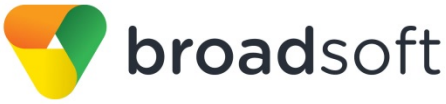

BroadSoft Partner Configuration Guide

CyberData SIP-Enabled IP Series

May 2017

Document Version 1.8

9737 Washingtonian Boulevard, Suite 350
Gaithersburg, MD USA 20878
Tel +1 301.977.9440

WWW.BROADSOFT.COM

BroadWorks® Guide

Copyright Notice

Trademarks

Document Revision History

Version	Reason for Change
1.1	Introduced document for CyberData SIP -enabled IP Series version 11.2.0b04 validation with BroadWorks Release 20.sp1.
1.2	Edited and published document.
1.3	Updated document for CyberData SIP-enabled IP Series version 11.3.0 Device Management validation with BroadWorks Release 20.sp1.
1.4	Edited changes and published document.
1.5	Updated document by adding CyberData VoIP V3 Paging Server and CyberData SIP Paging Adapter.
1.6	Edited changes and published document.
1.7	Updated document for CyberData SIP-enabled IP Series version 11.7.3 validation with BroadWorks Release 22.0.
1.8	Edited changes and published document.

Table of Contents

Table of Figures

1 Overview

This guide describes the configuration procedures required for the CyberData SIP-enabled IP Intercom, Paging, and Notification endpoints for interoperability with BroadWorks. This includes the following models:

Intercoms:

- CyberData SIP-enabled IP Outdoor Intercom
- CyberData SIP-enabled IP Emergency Indoor Intercom
- CyberData SIP-enabled IP Indoor Intercom
- CyberData SIP-enabled IP Indoor Intercom (Flush-Mounted)
- CyberData SIP-enabled IP Outdoor Keypad Intercom
- CyberData SIP-enabled IP Indoor Keypad Intercom (Wall-Mounted)
- CyberData SIP-enabled IP Indoor Keypad Intercom (Flush-Mounted)

Paging and Notification Endpoints:

- CyberData SIP-enabled IP Call Button
- CyberData SIP-enabled IP Strobe
- CyberData SIP-enabled IP Indoor Office Ringer
- CyberData SIP Paging Adapter
- CyberData VoIP V3 Paging Server
- CyberData SIP Paging Amplifier
- CyberData SIP Speaker
- CyberData SIP TalkBack Speaker

The SIP-enabled IP Series uses the Session Initiation Protocol (SIP) to communicate with BroadWorks for call control.

This guide describes the specific configuration items that are important for use with BroadWorks. It does not describe the purpose and use of all configuration items on the SIP-enabled IP Series. For those details, see the product's *Operations Guide* [1] supplied by CyberData.

2 Interoperability Status

This section provides the known interoperability status of the CyberData SIP-enabled IP Series with BroadWorks. This includes the version(s) tested, the capabilities supported, and known issues.

Interoperability testing validates that the device interfaces properly with 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 CyberData.

2.1 Verified Versions

The following table identifies the verified CyberData SIP-enabled IP Series and BroadWorks versions and the month/year the testing occurred. If the device 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 identify specific SIP-enabled IP Series versions that the partner has identified as compatible so should interface properly with 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 CyberData.

NOTE: Interoperability testing is usually performed with the latest generally available (GA) device firmware/software and the latest GA BroadWorks release and service pack at the time the testing occurs. If there is a need to use a non-verified mix of BroadWorks and device software versions, customers can mitigate their risk by self-testing the combination using the *BroadWorks SIP Phone Interoperability Test Plan* [5].

Verified Versions			
Date (mm/yyyy)	**BroadWorks Release**	**Intercom Series Verified Version**	**Intercom Series Compatible Versions**
05/2017	Release 22.0	11.7.3	Any maintenance revisions of the validate release.
05/2015	Release 20.sp1	11.3.0	Any maintenance revisions of the validate release.
01/2015	Release 20.sp1	11.2.0b04	Any maintenance revisions of the validate release.

2.2 Interface Capabilities Supported

This section identifies interface capabilities that have been verified through testing as supported by CyberData SIP-enabled IP Intercom Series.

The *Supported* column in the tables in this section identifies the CyberData SIP-enabled IP Intercom Series' 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 CyberData SIP-enabled IP Series has completed interoperability testing with BroadWorks using the *BroadWorks SIP Phone Interoperability Test Plan* [5]. The results are summarized in the following table.

The 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 BroadWorks with the intent to ensure interoperability sufficient to support the BroadWorks feature set.

NOTE: *DUT* in the following table refers to the *Device Under Test,* which in this case is the CyberData SIP-enabled IP Intercom Series.

BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
Basic	Call Origination	Yes	The IP Strobe, Paging Server, Paging Adapter, and Paging Amplifier only support call origination when the Sensor settings to play audio remotely when the sense input or intrusion trigger is triggered is set.
	Call Termination	Yes	The IP Strobe, Paging Server, Paging Adapter, and Paging Amplifier only support call termination by use of the SIP when call timer is enabled.
	Session Audit	Yes	Except DUT holding scenario.
	Session Timer	No	
	Ringback	Yes	The IP Strobe and IP Call Button do not support local ringback as neither device has a speaker.
	Forked Dialog	Yes	
	181 Call Being Forwarded	Yes	
	Dial Plan	Yes	
	DTMF – Inband	No	
	DTMF – RFC 2833	Yes	
	DTMF – DTMF Relay	No	

BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
	Codec Negotiation	Yes	
	Codec Renegotiation	Yes	Except transfers during call hold.
BroadWorks Services	Third-Party Call Control – Basic	Yes	
	Third-Party Call Control – Advanced	No	
	Voice Message Deposit/Retrieval	Yes	
	Message Waiting Indicator – Unsolicited	Yes	
	Message Waiting Indicator – Solicited	NA	
	Message Waiting Indicator – Detail	NA	
	Voice Portal Outcall	Yes	
	Advanced Alerting – Ringing	No	
	Advanced Alerting – Call Waiting	No	
	Advanced Alerting – Ring Splash	No	
	Advanced Alerting – Silent Alerting	No	
	Calling Line ID	NA	
	Calling Line ID with Unicode Characters	NA	
	Connected Line ID	NA	
	Connected Line ID with Unicode Characters	NA	
	Connected Line ID on UPDATE	NA	
	Connected Line ID on Re-INVITE	NA	
	Diversion Header	Yes	
	History-Info Header	Yes	
	Advice of Charge	No	
	Meet-Me Conferencing	NA	
	Meet-Me Conferencing – G722	NA	
	Meet-Me Conferencing – AMR-WB	NA	
	Meet-Me Conferencing – Opus	NA	
	Collaborate – Audio	NA	
	Collaborate – Audio – G722	NA	
	Collaborate – Audio – Opus	NA	
	Call Decline Policy	NA	
DUT Services – Call Control Services	Call Waiting	NA	
	Call Hold	NA	

BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
	Call Transfer	NA	
	Three-Way Calling	NA	
	Network-Based Conference	NA	
DUT Services – Registration and Authentication	Register Authentication	Yes	
	Maximum Registration	NT	Max. Registration only limited up to 3600 seconds.
	Minimum Registration	Yes	
	Invite Authentication	Yes	
	Re-Invite/Update Authentication	No	
	Refer Authentication	NA	
	Device Authenticating BroadWorks	No	
DUT Services – Emergency Call	Emergency Call	No	
	Emergency Call with Ringback	No	
DUT Services – P-Access-Network-Info Header	REGISTER with P-Access-Network-Info Header	No	
	INVITE with P-Access-Network-Info Header	No	
DUT Services – Miscellaneous	Do Not Disturb	No	
	Call Forwarding Always	No	
	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	NA	
	Call Park Notification	NA	
Advanced Phone Services – Feature Key Synchronization, Private Line	Do Not Disturb	NA	
	Do Not Disturb Ring Splash	NA	
	Call Forwarding	NA	
	Call Forwarding Always Ring Splash	NA	
	Call Forwarding Always Diversion Inhibitor	NA	
	Call Center Agent Logon/Logoff	NA	
	Call Center Agent Unavailable Code	NA	
	Executive – Call Filtering	NA	
	Executive-Assistant – Call Filtering	NA	
	Executive-Assistant – Diversion	NA	

BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
	Call Recording	NA	
	Security Classification	NA	
Advanced Phone Services – Feature Key Synchronization, Shared Line	Do Not Disturb	NA	
	Do Not Disturb Ring Splash	NA	
	Call Forwarding	NA	
	Call Forwarding Always Ring Splash	NA	
	Call Forwarding Always Diversion Inhibitor	NA	
	Security Classification	NA	
Advanced Phone Services – Missed Calls Display Synchronization	Missed Calls Display Sync	NA	
Advanced Phone Services – Shared Call Appearance using Call Info	Line-Seize	NA	
	Call-Info/Lamp Management	NA	
	Public Hold	NA	
	Private Hold	NA	
	Hybrid Key System	NA	
	Multiple Call Arrangement	NA	
	Bridge Active Line	NA	
	Bridge Active Line – Silent Monitor	NA	
	Call Park Notification	NA	
Advanced Phone Services – Call Park Notification	Call Park Notification	NA	
Advanced Phone Services – Call Center	Hold Reminder	NA	
	Call Information	NA	
	Hoteling Event	NA	
	Status Event	NA	
	Disposition Code	NA	
	Emergency Escalation	NA	
	Customer Originated Trace	NA	
Advanced Phone Services – Call Recording Controls	Pause/Resume	NA	
	Start/Stop	NA	
	Record Local Conference	NA	
	Record Network Conference	NA	
Advanced Phone Services – Call Recording Video	Basic Call	NA	
	Record Local Conference	NA	

BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
	Record Network Conference	NA	
Advanced Phone Services – Security Classification	Security Classification	NA	
Advanced Phone Services – Conference Event	Network-Based Conference Creator	NA	
	Network-Based Conference Participant	NA	
	Meet-Me Conference Participant	NA	
Redundancy	DNS SRV Lookup	Yes	
	Register Failover/Failback	No	
	Invite Failover/Failback	No	
	Bye Failover	No	
SBC/ALG - Basic	Register	Yes	
	Outgoing Invite	Yes	
	Incoming Invite	Yes	
SBC/ALG – Failover/Failback	Register Failover/Failback	No	
	Invite Failover/Failback	No	
Video – Basic Video Calls	Call Origination	NA	
	Call Termination	NA	
	Call Hold	NA	
	Call Waiting	NA	
	Call Transfer	NA	
Video – BroadWorks Video Services	Auto Attendant	NA	
	Auto Attendant – HD	NA	
	Voice Messaging	NA	
	Voice Messaging – HD	NA	
	Custom Ringback	NA	
Video – BroadWorks Video Conference	Network-based Conference	NA	
	Network-based Conference – HD	NA	
	Collaborate – Video	NA	
	Collaborate – Video – HD	NA	
Video – BroadWorks WebRTC Client	Call from WebRTC Client	NA	
	Call to WebRTC Client	NA	
TCP	Register	No	
	Outgoing Invite	No	
	Incoming Invite	No	

BroadWorks SIP Phone Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
IPV6	Call Origination	No	
	Call Termination	No	
	Session Audit	No	
	Ringback	No	
	Codec Negotiation/Renegotiation	No	
	Voice Message Deposit/Retrieval	No	
	Call Control	No	
	Registration with Authentication	No	
	Busy Lamp Field	No	
	Redundancy	No	
	SBC	No	
	Video	No	
	Dual Stack with Alternate Connectivity	No	

2.2.2 Other Interface Capabilities

The CyberData SIP-enabled IP Intercom Series may have implemented support for the following:

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

Support for these interfaces is demonstrated by completing the *BroadWorks SIP Phone Functional Test Plan* [6]. Support for these interfaces is summarized in the following table.

BroadWorks Xtended Services Interface (Xsi) and BroadCloud IM&P Support Table			
Interface	**Feature**	**Supported**	**Comments**
Xsi Features – Authentication	Authenticate with SIP Credentials	No	
	Authenticate with BroadWorks User Login Credentials	No	
	Authenticate with BroadWorks User Directory Number	No	
Xsi Features – User Service Configuration	Remote Office	No	
	BroadWorks Anywhere	No	
	Simultaneous Ringing	No	
	Caller ID Blocking	No	
	Call Forwarding Always	No	
	Call Forwarding Busy	No	
	Call Forwarding No Answer	No	

BroadWorks Xtended Services Interface (Xsi) and BroadCloud IM&P Support Table			
Interface	**Feature**	**Supported**	**Comments**
	Do Not Disturb	No	
Xsi Features – Directories	Enterprise Directory	No	
	Enterprise Common Phone List	No	
	Group Directory	No	
	Group Common Phone List	No	
	Personal Phone List	No	
	Search All Directories	No	
Xsi Features – Call Logs	Placed Calls	No	
	Received Calls	No	
	Missed Calls	No	
	All Calls	No	
	Sort by Name	No	
XMPP Features – Contact/Buddy List	Contacts	No	
	Favorites	No	
	Groups	No	
	Non-XMPP Contacts	No	
	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 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 BroadWorks release dependent.

The *Issue Number* is a tracking number for the issue. If it is a CyberData issue, the issue number is from CyberData's tracking system. If it is a BroadWorks issue, the issue number is from BroadSoft'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			
		11.7.3	11.3.0	11.2.0b04	
	No issues identified.				

3 BroadWorks Configuration

This section identifies the required BroadWorks device profile type for the CyberData SIP-enabled IP Series as well as any other unique BroadWorks configuration required for interoperability with the SIP Enabled IP Series.

3.1 BroadWorks Device Profile Type Configuration

This section identifies the device profile type settings to use when deploying the CyberData SIP-enabled IP Series with BroadWorks.

Create a device profile type for the CyberData SIP-enabled IP Series with settings as shown in the following example. The settings shown are recommended for use when deploying the CyberData SIP-enabled IP Series with BroadWorks. For an explanation of the profile parameters, see the *BroadWorks Device Management Configuration Guide* [2].

NOTE: All of the CyberData SIP-enabled IP Series models support one SIP line.

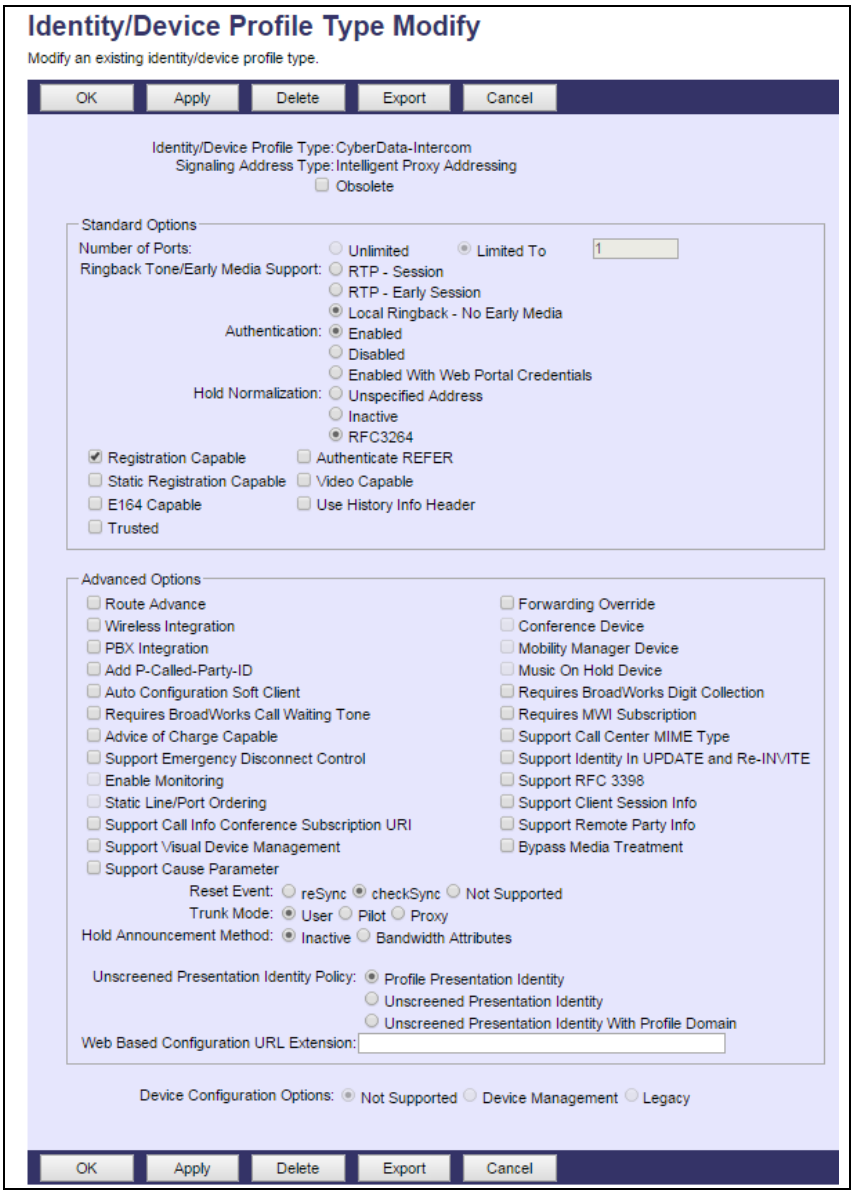

Figure 1 Device Identity/Profile Type

3.2 BroadWorks Configuration Steps

There are no additional BroadWorks configuration steps necessary.

4 CyberData SIP-enabled IP Series Configuration

This section describes the configuration settings required for the SIP Enabled IP Series integration with BroadWorks, primarily focusing on the SIP interface configuration. The Intercom configuration settings identified in this section have been derived and verified through interoperability testing with BroadWorks. For configuration details not covered in this section, see the *VoIP Outdoor Intercom Operations Guide* [1] for the SIP Enabled IP Series.

4.1 Configuration Method

CyberData SIP-enabled IP Intercom, Paging, and Notification endpoints can be configured using "autoprovisioning" files via HTTP, HTTPS, or TFTP protocols, or manually configured through the web interface using a web browser.

Upon boot, the device looks for an autoprovisioning server configured through the web interface or specified through a DHCP option. In addition to configuration through the web interface, the provisioning server address, file name, and other applicable settings may also be configured through an autoprovisioning file.

The default configuration attempts to use DHCP options 43, 72, 150, or 66 to obtain the provisioning server address in addition to IP network settings. The DHCP option determines the download protocol (HTTP, HTTPS, or TFTP) used to download the autoprovisioning file upon boot. When multiple DHCP options are specified, the device downloads autoprovisioning files from every server.

It is necessary to use an autoprovisioning file for the device's respective firmware release. A template in XML format is included in the firmware release folder on the product web page, or, a template may be downloaded from the device's web interface. See the *VoIP Outdoor Intercom Operations Guide*, or the specific model's operation guide, for more information.

Additional autoprovisioning file names can be configured through the autoprovisioning file and may contain a file, a file path, or directory. By default, the device downloads the following files when it finds a server (in order of preference):

- A file name configured through the web interface.
- A file named according to its MAC address (for example, *0020f7350058.xml*).
- The file named *000000cd.xml*.

Configuration Files

CyberData Configuration Files	Level	Description
version-uImage-product_name	System	Contains the device firmware load. The file name is used to determine when to automatically download firmware updates. If the file name has changed in the autoprovisioning file, it downloads the new file from the server.
000000cd.xml	System	Contains configurable parameters that apply to all devices in a given deployment.
<MACaddress>.xml Example*: 0020f7350058.xml*	Subscriber	Contains configurable parameters that apply to an individual device in a deployment.

4.2 System Level Configuration

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

4.2.1 Configure Network Settings

Step	Command	Description
Step 1	Set the IP Addressing Mode. `IPAddressMode = DHCP`	Set the preferred IP Addressing mode for the installation network. DHCP addressing mode is enabled on default. The device obtains IP addressing information and the provisioning server address from DHCP. If static IP addressing is desired, set *IPAddressMode* to "Static" and use the remaining *IPSettings* sub-elements in the XML template.
Step 2	Set the NTP Server address. Example: `NTPServer = north-america.pool.ntp.org`	Set a local or remote NTP server address. The address may be an IPv4 address or FQDN. The NTP server address used during interoperability testing is shown here.
Step 3	Set the NTP Time Zone. Example: `NTPTimezone = PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:01`	Set the appropriate NTP time zone for the installation network. The device uses POSIX time zone strings to specify the local time zone and daylight savings time where applicable. The POSIX time zone string value used during interoperability testing is shown here. For more information, see the *Operations Guide* [1].

4.2.2 Configure SIP Interface Settings

Step	Command	Description
Step 1	Set SIP Server address. `SIPServer = as.broadworks.net`	Set the SIP Server address to the Fully Qualified Domain Name (FQDN) for the BroadWorks Application Server cluster. This FQDN must match the domain configured for the BroadWorks subscriber's line/port domain.

Step 2	Set the Outbound Proxy address and port.
	`OutboundProxy = sbc.broadworks.net`
	`OutboundProxyPort = 5060`
		Set the Outbound Proxy to the Session Border Controller (SBC) if one is deployed between CyberData and BroadWorks.
		If there are redundant SBCs, set it to the FQDN for the SBC cluster.

Step	Command	Description
Step 3	Set the SIP Registration Timeout. `SIPRegistrationTimeout = 1200`	Set the SIP registration time (in seconds) required for BroadWorks. This setting may vary by each unique BroadWorks or SBC deployment. While the default setting is 360 seconds, the device honors any requested interval in the supported range of 30 – 3600 seconds when requested through a SIP binding from the SIP server or outbound proxy.
Step 4	Disable KeepAlive. `KeepAlive = 0`	The KeepAlive is a 60-byte, double CRLF packet sent over UDP to the SIP port used by the SIP server or outbound proxy. Disable the KeepAlive when an SBC is deployed between CyberData and BroadWorks. A value of "0" disables KeepAlive.
Step 5	Set Disable rport Discovery. `DisableRportDiscovery = Yes`	The Disable rport Discovery setting prevents the device from replacing its SIP contact address and port number with a different contact address and port number when provided by the SIP server or outbound proxy as described in *RFC 3581*. CyberData recommends setting Disable rport Discovery to Yes to prevent registration and call failures when an SBC is deployed between CyberData and BroadWorks.

4.3 Subscriber Level Configuration

This section identifies the device-specific parameters, including registration and authentication. These settings must be unique across devices to be matched with the settings for a BroadWorks SIP trunk or subscriber. SIP Registration requires that a unique address of record (AoR) be provisioned on BroadWorks and the device.

Step	Command	Description
Step 1	Set the SIP User ID. Example: `SIPUserID = 199`	Set the SIP User ID for the device's primary SIP line. The SIP User ID is the phone user portion of the unique AoR provisioned on BroadWorks. The device concatenates the SIP User ID with the SIP Server address to create the AoR for SIP registration. The AoR must match BroadWorks subscriber's line/port.
Step 2	Set the SIP Authorization ID. Example: `SIPAuthID = CyberDataUser1`	Set the SIP Authorization ID to be used for authentication. This should match the configured BroadWorks Authentication User Name.
Step 3	Set the SIP Authorization Password. Example: `SIPAuthPassword = cdpassword`	Set the SIP Authorization Password to be used for authentication. This should match the configured BroadWorks Authentication password.

Step	Command	Description
Step 4	Set the Dial Out Extension. Example: `DialoutExtension0 = 200`	Set the Dial Out Extension to be called when a user presses a device's Call button. This setting only applies to devices with a Call button and keypad intercoms in security mode. This setting does not apply to the IP Strobe.
Step 5	Set the Extension ID. Example: `DialoutID0 = frontDoorPhone`	Set the Extension ID the device should send upon outbound calls to appear in a caller ID screen. This value can be an alphanumeric string up to 64 characters in length.

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 CyberData SIP-enabled IP Series and the configuration steps required. For Device Management configuration details not covered here, see the *BroadWorks Device Management Configuration Guide* [2] and the *BroadWorks CPE Kit Usage Guide* [8].

5.1 Device Management Capabilities Supported

The CyberData SIP-enabled IP Series has completed Device Management interoperability testing with BroadWorks using the *BroadWorks Device Management Interoperability Test Plan* [7]. The results are summarized in the following table.

The 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 BroadWorks with the intent to ensure interoperability.

The *Supported* column in the following table identifies the CyberData SIP-enabled IP Series' 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 and clarifications are identified in the *Comments* column.

NOTE: *DUT* in the following table refers to the *Device Under Test*, which in this case is the CyberData SIP-enabled IP Series.

BroadWorks Device Management Interoperability Test Plan Support Table

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	Yes	
	HTTPS Download Using XSP FQDN	Yes	
	HTTPS Download Using XSP Cluster FQDN	Yes	

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

5.2 Device Management Configuration

This section identifies the steps required to enable the CyberData SIP-enabled IP Series for Device Management. For Device Management configuration details not covered here, see the *BroadWorks Device Management Configuration Guide* [2] and the *BroadWorks CPE Kit Usage Guide* [8].

5.2.1 Configure BroadWorks Tags

The template files in Device Management use tags to represent the data stored on 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 BroadWorks. There are default tags defined in the Device Management software and there are custom tags that the service provider can create and define via the web portal for use by Device Management. There are two types of custom tags that can be defined: system default tags that are common to all devices on the system and device type-specific tags that are common to CyberData device models only.

The CyberData SIP-enabled IP Series makes use of custom tags which can be configured by a BroadWorks administrator as either 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. The CyberData configuration templates make use of the tags in the following table. Add the tags if they do not already exist.

Tag Name	Valid Settings	Description
%SNTP_SERVER%	IP address/FQDN	Network Time Protocol (NTP) server address.
%SBC_ADDRESS%	IP address/FQDN	SBC SIP address when an SBC is deployed between CyberData and BroadWorks.
%SBC_PORT%	Port	SBC SIP port. The port should be set if the defined SBC address is an IP address. If the SBC address is an FQDN, then the SBC port should not be set.

Example System Default Tag Settings

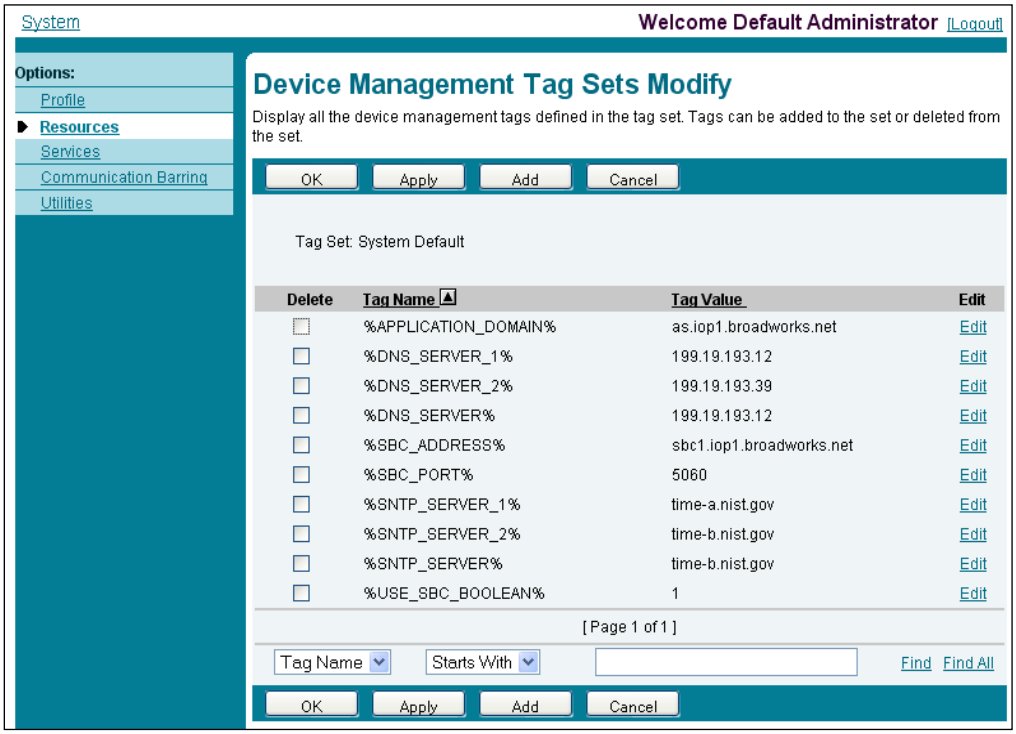

Figure 2 System Default Tag Settings

5.2.1.2 Create Device Type-specific Tags

Browse to *System* → *Resources* → *Device Management Tag Sets* and then click **Add** to add a new tag set. Configure the tag set name using the device name appended by *Tags*: *CyberData-Tags*. Add the device type-specific tags in the following table to the device tag set. If the tag set already exists, make sure the following tags are defined.

Tag Name	Valid Settings	Description
%DISABLE_RFC3581%	Yes or No	Corresponds to the "Disable rport Discovery" option in the web interface. Setting this parameter to Yes prevents the device from replacing its SIP contact address and port number with a different contact address and port number when provided by the SIP server or outbound proxy as described in *RFC 3581*. Set this parameter to Yes to prevent registration and call failures when an SBC is deployed between CyberData and BroadWorks.
%FIRMWARE_VERSION%	<xxxx> Example: 1173	Numeric firmware version number used in firmware file name.

Tag Name	Valid Settings	Description
%KEEP_ALIVE%	<xxxxxxxxx> Example: 0	Corresponds to "Keep Alive Period" option in web interface. The Keep Alive is a 60-byte, double CRLF packet sent over UDP to the SIP port used by the SIP server or outbound proxy. Disable the Keep Alive when an SBC is deployed between CyberData and BroadWorks. A value of "0" disables Keep Alive.
%MODEL%	outdoor_intercom emergency_intercom indoor_intercom outdoor_keypad indoor_keypad callbutton strobe officeringer paging_adapter paging_server paging_amplifier speaker	Specific product model used in firmware file name.
%SIP_EXPIRY%	<xxxx> Example: 1200	Corresponds to the SIP Re-registration interval (in seconds) in the web interface. The supported range is 30 to 3600 seconds.
%DIALMODE%	Telephone Speed_Dial Security Cellphone Example: Speed_Dial	Corresponds to the dial mode settings in web interface for keypad intercoms. For descriptions of each dial mode option, see the product's *Operations Guide*.
%DIALOUT_EXTENSION-0%	<xxxx> Example: 5021	Extension number a device calls when the Call button is pressed.
%DIALOUT_EXTENSION-1%	<xxxx> Example: 5022	Example of a tag used to specify an additional Dial Out Extension for a keypad intercom that supports dialing more than one pre-configured extension.
%DIALOUT_EXTENSION-2%	<xxxx> Example: 5023	Example of a tag used to specify an additional dial out extension for a keypad intercom which supports dialing more than one pre-configured extension.

Example Device Type-specific Tag Settings

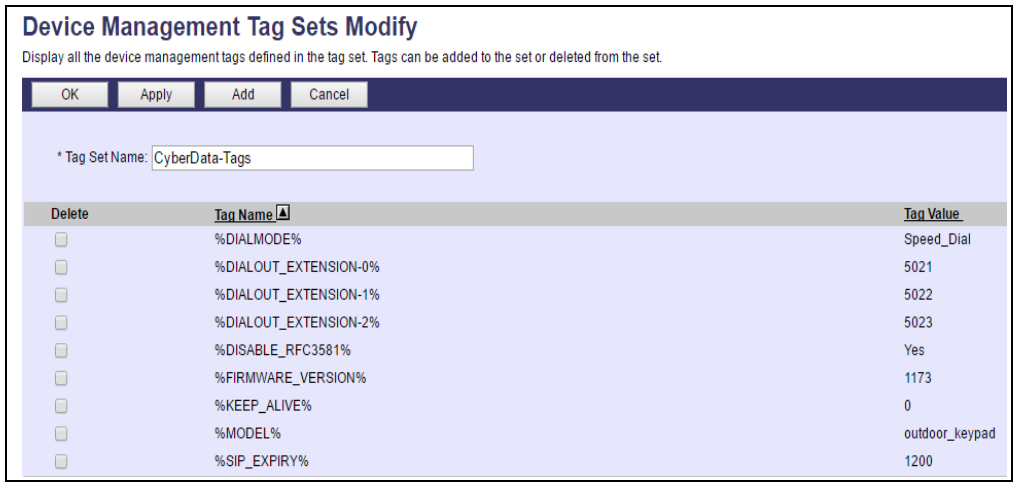

Figure 3 Device Type-specific Tag Settings

5.2.2 Configure BroadWorks Device Profile Type

The device profile type is a system-level structure that defines how the device interfaces with BroadWorks. It also identifies the default configuration files and other files, such as firmware, which are required for the device 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.

There are two BroadWorks device profile configuration methods described: import and manual. The import method takes a DTAF as input and builds the 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, then the import fails.)
- There is a DTAF file available for import with a 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, then the import can fail.

Otherwise, use the manual method.

For more detailed instructions, see the *BroadWorks CPE Kit Usage Guide* [8] and the *BroadWorks Device Management Configuration Guide* [2].

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 BroadWorks to add the CyberData SIP-enabled IP Series as a Device Management-enabled device type. In addition, see the *BroadWorks CPE Kit Usage Guide* [8].

Download the CyberData SIP-enabled IP Series CPE kit from BroadSoft Xchange at xchange.broadsoft.com/php/xchange/support/broadworks/integration/cpe. If you have trouble with the Xchange link, copy and paste it into a web browser. Extract the DTAF file(s) from the CPE kit. These are the import files. Repeat the following steps for each model you wish to import.

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

   After the import finishes, complete the following post-import configuration steps:

4) Browse to *System* → *Resources* → *Identity/Device Profile Types*.
5) Perform a search to find the imported CyberData device profile type, CyberData SIP-enabled IP Series.
6) Browse to the *Profile* page and change the Device Management Device Access FQDN to your Xtended Services Platform (Xsp) or Xtended Services Platform cluster address.

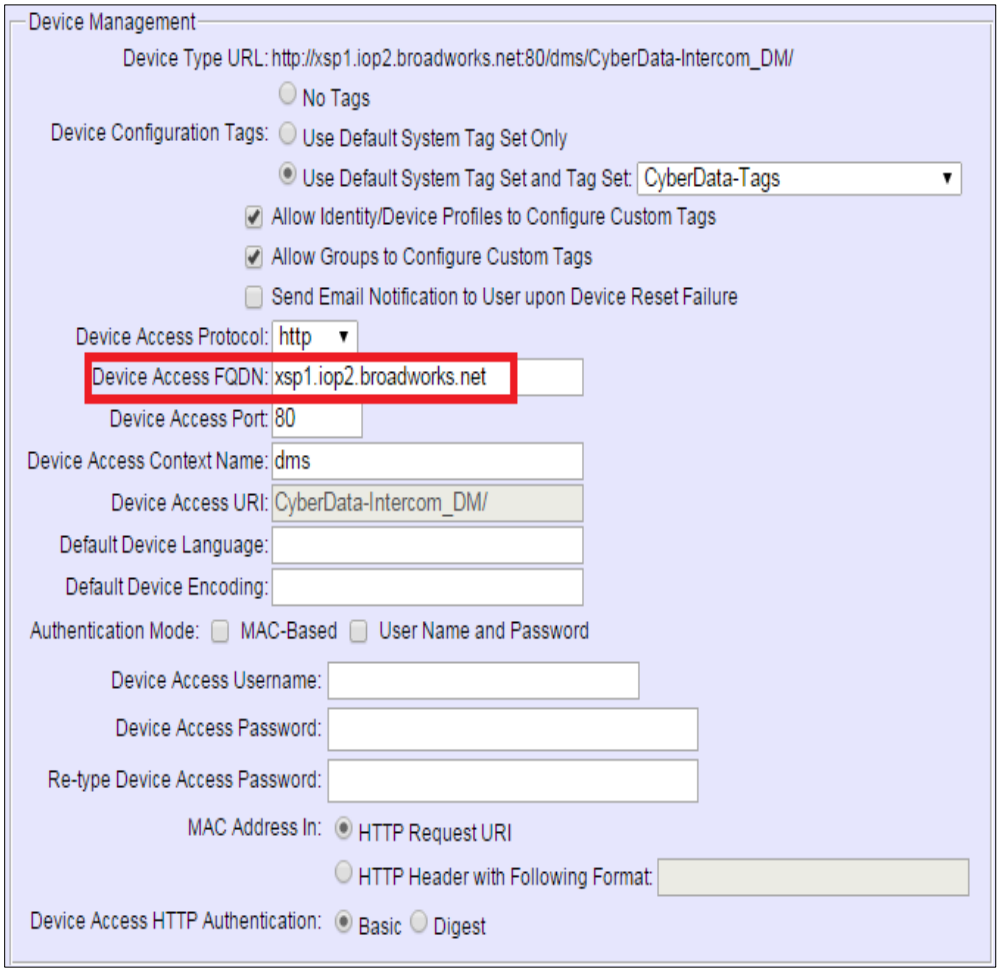

Figure 4 Device Access FQDN

7) Click the **Files and Authentication** link and then select the option to rebuild all the system files.

   Firmware files must be obtained from CyberData. These files are not included in the import. Complete the steps in section *5.2.2.2.2 Define Device Profile Type Files* to define the static firmware files and to upload the firmware.

   NOTE: The non-firmware static files in section *5.2.2.2.2 Define Device Profile Type Files* are normally included in the import.

8) After importing the DTAFs, restart the Application Server to load the *TimeZoneAlias* files.

5.2.2.2 Configuration Method 2: Manual

This section identifies the basic steps necessary for an administrator to manually configure BroadWorks to add the CyberData SIP-enabled IP Series as a Device Management-enabled device type. This method should not be used except in special cases as described in the opening to section *5.2.2 Configure BroadWorks Device Profile Type*.

For more detailed instruction on manual configuration, see the *BroadWorks CPE Kit Usage Guide* [8] and the *BroadWorks Device Management Configuration Guide* [2].

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.

If there are DTAFs for more than one device model, these steps must be completed for each model.

5.2.2.2.1 Create or Modify Device Profile Type

This section identifies the BroadWorks device profile type settings relevant to Device Management for the CyberData SIP-enabled IP Series.

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

Configure the device profile type *Signaling Address Type*, *Standard* and *Advanced* options settings to match the settings in section *3.1 BroadWorks Device Profile Type Configuration*.

Configure the device profile type *Device Management* options as shown in section *5.2.2.1 Configuration Method 1: Import*.

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

5.2.2.2.2 Define Device Profile Type Files

This section describes the BroadWorks Device Management configuration necessary to identify the configuration files and other files that the CyberData SIP-enabled IP Series downloads.

Configuration templates, firmware, and other files the CyberData SIP-enabled IP Series uses must be uploaded to BroadWorks. Download the CyberData SIP-enabled IP Series CPE kit from BroadSoft Xchange at xchange.broadsoft.com/php/xchange/support/broadworks/integration/cpe. If you have trouble with the Xchange link, copy and paste it into a Web browser. Extract the configuration files from the *Configuration Files* folder of CPE kit. Obtain the firmware files directly from CyberData.

The following table identifies the CyberData configuration files distributed with the 1130 CPE kit.

File Name	CPE Kit Template File Name	File Type	Description
Examples			
BWMACADDRESS.cfg	*%BWMACADDRESS%.cfg.template*	Device-specific	Contains configurable parameters that apply to an individual device in a deployment.
000000cd.xml	*000000cd.xml.template*	Device-specific	Contains configurable parameters that apply to all devices in a given deployment.
TimeZoneAliasLabels_<partner name>-<model>.properties	*TimeZoneAliasLabels_<partner name>-<model>.properties*	Time Zone Alias	The time zone alias file is a BroadWorks Device Management file used to map time zone identifiers between BroadWorks and <partner name> devices. A time zone alias file is required for each model.

The following table identifies other files that the CyberData SIP-enabled IP Series downloads from the server or uploads to the server. These files are not provided in the CPE kit and must be obtained from CyberData.

File Name	File Type	Description
1173-uImage-indoor_keypad	Static	The firmware file used for the Indoor Wall or Flush-Mounted Keypad Intercom.
1173-uImage-outdoor_intercom	Static	The firmware file used for the Outdoor Intercom.
1173-uImage-emergency_intercom	Static	The firmware file used for the Indoor Emergency Intercom.
1173-uImage-indoor_intercom	Static	The firmware file used for the Indoor and Indoor Flush-Mounted Intercom.
1173-uImage-outdoor_keypad	Static	The firmware file used for the Outdoor Keypad Intercom.
1176-uImage-callbutton	Static	The firmware file used for the Call Button Device.
1173-uImage-rgbstrobe	Static	The firmware file used for the Strobe Device.
1173-uImage-officeringer	Static	The firmware file used for the Indoor Office Ringer.
1161-uImage-spa31	Static	The firmware file used for the SIP Paging Adapter.
V12.0.0-uImage-pserver31	Static	The firmware file used for the VoIP V3 Paging Server.

File Name	File Type	Description
1164-uImage-pagingamp31	Static	The firmware file used for the Paging Amplifier.
1167-uImage-speakerround31	Static	The firmware file used for the Speaker devices.

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

5.2.2.2.2.1 Mac-Address Device-Specific Files

Add the %BWMACADDRESS%.xml file to the device profile type with the settings shown in *Figure 5 %BWMACADDRESS%.xml File Settings.*

After creating the device profile type file, upload *%BWMACADDRESS%.xml (*extracted from the CPE kit). Use the **Browse** button on the file definition screen. Be sure to click **Apply** after uploading the file.

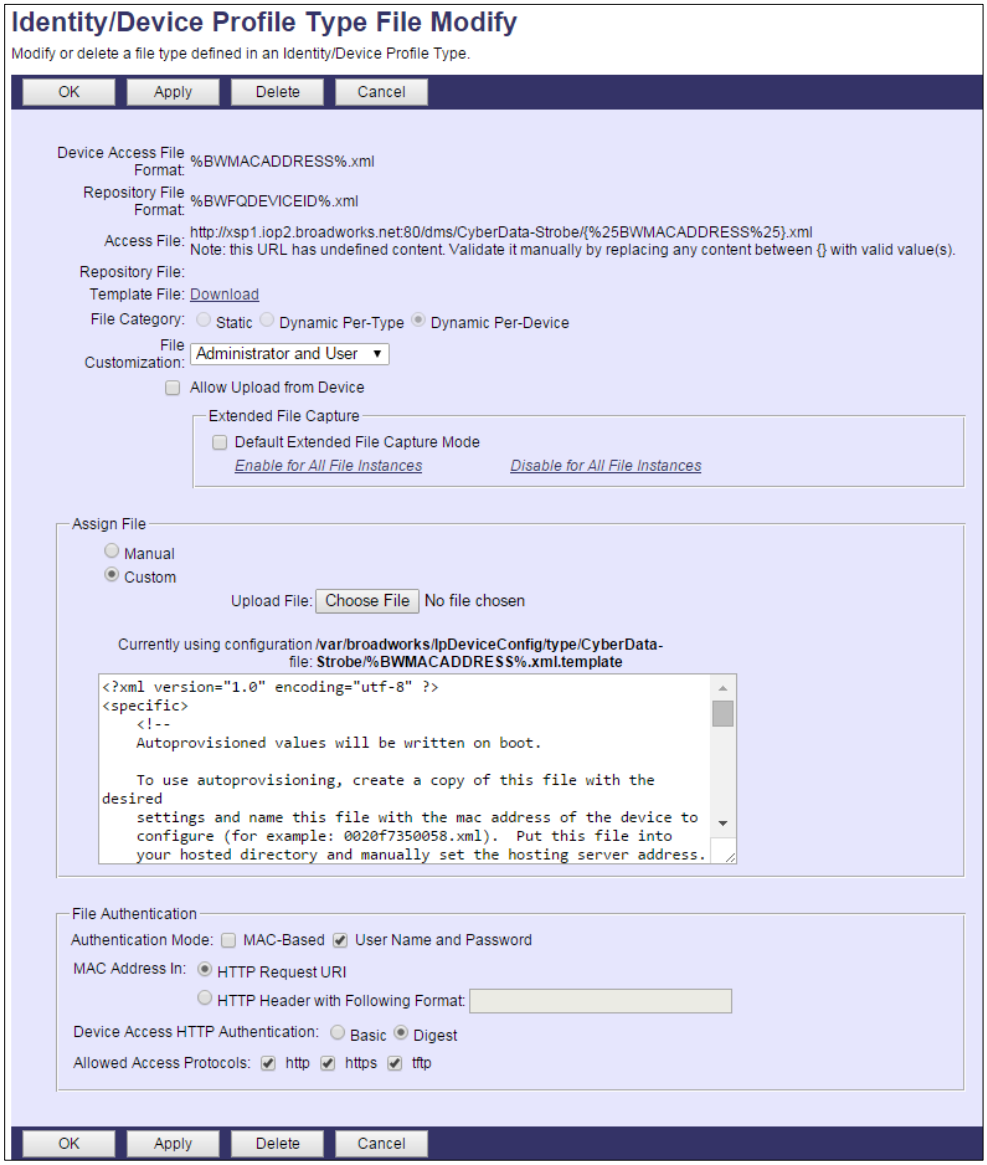

Figure 5 %BWMACADDRESS%.xml File Settings

5.2.2.2.2.2 000000cd.xml Device-Specific Files

Add the *000000cd.xml* file to the device profile type with the settings shown in *Figure 6 000000cd.xml File Settings*.

After creating the device profile type file, upload *000000cd.xml* (extracted from the CPE kit). Use the **Browse** button on the file definition screen. Be sure to click **Apply** after uploading the file.

Figure 6 000000cd.xml File Settings

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 BroadWorks Device Management tags.

Add the image file to the device profile type with the settings shown in *Figure 7 Firmware Image File*.

After creating the device profile type file, upload the firmware file (obtained from CyberData). Use the **Browse** button on the file definition screen. Be sure to click **Apply** after uploading the file.

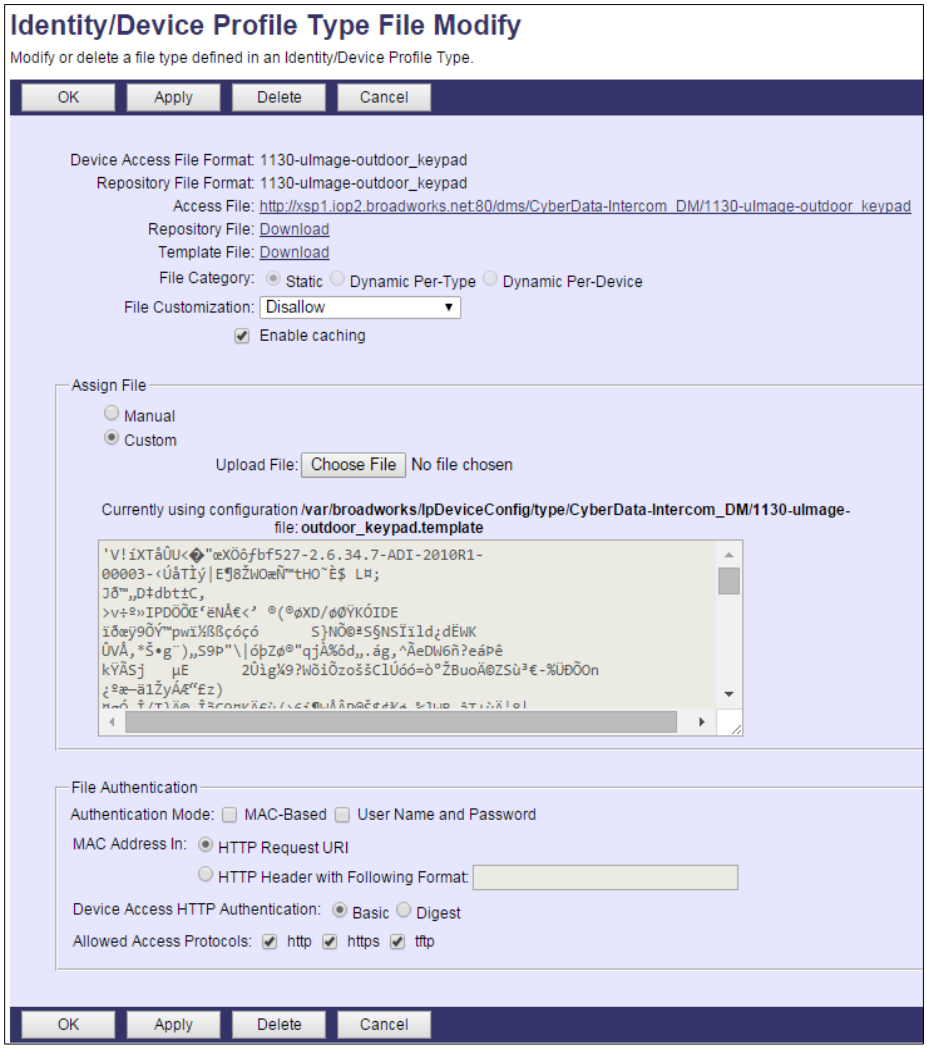

Figure 7 Firmware Image File

5.2.2.2.3 *Time Zone Mapping*

The CPE kit contains a time zone properties file for each device model. This file maps the BroadWorks user's time zone settings to the device's time zone settings.

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_CyberData-<Device_Type_Name>.properties*.

For example, if the device type name is *MyDevice T200,* the time zone mapping file name must be *TimeZoneAliasLabels_MyDevice+T200.properties*. (A space in the device name must be converted to a "+" in the file name.) A separate *TimeZoneAlias* file must be provided for each device profile type, corresponding to each CyberData model.

You must restart the Application Server for the *TimeZoneAlias* files to be picked up by the system. The following is an example of the file contents.

```
US_HAWAII=HST10
US_ALASKA=AKST9AKDT,M3.2.0,M11.1.0
CANADA_PACIFIC_TIME=PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00
MEXICO_PACIFIC_TIME=PST8PDT,M4.1.0/2:00:00,M10.5.0/2:00:00
US_PACIFIC_TIME=PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US_ARIZONA=MST7
CANADA_MOUNTAIN_TIME=MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
MEXICO_MOUNTAIN_TIME=MST7MDT,M4.1.0/2:00:00,M10.5.0/2:00:00
US_MOUNTAIN_TIME=MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
CANADA_CENTRAL_TIME=CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00
US_CENTRAL_TIME=CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00
US_INDIANA=EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00
CANADA_EASTERN_TIME=EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US_EASTERN_TIME=EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00
CANADA_ALTANTIC_TIME=AST4ADT,M3.2.0/2:00:00,M11.1.0/2:00:00
CANADA_NEWFOUNDLAND=NST3:30NDT,M3.2.0/2:00:00,M11.1.0/2:00:00
VENEZUELA_TIME=VET4:30
CHILE_TIME=CLT3CLST,M10.2.0,M3.2.0
ARGENTINA_TIME=ART3
GREENWICH_MEAN_TIME=GMT0BST,M3.5.0/1:00:00,M10.5.0/2:00:00
CENTRAL_EUROPEAN_TIME=CET-1CEST,M3.5.0/2:00:00,M10.5.0/3:00:00
EASTERN_EUROPEAN_TIME=EET-2EEST,M3.5.0/3:00:00,M10.5.0/4:00:00
EAST_AFRICAN_TIME=EAT-3
IRAN_TIME=IRST-3:30IRDT,M3.3.3,M9.3.5
AZERBAIJAN_TIME=AZT-4AZST,M3.5.0,M10.5.0
AFGHANISTAN_TIME=AFT-4:30
PAKISTAN_TIME=PKT-5
INDIA_TIME=IST-5:30
EASTERN_KAZAKHSTAN_TIME=ALMT-6
MYANMAR_TIME=MMT-6:30
THAILAND_TIME=ICT-7
CHINA_TIME=CST-8
JAPAN_TIME=JST-9
AUSTRALIAN_CENTRAL_STANDARD_TIME=CST-9:30CDT,M10.1.0,M4.1.0
AUSTRALIAN_EASTERN_STANDARD_TIME=EST-10EDT,M10.1.0,M4.1.0
NEWZEALAND_TIME=NZST-12NZDT,M9.5.0,M4.1.0
```

5.2.2.2.4 Language Mapping

Language mapping is not provided by CyberData.

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 BroadWorks interface to an individual CyberData device.

Browse to the BroadWorks *<group>* → *Resources* → *Identity/Device Profiles* page and then click **Add** to add a new CyberData SIP-enabled IP Series device profile. Configure the device profile as shown in the example in *Figure 8*.

The *Use Custom Credentials* option must be selected. Set the *Device Access User Name* and *Password* to the username and password the device will use for file download.

Figure 8 Device Profile Instance

5.2.4 Configure BroadWorks User

Configure the user with the desired BroadWorks configuration and services. Any services that require a specific configuration on the device are managed via Device Management and are defined in the device configuration files providing the template files are created with the correct Device Management tags.

The device profile created in the previous section must be assigned to the 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 BroadWorks *<user>* → *Addresses*.

5.2.5 Customize Tags

This section identifies custom tags used by the CyberData that may need to be customized at the group or device profile. Customizing a tag at the group level overrides the setting on the device profile type for the device profiles created within the group. Customizing a tag at the device profile level overrides the setting at the device profile type and/or group level for the individual device profile.

5.2.5.1 SBC Address Customization for Edge Device

In many deployments, an edge device, such as an enterprise SBC or application layer gateway, is deployed on the enterprise edge. The edge device's SIP server or outbound proxy setting is configured with the service provider's SBC IP address or FQDN. If there is no edge device, the customization below does not apply.

To integrate the edge device 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 edge device. To do so, perform the following steps:

1) At the *Group* → *Utilities* → *Configure Device* page, select the CyberData device profile (for example, CD-Strobe-prof1).
2) Click on the *Custom Tags* tab.
3) Click **Add**.
4) For the tag, enter "SBC_ADDRESS".
5) For the value, enter the edge device LAN IP address.
6) To save the tag data, click **OK**.

Repeat these steps for each CyberData model provisioned in the group.

5.2.6 Configure CyberData SIP-enabled IP Series

This section describes the steps necessary to configure the CyberData SIP-enabled IP Series to integrate with BroadWorks Device Management.

This configuration can be done as described in the following sections:

- *5.2.6.1 Manual Provisioning*
- *5.2.6.2 No Touch Provisioning via BroadWorks Device Management*
- *5.2.6.3 No Touch Provisioning via Cyberdata Device Management Redirect*

5.2.6.1 Manual Provisioning

The phone must be configured with the Device Management URL and authentication user name and password. The steps necessary to configure the CyberData SIP-enabled IP Series to integrate with BroadWorks Device Management are as below:

1) Click **Launch Browser** from the CyberData Discovery Utility or point the browser to the CyberData device's IP address to access the Home page of the web interface.
2) Enter the default credentials when prompted and then click the **Log In** button:
   - Username: admin
   - Password: admin
3) Browse to the *Autoprovisioning* page as shown in Figure 9 Autoprovisioning.

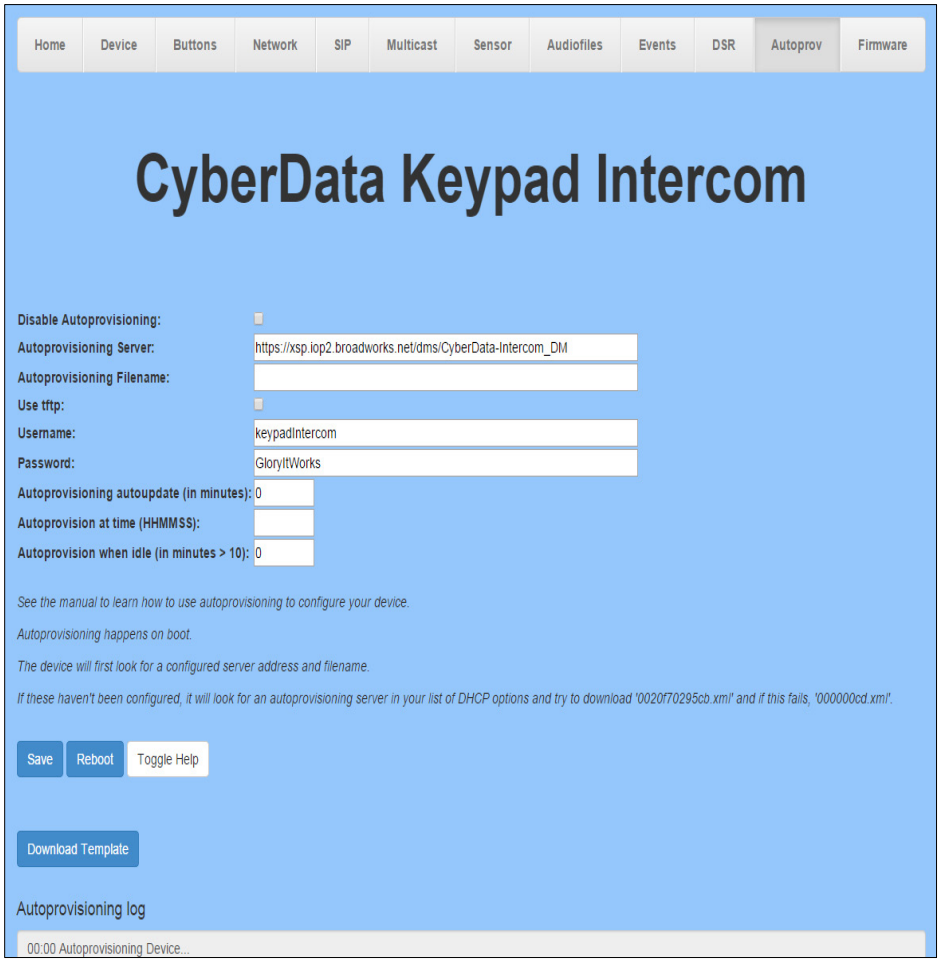

Figure 9 Autoprovisioning

4) Enter the Xtended Services Platform address into the *Autoprovisioning Server* field.
5) Enter the BroadWorks Custom Credentials for the Device Profile Instance into the *Username* and *Password* fields.
6) Click **Save** and then **Reboot** to store changes.

NOTE: There is an Autoprovisioning log at the bottom of the *Autoprovisioning* page that is updated with provisioning progress and results after the device has rebooted and initialized.

5.2.6.2 No Touch Provisioning via BroadWorks Device Management

Currently this feature is not supported by CyberData SIP-enabled IP devices.

5.2.6.3 No Touch Provisioning via Cyberdata Device Management Redirect

Currently this feature is not supported by CyberData SIP-enabled IP devices.

5.3 Upgrade from Previous CPE Kits

The previous configuration sections are primarily structured around importing or manually configuring the CyberData 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* [8].

Appendix A: Reference CyberData SIP-enabled IP Series Configuration Files

The following is a reference configuration for the Intercom configured for use with BroadWorks.

System Default File: 000000cd.xml

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

```
<?xml version="1.0" encoding="utf-8" ?>

<specific>

    <IPSettings>
        <IPAddressMode>DHCP</IPAddressMode>
    </IPSettings>

    <SIPSettings>
        <SIPServer>%BWHOST-1%</SIPServer>
        <OutboundProxy>%SBC_ADDRESS%</OutboundProxy>
        <OutboundProxyPort>%SBC_PORT%</OutboundProxyPort>
        <SIPRegistrationTimeout>%SIP_EXPIRY%</SIPRegistrationTimeout>
        <KeepAlive>%KEEP_ALIVE%</KeepAlive>
        <DisableRportDiscovery>%DISABLE_RFC3581%</DisableRportDiscovery>
    </SIPSettings>

    <NightringerSettings>
        <EnableNightringer>%BWLINE-ENABLED-2%</EnableNightringer>
           <NightringerSIPServer>%BWHOST-2%</NightringerSIPServer>
        <NightringerOutboundProxy>%SBC_ADDRESS%</NightringerOutboundProxy>

<NightringerOutboundProxyPort>%SBC_PORT%</NightringerOutboundProxyPort>

<NightringerRegistrationTimeout>%SIP_EXPIRY%</NightringerRegistrationTimeo
ut>
    </NightringerSettings>

    <ClockSettings>
        <NTPServer>%SNTP_SERVER%</NTPServer>
        <NTPTimezone>%BWTIMEZONE-1%</NTPTimezone>
           <NTPOnBoot>Yes</NTPOnBoot>
    </ClockSettings>

    <FirmwareSettings>
        <FirmwareFile>%FIRMWARE_VERSION%-uImage-%MODEL%</FirmwareFile>
    </FirmwareSettings>

</specific>
```

Device-specific File: <MACaddress>.xml

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

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
    <!--
    Autoprovisioned values will be written on boot.

    To use autoprovisioning, create a copy of this file with the desired
    settings and name this file with the mac address of the device to
    configure (for example: 0020f7350058.xml).  Put this file into
    your hosted directory and manually set the hosting server address.

    Alternately you can set your dhcp server to provide the
autoprovisioning
    server address in OPTION 43, 72, 150, or 66.

    On boot the device will download its autoprovisioning file and
configure
    itself with those settings.

    Though every setting that can be changed via autoprovisioning is shown
    below, it isn't necessary to set every value.

    See the documentation for other ways you can organize your
autoprovisioning
    files.
    -->

    <MiscSettings>
        <DeviceName>%BWNAME-1%</DeviceName>
           <AutoprovFile>000000cd.xml</AutoprovFile>
<!--    <AutoprovFile>common.xml</AutoprovFile>-->
<!--    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>-->
<!--    <AutoprovFile>audio[macaddress]</AutoprovFile>-->
<!--    <AutoprovFile>device[macaddress].xml</AutoprovFile>-->
    </MiscSettings>

    <AutoprovSettings>
        <DisableAutoprov>No</DisableAutoprov>
        <AutoprovServer></AutoprovServer>
        <AutoprovFilename></AutoprovFilename>
        <AutoprovUsername></AutoprovUsername>
        <AutoprovPassword></AutoprovPassword>
        <UseTFTP>No</UseTFTP>
        <AutoprovAutoupdate>0</AutoprovAutoupdate>
        <AutoprovAtTime></AutoprovAtTime>
        <AutoprovWhenIdle>0</AutoprovWhenIdle>
    </AutoprovSettings>

    <DeviceSettings>
        <SpeakerVolume>4</SpeakerVolume>    <!-- This is the volume for
SIP calls -->
        <MulticastVolume>4</MulticastVolume>
        <RingVolume>4</RingVolume>
        <SensorVolume>4</SensorVolume>
        <MicGain>4</MicGain>
        <BoostLevel>0</BoostLevel>
```

```
        <ActivateRelayWithDTMF>Yes</ActivateRelayWithDTMF>
        <DTMFActivationCode>321</DTMFActivationCode>
        <DTMFActivationDuration>2</DTMFActivationDuration>

        <ActivateRelayDuringRing>No</ActivateRelayDuringRing>
        <ActivateRelayDuringNightRing>No</ActivateRelayDuringNightRing>
        <ActivateRelayDuringCall>No</ActivateRelayDuringCall>


<ActivateRelayDuringButtonPress>No</ActivateRelayDuringButtonPress>
        <RelayOnButtonPressTimeout>3</RelayOnButtonPressTimeout>

        <AutoAnswerIncomingCalls>Yes</AutoAnswerIncomingCalls>
        <ButtonLitWhenIdle>Yes</ButtonLitWhenIdle>
        <KeypadLitWhenIdle>Yes</KeypadLitWhenIdle>
        <PlayRingbackTone>No</PlayRingbackTone>
        <PWMBrightness>255</PWMBrightness>
        <DisableHTTPS>No</DisableHTTPS>
    </DeviceSettings>


    <RemoteRelaySettings>
        <AssociatedDSR></AssociatedDSR>
        <ActivateDSRWithDTMF>No</ActivateDSRWithDTMF>
        <DSRActivationCode>321</DSRActivationCode>
        <DSRActivationDuration>2</DSRActivationDuration>
        <DSRToneOnRelay>No</DSRToneOnRelay>
        <ActivateDSRDuringRing>No</ActivateDSRDuringRing>
        <ActivateDSRDuringNightRing>No</ActivateDSRDuringNightRing>
        <ActivateDSRDuringCall>No</ActivateDSRDuringCall>
        <ActivateDSRDuringButtonPress>No</ActivateDSRDuringButtonPress>
        <DSROnButtonPressTimeout>3</DSROnButtonPressTimeout>
        <DSRListenPort>49999</DSRListenPort>
        <DSRDoorOpenTimeout>0</DSRDoorOpenTimeout>
        <DSRDoorOpenFlashLED>No</DSRDoorOpenFlashLED>
        <DSRDoorOpenPlayLocal>No</DSRDoorOpenPlayLocal>
        <DSRDoorOpenCall>No</DSRDoorOpenCall>
        <DSRDoorOpenPlayRemotely>No</DSRDoorOpenPlayRemotely>
        <DSRDoorOpenActivateLocalRelay>No</DSRDoorOpenActivateLocalRelay>
        <DSROpenDialOutExtension>204</DSROpenDialOutExtension>
        <DSROpenDialOutID>id204</DSROpenDialOutID>
    </RemoteRelaySettings>

    <IPSettings>
        <IPAddressMode>DHCP</IPAddressMode>
<!--        <IPAddressMode>Static</IPAddressMode>   -->
        <IPAddress>10.10.10.10</IPAddress>
        <SubnetMask>255.0.0.0</SubnetMask>
        <Gateway>10.0.0.1</Gateway>
        <DNS1>10.0.0.1</DNS1>
        <DNS2>10.0.0.1</DNS2>
        <Hostname>ChangeFromDefault</Hostname>
        <DHCPTimeout>60</DHCPTimeout>
        <VLANID>0</VLANID>
        <VLANPriority>0</VLANPriority>
    </IPSettings>


    <SIPSettings>
        <EnableSIPOperation>Yes</EnableSIPOperation>
        <SIPServer></SIPServer>
        <SIPUserID>%BWLINEPORT-1%</SIPUserID>
        <SIPAuthID>%BWAUTHUSER-1%</SIPAuthID>
```

```
        <SIPAuthPassword>%BWAUTHPASSWORD-1%</SIPAuthPassword>

        <BackupSIPServer1></BackupSIPServer1>
        <SIPUserID2></SIPUserID2>
        <SIPAuthID2></SIPAuthID2>
        <SIPAuthPassword2></SIPAuthPassword2>

        <BackupSIPServer2></BackupSIPServer2>
        <SIPUserID3></SIPUserID3>
        <SIPAuthID3></SIPAuthID3>
        <SIPAuthPassword3></SIPAuthPassword3>

        <UseCiscoSRST>No</UseCiscoSRST>
        <RemoteSIPPort>5060</RemoteSIPPort>
        <LocalSIPPort>5060</LocalSIPPort>
        <OutboundProxy></OutboundProxy>
        <OutboundProxyPort></OutboundProxyPort>

        <SIPRegisterOnBoot>Yes</SIPRegisterOnBoot>
        <SIPRegistrationTimeout></SIPRegistrationTimeout>
        <KeepAlive></KeepAlive>

        <CallTimeout>0</CallTimeout>

        <DisableRportDiscovery></DisableRportDiscovery>
        <RTPPort>10500</RTPPort>

        <DialoutExtension0>%DIALOUT_EXTENSION-0%</DialoutExtension0>
        <DialoutID0>%BWNAME-1%</DialoutID0>

        <DialoutExtension1>%DIALOUT_EXTENSION-1%</DialoutExtension1>
        <DialoutID1>%BWNAME-1%</DialoutID1>
        <DialoutExtension2>242</DialoutExtension2>
        <DialoutID2>id242</DialoutID2>
        <DialoutExtension3>243</DialoutExtension3>
        <DialoutID3>id243</DialoutID3>
        <DialoutExtension4>244</DialoutExtension4>
        <DialoutID4>id244</DialoutID4>
        <DialoutExtension5>245</DialoutExtension5>
        <DialoutID5>id245</DialoutID5>
        <DialoutExtension6>246</DialoutExtension6>
        <DialoutID6>id246</DialoutID6>
        <DialoutExtension7>247</DialoutExtension7>
        <DialoutID7>id247</DialoutID7>
        <DialoutExtension8>248</DialoutExtension8>
        <DialoutID8>id248</DialoutID8>
        <DialoutExtension9>249</DialoutExtension9>
        <DialoutID9>id249</DialoutID9>
        <DialoutExtension10>2410</DialoutExtension10>
        <DialoutID10>id2410</DialoutID10>
        <DialoutExtension11>2411</DialoutExtension11>
        <DialoutID11>id2411</DialoutID11>
        <DialoutExtension12>2412</DialoutExtension12>
        <DialoutID12>id2412</DialoutID12>
    </SIPSettings>

    <ButtonSettings>
        <PlayButtonTone>Yes</PlayButtonTone>

        <DialMode>%DIALMODE%</DialMode>
        <!--        <DialMode>Speed_Dial</DialMode>-->
        <!--        <DialMode>Security</DialMode>-->
        <!--        <DialMode>Cellphone</DialMode>-->
```



```
        <DialOutTimeout>2</DialOutTimeout>
        <SecurityRelayTimeout>6</SecurityRelayTimeout>
        <PlayToneWhileRelayActive>No</PlayToneWhileRelayActive>
        <Allow_Telephone_Dialout>Yes</Allow_Telephone_Dialout>
        <SecurityCode0>1234560</SecurityCode0>
        <ActivateDSR0AfterCode>No</ActivateDSR0AfterCode>
        <SecurityCode1>1234561</SecurityCode1>
        <ActivateDSR1AfterCode>No</ActivateDSR1AfterCode>
        <SecurityCode2>1234562</SecurityCode2>
        <ActivateDSR2AfterCode>No</ActivateDSR2AfterCode>
        <SecurityCode3>1234563</SecurityCode3>
        <ActivateDSR3AfterCode>No</ActivateDSR3AfterCode>
        <SecurityCode4>1234564</SecurityCode4>
        <ActivateDSR4AfterCode>No</ActivateDSR4AfterCode>
        <SecurityCode5>1234565</SecurityCode5>
        <ActivateDSR5AfterCode>No</ActivateDSR5AfterCode>
        <SecurityCode6>1234566</SecurityCode6>
        <ActivateDSR6AfterCode>No</ActivateDSR6AfterCode>
        <SecurityCode7>1234567</SecurityCode7>
        <ActivateDSR7AfterCode>No</ActivateDSR7AfterCode>
        <SecurityCode8>1234568</SecurityCode8>
        <ActivateDSR8AfterCode>No</ActivateDSR8AfterCode>
        <SecurityCode9>1234569</SecurityCode9>
        <ActivateDSR9AfterCode>No</ActivateDSR9AfterCode>
    </ButtonSettings>

    <MulticastSettings>
        <EnableMulticastOperation>No</EnableMulticastOperation>

        <MGROUPAddress9>239.168.3.10</MGROUPAddress9>
        <MGROUPPort9>11000</MGROUPPort9>
        <MGROUPName9>Emergency</MGROUPName9>
        <MGROUPBeep9>No</MGROUPBeep9>

        <MGROUPAddress8>239.168.3.9</MGROUPAddress8>
        <MGROUPPort8>10000</MGROUPPort8>
        <MGROUPName8>MG8</MGROUPName8>
        <MGROUPBeep8>No</MGROUPBeep8>

        <MGROUPAddress7>239.168.3.8</MGROUPAddress7>
        <MGROUPPort7>9000</MGROUPPort7>
        <MGROUPName7>MG7</MGROUPName7>
        <MGROUPBeep7>No</MGROUPBeep7>

        <MGROUPAddress6>239.168.3.7</MGROUPAddress6>
        <MGROUPPort6>8000</MGROUPPort6>
        <MGROUPName6>MG6</MGROUPName6>
        <MGROUPBeep6>No</MGROUPBeep6>

        <MGROUPAddress5>239.168.3.6</MGROUPAddress5>
        <MGROUPPort5>7000</MGROUPPort5>
        <MGROUPName5>MG5</MGROUPName5>
        <MGROUPBeep5>No</MGROUPBeep5>

        <MGROUPAddress4>239.168.3.5</MGROUPAddress4>
        <MGROUPPort4>6000</MGROUPPort4>
        <MGROUPName4>MG4</MGROUPName4>
        <MGROUPBeep4>No</MGROUPBeep4>

        <MGROUPAddress3>239.168.3.4</MGROUPAddress3>
        <MGROUPPort3>5000</MGROUPPort3>
        <MGROUPName3>MG3</MGROUPName3>
```

```
        <MGROUPBeep3>No</MGROUPBeep3>

        <MGROUPAddress2>239.168.3.3</MGROUPAddress2>
        <MGROUPPort2>4000</MGROUPPort2>
        <MGROUPName2>MG2</MGROUPName2>
        <MGROUPBeep2>No</MGROUPBeep2>

        <MGROUPAddress1>239.168.3.2</MGROUPAddress1>
        <MGROUPPort1>3000</MGROUPPort1>
        <MGROUPName1>MG1</MGROUPName1>
        <MGROUPBeep1>No</MGROUPBeep1>

        <MGROUPAddress0>239.168.3.1</MGROUPAddress0>
        <MGROUPPort0>2000</MGROUPPort0>
        <MGROUPName0>Background Music</MGROUPName0>
        <MGROUPBeep0>No</MGROUPBeep0>
    </MulticastSettings>

    <NightringerSettings>
        <EnableNightringer></EnableNightringer>
        <NightringerSIPServer></NightringerSIPServer>
        <NightringerRemotePort>5060</NightringerRemotePort>
        <NightringerLocalPort>5061</NightringerLocalPort>
        <NightringerOutboundProxy></NightringerOutboundProxy>
        <NightringerOutboundProxyPort></NightringerOutboundProxyPort>
        <NightringerUserID>%BWLINEPORT-2%</NightringerUserID>
        <NightringerAuthID>%BWAUTHUSER-2%</NightringerAuthID>
        <NightringerAuthPassword>%BWAUTHPASSWORD-
2%</NightringerAuthPassword>

        <NightringerRegistrationTimeout></NightringerRegistrationTimeout>
    </NightringerSettings>

    <!--
    <AudioSettings>
        <AudioServer>10.0.1.3</AudioServer>
        <Zero>default</Zero>
        <One>default</One>
        <Two>default</Two>
        <Three>default</Three>
        <Four>default</Four>
        <Five>default</Five>
        <Six>default</Six>
        <Seven>default</Seven>
        <Eight>default</Eight>
        <Nine>default</Nine>
        <Dot>default</Dot>
        <Audiotest>default</Audiotest>
        <Pagetone>default</Pagetone>
        <YourIPAddressIs>default</YourIPAddressIs>
        <RestoringDefault>default</RestoringDefault>
        <Rebooting>default</Rebooting>
        <RingbackTone>default</RingbackTone>
        <RingTone>default</RingTone>
        <NightRing>default</NightRing>
        <IntrusionSensorTriggered>default</IntrusionSensorTriggered>
        <DoorSensorTriggered>default</DoorSensorTriggered>
    </AudioSettings>
    -->

    <ClockSettings>
        <NTPServer></NTPServer>
        <NTPTimezone></NTPTimezone>
```

```
        <NTPOnBoot></NTPOnBoot>
        <NTPAutoupdate>No</NTPAutoupdate>
        <NTPAutoupdateDelay>24</NTPAutoupdateDelay>
    </ClockSettings>

    <SensorSettings>
        <SensorNormallyClosed>No</SensorNormallyClosed>
        <SensorTimeout>0</SensorTimeout>
        <SensorFlashLED>No</SensorFlashLED>
        <SensorActivateRelay>No</SensorActivateRelay>
        <SensorPlayLocally>No</SensorPlayLocally>
        <SensorCall>No</SensorCall>
        <SensorPlayRemotely>No</SensorPlayRemotely>
        <SensorDialOutExtension>204</SensorDialOutExtension>
        <SensorDialOutID>id204</SensorDialOutID>
        <SensorRepeat>0</SensorRepeat>

        <IntrusionFlashLED>No</IntrusionFlashLED>
        <IntrusionActivateRelay>No</IntrusionActivateRelay>
        <IntrusionPlayLocally>No</IntrusionPlayLocally>
        <IntrusionCall>No</IntrusionCall>
        <IntrusionPlayRemotely>No</IntrusionPlayRemotely>
        <IntrusionDialOutExtension>204</IntrusionDialOutExtension>
        <IntrusionDialOutID>id204</IntrusionDialOutID>
        <IntrusionRepeat>0</IntrusionRepeat>
    </SensorSettings>


    <EventSettings>
        <EnableEventGeneration>No</EnableEventGeneration>
        <EventServerIP>10.0.0.250</EventServerIP>
        <EventServerPort>8080</EventServerPort>
        <EventServerURL>xmlparse_engine</EventServerURL>

        <EnableButtonEvents>No</EnableButtonEvents>
        <EnableCallActiveEvents>No</EnableCallActiveEvents>
        <EnableCallTerminatedEvents>No</EnableCallTerminatedEvents>
        <EnableRelayActivatedEvents>No</EnableRelayActivatedEvents>
        <EnableRelayDeactivatedEvents>No</EnableRelayDeactivatedEvents>
        <EnableRingEvents>No</EnableRingEvents>
        <EnableNightRingEvents>No</EnableNightRingEvents>
        <EnableMulticastStartEvents>No</EnableMulticastStartEvents>
        <EnableMulticastStopEvents>No</EnableMulticastStopEvents>
        <EnablePowerOnEvents>No</EnablePowerOnEvents>
        <EnableSensorEvents>No</EnableSensorEvents>
        <EnableSecurityEvents>No</EnableSecurityEvents>
        <EnableHeartbeatEvents>No</EnableHeartbeatEvents>
    </EventSettings>

    <FirmwareSettings>
        <FirmwareFile></FirmwareFile>
    </FirmwareSettings>

</specific>
```

References

[1] CyberData Corporation. 2017. *Operations Guide.* Available from CyberData at http://www.cyberdata.net/products/voip/index.html.

[2] BroadSoft, Inc. 2017. *BroadWorks Device Management Configuration Guide*, *Release 22.0*. Available from BroadSoft at xchange.broadsoft.com.

[3] BroadSoft, Inc. 2016. *BroadWorks Redundancy Guide, Release 22.0*. Available from BroadSoft at xchange.broadsoft.com.

[4] BroadSoft, Inc. 2016. *BroadWorks SIP Access Interface Interworking Guide, Release 22.0.* Available from BroadSoft at xchange.broadsoft.com.

[5] BroadSoft, Inc. 2017. *BroadWorks SIP Phone Interoperability Test Plan, Release 22.0*. Available from BroadSoft at xchange.broadsoft.com.

[6] BroadSoft, Inc. 2017. *BroadWorks SIP Phone Functional Test Plan, Release 22.0*. Available from BroadSoft at xchange.broadsoft.com.

[7] BroadSoft, Inc. 2017. *BroadWorks Device Management Interoperability Test Plan*, *Release 22.0*. Available from BroadSoft at xchange.broadsoft.com.

[8] BroadSoft, Inc. 2016. *BroadWorks CPE Kit Usage Guide*, *Release 22.0*. Available from BroadSoft at xchange.broadsoft.com

