BroadSoft Partner Configuration Guide

Spectralink IP-DECT Server Series

February 2015

Document Version 1.4

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

WWW.BROADSOFT.COM

BroadWorks® Guide

Copyright Notice

Trademarks

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

This document is printed in the United States of America.

Document Revision History

Version	Reason for Change
1.1	Introduced document for Spectralink IP-DECT Server Series version PCS14A_ validation with BroadWorks Release 20.sp1.
1.2	Edited changes and published document.
1.3	Expanded document with the support of Device Management.
1.4	Edited changes and published document.

Table of Contents

Table of Figures

1 Overview

This guide describes the configuration procedures required for the Spectralink IP-DECT Server Series for interoperability with BroadWorks. This includes the following Spectralink IP DECT Server Series models:

- IP DECT Server 400
- IP DECT Server 6500

The IP-DECT Server Series is an access device that 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 IP-DECT Server Series. For those details, see the *Spectralink IP DECT Server 400 Installation and Configuration Guide* [1] or the *Spectralink IP DECT Server 6500 Installation and Configuration Guide* [2] supplied by Spectralink.

2 Interoperability Status

This section provides the known interoperability status of the Spectralink IP-DECT Server 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 Spectralink.

2.1 Verified Versions

The following table identifies the verified Spectralink IP-DECT Server 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 IP-DECT Server Series versions, which the partner has identified as compatible and they 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 Spectralink.

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 Access Device Interoperability Test Plan* [7].

Verified Versions

Date	BroadWorks Release	IP-DECT Server Series Verified Version	IP-DECT Server Series Compatible Versions
08/2014	Release 20.sp1	PCS14A_	Any maintenance release of PCS14A_.

2.2 Interface Capabilities Supported

This section identifies interface capabilities that have been verified through testing as supported by Spectralink IP-DECT Server Series.

The *Supported* column in the tables in this section identifies the Spectralink IP-DECT Server Series's 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 Spectralink IP-DECT Server Series has completed interoperability testing with BroadWorks using the *BroadWorks SIP Access Device 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, 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 Spectralink IP-DECT Server Series.

BroadWorks SIP Access Device Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
Basic	Call Origination	Yes	
	Call Termination	Yes	
	Session Audit	Yes	
	Session Timer	No	
	Ringback	Yes	
	Forked Dialog	Yes	
	Early UPDATE	No	
	Early-Session	No	
	181 Call Being Forwarded	Yes	
	Dial Plan	Yes	
	DTMF – Inband	No	
	DTMF – RFC 2833	Yes	
	DTMF – DTMF Relay	Yes	
	Codec Negotiation	Yes	
	Codec Renegotiation	Yes	
BroadWorks Services	Third-Party Call Control – Basic	Yes	
	Voice Message Deposit and Retrieval	Yes	
	Message Waiting Indicator	Yes	DUT does not support Message Waiting Saved and Urgent Information.
	Voice Portal Outcall	Yes	
	Advanced Alerting – Ringing	No	

BroadWorks SIP Access Device Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
	Advanced Alerting – Call Waiting	No	
	Advanced Alerting – Ring Splash	No	
	Calling Line ID	Yes	
	Calling Line ID with Unicode Characters	Yes	
	Connected Line ID	Yes	DUT does not support Connected Line Restriction after Call Forward.
	Connected Line ID with Unicode Characters	Yes	
	Connected Line ID on UPDATE	Yes	
	Connected Line ID on Re-INVITE	Yes	
	Diversion Header	Yes	
	History-Info Header	Yes	
	Advice of Charge	No	
	Meet-Me Conferencing	Yes	
	Meet-Me Conferencing – G722	No	
	Meet-Me Conferencing – AMR-WB	No	
DUT Services – Call Control Services	Call Waiting	Yes	
	Call Hold	Yes	
	Call Transfer	Yes	
	Three-Way Calling	No	
	Network-Based Conference	No	
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	No	
DUT Services – Fax	G711 Fax Passthrough	No	
	G711 Fax Fallback	No	
	T38 Fax Messaging	No	
DUT Services – Emergency Call	Emergency Call	No	
	Emergency Call with Ringback	No	
DUT Services –	Do Not Disturb	No	

BroadWorks SIP Access Device Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
Miscellaneous	Call Forwarding Always	Yes	
	Call Forwarding Always Diversion Inhibitor	No	
	Anonymous Call	No	
	Anonymous Call Block	No	
	Remote Restart Via Notify	Yes	
Redundancy	DNS SRV Lookup	Yes	
	Register Failover/Failback	Yes	
	Invite Failover/Failback	Yes	
	Bye Failover	Yes	
Session Border Controller (SBC)/Application Layer Gateway (ALG)	Register	Yes	
	Outgoing Invite	Yes	
	Incoming Invite	Yes	
TCP	Register	Yes	
	Outgoing Invite	Yes	
	Incoming Invite	Yes	
IPV6	Call Origination	Yes	
	Call Termination	Yes	
	Session Audit	Yes	
	Ringback	Yes	
	Codec Negotiation/Renegotiation	Yes	
	Voice Message Deposit/Retrieval	Yes	
	Call Control	Yes	DUT does not support 3-way and network based 3-way call.
	Registration with Authentication	Yes	
	T38 Fax Messaging	No	
	Redundancy	Yes	
	SBC	Yes	
	Dual Stack with Alternate Connectivity	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.

If the testing was performed by BroadSoft, then the *Issue Number* is a BroadSoft ExtraView partner issue number. If the testing was performed by the partner or a third party, then the partner may or may not supply a tracking number.

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

Issue Number	Issue Description	Partner Version			
		PCS14A_			
-----	None				

3 BroadWorks Configuration

This section identifies the required BroadWorks device profile type for the Spectralink IP-DECT Server Series as well as any other unique BroadWorks configuration required for interoperability with the Spectralink IP-DECT Server.

3.1 BroadWorks Device Profile Type Configuration

This section identifies the device profile type settings to use when deploying the Spectralink IP-DECT Server with BroadWorks.

Create a device profile type for the Spectralink IP-DECT Server Series as shown in the following example. A separate device profile type should be created for each Spectralink IP-DECT Server Series model. The settings shown are recommended for use when deploying the Spectralink IP-DECT Server 400 with BroadWorks. For an explanation of the profile parameters, see the *BroadWorks Device Management Configuration Guide* [4].

The following device profile type shown provides the *Number of Ports* (number of SIP lines) setting for Spectralink IP-DECT Server Series. For other IP-DECT Server Series 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
IP DECT 400	30
IP DECT 6500	4096

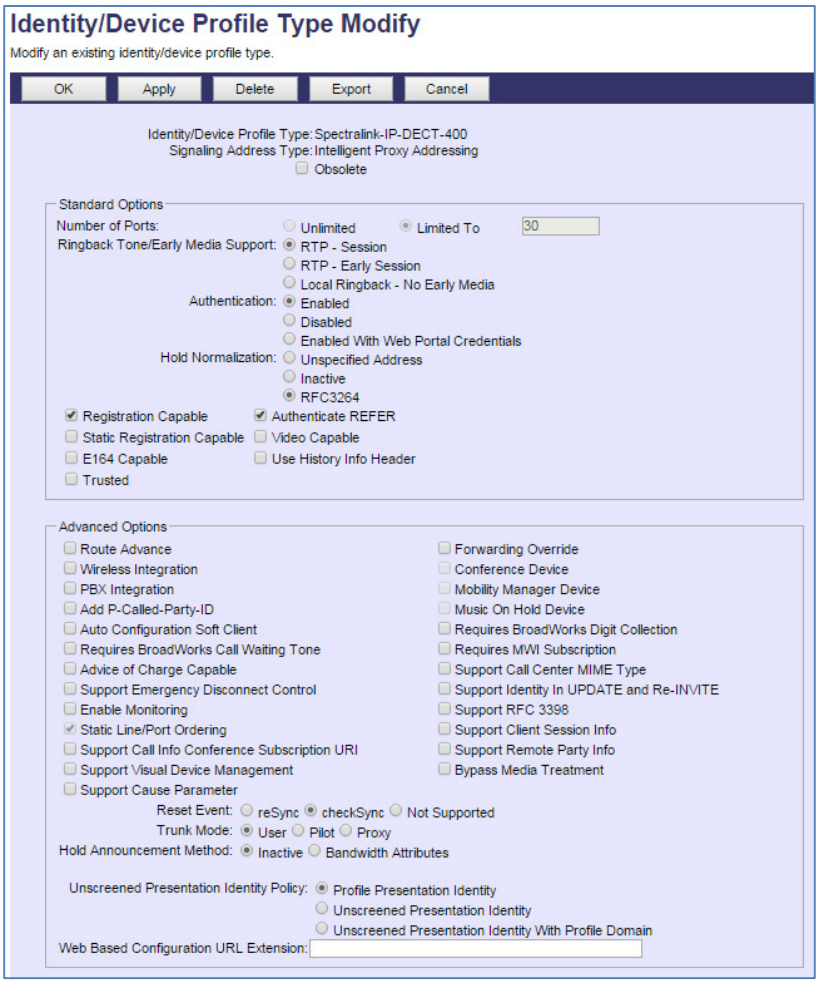

Figure 1 Device Profile Type Configuration

3.2 BroadWorks Configuration Steps

No additional BroadWorks configuration steps are required.

4 IP-DECT Server Configuration

The IP DECT Server Series can be configured with configuration files using the TFTP, FTP, HTTP(S), or through its embedded Web Interface. The following examples describe how to set the parameters using a configuration file. The IP DECT Server Series can use DHCP to obtain an IP address, provisioning server (TFTP, FTP or HTTP(S)), and other network settings. These settings can also, be configured manually through the embedded Web Interface. If provisioning is used the IP DECT Server Series should be configured to load the configuration file each time it resets or re-synchronizes. For detailed information on automated provisioning, see the *Provisioning Guide Spectralink IP-DECT Servers and BroadSoft Device Management* [3] (under each server name in the list).

The capabilities of the IP DECT Server Series have been verified for use with 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 *Spectralink IP DECT Server 400 Installation and Configuration Guide* [1] or the *Spectralink IP DECT Server 6500 Installation and Configuration Guide* [2] supplied by Spectralink.

4.1 Configuration Method

The IP DECT Server Series can be configured either manually using the web browser interface or provisioned using .xml files according to the guides referenced above.

Configuration Files

IP-DECT Server Series Configuration Files	Level	Description
14218500-hermod-firmware-pcs14A_.bin	System	Contains the device firmware load.
14218500-hermod-firmware-pcs14A_.bin.ver	System	Contains the device's firmware version.
<IP DECT Server MAC address>config.xml *Example: 0013d1813a18-config.xml*	System	Contains configurable parameters that apply to an individual device in a deployment.
<IP DECT Server MAC address>users.xml *Example: 0013d1813a18-users.xml*	Subscriber	Contains the list of users (handsets) to configure for an individual device in a deployment.

4.2 System Level Configuration

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

4.2.1 Configure Network Settings

System Configuration File <IP DECT Server MAC address> config.xml	
XML File Tag	**Description**
network.bootproto	Method used to assign an IPv4 address. Choice of either dhcp or static assigned.
network.ipaddr	IPv4 address Not required if DHCP assigned

System Configuration File <IP DECT Server MAC address> config.xml	
XML File Tag	**Description**
network.netmask	IPv4 netmask. Not required if DHCP assigned.
network.gateway	IPv4 gateway. Not required if DHCP assigned.
network.dns1	Primary DNS server IPv4 or IPv6 address. Not required if DHCP assigned.
network.dns2	Secondary DNS server IPv4 or IPv6 address. Not required if DHCP assigned.
network.vlan	Choose your VLAN Settings (optional).

4.2.1.1 Configure IPv6 Settings (Optional)

XML File Tag	Description
network.ipv6.method	Specifies the method used to obtain an IPv6 configuration. Values: ▪ "slaac" Use router advertisements to obtain an IPv6 address. ▪ "dhcp" Use DHCPv6 to obtain an IPv6 address. ▪ "static" Configure IPv6 address and gateway manually. ▪ "disabled" Disable IPv6 support. ▪ Default: "disabled".
network.ipv6.ipaddr	Specify a static IPv6 address including the prefix length. Values: <IPv6 address>/prefix. Example: 3000::2/64. Not required if automatically assigned.
network.ipv6.gateway	Specify a static IPv6 gateway. Values: <IPv6 address>. Example: 3000::1. Not required if automatically assigned.

4.2.2 Configure SIP Interface Settings

XML File	Description
sip.transport	Set the transport protocol to UDP or TCP. Values: udp or tcp. Default: udp.
sip.defaultdomain	Set the IP DECT Server Series SIP server to the Fully Qualified Domain Name (FQDN) of the BroadWorks Application Server cluster. The domain must match the domain configured for the BroadWorks subscriber's line/port domain.

XML File	Description
sip.proxy.domain	Set the Outbound Proxy to the Session Border Controller (SBC) if one is deployed between the IP DECT Server Series and BroadWorks. If there are redundant SBCs, set it to the FQDN for the SBC cluster.
sip.dnsmethod = dnssrv	Set the DNS method used to resolve the SIP server. Values: "arecord": Use DNS A records only. "dnssrv": Use DNS SRV records and A records. Default: arecord. Recommended setting for BroadWorks: dnssrv.

4.2.1 Configure Service Settings

XML File Tag	Description
feature_codes.enable = true	To activate the call forward feature, the setting needs to be enabled. On Handset activated via feature code: *21*[forwarding number]#. Disabled on handset via #21#.

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) is provisioned on BroadWorks and the device.

XML file tag	Description
user.username = 123456	The register user ID must correspond with the line/port setting on BroadWorks.
user.authuser = SpectralinkUser1 *user.authpassword = Spectralink01*	If the Authentication service is configured on BroadWorks, these parameters must be configured to match the BroadWorks settings. Note that the password can be saved as hashed value as well.
user.displayname = User 1	The name to be displayed (caller ID) at other SIP devices, for example, User 1 in User 1<1234566@somecompany.com.
user.standbytext = 123456 User 1	Configure the text to be displayed on the device.

4.4 SIP Feature Configuration

This section provides configuration instructions for advanced SIP features supported by the device such as Advice of Charge, Emergency Call, and Fax.

4.4.1 Emergency Call Configuration

This section provides configuration instructions for configuring the device to enable emergency call headers and ringback after hang up.

Not Supported.

4.4.2 Advice of Charge Configuration

This section provides configuration instructions for configuring the device to enable Advice of Charge.

Not Supported.

4.4.3 Fax Configuration

This section provides configuration instructions for configuring the device to enable fax.

Not Supported.

5 Device Management

The BroadWorks Device Management feature provides the capability to automate generation of device configuration files to support mass deployment of devices up to 1024 lines. This section identifies the Device Management capabilities supported by the Spectralink IP DECT Server and the configuration steps required. For Device Management configuration details not covered here, see the *BroadWorks Device Management Configuration Guide* [4].

The basic steps to integrate a device with Device Management are as follows:

1) Create device template files for the device with the appropriate BroadWorks Device Management tags.
2) Define custom and system tags and add them to the *device template* files. Note that these custom and system tags must also be defined on BroadWorks.
3) Create a device profile type on BroadWorks for each device model to be integrated with Device Management.
4) Add the device template files and other associated files to the device profile type.
5) Create a device profile instance of the device profile type and assign it to a user. A user name and password are assigned to this device profile.
6) Configure the end device with the Device Management URL for device files, as well as the user name and password access credentials.

This section describes the steps to integrate the Spectralink IP DECT Server products.

As part of the Spectralink IP DECT Server customer premises equipment (CPE) kit, BroadSoft has defined a standard device configuration in the device template files that service providers can use on their systems. These files can be uploaded directly to Device Management without modification. However, the service provider also has the option to modify these template files as required to fit their deployment needs.

The CPE kit contains Device Type Archive File (DTAF) files that are used to import the device type and template files.

NOTE: The BroadWorks Device Management is capable of supporting up to 1024 lines. If the deployment of Spectralink IP DECT Server requires more than the supported line, contact Spectralink.

5.1 Device Management Capabilities Supported

The Spectralink IP DECT Server has completed Device Management interoperability testing with BroadWorks using the *BroadWorks Device Management Interoperability Test Plan* [8]. 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 Spectralink IP DECT Server's 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 Spectralink IP DECT Server.

BroadWorks Device Management Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
HTTP File Download	HTTP Download Using Xtended Services Platform (Xsp) IP Address	Yes	
	HTTP Download Using Xtended Services Platform FQDN	Yes	
	HTTP Download Using Xtended Services Platform Cluster FQDN	Yes	
	HTTP Download With Double Slash	Yes	
HTTPS File Download	HTTPS Download Using Xtended Services Platform IP Address	NT	
	HTTPS Download Using Xtended Services Platform FQDN	Yes	
	HTTPS Download Using Xtended Services Platform Cluster FQDN	NT	
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 Xtended Services Platform IP Address	No	
	HTTP Upload Using Xtended Services Platform FQDN	No	
	HTTP Upload Using Xtended Services Platform Cluster FQDN	No	

BroadWorks Device Management Interoperability Test Plan Support Table			
Test Plan Package	**Test Plan Package Items**	**Supported**	**Comments**
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	NA	
	Association via Phone	NA	

5.2 Device Management Configuration

This section identifies the steps required to enable the Spectralink IP DECT Server for Device Management. For Device Management configuration details not covered here, see the *BroadWorks Device Management Configuration Guide* [4].

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 Spectralink device models only.

The Spectralink IP DECT Server makes use of dynamic 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 Spectralink 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.
%DNS_SERVER_1%	IP address	DNS server address.
%DNS_SERVER_2%	IP address	DNS server address alternate.
%SBC_ADDRESS%	IP address/FQDN	SBC SIP address.

Example System Default Tag Settings

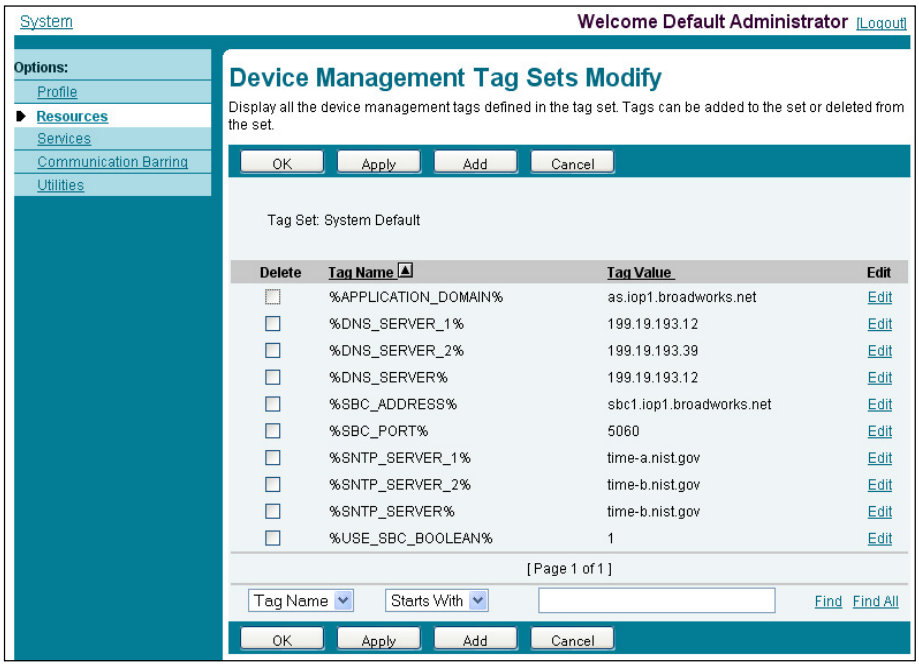

Figure 2 System Default Tag Settings

5.2.1.2 Create Device Type-specific Tags

Browse to *System* → *Resources* → *Device Management Tag Sets* and click **Add** to add a new tag set. Configure the tag set name using the device name appended by *Tags*: *Spectralink-IP-DECT 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 at least the tags marked as required are defined.

Tag Name	Valid Settings	Description
%IP-DECT-DECT-ACCESSCODE%	1-8 digits	Access code is required to subscribe handsets.
%IP-DECT-DECT-SUBSCRIPTIONALLOWED%	true/false	If allowed it is possible to subscribe new handsets to the system.
%IP-DECT-LANGUAGE%	da - Danish de - German en - English es - Spanish fr - French it - Italian nl - Dutch no - Norwegian pt - Portuguese ru - Russian sv - Swedish	Language used for messages sent from IP DECT Server to handsets.
%IP-DECT-LICENSE%	A comma separated list of license codes	License code to activate extra features.
%IP-DECT-LOG-SYSLOG-	0-18	Syslog facility used for log

Tag Name	Valid Settings	Description
FACILITY%		messages.
%IP-DECT-LOG-SYSLOG-HOST%	IPv4/IPv6 address/FQDN	Remote syslog server.
%IP-DECT-LOG-SYSLOG-LEVEL%	debug, info, notice, warning, error, critical, emergency	Minimum syslog level that will be sent to the server.
%IP-DECT-LOG-SYSLOG-PORT%	0-65535	Remote syslog server port.
%IP-DECT-NETWORK-BOOTPROTO%	static/dhcp	IPv4 address assigning method.
%IP-DECT-NETWORK-IPADDR%	IPv4 address	Device IPv4 address.
%IP-DECT-NETWORK-GATEWAY%	IPv4 address	IPv4 default gateway.
%IP-DECT-NETWORK-IPV6-GATEWAY%	IPv6 address	IPv6 gateway.
%IP-DECT-NETWORK-IPV6-IPADDR%	IPv6 address with prefix length	Device IPv6 address with prefix length.
%IP-DECT-NETWORK-IPV6-METHOD%	static/dhcp/slaac/disabled	IPv6 address assigning method.
%IP-DECT-NETWORK-NETMASK%	IPv4 network mask	IPv4 network mask.
%IP-DECT-PHONEBOOK-LDAP-ATTRIBUTES%	A comma separated list of LDAP attribute names.	Attributes to return from LDAP search.
%IP-DECT-PHONEBOOK-LDAP-BASE%	Base for LDAP search	Base for LDAP search.
%IP-DECT-PHONEBOOK-LDAP-BIND-PASSWORD%	Valid LDAP server password.	LDAP server bind password.
%IP-DECT-PHONEBOOK-LDAP-BIND-USER%	Valid LDAP server username.	LDAP server bind user.
%IP-DECT-PHONEBOOK-LDAP-FILTER%	See RFC 4515.	Filter for LDAP search.
%IP-DECT-PHONEBOOK-LDAP-NAMES%	A comma separated list of names to display for each attribute.	Name to display for each attribute.
%IP-DECT-PHONEBOOK-LDAP-NUMBER-ATTRIBUTES%	A comma separated list of dial-able attributes	Attributes containing dial-able numbers.
%IP-DECT-PHONEBOOK-LDAP-PREFIXES%	A comma separated list of prefix transformations	Prefixes to replace or strip before dialing numbers.
%IP-DECT-PHONEBOOK-LDAP-REFRESHINTERVAL%	seconds	Time between LDAP reloads.
%IP-DECT-PHONEBOOK-LDAP-URI%	ldap://IPv4/IPv6 address / FQDN	URI for LDAP server.
%IP-DECT-PHONEBOOK-SOURCE%	ldap/csv/disabled	Phonebook source.

Tag Name	Valid Settings	Description
%IP-DECT-PROVISIONING-CHECK-INTERVAL%	minutes	Provisioning check interval.
%IP-DECT-PROVISIONING-SERVER-PROTOCOL%	http/https	Provisioning server protocol. (Required)
%IP-DECT-PROVISIONING-SERVER-USER%	Device Access User Name	Provisioning authentication username. (Required)
%IP-DECT-PROVISIONING-SERVER-PASSWORD%	Device Access Password	Provisioning authentication password. (Required)
-%IP-DECT-FWVERSION%	A valid IP DECT Server firmware version string. For example pcs14a_.	The version of the IP-DECT Server firmware that will be provisioned. (Required)
%IP-DECT-SECURITY-ALLOW-NEW-MR%	true/false	If enabled new media resources will be allowed to connect to the server.
%IP-DECT-SECURITY-ALLOW-NEW-RFP%	true/false	If enabled new base stations will be allowed to connect to the server.
%IP-DECT-SECURITY-FORCE-HTTPS%	true/false	If enabled remote access will be forced to https.
%IP-DECT-SECURITY-PASSWORD%	Clear text password / md5(<user>:IP6000:<password>)	Remote access password.
%IP-DECT-SIP-MEDIA-TOS%	value in decimal	TOS used for RTP.
%IP-DECT-SIP-MEDIA-VLANCOS%	Value in decimal	Media 802.1p Class-of-Service.
%IP-DECT-SIP-TOS%	Value in decimal	SIP type of service.
%IP-DECT-SIP-VLANCOS%	Value in decimal	SIP 802.1p Class-of-Service.
%IP-DECT-SNMP-COMMUNITY%	Community name	SNMP community name.
%IP-DECT-SNMP-ENABLE%	enabled/disabled	Enable/disable SNMP.
%IP-DECT-SNMP-SYSCONTACT%	text	SNMP contact information.
%IP-DECT-SNMP-SYSLOCATION%	text	SNMP location information.
%IP-DECT-SNMP-TRAPCOMMUNITY%	trap community name	SNMP trap community name.
%IP-DECT-SNMP-TRAPHOST%	IPv4/IPv6 address / FQDN	SNMP trap host.
%IP-DECT-TIMEZONE%	POSIX time zone string	Time zone used when displaying date and time.

Example Device Type-specific Tag Settings

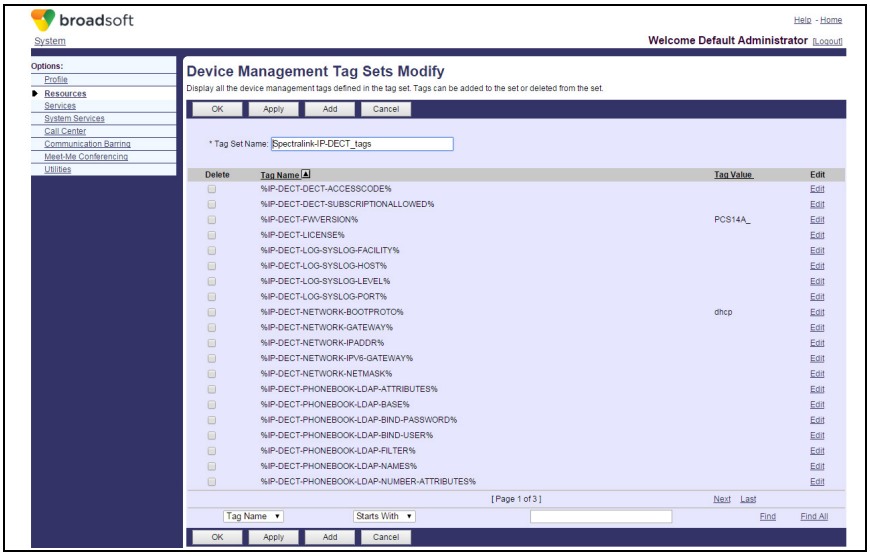

Figure 3 Device Type-specific Tag Settings

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.

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 Spectralink IP DECT Server as a Device Management-enabled device type.

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 Spectralink IP DECT Server CPE kit from BroadSoft Xchange at xchange.broadsoft.com. 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:

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 Spectralink device profile type, Spectralink-IP-DECT.
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.

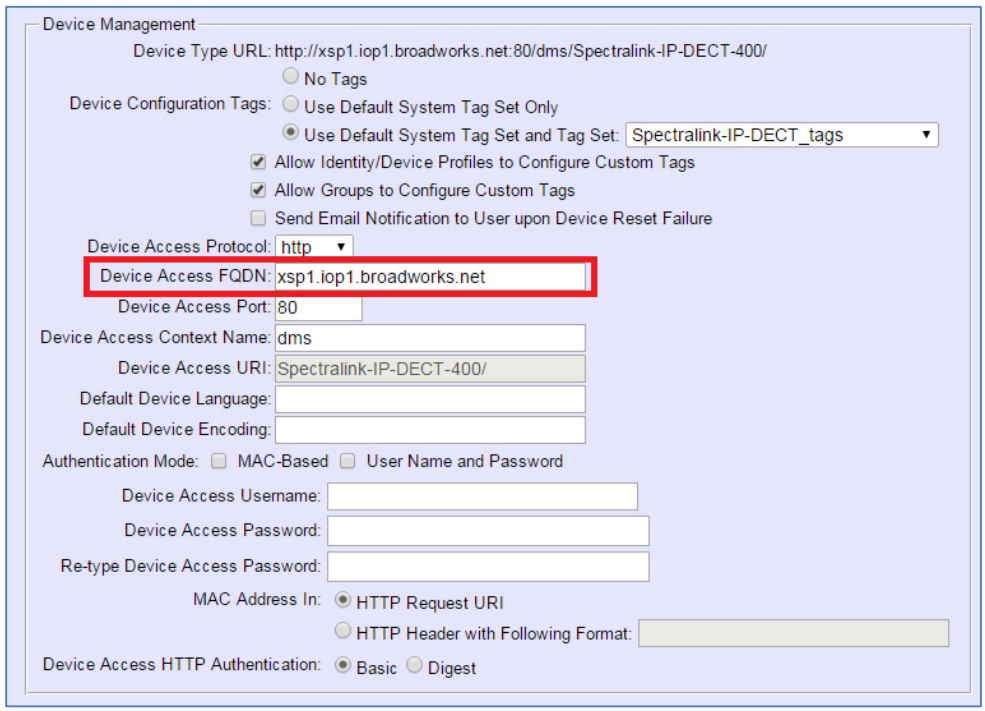

Figure 4 Device Access FQDN

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

   Firmware files must be obtained from Spectralink. These files are not included in the import. Complete the steps in section *5.2.2.2.2.2 Static Files* to define the static firmware files and to upload the firmware.

5.2.2.2 Configuration Method 2: Manual

This section identifies the manual steps necessary to configure BroadWorks to add the Spectralink IP DECT Server as a Device Management-enabled device type.

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. To determine when to use the manual method, see section *5.2.2 Configure BroadWorks Device Profile Type*. 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.

These steps must be completed for the device type for each Spectralink model.

5.2.2.2.1 Modify Device Profile Type

This section identifies the BroadWorks device profile type settings relevant to Device Management for the Spectralink IP DECT Server.

Browse to *System* → *Resources* → *Identity/Device Profile Types* and perform a search to find the Spectralink 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.

The *Standard Options* and *Advanced Options* should already be configured as specified in section *3.1 BroadWorks Device Profile Type Configuration*. If there are differences, perform an update to match the settings in section *3.1 BroadWorks Device Profile Type Configuration*.

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 previously enabled for the device profile type(s), go to the next section.

Device Configuration is enabled differently depending on the deployed BroadWorks release.

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

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

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

Figure 5 Enable Device Management (Release 18.0 and Later)

For BroadWorks releases prior to Release 18.0, configure as shown in the following table.

NOTE: 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. Set it to “not_used”.
Device File Format	not_used	This parameter must not be blank. Set it to “not_used”.

The following screen capture shows Device Management enabled for BroadWorks prior to Release 18.0.

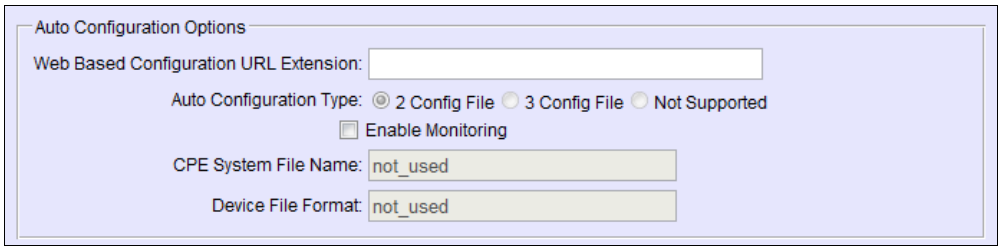

Figure 6 Enable Device Management (pre-Release 18.0)

5.2.2.2.1.2 *Configure Device Management Options*

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

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

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

Parameter	Value	Description
Device Configuration Tags	Use Default System Tag Set and Tag Set. Select the device tag set created 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	

Parameter	Value	Description
Device Access FQDN	<BroadWorks-XSP-Cluster-Address> Example: xsp.iop1.broadworks.net	Set to the Xtended Services Platform cluster FQDN if using an Xtended Services Platform farm. 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. BroadWorks defaults to the system-defined value.
Device Access URI	<model name> Example: Spectralink-IP-Dect-400	This defines the directory the Xtended Services Platform uses to access the configuration files.

Example Device Management Options Settings

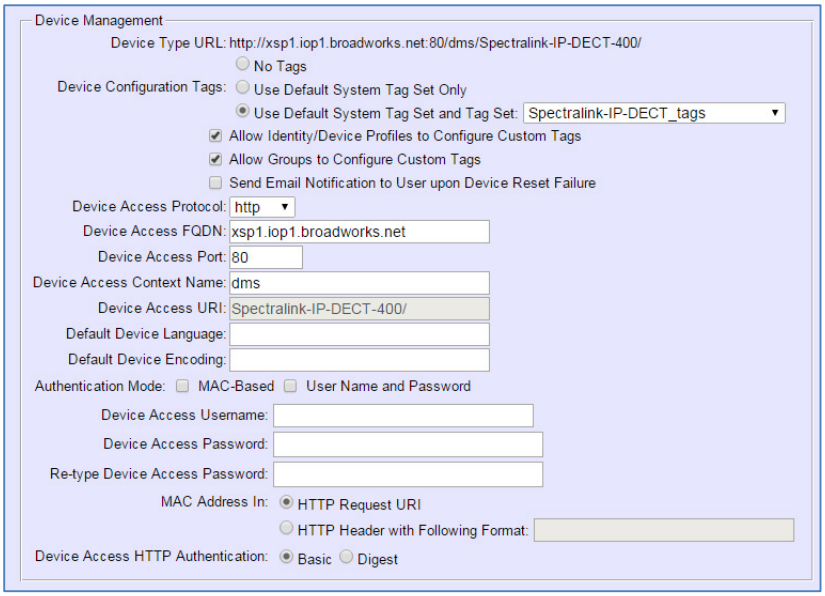

Figure 7 Device Management Options Settings

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 Spectralink IP DECT Server downloads.

Configuration templates, firmware, and other files the IP DECT Server uses must be uploaded to BroadWorks. Download the Spectralink IP DECT Server CPE kit from BroadSoft Xchange at xchange.broadsoft.com. Extract the configuration files from the *Configuration Files* folder of CPE kit. Obtain the firmware files directly from Spectralink.

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

File Name	CPE Kit Template File Name	File Type	Description
Examples			
BWMACADDRESS-config.xml	*BWMACADDRESS-config.xml.template*	Device-specific	This file contains all IP DECT system configurations.
BWMACADDRESS-users.xml	*BWMACADDRESS-users-30.xml.template* *BWMACADDRESS-users-1024.xml.template*	Device-specific	This file contains all IP DECT user configurations. There are two template files included for different system capacity. IP DECT 400: 30 IP DECT 6500: 1024

The following table identifies other files that the Spectralink IP DECT Server downloads from the server or uploads to the server. These files are not provided in the CPE kit and must be obtained from Spectralink.

File Name	File Type	Description
14218500-hermod-firmware-%IP-DECT-FWVERSION%.bin	Static	Firmware file for the IP DECT Server.
14218500-hermod-firmware-%IP-DECT-FWVERSION%.bin.ver	Static	Firmware version file for the IP DECT Server.

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 Device-specific Files

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

Each IP DECT Server downloads two device-specific file based on the MAC address using the following file name format:

<MAC Address>-config.xml

<MAC Address>-users.xml

Add a BroadWorks device profile type file to the Spectralink IP DECT Server device profile for the device-specific file using the settings described in the following table.

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

Parameter	Value	Description
Device Access File Format	<device-specific-file-format> Example: *%BWMACADDRESS%-config.xml* *%BWMACADDRESS%-users.xml*	This is the file name format the device uses to request the file.
Repository File Format	*%BWFQDEVICEID%-config.xml* *%BWFQDEVICEID%-users.xml*	This is the file name format stored on 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	Not set	Caching should not be enabled for device-specific files.
Assign File	Custom	
Authentication Mode	User Name and Password	The device-specific file is authenticated with the 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 BroadSoft Xchange. Use the **Browse** button on the file definition screen. Be sure to click **Apply** after uploading the file.

Example Device-specific File Settings

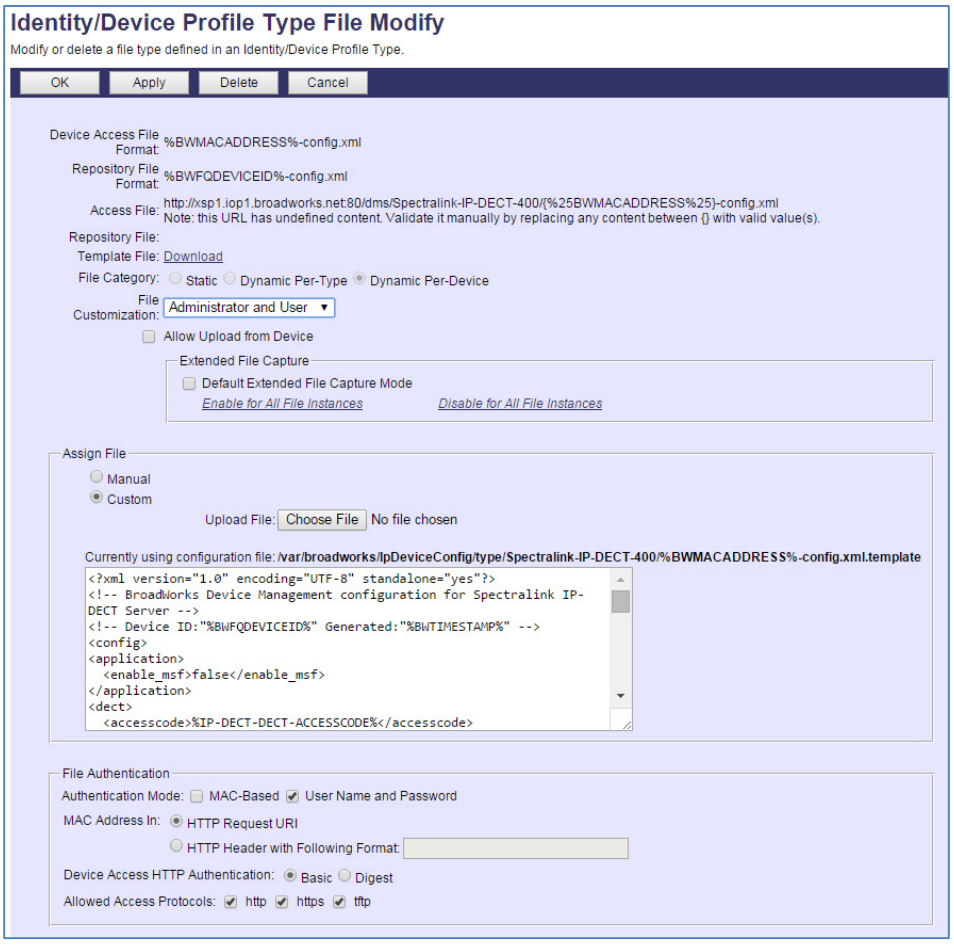

Figure 8 %BWMACADDRESS%-config.cfg File

5.2.2.2.2.2 *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.

The Spectralink IP DECT Server requires the following static file:

- *14218500-hermod-firmware-<firmware-version>.bin*
- *14218500-hermod-firmware-<firmware-version>.bin.ver*

Add a BroadWorks device profile type file to the Spectralink IP DECT Server device profile for each of the static files using the settings described in the following table.

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

Parameter	Value	Description
Device Access File Format	<file-name> Examples: *14218500-hermod-firmware-<firmware-version>.bin* *14218500-hermod-firmware-<firmware-version>.bin.ver*	This is the file name that the device uses when requesting the file.

Parameter	Value	Description
Repository File Format	<file-name> Examples: *14218500-hermod-firmware-<firmware-version>.bin* *14218500-hermod-firmware-<firmware-version>.bin.ver*	This is the file name as stored on 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 is recommended for static files.
Assign File	Custom	
Authentication Mode	Not set	The static files are not authenticated. Do not select either of these options.

After defining the static file types, upload the corresponding static files. Firmware must be obtained from Spectralink. Use the **Browse** button on the file definition screen. Be sure to select **Apply** after uploading the file.

Example Static File Settings

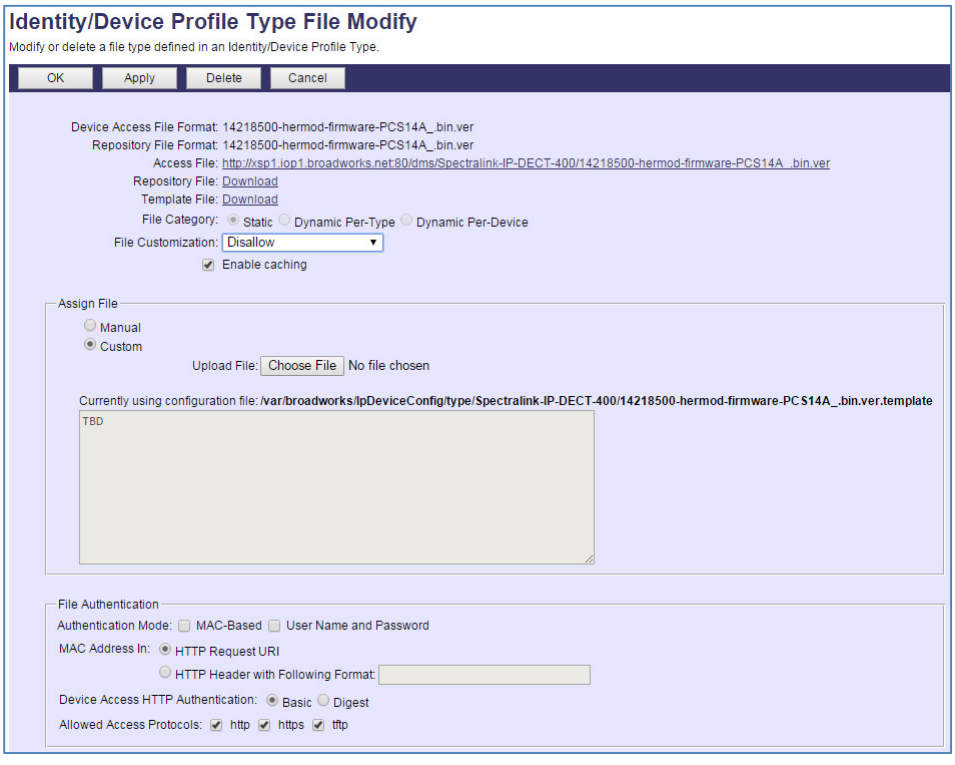

Figure 9 Firmware File

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 a particular Spectralink device.

This section describes how to create a BroadWorks device profile instance for an individual Spectralink IP DECT Server device. Device profile instances are usually created at the BroadWorks group level and assigned to users.

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

Browse to the BroadWorks *<group>* → *Resources* → *Identity/Device Profiles* page and then select **Add** to add a new Spectralink IP DECT Server 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 at the default values.

Parameter	Value	Description
Identity/Device Profile Name	<device-profile-name> Example: SP-DECT400	The device profile name is a unique identifier for the device profile instance.
Identity/Device Profile Type	<device-profile-type> Example: Spectralink-IP-DECT-400	From the drop-down list, select the Spectralink IP DECT device profile type created in the previous section.
Authentication	Use Custom Credentials	Use the unique login name and password for each device.
Device Access User Name	<device-login-name> Example: DM-SP-DECT400	This is the user name used to log in from the device. The device login user naming convention must be determined by the service provider.
Device Access Password	<device-login-password> Example: 654321	This is the password used to log in from the device.

Example Identity/Device Profile Settings

Figure 10 Device Profile Instance

In addition, the IP DECT Server requires these following parameters to be customized for each device profile:

%IP-DECT-PROVISIONING-SERVER-USER%	Device Access User Name	Device Access User Name
%IP-DECT-PROVISIONING-SERVER-PASSWORD%	Device Access Password	Device Access User Password

Provide the device profile specific values to these tags.

Example Custom Tags

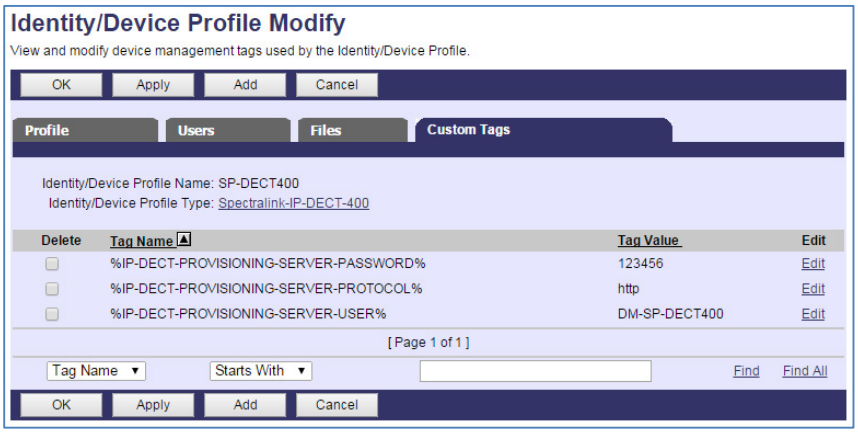

Figure 11 Custom Tags

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, if 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* page and set the parameters as described in the following table.

It is expected that parameters not identified in the following table are already set or are self-explanatory.

Parameter	Value	Description
Identity/Device Profile Name	<device-profile-name> Example: SP-DECT400	From the drop-down list, select the device profile instance created in the previous section.
Line/Port	<SIP register address-of-record> Example: 8881001023@as.iop1.broadworks.net	Supply the desired SIP register *address-of-record*.

Example User Addresses Settings

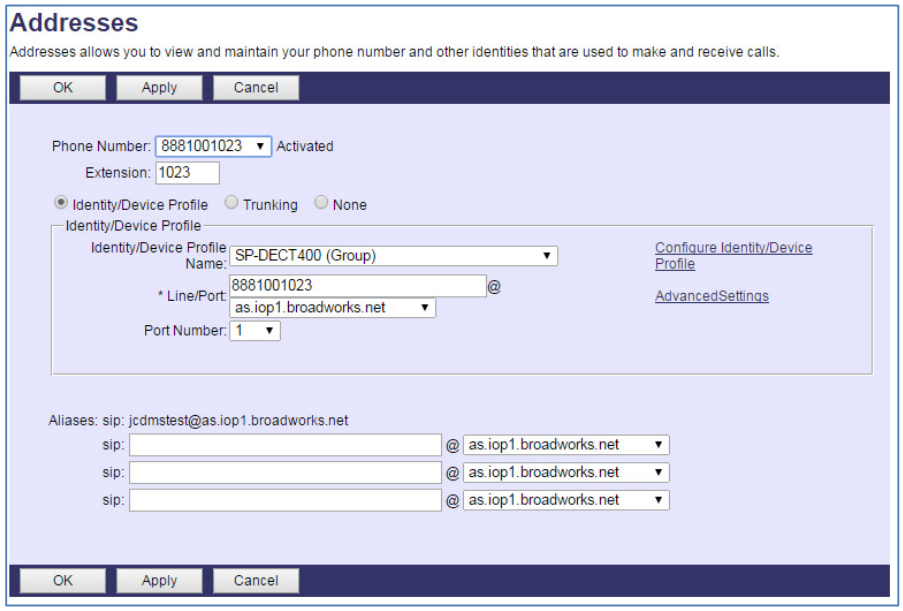

Figure 12 Assign Device Profile to User

5.2.5 Configure Edge Device

In many deployments, an edge device is deployed on the enterprise edge. Configure the edge device SIP server setting with the service provider's SBC IP address or FQDN.

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. At the *Group* →

Utilities → *Configure Device* page, select the Spectralink device profile (for example, SP-DECT400). Perform the following steps:

1) Click on the *Custom Tags* tab.
2) Click **Add**.
3) Add the SBC tag.
4) For the tag, enter "SBC_ADDRESS".
5) For the value, enter the IP address (that is, the edge device LAN IP address).
6) To save the tag data, click **OK**.

   This Tag/Value is applied to all Spectralink model devices in the group using the modified *Device Profile Type*.

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

5.2.6 Configure Spectralink IP DECT Server

This section describes the steps necessary to configure the Spectralink IP DECT Server to integrate with BroadWorks Device Management.

Browse to the web interface of the IP-DECT Server, http://<IP-DECT and log in. The default credentials are "admin/admin".

Go to *Configuration* → *Provisioning* and configure the method and URL. The Method must be "Static" and the URL must contain the protocol, credentials, address and path to the provisioning files.

Format: http|https://<username>:<password>@<host>:<port>/<path>

Example: http://KWS400-cluj:123456@xsp1.iop1.broadworks.net:80/dms/Spectralink-IP-DECT/

Where:

<username> is the Device Access User Name.

<password> is the Device Access Password.

<host>:<port>/<path> is the Device Type URL.

Example Provisioning Configuration Screen

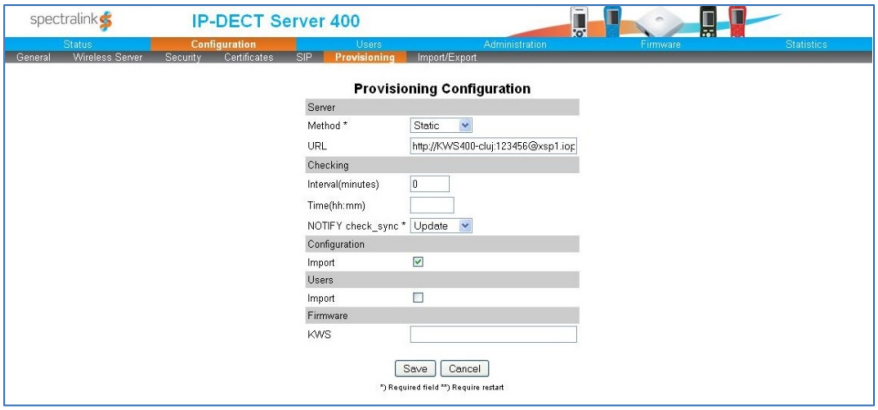

Figure 13 Example Provisioning Configuration Screen

Appendix A: Reference IP-DECT Server Series Configuration Files

The following is a reference configuration for the IP-DECT Server Series configured for use with BroadWorks.

System Default File: <IP DECT Server MAC address>-config.xml

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

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- BroadWorks Device Management configuration for Spectralink IP-DECT
Server -->
<!-- Device ID:"%BWFQDEVICEID%" Generated:"%BWTIMESTAMP%" -->
<config>
<application>
  <enable_msf>false</enable_msf>
</application>
<dect>
  <accesscode>%IP-DECT-DECT-ACCESSCODE%</accesscode>
  <subscription_allowed>%IP-DECT-DECT-
SUBSCRIPTIONALLOWED%</subscription_allowed>
</dect>
<language>%IP-DECT-LANGUAGE%</language>
<license>%IP-DECT-LICENSE%</license>
<log>
  <syslog>
    <facility>%IP-DECT-LOG-SYSLOG-FACILITY%</facility>
    <host>%IP-DECT-LOG-SYSLOG-HOST%</host>
    <level>%IP-DECT-LOG-SYSLOG-LEVEL%</level>
    <port>%IP-DECT-LOG-SYSLOG-PORT%</port>
  </syslog>
</log>
<network>
  <bootproto>%IP-DECT-NETWORK-BOOTPROTO%</bootproto>
  <ipaddr>%IP-DECT-NETWORK-IPADDR%</ipaddr>
  <dns1>%DNS_SERVER_1%</dns1>
  <dns2>%DNS_SERVER_2%</dns2>
  <gateway>%IP-DECT-NETWORK-GATEWAY%</gateway>
  <ipv6>
    <gateway>%IP-DECT-NETWORK-IPV6-GATEWAY%</gateway>
    <ipaddr>%IP-DECT-NETWORK-IPV6-IPADDR%</ipaddr>
    <method>%IP-DECT-NETWORK-IPV6-METHOD%</method>
  </ipv6>
  <netmask>%IP-DECT-NETWORK-NETMASK%</netmask>
  <ntp>%SNTP_SERVER%</ntp>
  <timezone>%IP-DECT-TIMEZONE%</timezone>
</network>
<phonebook>
  <ldap_attributes>%IP-DECT-PHONEBOOK-LDAP-ATTRIBUTES%</ldap_attributes>
  <ldap_base>%IP-DECT-PHONEBOOK-LDAP-BASE%</ldap_base>
  <ldap_bind_password>%IP-DECT-PHONEBOOK-LDAP-BIND-
PASSWORD%</ldap_bind_password>
  <ldap_bind_user>%IP-DECT-PHONEBOOK-LDAP-BIND-USER%</ldap_bind_user>
  <ldap_filter>%IP-DECT-PHONEBOOK-LDAP-FILTER%</ldap_filter>
  <ldap_names>%IP-DECT-PHONEBOOK-LDAP-NAMES%</ldap_names>
  <ldap_number_attributes>%IP-DECT-PHONEBOOK-LDAP-NUMBER-
ATTRIBUTES%</ldap_number_attributes>
  <ldap_prefixes>%IP-DECT-PHONEBOOK-LDAP-PREFIXES%</ldap_prefixes>
```

```
  <ldap_refresh_interval>%IP-DECT-PHONEBOOK-LDAP-
REFRESHINTERVAL%</ldap_refresh_interval>
  <ldap_uri>%IP-DECT-PHONEBOOK-LDAP-URI%</ldap_uri>
  <source>%IP-DECT-PHONEBOOK-SOURCE%</source>
</phonebook>
<provisioning>
  <check>
    <check_sync>update</check_sync>
    <interval>%IP-DECT-PROVISIONING-CHECK-INTERVAL%</interval>
  </check>
  <firmware>
    <kws>14218500-hermod-firmware-%IP-DECT-FWVERSION%.bin</kws>
  </firmware>
  <server>
    <method>static</method>
    <url>%IP-DECT-PROVISIONING-SERVER-PROTOCOL%://%IP-DECT-PROVISIONING-
SERVER-USER%:%IP-DECT-PROVISIONING-SERVER-
PASSWORD%@%BWDEVICEACCESSFQDN%:%BWDEVICEACCESSPORT%/%BWDMSCONTEXT%/%BWDEVI
CEACCESSURI%</url>
  </server>
  <users>
    <check>true</check>
  </users>
</provisioning>
<security>
  <allow_new_media_resource>%IP-DECT-SECURITY-ALLOW-NEW-
MR%</allow_new_media_resource>
  <allow_new_rfp>%IP-DECT-SECURITY-ALLOW-NEW-RFP%</allow_new_rfp>
  <force_https>%IP-DECT-SECURITY-FORCE-HTTPS%</force_https>
  <password>%IP-DECT-SECURITY-PASSWORD%</password>
</security>
<sip>
  <defaultdomain>%BWSERVERADDRESS%</defaultdomain>
  <dnsmethod>dnssrv</dnsmethod>
  <media>
    <tos>%IP-DECT-SIP-MEDIA-TOS%</tos>
    <vlan_cos>%IP-DECT-SIP-MEDIA-VLANCOS%</vlan_cos>
  </media>
  <proxy>
    <domain>%SBC_ADDRESS%</domain>
  </proxy>
  <tos>%IP-DECT-SIP-TOS%</tos>
  <transport>tcp</transport>
  <vlan_cos>%IP-DECT-SIP-VLANCOS%</vlan_cos>
</sip>
<snmp>
  <community>%IP-DECT-SNMP-COMMUNITY%</community>
  <enable>%IP-DECT-SNMP-ENABLE%</enable>
  <syscontact>%IP-DECT-SNMP-SYSCONTACT%</syscontact>
  <syslocation>%IP-DECT-SNMP-SYSLOCATION%</syslocation>
  <trapcommunity>%IP-DECT-SNMP-TRAPCOMMUNITY%</trapcommunity>
  <traphost>%IP-DECT-SNMP-TRAPHOST%</traphost>
</snmp>
</config>
```

Device-Specific File: <IP DECT Server MAC Address>-users.xml

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

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- BroadWorks Device Management configuration for Spectralink IP-DECT
Server -->
<!-- Device ID:"%BWFQDEVICEID%" Generated:"%BWTIMESTAMP%" -->
<users>
  <user>
    <standbytext>%BWFIRSTNAME-1%</standbytext>
    <username>%BWLINEPORT-1%</username>
    <displayname>%BWNAME-1%</displayname>
    <authpassword>%BWAUTHPASSWORD-1%</authpassword>
    <authuser>%BWAUTHUSER-1%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-2%</standbytext>
    <username>%BWLINEPORT-2%</username>
    <displayname>%BWNAME-2%</displayname>
    <authpassword>%BWAUTHPASSWORD-2%</authpassword>
    <authuser>%BWAUTHUSER-2%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-3%</standbytext>
    <username>%BWLINEPORT-3%</username>
    <displayname>%BWNAME-3%</displayname>
    <authpassword>%BWAUTHPASSWORD-3%</authpassword>
    <authuser>%BWAUTHUSER-3%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-4%</standbytext>
    <username>%BWLINEPORT-4%</username>
    <displayname>%BWNAME-4%</displayname>
    <authpassword>%BWAUTHPASSWORD-4%</authpassword>
    <authuser>%BWAUTHUSER-4%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-5%</standbytext>
    <username>%BWLINEPORT-5%</username>
    <displayname>%BWNAME-5%</displayname>
    <authpassword>%BWAUTHPASSWORD-5%</authpassword>
    <authuser>%BWAUTHUSER-5%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-6%</standbytext>
    <username>%BWLINEPORT-6%</username>
    <displayname>%BWNAME-6%</displayname>
    <authpassword>%BWAUTHPASSWORD-6%</authpassword>
    <authuser>%BWAUTHUSER-6%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-7%</standbytext>
    <username>%BWLINEPORT-7%</username>
    <displayname>%BWNAME-7%</displayname>
    <authpassword>%BWAUTHPASSWORD-7%</authpassword>
    <authuser>%BWAUTHUSER-7%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-8%</standbytext>
    <username>%BWLINEPORT-8%</username>
    <displayname>%BWNAME-8%</displayname>
    <authpassword>%BWAUTHPASSWORD-8%</authpassword>
    <authuser>%BWAUTHUSER-8%</authuser>
  </user>
  <user>
```

```
    <standbytext>%BWFIRSTNAME-9%</standbytext>
    <username>%BWLINEPORT-9%</username>
    <displayname>%BWNAME-9%</displayname>
    <authpassword>%BWAUTHPASSWORD-9%</authpassword>
    <authuser>%BWAUTHUSER-9%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-10%</standbytext>
    <username>%BWLINEPORT-10%</username>
    <displayname>%BWNAME-10%</displayname>
    <authpassword>%BWAUTHPASSWORD-10%</authpassword>
    <authuser>%BWAUTHUSER-10%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-11%</standbytext>
    <username>%BWLINEPORT-11%</username>
    <displayname>%BWNAME-11%</displayname>
    <authpassword>%BWAUTHPASSWORD-11%</authpassword>
    <authuser>%BWAUTHUSER-11%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-12%</standbytext>
    <username>%BWLINEPORT-12%</username>
    <displayname>%BWNAME-12%</displayname>
    <authpassword>%BWAUTHPASSWORD-12%</authpassword>
    <authuser>%BWAUTHUSER-12%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-13%</standbytext>
    <username>%BWLINEPORT-13%</username>
    <displayname>%BWNAME-13%</displayname>
    <authpassword>%BWAUTHPASSWORD-13%</authpassword>
    <authuser>%BWAUTHUSER-13%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-14%</standbytext>
    <username>%BWLINEPORT-14%</username>
    <displayname>%BWNAME-14%</displayname>
    <authpassword>%BWAUTHPASSWORD-14%</authpassword>
    <authuser>%BWAUTHUSER-14%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-15%</standbytext>
    <username>%BWLINEPORT-15%</username>
    <displayname>%BWNAME-15%</displayname>
    <authpassword>%BWAUTHPASSWORD-15%</authpassword>
    <authuser>%BWAUTHUSER-15%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-16%</standbytext>
    <username>%BWLINEPORT-16%</username>
    <displayname>%BWNAME-16%</displayname>
    <authpassword>%BWAUTHPASSWORD-16%</authpassword>
    <authuser>%BWAUTHUSER-16%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-17%</standbytext>
    <username>%BWLINEPORT-17%</username>
    <displayname>%BWNAME-17%</displayname>
    <authpassword>%BWAUTHPASSWORD-17%</authpassword>
    <authuser>%BWAUTHUSER-17%</authuser>
  </user>
```

```
  <user>
    <standbytext>%BWFIRSTNAME-18%</standbytext>
    <username>%BWLINEPORT-18%</username>
    <displayname>%BWNAME-18%</displayname>
    <authpassword>%BWAUTHPASSWORD-18%</authpassword>
    <authuser>%BWAUTHUSER-18%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-19%</standbytext>
    <username>%BWLINEPORT-19%</username>
    <displayname>%BWNAME-19%</displayname>
    <authpassword>%BWAUTHPASSWORD-19%</authpassword>
    <authuser>%BWAUTHUSER-19%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-20%</standbytext>
    <username>%BWLINEPORT-20%</username>
    <displayname>%BWNAME-20%</displayname>
    <authpassword>%BWAUTHPASSWORD-20%</authpassword>
    <authuser>%BWAUTHUSER-20%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-21%</standbytext>
    <username>%BWLINEPORT-21%</username>
    <displayname>%BWNAME-21%</displayname>
    <authpassword>%BWAUTHPASSWORD-21%</authpassword>
    <authuser>%BWAUTHUSER-21%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-22%</standbytext>
    <username>%BWLINEPORT-22%</username>
    <displayname>%BWNAME-22%</displayname>
    <authpassword>%BWAUTHPASSWORD-22%</authpassword>
    <authuser>%BWAUTHUSER-22%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-23%</standbytext>
    <username>%BWLINEPORT-23%</username>
    <displayname>%BWNAME-23%</displayname>
    <authpassword>%BWAUTHPASSWORD-23%</authpassword>
    <authuser>%BWAUTHUSER-23%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-24%</standbytext>
    <username>%BWLINEPORT-24%</username>
    <displayname>%BWNAME-24%</displayname>
    <authpassword>%BWAUTHPASSWORD-24%</authpassword>
    <authuser>%BWAUTHUSER-24%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-25%</standbytext>
    <username>%BWLINEPORT-25%</username>
    <displayname>%BWNAME-25%</displayname>
    <authpassword>%BWAUTHPASSWORD-25%</authpassword>
    <authuser>%BWAUTHUSER-25%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-26%</standbytext>
    <username>%BWLINEPORT-26%</username>
    <displayname>%BWNAME-26%</displayname>
    <authpassword>%BWAUTHPASSWORD-26%</authpassword>
    <authuser>%BWAUTHUSER-26%</authuser>
```

```
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-27%</standbytext>
    <username>%BWLINEPORT-27%</username>
    <displayname>%BWNAME-27%</displayname>
    <authpassword>%BWAUTHPASSWORD-27%</authpassword>
    <authuser>%BWAUTHUSER-27%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-28%</standbytext>
    <username>%BWLINEPORT-28%</username>
    <displayname>%BWNAME-28%</displayname>
    <authpassword>%BWAUTHPASSWORD-28%</authpassword>
    <authuser>%BWAUTHUSER-28%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-29%</standbytext>
    <username>%BWLINEPORT-29%</username>
    <displayname>%BWNAME-29%</displayname>
    <authpassword>%BWAUTHPASSWORD-29%</authpassword>
    <authuser>%BWAUTHUSER-29%</authuser>
  </user>
  <user>
    <standbytext>%BWFIRSTNAME-30%</standbytext>
    <username>%BWLINEPORT-30%</username>
    <displayname>%BWNAME-30%</displayname>
    <authpassword>%BWAUTHPASSWORD-30%</authpassword>
    <authuser>%BWAUTHUSER-30%</authuser>
  </user>
</users>
```

References

[1] Spectralink, Inc. 2014. *Spectralink IP DECT Server 400 Installation and Configuration Guide*. Available from Spectralink at support.spectralink.com.

[2] Spectralink, Inc. 2014. *Spectralink IP DECT Server 6500 Installation and Configuration Guide*. Available from Spectralink at support.spectralink.com.

[3] Spectralink, Inc. 2014. *Provisioning Guide Spectralink IP-DECT Servers and BroadSoft Device Management.* Available from Spectralink at support.spectralink.com.

[4] BroadSoft, Inc. 2014. *BroadWorks Device Management Configuration Guide*, *Release 20.0*. Available from BroadSoft at xchange.broadsoft.com.

[5] BroadSoft, Inc. 2014. *BroadWorks Redundancy Guide, Release 20.0*. Available from BroadSoft at xchange.broadsoft.com.

[6] BroadSoft, Inc. 2014. *BroadWorks SIP Access Interface Interworking Guide, Release 20.0.* Available from BroadSoft at xchange.broadsoft.com.

[7] BroadSoft, Inc. 2014. *BroadWorks SIP Access Device Interoperability Test Plan, Release 20.0*. Available from BroadSoft at xchange.broadsoft.com.

[8] BroadSoft, Inc. 2014. *BroadWorks Device Management Interoperability Test Plan*, *Release 20.0*. Available from BroadSoft at xchange.broadsoft.com.