above for each model to which the license applies.

To apply the license to a specific group, perform the following steps.

- 1) Search for and select the Cisco BroadWorks group.
- 2) Select the *Utilities* link in the left column from the *Group* page.
- 3) Select the *Device Configuration* link.
- 4) Search for and select the Polycom model to be licensed for the group (for example, "Polycom_VVX500"). Note that only models already assigned within the group appear on the list.
- 5) Select the *Files* tab.
- 6) Edit the %BWMACADDRESS%-license.cfg file.
- 7) Select the Custom file and click **Browse** to upload the site license file received from Polycom (000000000000-license.cfg) to the group.
- 8) Click **OK** to store the file settings.
- 9) Repeat for each Polycom model to be licensed for the group.

To apply the license to a specific user, complete the following steps.

- 1) Search for and select the Cisco BroadWorks user.
- 2) From the user's *Profile* page, click on the *Addresses* link. If the user does not have a device assigned, assign a device profile to that user.

- 3) Click the *Configure Identity/Device Profile* link to access the user's device profile.
- 4) Select the *Files* tab.
- 5) Edit the `%BWMACADDRESS%-license.cfg` file.
- 6) Select the *Custom* file and click **Browse** to upload the site license file received from Polycom (000000000000-license.cfg) to the user.
- 7) Click **OK** to store the file settings.
- 8) Repeat for each user to be licensed.

5.2.2.2.3.7 Polycom Phone Service (Optional)

The Polycom Phone Service provides phone directory integration with Cisco BroadWorks.

To enable this feature on the device profile type, select *Services* for the Polycom device profile type and select the *Supports Polycom Phone Services* check box. Selecting this check box automatically loads the `%BWMACADDRESS%-directory.xml` file to the device profile type.

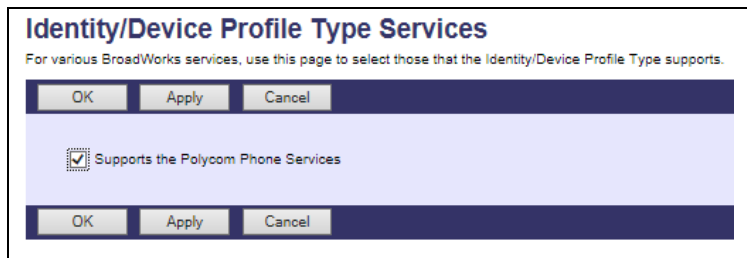


Figure 21 Enable Polycom Phone Services

Next, browse to *Files and Authentication* for the Polycom VVX device profile type, select the `%BWMACADDRESS%-directory.xml` file, and change the file settings as necessary to match the settings in the following table.

Parameter	Value	Description
Device Access File Format	<code>%BWMACADDRESS%-directory.xml</code>	This is the file name, which the phone uses to request the file.
Repository File Format	<code>%BWFQDEVICEID%-directory.xml</code>	This is the file name, (as stored in the Device Management repository).
File Category	Dynamic Per-Device	This file is unique per device.
File Customization	Disallow	This identifies who can customize this file template.
Enable Caching	This is not set.	Caching should not be enabled for device specific files.
Assign File	Custom	The file is pre-loaded.
Authentication Mode	MAC Address	The phone-specific file is authenticated with MAC address.

This initially enables the Polycom Phone Service for all users assigned to this device profile type. An additional configuration step is required to enable this service. This step is completed on the device profile assigned to the user and is described in section [5.2.4.1 Complete Polycom Phone Services Enablement](#).

5.2.3 Create Device Profile Instance

The previous sections defined the device profile type such that the system is ready to mass deploy device profiles. A device profile is an instance of the device profile type and defines the Cisco BroadWorks interface to a Polycom VVX phone deployed at a user's desk.

This section describes how to create a Cisco BroadWorks device profile instance for an individual Polycom UC Software device. Device profile instances are usually created at the Cisco BroadWorks group level and assigned to users.

When the device profile is created, the authentication data must be defined. The authentication data is used by Device Management to challenge a request from a phone to download a configuration file. The device must send the credentials that match the credentials stored in the device profile.

Browse to the Cisco BroadWorks *<group>* → *Resources* → *Identity/Device Profiles* and select *Add* to add a new Polycom UC Software device profile. Define the device profile instance using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Identity/Device Profile Name	<device-profile-name> Example: jc_vvx500	The device profile name is a unique identifier for the device profile instance.
Identity/Device Profile Type	<Polycom VVX device profile type> Example: Polycom_VVX500	From the drop-down menu, select the Polycom device profile type (created in the previous section).
Authentication	Use custom credentials	Set a unique login ID and password for each phone.
Device Access User Name	<phone-login-name> Example: jc_vvx500	This is the user name to log in from the phone. The phone login user naming convention must be determined by the service provider.
Device Access Password	<phone-login-password> Example: 654321	This is the password to log in from the phone.
MAC Address (Optional)	<MAC Address of the VVX Phone>	Populate this field only if the device is using the Polycom Phone Service or when using MAC address authentication.

Example *Identity/Device Profile Add* settings:

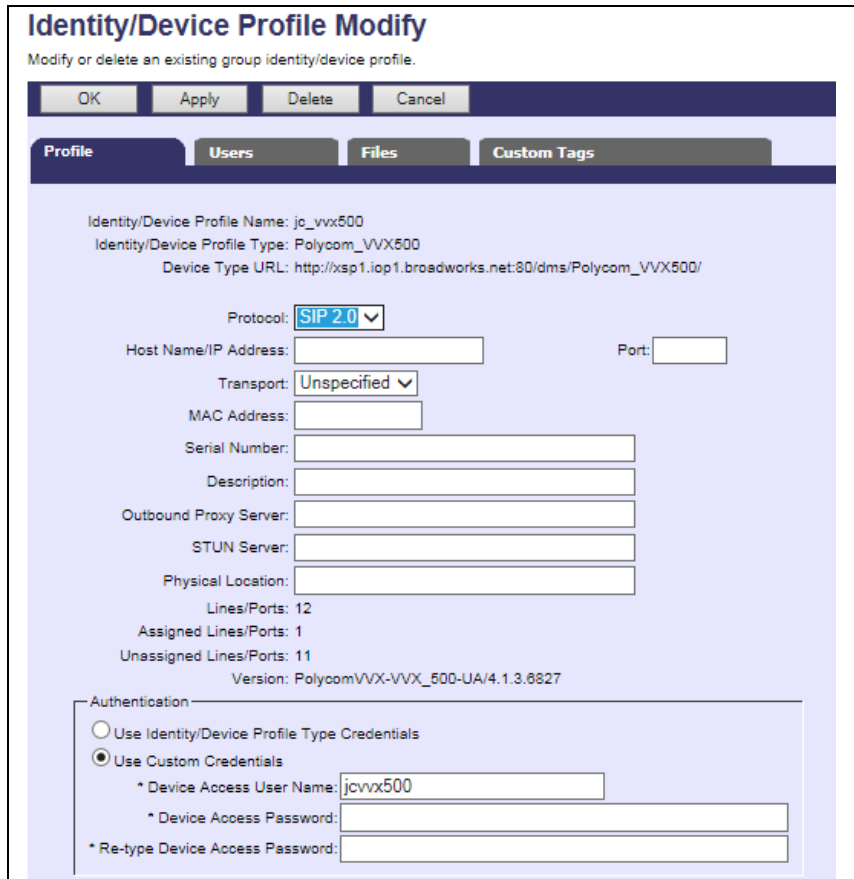


Figure 22 Identity/Device Profile Add

5.2.4 Configure Cisco BroadWorks User

The user should be configured with the desired Cisco BroadWorks configuration and services. Any services that require a specific configuration on the device are managed using Device Management and defined in the device configuration files, given that the template files are created with the correct Device Management tags.

The device profile created in the previous section should be assigned to the Cisco BroadWorks user. Assigning the device profile to the user automatically causes the Device Management feature to generate the device configuration files for this user's device.

To assign the device profile to the user, browse to the Cisco BroadWorks *<user>* → *Addresses* page and then set the parameters as described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Identity/Device Profile Name	<device-profile-name> Example: jc_vvx500	From the drop-down menu, select the device profile instance (created in the previous section).

Parameter	Value	Description
Line/Port	<SIP register address-of-record> Example: 8881001021@as.iop1.broadworks.net	Enter the SIP register address of record.

Example user *Addresses* settings:

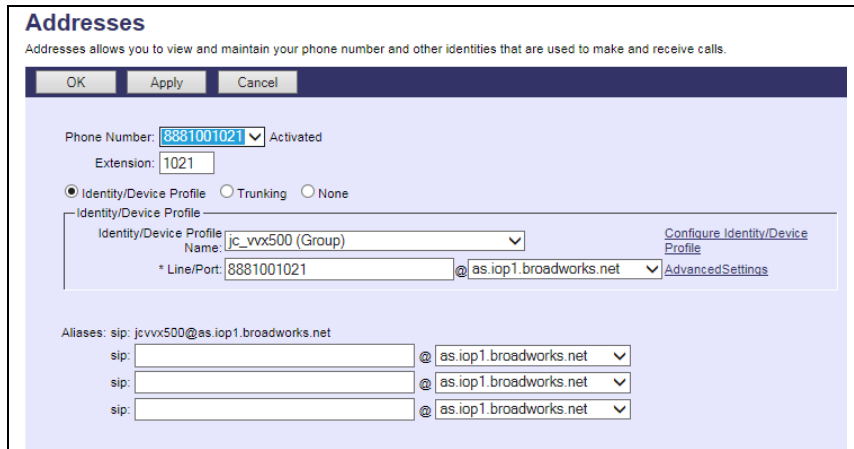


Figure 23 Assign Device Profile to User

5.2.4.1 Complete Polycom Phone Services Enablement

If the Polycom Phone Service was activated (see section [5.2.2.2.3.7 Polycom Phone Service](#)), then complete the enablement with the following configuration steps.

- 1) From the user's *Addresses* page, click the *Configure Identity/Device Profile* link.
- 2) Select the *Users* tab on the *Device Profile Modify* page.
- 3) Click the **Search** button to list all SIP lines configured on this device.
- 4) Check the *Primary Line/Port* check box next to the primary user's line.
- 5) Click **OK** to store the primary line setting.

The user or group administrator can now activate the service by accessing the *Polycom Phone Services* link on the *Client Applications* page. From the *Polycom Phone Services* page, the user can edit their primary line settings. On this page, the user can activate the service and choose to include their personal phone list and/or select a custom group contact list as the contacts to be synchronized with the phone.

5.2.5 Configure Edge Device

In many deployments, an edge device, such as an Edgewater EdgeMarc, is deployed on the enterprise edge. Configure the edge device SIP server setting with the service provider's Acme Packet (or other session border controller) IP address or FQDN. However, if there is no edge device and the phones communicate directly with the service provider's SBC, skip this section.

To integrate the EdgeMarc with Device Management, the SBC address tag (%SBC_ADDRESS%) defined in section [5.2.1.1 Create System Default Tags](#) must be overridden at the group level with the LAN address of the EdgeMarc device. At the *Group* → *Utilities* → *Configure Device* page, select the Polycom device profile (for example, "Polycom_VVX500"). Perform the following steps.

- 1) Click on the *Custom Tags* tab.
- 2) Click the **Add** button.
- 3) Add the SBC tag.
- 4) Enter *SBC_ADDRESS* as the tag.
- 5) Enter the IP address as the value (that is, the EdgeMarc LAN IP address).
- 6) To save the tag data, click **OK**.

This tag/value is applied to all Polycom_VVX500 phones in the group using the modified *Device Profile Type*.

Repeat for each Polycom model provisioned in the group.

5.2.6 Enable HTTPS for Polycom UC Software Devices

Polycom VVX phones can be configured to download device files using the HTTPS protocol; however, there are some limitations to be considered. The Polycom bootROM does not currently support HTTPS. The bootROM downloads the *bootrom.ld*, *sip.ld*, and *MAC.cfg* files. These files must be accessible from Device Management using the HTTP protocol. The Polycom application (*sip.ld*) supports HTTPS and downloads the remaining device configuration files using HTTPS when selected as the protocol type. The Cisco BroadWorks Xtended Services Platform (Xsp) must be configured to support both HTTP and HTTPS protocols, so that the bootROM and application files can download the required files.

To set up the phone for HTTPS support, the Root Certification Authority (CA) certificate must be loaded to the Polycom phone. The certificate cannot be a chained certificate and must point directly to the CA.

- 1) The certificate is loaded on the phone from the *SSL Security* menu. To go to this menu, press the **Home** button and then select *Settings* → *Advanced* buttons.
- 2) Enter the *Advanced* menu access password and select *TLS Security* → *Custom CA Certificates* → *Platform CA1* → *Install Custom CA Cert*. At this location, enter the HTTP uniform resource locator (URL) for the Root CA certificate.
- 3) When the certificate is loaded, the phone displays the MD5 checksum. If the checksum is correct, press the **Accept** button to store the certificate to the phone.
- 4) When the certificate is saved, press the **Back** button and then select the *Configure TLS Profiles* menu. From this menu, choose a TLS Platform Profile to be configured for TLS provisioning.
- 5) Under the *TLS Platform Profiles* menu, select *CA Certificates* and then select the *All Certificates* check box.

- 6) Press the **Back** button repeatedly until *TLS Security* menu is reached.
- 7) From the *TLS Security* menu, select *TLS APPLICATIONS* → *Provisioning* → *Profile Selection*, select the TLS Platform Profile chosen previously.
- 8) At this point, the phone is configured to trust the Device Management system, if the correct certificates have been loaded.

For more information about support for HTTPS on Polycom phones, see the *Polycom Technical Bulletin 52609* available from the Polycom support web site.

5.2.7 File Authentication Using MAC Address from Client Certificate

This section describes the steps necessary to configure Cisco BroadWorks to perform device management file authentication using the MAC address obtained from the phone's HTTPS client certificate. This secure authentication method based on MAC address is a new feature available from BroadWorks Release 22.0.

Prior to configuring for the MAC address authentication, mutual HTTPS authentication must be established among the UC Software VVX phones and Cisco BroadWorks. That is by the implication of client certificate authentication, HTTPS must be enabled on the phones to trust Cisco BroadWorks server certificate per section [5.2.6 Enable HTTPS for Polycom UC Software Devices](#). Furthermore, HTTPS client certificates offered by the VVX devices containing the phone's MAC address must also be trusted by Cisco BroadWorks.

From factory, each Polycom UC Software VVX Phone is installed with a client certificate that is signed by Polycom's certificate authority. The public certificates of Polycom's certificate authority can be obtained from Polycom. The Polycom certificate should be installed on the Device Management deploying Xtended Services Platform.

The Polycom UC Software VVX CPE kit starting from version 5.5.1 contains additional Device Management DTAF files with support of MAC address authentication using client certificate. These DTAF files can be identified with the appending suffix of “_MAC” (Example: Polycom_VVX101_MAC.DTAF.zip); follow the instructions in section [5.2.2.1 Configuration Method 1: Import](#) to import these DTAF onto Cisco BroadWorks. After importing the DTAF files, follow instructions in section [5.2.7.1 Create or Modify Device Profile Instance using MAC Address from Client Certificate](#) to create corresponding device profile instances.

Alternatively, use the instructions detailed in the following sub-sections to manually alter files in the existing device profile types and device profile instances to switch the file authentication mode.

Caution: Altering the authentication mode from “username/password” to “MAC address in client certificate” for a given device profile type will affect all existing device profile instances on the Cisco BroadWorks system. Prepare the authentication mode switch by collecting all MAC addresses of the existing Polycom UC Software VVX Phones and follow instructions below in the specified order.

5.2.7.1 Create or Modify Device Profile Instance using MAC Address from Client Certificate

When MAC address authentication is chosen as the file authentication mode, every single UC Software VVX phone's MAC address must be added to the corresponding device profile on Cisco BroadWorks. The device MAC address is to be configured for the device profile as shown in the following figure. Further, select or update the *Authentication* method of *Use Custom Credentials* instead of *Use Identity/Device Profile Type Credentials*. If altering the authentication mode, repeat the steps to modify all existing device profiles on the Cisco BroadWorks system.

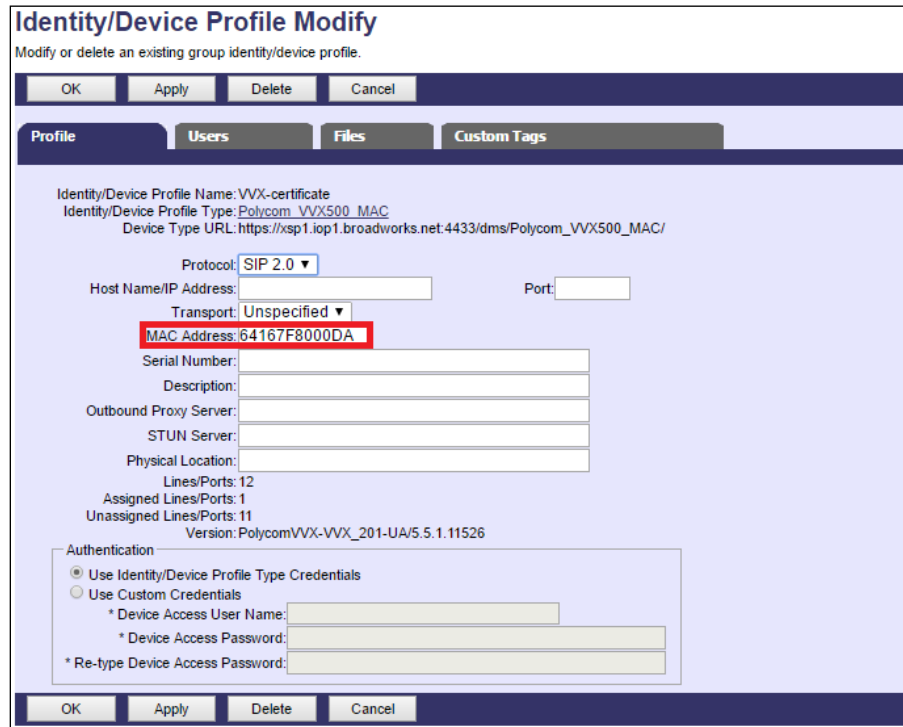


Figure 24 MAC Address Definition for Device Profile Instance

5.2.7.2 Update Device Management Authentication Mode on the Device Profile Type

Instructions in this section are only applicable to updating Cisco BroadWorks systems with existing Polycom UC Software VVX device profile types. Perform the changes as shown on the device profile type to be updated with MAC address authentication using Client Certificate.

Parameter	Value	Description
Device Access Protocol	https	HTTPS protocol is a must when using client mutual authentication with signed certificates.
Device Access Port	XSP's listening port of HTTPS mutual authentication.	Enter the corresponding TCP port.
Authentication Mode	MAC-Based checked	MAC-Based authentication method is used.

Parameter	Value	Description
MAC Address in	Client Certificate radio button selected	MAC address used for authentication is to be obtained from the client certificate to compare to the provisioned values on the device profiles.
MAC Address Format	.*([0-9a-fA-F]{12}).*	Regular expression used to parse the MAC address from the CN field of the client certificate.

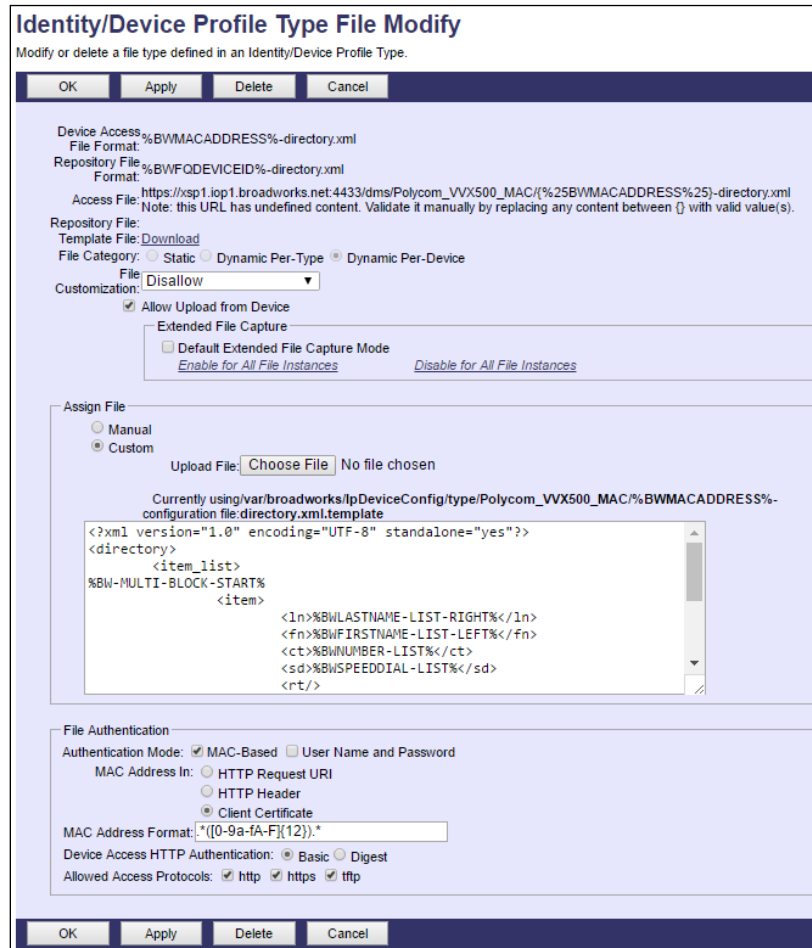
Figure 25 Device Profile Type Update for MAC-Based Auth using Client Certificate

5.2.7.3 Change File Authentication Mode to MAC address in Client Certificate

Instructions in this section are only applicable to updating Cisco BroadWorks systems with existing Polycom UC Software VVX device profile types. Perform corresponding changes on the authentication mode of all files listed under section [5.2.2.2.2 Device-Specific Files](#) as shown in the following figure. The regular expression used in MAC Address Format is: .*([0-9a-fA-F]{12}).*

Figure 26 Authentication Mode Set to MAC-Based and Sourced from Client Certificate

If Polycom Phone Services is enabled, the alteration of file authentication method is also necessary on the automatically created `%BWMACADDRESS%-directory.xml` file as shown.



Identity/Device Profile Type File Modify
Modify or delete a file type defined in an Identity/Device Profile Type.

OK Apply Delete Cancel

Device Access: %BWMACADDRESS%-directory.xml
File Format: %BWMACADDRESS%-directory.xml
Repository File: %BWFQDEVICEID%-directory.xml
Format: %BWFQDEVICEID%-directory.xml
Access File: https://xsp1.iop1.broadworks.net:4433/dms/Polycom_VVX500_MAC/{%25BWMACADDRESS%25}-directory.xml
Note: this URL has undefined content. Validate it manually by replacing any content between {} with valid value(s).

Repository File: Download
Template File: Static Dynamic Per-Type Dynamic Per-Device
File Category: Static Dynamic Per-Type Dynamic Per-Device
File: Disallow
Customization: Allow Upload from Device
Extended File Capture
 Default Extended File Capture Mode
[Enable for All File Instances](#) [Disable for All File Instances](#)

Assign File
 Manual
 Custom
Upload File: No file chosen
Currently using: /var/broadworks/lpDeviceConfig/type/Polycom_VVX500_MAC/%BWMACADDRESS%-configuration file directory.xml.template

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<directory>
  <item_list>
    %BW-MULTI-BLOCK-START%
    <item>
      <ln>%BWLASTNAME-LIST-RIGHT%</ln>
      <fn>%BWFIRSTNAME-LIST-LEFT%</fn>
      <ct>%BWNUMBER-LIST%</ct>
      <sd>%BWSPEEDDIAL-LIST%</sd>
    </item>
  </item_list>
</directory>
```

File Authentication
Authentication Mode: MAC-Based User Name and Password
MAC Address In: HTTP Request URI
 HTTP Header
 Client Certificate
MAC Address Format:
Device Access HTTP Authentication: Basic Digest
Allowed Access Protocols: http https tftp

OK Apply Delete Cancel

Figure 27 Polycom Phone Service setting for MAC Authentication Using Client Certificate

5.2.8 Configure Polycom UC Software Phone

This section describes the steps necessary to configure the Polycom UC Software VVX phones to integrate with BroadWorks Device Management.

The phone must be configured with the Device Management URL and authentication user name and password. This configuration can be accomplished as described in the sections:

- [5.2.8.1 Manual Provisioning](#)
- [5.2.8.2 No Touch Provisioning via BroadWorks Device Management](#)
- [5.2.8.3 No Touch Provisioning via Polycom Zero Touch Provisioning](#)

5.2.8.1 Manual Provisioning

The manual provisioning method to configure the Polycom device involves using the phone's menus to configure the Device Management settings.

5.2.8.1.1 Check Enterprise/Business DHCP Server Settings

The Polycom phone uses the file server parameters configured on the phone unless *Option 66* has been defined on the DHCP server. If the DHCP server returns data set for the *Option 66* parameter, then the Polycom phone uses the address defined in this field as the server address to retrieve its configuration data.

When using manual provisioning, to make sure that the phone interfaces properly with Device Management, the *Option 66* parameter must not be set on the DHCP server. If *Option 66* is defined and cannot be cleared, then the Polycom *boot server* parameter in the DHCP menu must be set to “Static”. This parameter is set at boot time by accessing the *Setup* menu.

- 1) Click the **Setup** button.
- 2) Enter “456” as the password.
- 3) Select the *DHCP* menu.
- 4) Set the *Boot Server* parameter to “Static”.
- 5) Save the configuration changes and start the phone initialization.

5.2.8.1.2 Provision Device Management Settings

Launch the web interface of the phone by accessing *http://<phone’s IP address>*. Log in as *Admin* by selecting the respective button, provide the password, and then click **Submit**. The default admin password is “456”.

At the phone’s admin configuration page, from the *Settings* menu, select *Provisioning Server* from the drop-down menu.

Provision the following settings on the phone:

Settings	Description
Server Type	Indicate the server type, that is, HTTP (or, HTTPS can be used as an option).
Server Address	Enter the device access FQDN and device access URI. Example: http://xsp.iop1.broadworks.net:80/dms/Polycom_VVX500/
Server User	This is the Device Management user name. Leave the field blank if MAC address authentication is used.
Server Password	This is the Device Management password. Leave the field blank if MAC address authentication is used.

Provisioning Server

Provisioning Server

Server Type

Server Address

Server User

Server Password

File Transmit Tries

Retry Wait (s)

Tag SN to UA Enable Disable

DHCP Menu

* Boot Server

* Boot Server Option

* Boot Server Type

Option 60 Format

Note:
* Fields may require phone reboot/restart.

Figure 28 Provisioning Server Configuration

The settings must match those of the device profile instance assigned to the user. The applicable settings are highlighted in the following example.



Identity/Device Profile Modify
Modify or delete an existing group identity/device profile.

OK Apply Delete Cancel

Profile Users Files Custom Tags

Identity/Device Profile Name: jc_vvx500
Identity/Device Profile Type: Polycom_VVX500
Device Type URL: http://xsp1.iop1.broadworks.net:80/dms/Polycom_VVX500/

Protocol: SIP 2.0
Host Name/IP Address: Port:
Transport: Unspecified
MAC Address:
Serial Number:
Description:
Outbound Proxy Server:
STUN Server:
Physical Location:

Lines/Ports: 12
Assigned Lines/Ports: 1
Unassigned Lines/Ports: 11
Version: Polycom/VVX-VVX_500-UA/4.1.3.6827

Authentication

Use Identity/Device Profile Type Credentials
 Use Custom Credentials
* Device Access User Name:
* Device Access Password:
* Re-type Device Access Password:

Figure 29 Identity/Device Type Credentials – Custom Credentials

After all parameters are entered, click the **Save** button. Allow the phone to reboot and retrieve the new configuration parameters from Device Management.

5.2.8.2 No Touch Provisioning via Cisco BroadWorks Device Management

The No Touch Provisioning method via Cisco BroadWorks Device Management uses DHCP and Device Management default configuration files. This enables configuration of the phone out-of-the-box without pre-provisioning before sending it to a customer's site.

No Touch Provisioning is done using the DHCP options provided by the end customer's DHCP server. The steps are as follows:

- 1) The phones are shipped to the end customer without pre-provisioning.
- 2) The end customer's DHCP server is configured with *Option 66* or *160* with the default Device Management URL.
- 3) The phone is plugged in and it receives the default Device Management URL from the DHCP server.
- 4) The phone queries for the default product file from Device Management.
- 5) The phone receives the default device file from Device Management and provisions the phone with the physical Device Management URL for the specific device model.
- 6) The phone resynchronizes with Device Management and activates a login soft key.
- 7) The end user or administrator enters the device user ID and password using the **QSetup** button on the phone.

- 8) The phone resynchronizes with Device Management and downloads the files associated with the credentials supplied via the **QSetup** button.

Device Management must be configured to facilitate the No Touch Provisioning method. Configuration can be performed using the Device Management import function or done manually. Each method is described in the following subsections.

5.2.8.2.1 Configuration Method 1: Import

This section identifies the steps necessary to make use of the Device Management import feature to configure Cisco BroadWorks to add the Device Management Defaults device type for No Touch Provisioning.

The import method is available in BroadWorks Release 17.0 and later. For previous releases, use the manual configuration method described in the next section.

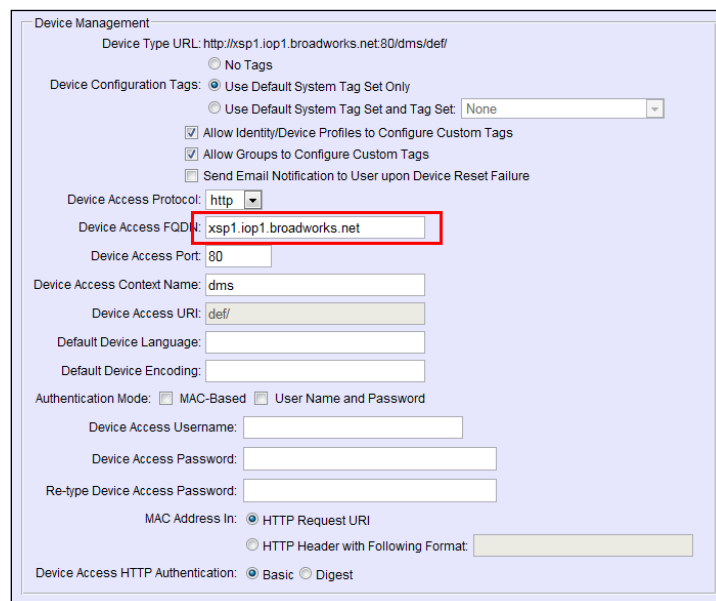
Download the Polycom UC Software device CPE kit from Cisco Xchange at www.broadsoft.com/xchange. Extract the *DeviceManagementDefaults.DTAF.zip* file from the CPE kit. This is the import file.

Log in to Cisco BroadWorks as an administrator. Browse to *System* → *Resources* → *Identity/Device Profile Types* and select *Import*. Select *Browse* to find the extracted DTAF file and click **OK** to start the import.

After the import finishes, the following post-import configuration steps must be completed.

Browse to *System* → *Resources* → *Identity/Device Profile Types* and perform a search to find the imported *DeviceManagementDefaults* device profile type. Browse to the *Profile* page and change the Device Management Device Access FQDN to your Xtended Services Platform or Xtended Services Platform cluster address.

Example:



The screenshot shows the 'Device Management' configuration page. The 'Device Access FQDN' field is highlighted with a red box and contains the value 'xsp1.iop1.broadworks.net'. Other visible fields include 'Device Type URL', 'Device Configuration Tags', 'Device Access Protocol' (set to 'http'), 'Device Access Port' (set to '80'), 'Device Access Context Name' (set to 'dms'), 'Device Access URI' (set to 'def/'), and 'Device Access HTTP Authentication' (set to 'Basic').

Figure 30 Device Access FQDN

Next, using the *Files and Authentication* link, select the option to rebuild all the system files.

Firmware files must be obtained from Polycom. These files are not included in the import. For firmware upload instructions, see section [5.2.2.2.3.1 Application Firmware](#).

5.2.8.2.2 Configuration Method 2: Manual

This section identifies the manual steps necessary configure Cisco BroadWorks to add the Device Management Defaults device type for No Touch Provisioning

The manual method must be used for BroadWorks releases prior to Release 17.0. It is an optional method in Release 17.0 and later. The steps in this section can also be followed to update previously imported or configured device profile type(s) with new configuration files and firmware.

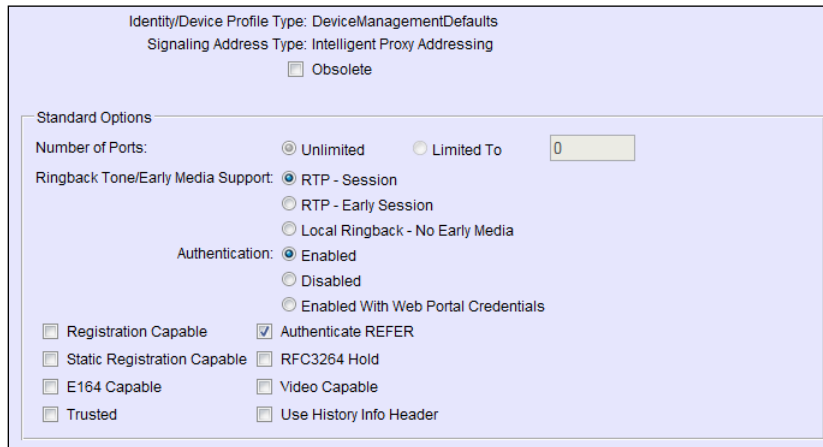
5.2.8.2.2.1 Create Default Device Profile Type

A Device Management default device profile type must be created. This device profile type can be configured to serve default provisioning files to Polycom endpoints, as well as other vendor devices.

Create a default device profile type as shown in the following figure. Only the device management settings are important in this context since the profile type is used only to serve default provisioning files. The standard and advanced settings do not matter.

5.2.8.2.2.1.1 Configure Standard Options

The device profile type name and standard options do not matter, but an example is provided for reference. All settings can be left with their default values.



Identity/Device Profile Type: DeviceManagementDefaults
 Signaling Address Type: Intelligent Proxy Addressing
 Obsolete

Standard Options

Number of Ports: Unlimited Limited To

Ringback Tone/Early Media Support: RTP - Session
 RTP - Early Session
 Local Ringback - No Early Media

Authentication: Enabled
 Disabled
 Enabled With Web Portal Credentials

Registration Capable Authenticate REFER
 Static Registration Capable RFC3264 Hold
 E164 Capable Video Capable
 Trusted Use History Info Header

Figure 31 Default Device Profile Type

5.2.8.2.2.1.2 Configure Advanced Options

The advanced options do not matter, but an example is provided for reference. All settings can be left with their default values.

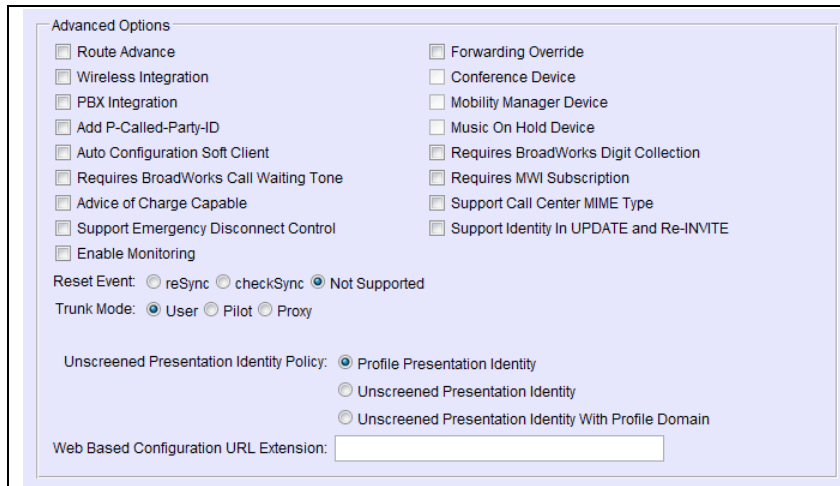


Figure 32 Configure Advanced Options

5.2.8.2.2.1.3 Configure Device Management Options

Configure the device profile type *Device Management Options* as directed in the following table. These are common settings, which apply to all devices enabled for Device Management.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Configuration Tags	Use Default System Tag Set Only	
Allow Identity/Device Profiles to Configure Custom Tags	Checked	Optional
Allow Groups to Configure Custom Tags	Checked	Optional
Device Access Protocol	http	
Device Access FQDN	<BroadWorks-XSP-Cluster-Address> Example: xsp.iop1.broadworks.net	If using an Xtended Services Platform farm, set this to the Xtended Services Platform cluster FQDN. Otherwise, set it to the individual Xtended Services Platform FQDN or IP address.
Device Access Port	<BroadWorks-XSP-Port> Example: 80	This should be set to "80".
Device Access Context Name	dms	This does not need to be defined. Cisco BroadWorks defaults to the system-defined value.
Device Access URI	def	This defines the directory the Xtended Services Platform uses to access the default configuration files.

Example *Device Management Options* settings:

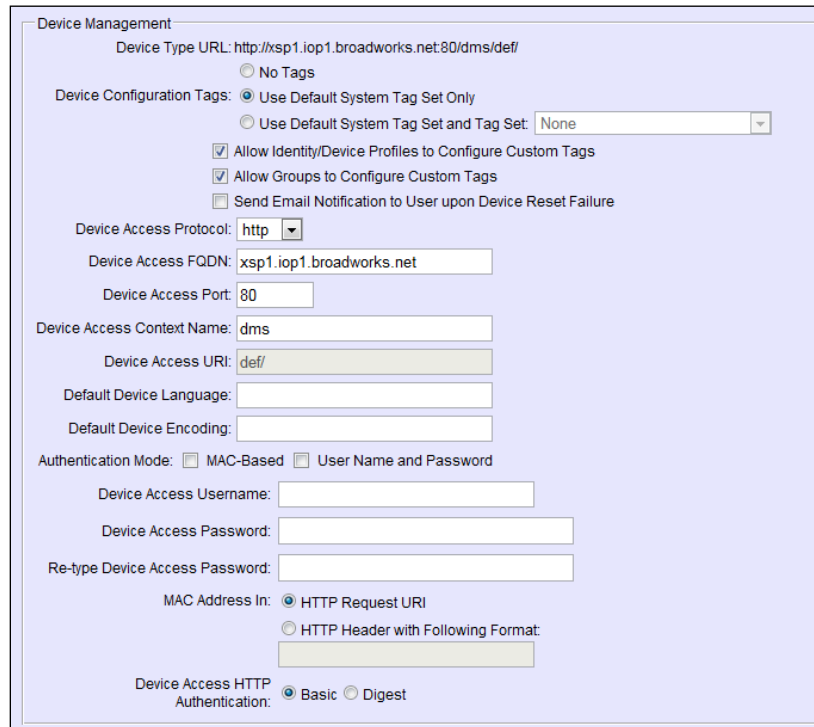


Figure 33 Device Management Options Settings

5.2.8.2.2.2 Define Device Profile Type Files

This section describes the Cisco BroadWorks Device Management configuration necessary to identify the configuration files used to enable the *DeviceManagementDefaults* device type for Polycom UC Software devices. The files must be defined as described in the following sections:

- [5.2.8.2.2.2.1 000000000000.cfg](#)
- [5.2.8.2.2.2.2 qsetup.cfg](#)
- [5.2.8.2.2.2.3 provisioning.cfg](#)
- [5.2.8.2.2.2.4 sip.ld](#)

5.2.8.2.2.2.1 000000000000.cfg

Polycom devices request the default *macaddress* file (*000000000000.cfg*) from Device Management if a request for the *macaddress.cfg* file fails. Since the phone does not know the URL for the *macaddress.cfg* file, it must fall back to the default file. The *000000000000.cfg* file provides default instructions applicable to any Polycom device. This file identifies the following files for the phone to download:

- *sip.ld* firmware file
- *qsetup.cfg* file to trigger the Quick Setup soft key and its functionality
- *provisioning.cfg* identifies the Device Management URL for each model

Add a Cisco BroadWorks device profile type file to the *DeviceManagementDefaults* device profile for the *000000000000.cfg* file using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

After defining the file, upload the *000000000000-default.cfg* file template downloaded from Cisco Xchange. Be sure to upload the *000000000000-default.cfg* and not the *000000000000.cfg* file. Use the **Browse** button on the *File Definition* screen. Be sure to click **Apply** after uploading the file.

Example *000000000000.cfg* file settings:

Figure 34 000000000000.cfg File

5.2.8.2.2.2.2 qsetup.cfg

Polycom has implemented a Quick Setup (QSetup) soft key. Pressing this soft key at phone initialization automatically brings up the file server menu and the associated parameters on the Polycom UC Software device. By identifying this configuration file name in the *000000000000.cfg* file, the Quick Setup soft key is presented on the device.

Add a Cisco BroadWorks device profile type file to the *DeviceManagementDefaults* device profile for the *qsetup.cfg* file using the settings described in the following table.

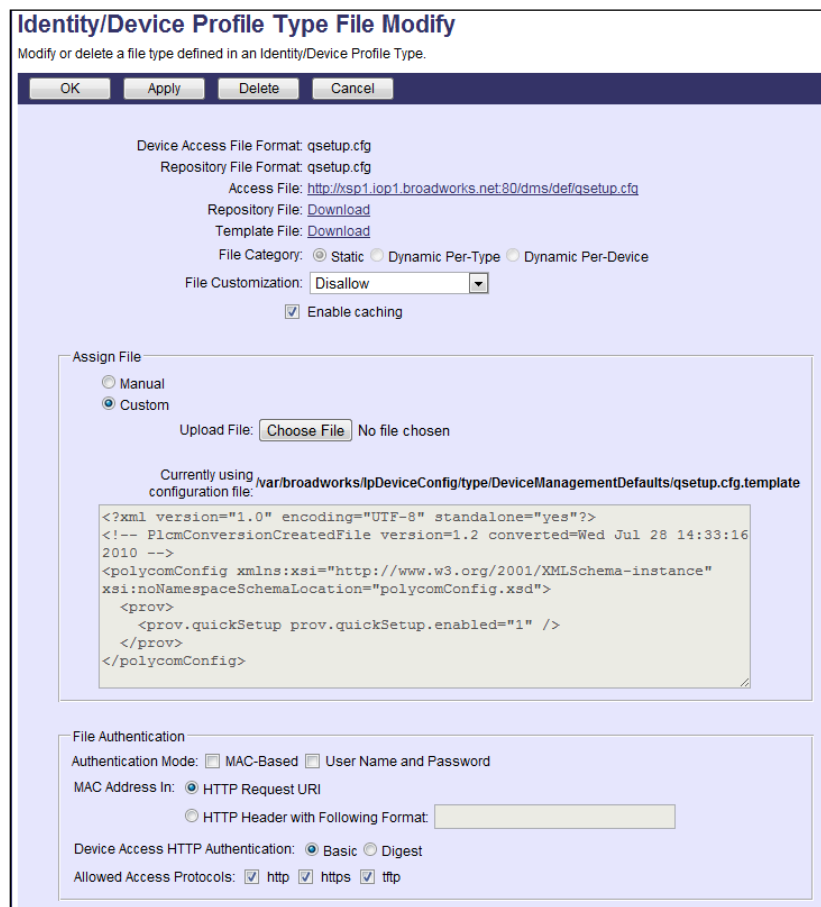
Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	qsetup.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	qsetup.cfg	This is the file name, (as stored in the Device Management repository).
File Category	Static	This file is a static file. There are no dynamic tags in the file.

Parameter	Value	Description
File Customization	Disallow	This identifies who can customize this file template.
Enable Caching	Selected	Caching is recommended for this file.
Assign File	Custom	
Authentication Mode	None	The static files are not authenticated so do not select either of the options.

After defining the file, upload the corresponding *qsetup.cfg* file template downloaded from Cisco Xchange. Use the *Browse* button on the file definition screen. Be sure to select *Apply* after uploading the file.

Example *qsetup.cfg* file settings:



Identity/Device Profile Type File Modify
Modify or delete a file type defined in an Identity/Device Profile Type.

OK Apply Delete Cancel

Device Access File Format: qsetup.cfg
Repository File Format: qsetup.cfg
Access File: <http://xsp1.iop1.broadworks.net:80/dms/def/qsetup.cfg>
Repository File: [Download](#)
Template File: [Download](#)
File Category: Static Dynamic Per-Type Dynamic Per-Device
File Customization:
 Enable caching

Assign File
 Manual
 Custom
Upload File: No file chosen

Currently using configuration file: `/var/broadworks/lpDeviceConfig/type/DeviceManagementDefaults/qsetup.cfg.template`

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- PlcmConversionCreatedFile version=1.2 converted=Wed Jul 28 14:33:16
2010 -->
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
  <prov>
    <prov.quickSetup prov.quickSetup.enabled="1" />
  </prov>
</polycomConfig>
```

File Authentication
Authentication Mode: MAC-Based User Name and Password
MAC Address In: HTTP Request URI
 HTTP Header with Following Format:
Device Access HTTP Authentication: Basic Digest
Allowed Access Protocols: http https tftp

Figure 35 qsetup.cfg File

5.2.8.2.2.3 provisioning.cfg

The *provisioning.cfg* file identifies the specific Device Management URL for each model. This provides the proper URL for the phone to download the *macaddress.cfg* file.

Add a Cisco BroadWorks device profile type file to the DeviceManagementDefaults device profile for the *provisioning.cfg* file using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	provisioning.cfg	This is the file name, which the phone uses to request the file.
Repository File Format	provisioning-%BWTIMESTAMP%.cfg	This is the file name, (as stored in the Device Management repository).
File Category	Dynamic Per-Type	This file is a static file. There are no dynamic tags in the file.
File Customization	Disallow	This identifies who can customize this file template.
Enable Caching	Selected	Caching is recommended for this file.
Assign File	Custom	
Authentication Mode	None	This file is not authenticated so do not select either of the options.

The *provisioning.cfg* template file in the CPE kit downloaded from Cisco Xchange is tailored to work with the device profile types imported from the DTAF files included in the CPE kit. If the device access URI of any device profile type is different from the defined values in the CPE kit, the Device Management URLs for each phone model in the file must be modified to match that of the service provider's Device Management URL.

After modifying the *provisioning.cfg* template file, upload the file. Use the *Browse* button on the file definition screen. Be sure to select *Apply* after uploading the file.

Example *provisioning.cfg* file settings:

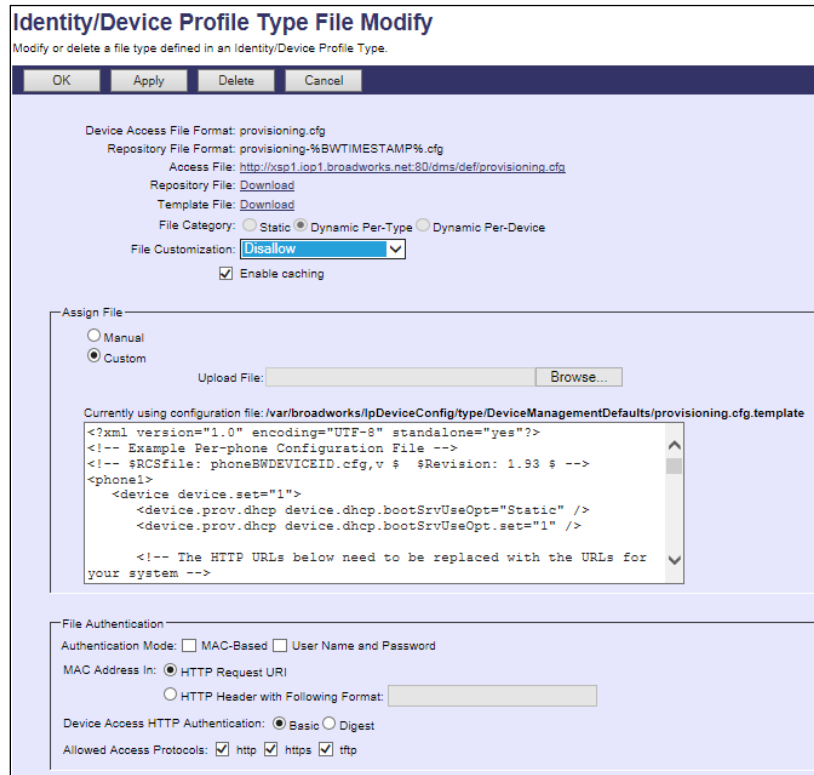


Figure 36 provisioning.cfg File

5.2.8.2.2.2.4 sip.ld

The *sip.ld* is the combined firmware file for the Polycom VVX Phones. In scenarios after factory default or file system format, the VVX phones may need to load this firmware file through no touch provisioning. This file is not included in the CPE kit and should be obtained from Polycom.

Add a Cisco BroadWorks static profile type file to the DeviceManagementDefaults device profile for the *sip.ld* file using the settings described in the following table.

Parameters not identified in the following table can usually be left with their default values.

Parameter	Value	Description
Device Access File Format	sip.ld	This is the file name, which the phone uses to request the file.
Repository File Format	sip.ld	This is the file name, (as stored in the Device Management repository).
File Category	Static	This file is a static file. There are no dynamic tags in the file.
File Customization	Disallow	This identifies who can customize this file template.
Enable Caching	Selected	Caching is recommended for this file.
Assign File	Custom	

Parameter	Value	Description
Authentication Mode	None	The static files are not authenticated so do not select either of the options.

Example *sip.id* file settings:

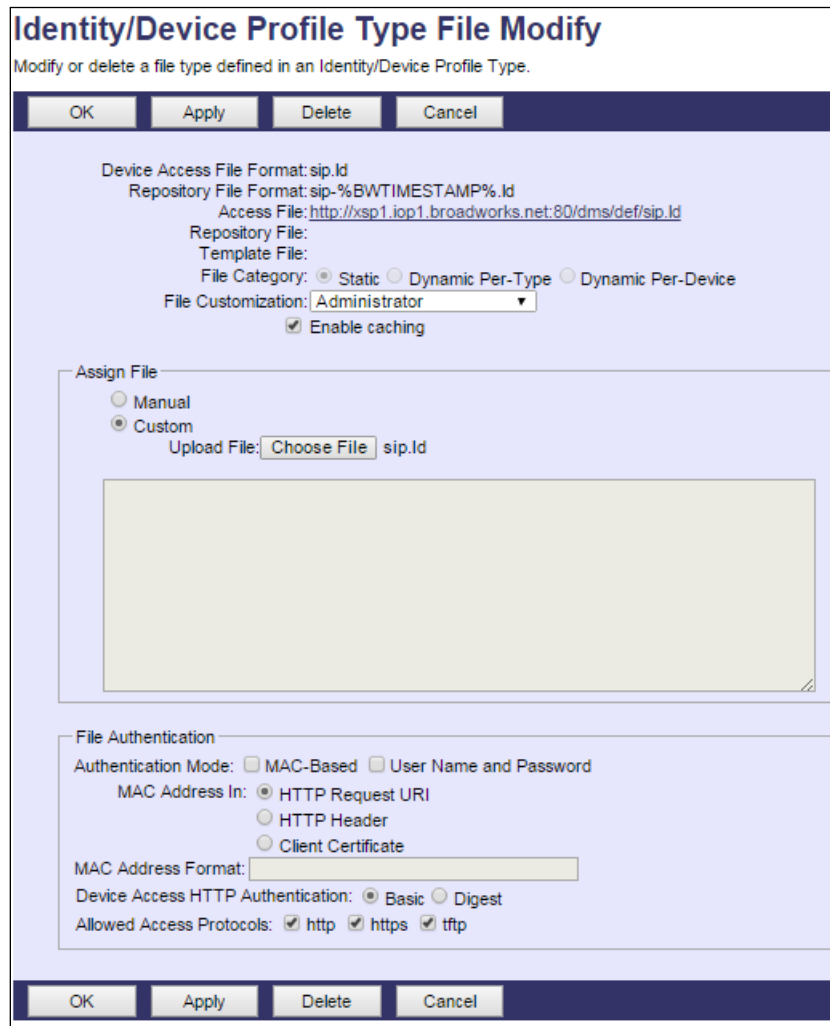


Figure 37 sip.id File

5.2.8.3 No Touch Provisioning via Polycom Zero Touch Provisioning

Polycom Zero Touch Provisioning (ZTP) is a service that is hosted by Polycom. At boot time, the Polycom phone automatically queries the Polycom ZTP server for provisioning data. For phones served by Cisco BroadWorks, the server is configured to provide the Device Management URL required for the phone to fully provision. For more information about this service, contact Polycom.

5.3 Upgrade from Previous CPE Kits

The previous configuration sections are primarily structured around importing or manually configuring the Polycom device profile types for the first time. Many of the steps are unnecessary when upgrading to a new firmware release or CPE kit version. For general instructions on upgrading, see the *BroadWorks CPE Kit Usage Guide* [10].

Appendix A: Sample Polycom® Phone Configuration Files

NOTE: The following samples are examples only and they should only be used as a reference. DO NOT CUT AND PASTE THESE EXAMPLES TO GENERATE YOUR CONFIGURATION FILES. The Polycom configuration files change between releases so be sure to use the configuration files from Polycom for the specific release to generate your configuration files.

Phone-specific Master Configuration File: <mac-address>.cfg

NOTE: This is an example file and it should only be used for reference. This file is distributed by Polycom as 000000000000.cfg. It must be renamed to <mac-address>.cfg using the MAC address for the specific phone.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<!-- Default Master SIP Configuration File-->
<!-- For information on configuring Polycom VoIP phones please refer to
the -->
<!-- Configuration File Management white paper available from: -->
<!--
http://www.polycom.com/common/documents/whitepapers/configuration_file_ma
nagement_on_soundpoint_ip_phones.pdf -->
<!-- $RCSfile: 000000000000.cfg,v $ $Revision: 1.23.8.3 $ -->
<APPLICATION APP_FILE_PATH="%APP_VERSION%.sip.ld"
CONFIG_FILES="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg" SERVICE_FILES=""
MISC_FILES="" LOG_FILE_DIRECTORY="" OVERRIDES_DIRECTORY=""
CONTACTS_DIRECTORY="" LICENSE_DIRECTORY="" USER_PROFILES_DIRECTORY=""
CALL_LISTS_DIRECTORY="" COREFILE_DIRECTORY="">
  <APPLICATION_VVX101 APP_FILE_PATH_VVX101="%APP_VERSION_VVX-101-
201%.sip.ld" CONFIG_FILES_VVX101="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg"/>
  <APPLICATION_VVX201 APP_FILE_PATH_VVX201="%APP_VERSION_VVX-101-
201%.sip.ld" CONFIG_FILES_VVX201="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg"/>

  <APPLICATION_VVX301 APP_FILE_PATH_VVX301="%APP_VERSION_VVX-301-
401%.sip.ld" CONFIG_FILES_VVX301="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg"/>

  <APPLICATION_VVX311 APP_FILE_PATH_VVX311="%APP_VERSION_VVX-301-
401%.sip.ld" CONFIG_FILES_VVX311="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg"/>

  <APPLICATION_VVX401 APP_FILE_PATH_VVX401="%APP_VERSION_VVX-301-
401%.sip.ld" CONFIG_FILES_VVX401="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg"/>

  <APPLICATION_VVX411 APP_FILE_PATH_VVX411="%APP_VERSION_VVX-301-
401%.sip.ld" CONFIG_FILES_VVX411="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg"/>

  <APPLICATION_VVX501 APP_FILE_PATH_VVX501="%APP_VERSION_VVX-501-
601%.sip.ld" CONFIG_FILES_VVX501="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg"/>

  <APPLICATION_VVX601 APP_FILE_PATH_VVX601="%APP_VERSION_VVX-501-
601%.sip.ld" CONFIG_FILES_VVX601="phone[PHONE_MAC_ADDRESS].cfg,sys.cfg"/>
```

System Default File: sys.cfg

NOTE: This is an example file and it should only be used for reference.

Note that in the following example, only the top portion of the file is shown.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- PlcmConversionCreatedFile version=1.2 converted=Wed Jul 28 14:33:16
2010 -->
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
  <bg>

    <bg.hiRes>
      <bg.hiRes.color>
        <bg.hiRes.color.bm bg.hiRes.color.bm.2.name="">
          <bg.hiRes.color.bm.2.em bg.hiRes.color.bm.2.em.name="" />
        </bg.hiRes.color.bm>
      </bg.hiRes.color>
      <bg.hiRes.gray bg.hiRes.gray.selection="3,2">
        <bg.hiRes.gray.bm bg.hiRes.gray.bm.2.adj="-2"
bg.hiRes.gray.bm.2.name="">
          <bg.hiRes.gray.bm.2.em bg.hiRes.gray.bm.2.em.name="" />
        </bg.hiRes.gray.bm>
      </bg.hiRes.gray>
    </bg.hiRes>
    <bg.medRes>
      <bg.medRes.gray>
        <bg.medRes.gray.bm bg.medRes.gray.bm.2.adj="-2"
bg.medRes.gray.bm.2.name="" />
      </bg.medRes.gray>
    </bg.medRes>
  </bg>
  <call>
    <call.shared call.shared.exposeAutoHolds="1"
call.shared.oneTouchResume="1" />
  </call>
  <dialplan dialplan.digitmap="%DIAL_PLAN%" />
  <feature>
    <feature.enhancedFeatureKeys feature.enhancedFeatureKeys.enabled="1"
/>
    <feature.callRecording feature.callRecording.enabled="1" />
    <feature.nWayConference feature.nWayConference.enabled="1" />
    <feature.urlDialing feature.urlDialing.enabled="0" />
  </feature>

  <video video.autoFullScreen="%VIDEO_SCREEN_MODE%"
video.maxCallRate="%VIDEO_CALL_RATE%" video.quality="%VIDEO_QUALITY%">
    <video.camera video.camera.frameRate="%VIDEO_FRAME_RATE%" />
    <video.localCameraView>
      <video.localCameraView.fullScreen
video.localCameraView.fullScreen.mode="%VIDEO_LOCAL_MODE%" />
    </video.localCameraView>
  </video>
  <voIpProt>
    <voIpProt.SIP voIpProt.SIP.useRFC3264HoldOnly="1"
voIpProt.SIP.keepalive.sessionTimers="1">
```

```

        <voIpProt.SIP.alertInfo voIpProt.SIP.alertInfo.1.class="custom1"
voIpProt.SIP.alertInfo.1.value="http://127.0.0.1/Bellcore-dr2"
voIpProt.SIP.alertInfo.2.class="custom2"
voIpProt.SIP.alertInfo.2.value="http://127.0.0.1/Bellcore-dr3"
voIpProt.SIP.alertInfo.3.class="custom3"
voIpProt.SIP.alertInfo.3.value="http://127.0.0.1/Bellcore-dr4"
voIpProt.SIP.alertInfo.4.class="custom1"
voIpProt.SIP.alertInfo.4.value="http://127.0.0.1/Bellcore-dr5"
voIpProt.SIP.alertInfo.5.class="autoAnswer"
voIpProt.SIP.alertInfo.5.value="auto-answer"
voIpProt.SIP.alertInfo.6.value="http://127.0.0.1/silent"
voIpProt.SIP.alertInfo.6.class="visual" />
        <voIpProt.SIP.outboundProxy
voIpProt.SIP.outboundProxy.address="%SBC_ADDRESS%"
voIpProt.SIP.outboundProxy.port="%SBC_PORT%"
voIpProt.SIP.outboundProxy.transport="%SBC_TRANSPORT%" />
        <voIpProt.SIP.requestValidation>
        <voIpProt.SIP.requestValidation.digest
voIpProt.SIP.requestValidation.digest.realm="%BWASCLUSTERFQDN%" />
        </voIpProt.SIP.requestValidation>
        <voIpProt.SIP.specialEvent>
        <voIpProt.SIP.specialEvent.checkSync
voIpProt.SIP.specialEvent.checkSync.alwaysReboot="1" />
        </voIpProt.SIP.specialEvent>
        </voIpProt.SIP>
        <voIpProt.server voIpProt.server.1.address="%BWASCLUSTERFQDN%"
voIpProt.server.1.transport="UDPOnly" />
        </voIpProt>
<httpd httpd.cfg.secureTunnelRequired="%HTTPS_CFG_REQ%" />
</polycomConfig>

```

Phone-Specific File: phone<BWMACADDRESS>.cfg

NOTE: This is an example file and it should only be used for reference.

This file is distributed by Polycom as *phone1.cfg*. The file must be renamed to make it unique for each device.

```

<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<!-- PlcmConversionCreatedFile version=1.2 converted=Wed Jul 28 14:33:16
2010 -->
<!-- Example Per-phone Configuration File -->
<!-- $RCSfile: phoneBWDEVICEID.cfg,v $ $Revision: 1.93 $ -->
<polycomConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="polycomConfig.xsd">
  <attendant attendant.uri="%BWBLF-URI-1%" />
  <device>
    <device.prov
device.prov.serverName="%BWDEVICEACCESSFQDN%:%BWDEVICEACCESSPORT%/%BWDMSC
ONTEXT%/%BWDEVICEACCESSURI%" />
    </device>
  <lcl>
    <lcl.ml lcl.ml.lang="%BWLANGUAGE-1%" />
  </lcl>
  <msg msg.bypassInstantMessage="1">

```

```
<msg.mwi msg.mwi.1.callBack="%BWVOICE-PORTAL-NUMBER-1%"
msg.mwi.1.callBackMode="contact" msg.mwi.10.callBack="%BWVOICE-PORTAL-
NUMBER-10%" msg.mwi.10.callBackMode="contact"
msg.mwi.11.callBack="%BWVOICE-PORTAL-NUMBER-11%"
msg.mwi.11.callBackMode="contact" msg.mwi.12.callBack="%BWVOICE-PORTAL-
NUMBER-12%" msg.mwi.12.callBackMode="contact"
msg.mwi.2.callBack="%BWVOICE-PORTAL-NUMBER-2%"
msg.mwi.2.callBackMode="contact" msg.mwi.3.callBack="%BWVOICE-PORTAL-
NUMBER-3%" msg.mwi.3.callBackMode="contact" msg.mwi.4.callBack="%BWVOICE-
PORTAL-NUMBER-4%" msg.mwi.4.callBackMode="contact"
msg.mwi.5.callBack="%BWVOICE-PORTAL-NUMBER-5%"
msg.mwi.5.callBackMode="contact" msg.mwi.6.callBack="%BWVOICE-PORTAL-
NUMBER-6%" msg.mwi.6.callBackMode="contact" msg.mwi.7.callBack="%BWVOICE-
PORTAL-NUMBER-7%" msg.mwi.7.callBackMode="contact"
msg.mwi.8.callBack="%BWVOICE-PORTAL-NUMBER-8%"
msg.mwi.8.callBackMode="contact" msg.mwi.9.callBack="%BWVOICE-PORTAL-
NUMBER-9%" msg.mwi.9.callBackMode="contact" />
</msg>
```

```

    <reg reg.1.address="%BWLINERPORT-1%" reg.1.bargeInEnabled="%BWSCA-
BRIDGING-BINARY-1%" reg.1.displayName="%BWFIRSTNAME-1% %BWLASTNAME-1%"
reg.1.label="%BWEXTENSION-1%" reg.1.type="%BWSHAREDLINE-1%"
reg.1.broadsoft.userId="%BWLOGIN-ID-1%" reg.1.lineAddress="%BWEXTENSION-
1%" reg.1.lineKeys="1" reg.1.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.10.address="%BWLINERPORT-10%" reg.10.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-10%" reg.10.label="%BWEXTENSION-10%" reg.10.type="%BWSHAREDLINE-
10%" reg.10.broadsoft.userId="%BWLOGIN-ID-10%"
reg.10.lineAddress="%BWEXTENSION-10%"
reg.10.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.11.address="%BWLINERPORT-11%" reg.11.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-11%" reg.11.label="%BWEXTENSION-11%" reg.11.type="%BWSHAREDLINE-
11%" reg.11.broadsoft.userId="%BWLOGIN-ID-11%"
reg.11.lineAddress="%BWEXTENSION-11%"
reg.11.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.12.address="%BWLINERPORT-12%" reg.12.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-12%" reg.12.label="%BWEXTENSION-12%" reg.12.type="%BWSHAREDLINE-
12%" reg.12.broadsoft.userId="%BWLOGIN-ID-12%"
reg.12.lineAddress="%BWEXTENSION-12%"
reg.12.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.2.address="%BWLINERPORT-2%" reg.2.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-2%" reg.2.label="%BWEXTENSION-2%" reg.2.type="%BWSHAREDLINE-2%"
reg.2.broadsoft.userId="%BWLOGIN-ID-2%" reg.2.lineAddress="%BWEXTENSION-
2%" reg.2.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.3.address="%BWLINERPORT-3%" reg.3.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-3%" reg.3.displayName="%BWFIRSTNAME-3% %BWLASTNAME-3%"
reg.3.label="%BWEXTENSION-3%" reg.3.type="%BWSHAREDLINE-3%"
reg.3.broadsoft.userId="%BWLOGIN-ID-3%" reg.3.lineAddress="%BWEXTENSION-
3%" reg.3.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.4.address="%BWLINERPORT-4%" reg.4.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-4%" reg.4.displayName="%BWFIRSTNAME-4% %BWLASTNAME-4%"
reg.4.label="%BWEXTENSION-4%" reg.4.type="%BWSHAREDLINE-4%"
reg.4.broadsoft.userId="%BWLOGIN-ID-4%" reg.4.lineAddress="%BWEXTENSION-
4%" reg.4.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.5.address="%BWLINERPORT-5%" reg.5.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-5%" reg.5.displayName="%BWFIRSTNAME-5% %BWLASTNAME-5%"
reg.5.label="%BWEXTENSION-5%" reg.5.type="%BWSHAREDLINE-5%"
reg.5.broadsoft.userId="%BWLOGIN-ID-5%" reg.5.lineAddress="%BWEXTENSION-
5%" reg.5.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.6.address="%BWLINERPORT-6%" reg.6.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-6%" reg.6.displayName="%BWFIRSTNAME-6% %BWLASTNAME-6%"
reg.6.label="%BWEXTENSION-6%" reg.6.type="%BWSHAREDLINE-6%"
reg.6.broadsoft.userId="%BWLOGIN-ID-6%" reg.6.lineAddress="%BWEXTENSION-
6%" reg.6.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.7.address="%BWLINERPORT-7%" reg.7.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-7%" reg.7.label="%BWEXTENSION-7%" reg.7.type="%BWSHAREDLINE-7%"
reg.7.broadsoft.userId="%BWLOGIN-ID-7%" reg.7.lineAddress="%BWEXTENSION-
7%" reg.7.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.8.address="%BWLINERPORT-8%" reg.8.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-8%" reg.8.label="%BWEXTENSION-8%" reg.8.type="%BWSHAREDLINE-8%"
reg.8.broadsoft.userId="%BWLOGIN-ID-8%" reg.8.lineAddress="%BWEXTENSION-
8%" reg.8.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%"
reg.9.address="%BWLINERPORT-9%" reg.9.bargeInEnabled="%BWSCA-BRIDGING-
BINARY-9%" reg.9.label="%BWEXTENSION-9%" reg.9.type="%BWSHAREDLINE-9%"
reg.9.broadsoft.userId="%BWLOGIN-ID-9%" reg.9.lineAddress="%BWEXTENSION-
9%" reg.9.enablePvtHoldSoftKey="%FEATURE_PVT_HOLD%">
    <reg.1.auth reg.1.auth.password="%BWAUTHPASSWORD-1%"
reg.1.auth.userId="%BWAUTHUSER-1%"
reg.1.auth.loginCredentialType="usernameAndPassword" />
    <reg.1.server reg.1.server.1.address="%BWHOST-1%" />

```



```

    <reg.1.serverFeatureControl
reg.1.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.1.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.1.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-1%"
reg.1.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-1%" />
    <reg.1.enhancedCallPark
reg.1.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
    <reg.10.auth reg.10.auth.password="%BWAUTHPASSWORD-10%"
reg.10.auth.userId="%BWAUTHUSER-10%"
reg.10.auth.loginCredentialType="usernameAndPassword" />
    <reg.10.server reg.10.server.1.address="%BWHOST-10%" />
    <reg.10.serverFeatureControl
reg.10.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.10.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.10.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-10%"
reg.10.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-10%" />
    <reg.10.enhancedCallPark
reg.10.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
    <reg.11.auth reg.11.auth.password="%BWAUTHPASSWORD-11%"
reg.11.auth.userId="%BWAUTHUSER-11%"
reg.11.auth.loginCredentialType="usernameAndPassword" />
    <reg.11.server reg.11.server.1.address="%BWHOST-11%" />
    <reg.11.serverFeatureControl
reg.11.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.11.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.11.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-11%"
reg.11.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-11%" />
    <reg.11.enhancedCallPark
reg.11.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
    <reg.12.auth reg.12.auth.password="%BWAUTHPASSWORD-12%"
reg.12.auth.userId="%BWAUTHUSER-12%"
reg.12.auth.loginCredentialType="usernameAndPassword" />
    <reg.12.server reg.12.server.1.address="%BWHOST-12%" />
    <reg.12.serverFeatureControl
reg.12.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.12.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.12.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-12%"
reg.12.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-12%" />
    <reg.12.enhancedCallPark
reg.12.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
    <reg.2.auth reg.2.auth.password="%BWAUTHPASSWORD-2%"
reg.2.auth.userId="%BWAUTHUSER-2%"
reg.2.auth.loginCredentialType="usernameAndPassword" />
    <reg.2.server reg.2.server.1.address="%BWHOST-2%" />
    <reg.2.serverFeatureControl
reg.2.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.2.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.2.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-2%"
reg.2.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-2%" />
    <reg.2.enhancedCallPark
reg.2.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
    <reg.3.auth reg.3.auth.password="%BWAUTHPASSWORD-3%"
reg.3.auth.userId="%BWAUTHUSER-3%"
reg.3.auth.loginCredentialType="usernameAndPassword" />
    <reg.3.server reg.3.server.1.address="%BWHOST-3%" />

```

```

<reg.3.serverFeatureControl
reg.3.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.3.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.3.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-3%"
reg.3.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-3%" />
<reg.3.enhancedCallPark
reg.3.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
<reg.4.auth reg.4.auth.password="%BWAUTHPASSWORD-4%"
reg.4.auth.userId="%BWAUTHUSER-4%"
reg.4.auth.loginCredentialType="usernameAndPassword" />
<reg.4.server reg.4.server.1.address="%BWHOST-4%" />
<reg.4.serverFeatureControl
reg.4.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.4.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.4.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-4%"
reg.4.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-4%" />
<reg.4.enhancedCallPark
reg.4.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
<reg.5.auth reg.5.auth.password="%BWAUTHPASSWORD-5%"
reg.5.auth.userId="%BWAUTHUSER-5%"
reg.5.auth.loginCredentialType="usernameAndPassword" />
<reg.5.server reg.5.server.1.address="%BWHOST-5%" />
<reg.5.serverFeatureControl
reg.5.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.5.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.5.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-5%"
reg.5.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-5%" />
<reg.5.enhancedCallPark
reg.5.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
<reg.6.auth reg.6.auth.password="%BWAUTHPASSWORD-6%"
reg.6.auth.userId="%BWAUTHUSER-6%"
reg.6.auth.loginCredentialType="usernameAndPassword" />
<reg.6.server reg.6.server.1.address="%BWHOST-6%" />
<reg.6.serverFeatureControl
reg.6.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.6.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.6.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-6%"
reg.6.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-6%" />
<reg.6.enhancedCallPark
reg.6.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
<reg.7.auth reg.7.auth.password="%BWAUTHPASSWORD-7%"
reg.7.auth.userId="%BWAUTHUSER-7%"
reg.7.auth.loginCredentialType="usernameAndPassword" />
<reg.7.server reg.7.server.1.address="%BWHOST-7%" />
<reg.7.serverFeatureControl
reg.7.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.7.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.7.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-7%"
reg.7.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-7%" />
<reg.7.enhancedCallPark
reg.7.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
<reg.8.auth reg.8.auth.password="%BWAUTHPASSWORD-8%"
reg.8.auth.userId="%BWAUTHUSER-8%"
reg.8.auth.loginCredentialType="usernameAndPassword" />
<reg.8.server reg.8.server.1.address="%BWHOST-8%" />
<reg.8.serverFeatureControl
reg.8.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.8.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.8.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-8%"
reg.8.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-8%" />
<reg.8.enhancedCallPark
reg.8.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />

```

```

    <reg.9.auth reg.9.auth.password="%BWAUTHPASSWORD-9%"
reg.9.auth.userId="%BWAUTHUSER-9%"
reg.9.auth.loginCredentialType="usernameAndPassword" />
    <reg.9.server reg.9.server.1.address="%BWHOST-9%" />
    <reg.9.serverFeatureControl
reg.9.serverFeatureControl.cf="%FEATURE_SYNC_CF%"
reg.9.serverFeatureControl.dnd="%FEATURE_SYNC_DND%"
reg.9.serverFeatureControl.securityClassification="%BWSECCLASS-BINARY-9%"
reg.9.serverFeatureControl.callRecording="%BWCALLRECORDING-BINARY-9%" />
    <reg.9.enhancedCallPark
reg.9.enhancedCallPark.enabled="%FEATURE_ENHANCED_CP%" />
</reg>
    <tcpIpApp>
    <tcpIpApp.snmp tcpIpApp.snmp.gmtOffset="%BWTIMEZONE-1%"
tcpIpApp.snmp.address="%SNTP_SERVER%" />
    </tcpIpApp>
    <!-- ACD Feature -->
    <feature feature.autoLocalHold="0">
    <feature.acdAgentAvailability
feature.acdAgentAvailability.enabled="%FEATURE_SYNC_ACD%" />
    <feature.acdLoginLogout
feature.acdLoginLogout.enabled="%FEATURE_SYNC_ACD%" />
    <feature.acdServiceControlUri
feature.acdServiceControlUri.enabled="%FEATURE_SYNC_ACD%" />
    <feature.acdPremiumUnavailability
feature.acdPremiumUnavailability.enabled="%FEATURE_CALL_CENTER%" />
    <feature.bluetooth feature.bluetooth.enabled="1"></feature.bluetooth>
    <!--feature.broadsoftPersonalDir.enabled="%FEATURE_BW_DIR_PERSONAL%"
added-->
    <!-- 0 (default) - Personal Directory feature is disabled. -->
    <!-- 1 - Personal Directory feature is enabled. -->
    <!--feature.broadsoftGroupDir.enabled="%FEATURE_BW_DIR_GROUP%" added-
->
    <!-- 0 (default) - Disable the BroadSoft Group Directory.-->
    <!-- 1 - Enable the BroadSoft Group Directory -->
    <!--
feature.broadsoftdir.showDefaultSearch="%FEATURE_BW_DIR_DEFAULT_SEARCH%"
added-->
    <!-- 0 (default) - Disables the Enterprise Directory default search
feature.-->
    <!-- 1 - The Enterprise Directory default search feature allows the
users to view the initial list of contacts by default. -->
    <feature.broadsoftdir feature.broadsoftdir.enabled="%FEATURE_BW_DIR%"
feature.broadsoftPersonalDir.enabled="%FEATURE_BW_DIR_PERSONAL%"
feature.broadsoftGroupDir.enabled="%FEATURE_BW_DIR_GROUP%"
feature.broadsoftdir.showDefaultSearch="%FEATURE_BW_DIR_DEFAULT_SEARCH%">
</feature.broadsoftdir>
    <feature.broadsoftUcOne
feature.broadsoftUcOne.enabled="%FEATURE_BW_UC_ONE%"></feature.broadsoftU
cOne>
    <feature.callCenterStatus
feature.callCenterStatus.enabled="%FEATURE_CALL_CENTER%"></feature.callCe
nterStatus>
    <feature.callList feature.callList.enabled="1"></feature.callList>
    <feature.callListMissed
feature.callListMissed.enabled="1"></feature.callListMissed>
    <feature.callListPlaced
feature.callListPlaced.enabled="1"></feature.callListPlaced>
    <feature.callListReceived
feature.callListReceived.enabled="1"></feature.callListReceived>
    <feature.callPark
feature.callPark.enabled="%FEATURE_CALLPARK%"></feature.callPark>

```

```

    <feature.callRecording
feature.callRecording.enabled="0"></feature.callRecording>
    <feature.directory feature.directory.enabled="1"></feature.directory>
    <feature.hoteling feature.hoteling.enabled="%BWHOTELINGMODE-
1%"></feature.hoteling>
    <feature.messaging feature.messaging.enabled="0"></feature.messaging>
    <feature.moh feature.moh.enabled="0"
feature.moh.filename=""></feature.moh>
    <feature.presence
feature.presence.enabled="%FEATURE_PRESENCE%"></feature.presence>
    <feature.qml feature.qml.enabled="1"></feature.qml>
    <!--
feature.broadsoft.xsi.callWaiting.enabled="%FEATURE_SERVER_CWAIT%" added-
->
    <!-- 0 (Default) - Disables the feature to manage incoming calls by
the server. -->
    <!-- 1 - Allows the server to manage the incoming calls. -->
    <feature.broadsoft
feature.broadsoft.xsi.RemoteOffice.enabled="%FEATURE_REMOTE_OFFICE%"
feature.broadsoft.xsi.BroadWorksAnywhere.enabled="%FEATURE_BW_ANYWHERE%"
feature.broadsoft.xsi.SimultaneousRing.enabled="%FEATURE_SIM_RING%"
feature.broadsoft.xsi.LineIdblock.enabled="%FEATURE_CLID_BLOCK%"
feature.broadsoft.xsi.AnonymousCalReject.enabled="%FEATURE_ANONYMOUS_REJ%
"
feature.broadsoft.xsi.callWaiting.enabled="%FEATURE_SERVER_CWAIT%"></feat
ure.broadsoft>
    <feature.callCenterCallInformation
feature.callCenterCallInformation.enable="0" />
    <feature.executiveadmin
feature.BSExecutiveAssistant.enabled="%FEATURE_EXEC_ADMIN%"
feature.BSExecutiveAssistant.regIndex="1"
feature.BSExecutiveAssistant.userRole="%EXEC_ASSIST_ROLE%"></feature.exec
utiveadmin>
    <!--feature.broadsoft.callLogs="%FEATURE_CALL_LOGS%" added -->
    <!-- Basic - Enables the BSFT server call logs feature. -->
    <!-- Disabled - Disables the BSFT server call logs feature. -->
    <!--
feature.broadsoft.basicCallLogs.redial.enabled="%FEATURE_SERVER_REDIAL%"
added-->
    <!-- 0 (default) - Disables the feature to redial the last number
called from any device connected to same line -->
    <!-- 1 - Allows you to redial the last number called from any device
connected to same line. -->
    <feature.broadsoftCallLogs
feature.broadsoft.callLogs="%FEATURE_CALL_LOGS%"
feature.broadsoft.basicCallLogs.redial.enabled="%FEATURE_SERVER_REDIAL%">
</feature.broadsoftCallLogs>
    </feature>
    <dir>
    <dir.broadsoft>
    <dir.broadsoft.xsp
dir.broadsoft.xsp.address="http://%XSP_ADDRESS_XSI_ACTIONS%/"
dir.broadsoft.useXspCredentials="0" dir.broadsoft.regMap="%DIR_LINE%" />
    </dir.broadsoft>
    </dir>

```

```

    <xmpp xmpp.1.auth.domain="%BW_IMP_SERVICE_NET_ADDRESS-1%"
xmpp.1.auth.password="%BW_USER_IMP_PWD-1%"
xmpp.1.auth.useLoginCredentials="0" xmpp.1.dialMethod="sip"
xmpp.1.enable="%FEATURE_BW_UC_ONE%" xmpp.1.jid="%BW_USER_IMP_ID-1%"
xmpp.1.privacy="0" xmpp.1.regMap="1" xmpp.1.roster.invite.accept="prompt"
xmpp.1.roster.invite.addMethod="h350Person"
xmpp.1.server="%BW_IMP_SERVICE_NET_ADDRESS-1%"
xmpp.1.verifyCert="0"></xmpp>
    <acd acd.reg="%ACD_LINE%" acd.stateAtSignIn="%ACD_SIGNIN_STATE%"
acd.1.unavailreason.active="1" acd.1.unavailreason.codeValue="10001"
acd.1.unavailreason.codeName="Out to lunch"
acd.2.unavailreason.active="1" acd.2.unavailreason.codeValue="10002"
acd.2.unavailreason.codeName="On the phone"
acd.3.unavailreason.active="1" acd.3.unavailreason.codeValue="10003"
acd.3.unavailreason.codeName="Out for coffee"
acd.4.unavailreason.active="1" acd.4.unavailreason.codeValue="10004"
acd.4.unavailreason.codeName="In a meeting"
acd.5.unavailreason.active="1" acd.5.unavailreason.codeValue="10005"
acd.5.unavailreason.codeName="On vacation" acd.6.unavailreason.active="1"
acd.6.unavailreason.codeValue="10006" acd.6.unavailreason.codeName="In
training" />
    <!-- CALL INFORMATION / CALL MIME TYPE: FEATURE_ACD_CALL_INFORMATION --
>
    <push apps.push.messageType="3" apps.push.serverRootURL=""
apps.push.username="" apps.push.password="" />
    <!-- Set the Network Conference URI and Hoteling|Flexible Seating mode
-->
    <voIpProt>
        <voIpProt.SIP.conference voIpProt.SIP.conference.address="%BWNWORK-
CONFERENCE-SIPURI-1%" />
        <voIpProt.SIP.acd
voIpProt.SIP.acd.signalingMethod="%FEATURE_SYNC_ACD%" />
        <voIpProt.SIP.serverFeatureControl.localProcessing
voIpProt.SIP.serverFeatureControl.localProcessing.cf="0"
voIpProt.SIP.serverFeatureControl.localProcessing.dnd="0"></voIpProt.SIP.
serverFeatureControl.localProcessing>
    </voIpProt>
    <Call call.parkedCallRetrieveString="%BWFAC-CALL-PARK-RETRIEVE-1%"
call.shared.disableDivert="0" call.shared.reject="%CALL_DECLINE%" />
    <divert divert.1.sharedDisabled="0" divert.2.sharedDisabled="0"
divert.3.sharedDisabled="0" divert.4.sharedDisabled="0"
divert.5.sharedDisabled="0" divert.6.sharedDisabled="0"
divert.7.sharedDisabled="0" divert.8.sharedDisabled="0"
divert.9.sharedDisabled="0" divert.10.sharedDisabled="0"
divert.11.sharedDisabled="0" divert.12.sharedDisabled="0" />
    <flexibleSeating hoteling.reg="%BWHOTELINGLINE-1%"
fs.unLockPhone.pin="%BWFLEXIBLESEATINGUNLOCKPIN-1%"
hotelingMode.type="%BWHOTELINGMODE-1%" />
</polycomConfig>

```

Appendix B: Server Side Configuration for Device Management Extended File Capture

The following configurations are the server side provisioning steps for enabling the BroadWorks Device Management's Extended File Capture capability. The following instructions provided only need to be performed once per server/repository instance and they are Device Profile Type independent. The Device Profile Dependent configurations are provided in the Device Management section of this document.

Profile Server Configuration

Install, activate, and deploy the Extended File Capture Repository Web Application (BroadworksFileReposExtdCapture):

```
PS_CLI/Maintenance/ManagedObjects> get broadworks
BroadWorks Managed Objects
=====

* Server:
  Identity.....: PS
  Version.....: Rel_20.sp1_1.606
  Administrative State..: Unlocked

* Applications:
      Name          Version  Deployed  Administrative State
Effective State
=====
Unlocked      CCReportingDBManagement  20.sp1_1.606      true      Unlocked
Unlocked      EnhancedCallLogsDBManagement  20.sp1_1.606      true      Unlocked
Unlocked      WebContainer  20.sp1_1.606      true      Unlocked

3 entries found.

* Hosted Applications:
      Name          Version          Context
Path  Deployed
=====
/      true      BroadworksFileRepos  20.sp1_1.606
/      true      BroadworksFileReposExtdCapture  20.sp1_1.606
/BroadworksFileReposExtdCapture  true
      CCReporting  20.sp1_1.606
/CCReporting      true
      CCReportingRepository  20.sp1_1.606
/CCReportingRepository  true
      LogRepository  20.sp1_1.606
/logrepos      true

5 entries found.
```

Set the file delete and max file per directory policy:

```
PS_CLI/Applications/BroadworksFileReposExtdCapture/StorageManagement/Root>
get
deletionDelayInDays = 30
maxNbFilesPerDirectory = 25
```

Create the extended file capture repository root directory, this following example is chosen such that the directory is alongside the device management file repository:

```
PS_CLI/Applications/BroadworksFileReposExtdCapture/GeneralSettings> 0
/var/broadworks/BroadworksFileReposExtdCapture
userAuthentication = none
```

Create a user for accessing the newly created repository. Later, this user also needs to be provisioned on the Application Server for file access:

```
PS_CLI/Applications/BroadworksFileReposExtdCapture/Users> add extadmin
get,put,delete

PS_CLI/Applications/BroadworksFileReposExtdCapture/Users> 0
Username Password Access Privilege
=====
extadmin ***** get,put,delete
```

Add the Network Access List to allow repository access from other BroadWorks servers:

```
PS_CLI/Applications/BroadworksFileReposExtdCapture/NetworkAccessLists/WebDav> 0
IP Address Description
=====
<IP address of your XSP> xsp
<IP address of your AS> as
<IP address of your PS> ps
127.0.0.1 local
```

Restart the BroadWorks on the Profile Server. After the restart, the extended file capture repository's root directory is created automatically in the file system.

Application Server Configuration

Add the extended file capture repository using the same deploy context path on the Profile Server Web Application as the Root Directory. Further, make sure to toggle the Extended File Capture Support flag to "true":

```
AS_CLI/System/Device/FileRepos> get
Name Protocol Root Directory Extended File Capture Support
=====
PSExtended webdav /BroadworksFileReposExtdCapture true
ProfileServer webdav / false

AS_CLI/System/Device/FileRepos> detail PSExtended
name = PSExtended
FQDN = <Your PS IP address>
rootDirectory = /BroadworksFileReposExtdCapture
protocol = webdav
secure = false
extendedFileCaptureSupport = true
ftpPassive =
port = 80
ftpRemoteVerification =
```

Provision the same access user for the extended file capture repository as provisioned on the Profile Server previously. The password will also need to match with that of the Profile Server configuration. Further, allow the access user with all permissions:

```
AS_CLI/System/Device/FileRepos/Users> 0 PSExtended
User Name  Allow Get  Allow Delete  Allow Put
=====
extadmin   true      true         true
1 entry found.
```

Fine-tuning the File Retention Period and File Instances Archived

The file retention period and the max number of file instances kept per file can be specified on the Profile Server through the following parameters:

```
PS_CLI/Applications/BroadworksFileReposExtdCapture/StorageManagement/Root> get
deletionDelayInDays = 30
maxNbFilesPerDirectory = 25
```


References

- [1] Polycom, Inc. 2019. *Polycom® UC Software Administrator's Guide – UCS 5.9.0*. Available from Polycom, Inc. at <http://supportdocs.polycom.com>.
- [2] Cisco Systems, Inc. 2019. *BroadWorks Device Management Configuration Guide, Release 22.0*. Available from Cisco at xchange.broadsoft.com.
- [3] Cisco Systems, Inc. 2017. *BroadWorks Redundancy Guide, Release 22.0*. Available from Cisco at xchange.broadsoft.com.
- [4] Cisco Systems, Inc. 2019. *BroadWorks SIP Phone Interoperability Test Plan, Release 22.0*. Available from Cisco at xchange.broadsoft.com.
- [5] Cisco Systems, Inc. 2019. *BroadWorks Device Management Interoperability Test Plan, Release 22.0*. Available from Cisco at xchange.broadsoft.com.
- [6] Cisco Systems, Inc. 2011. *BroadSoft Partner Configuration Guide Acme Packet Net-Net 3000/4000 Series*. Available from BroadSoft at xchange.broadsoft.com.
- [7] Cisco Systems, Inc. 2015. *BroadSoft Partner Configuration Guide Edgewater EdgeMarc*. Available from Cisco at xchange.broadsoft.com.
- [8] Cisco Systems, Inc. 2019. *BroadWorks SIP Phone Functional Test Plan, Release 22.0*. Available from Cisco at xchange.broadsoft.com.
- [9] Cisco Systems, Inc. 2019. *BroadWorks SIP Phone Xsi and XMPP Test Plan, Release 22.0*. Available from Cisco at xchange.broadsoft.com.
- [10] Cisco Systems, Inc. 2019. *BroadWorks CPE Kit Usage Guide, Release 22.0*. Available from Cisco at xchange.broadsoft.com.