



Cisco IP DECT 6800 Series Administration Guide

First Published: 2019-02-18

Last Modified: 2023-11-24

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Cisco IP DECT 6800 Series 1

Cisco IP DECT 6800 Series Overview	1
Base Station and Repeater Identification	3
New and Changed Information	4
New and Changed Information for Firmware Release 5.1(2)	4
New and Changed Information for Firmware Release 5.1(1)	4
New and Changed Information for Firmware Release 5.0	7
New and Changed Information for Firmware Release 4.8	10
New and Changed Information for Firmware Release 4.7	13
New and Changed Information for Firmware Release V460	15
Set Up the Cisco IP DECT 6800 Series (Workflow)	16
Set Up a 110 Repeater in Your Network	18
Base Station Accounts	19
System Behavior During Times of Network Congestion	19
Power Outage	19
Terminology Differences	20
Supported Characters	20
Cisco IP DECT 6800 Series Documentation	21

CHAPTER 2

Hardware Installation 23

Installation Requirements	23
Handset Registrations	25
Single Cell, Dualcell, and Multicell Networks	26
Base Station Package Contents	28
Repeater Package Contents	28
Handset package contents	28

Power Requirements	29
Install the Base Station	29
Mount the base station or repeater on the ceiling	30
Mount the base station or repeater on a desk	34
Mount the base station or repeater on the wall	35
Install the battery in the handset	39
Set Up the charging cradle	42
Charge the handset battery	42

CHAPTER 3**Phone Administration 45**

Find the base station IP address	45
Sign in to the administration web page	46
Sign in to the User Web Page	47
Automatic Configuration	47
Set Up a Handset Automatically with the Username and Password	48
Set Up a Handset Automatically with a Short Activation Code	49
Set Up the Handset Automatically	49
Manual Configuration	50
Configure the Base Station	50
Set the Base Station Country	51
Configure the Network Settings	51
Configure the SIP Transport	52
Configure the SIP Notify Authentication	53
Add Handsets to the Base Station	54
Assign handsets to users	55
Start handset registration	56
Connect the handset to the base station	56
Turn on your handset	57
Add a Repeater	57
EDOS Profile and XML Parameters	58
Change the Handset Information	59
Change the Extension	60
Configure Language and Text Settings for a Handset	60
Security	61

Set Up a Device Certificate and Key Pair	61
Set Up a Trusted Server Certificate	62
Set Up a Trusted Root Certificate	62
Set Up the Media Security	63
Configure On-Device Firewall	63
Firewall Default Port Settings	64
Change the Web Page Administrator or User Password	65
Set a Password Rule	66
Set Up the Web Server for HTTP or HTTPS	66
Cisco Product Security Overview	67
Local Contacts Setup	67
Import a Contact List	67
Export a Contact List	68
Central Directory Setup	69
Set Up a Text Central Directory	69
Set Up an LDAP Central Directory	70
Set Up an XML Central Directory	71
Feature Setup	72
Set Up Management Settings	72
Configure Text Messaging	73
Configure Paging	74
Change Star Codes	75
Change Call Progress Tones	75
Set Up Call Quality Statistics to Call Server	76
Configure Alarms	76
Configure the Location Server for Emergency Calls	77
Configure Emergency Numbers	78
Add or Edit Local Call Groups	78
Configure Handsets to the Call Group	79
Configure Handset Intercom Function	80
Temporary Handset Addition to the Base Station	80
Turn On Promiscuous Mode from the Firmware	81
Turn On Promiscuous Mode with the Base Station Reset Button	81
Add a Second Line to a Handset	82

- Share a Line Between Handsets 82
- Modification to Handset Settings 83
 - Configure the Handset Server 83
 - Update Handset Settings 84
- Dial Plan 85
 - Dial Plan Overview 85
- Configure the HEBU Mode in the Base Station 92
 - Configure the HEBU Username and Password in the Base Station 93
- Add an Additional Base Station to Make a Dualcell Network (Workflow) 93
 - Set Up a Dualcell System on the Primary Base Station 94
 - Set Up a Dualcell System on the Secondary Base Station 95
 - Set Up Base Station Replace Timeout in Dualcell Network 96
- Add Additional Base Stations to Make a Multicell Network (Workflow) 97
 - Set Up a Multicell System on the Primary Base Station 97
 - Set Up a Multicell System on a Secondary Base Station 98
- Add or Edit the Caller ID on IP DECT Phone 99
 - Configure Caller ID for the Handset 100
- Configure Problem Report Tool Server 101
- Export the Base Station's Status File 102

CHAPTER 4

- Headsets 103**
 - Supported Headsets 103
 - Important Headset Safety Information 103
 - Audio Quality 104

CHAPTER 5

- Monitoring 105**
 - Base Station Web Pages 105
 - Home/Status Web Page Fields 105
 - Extensions Web Page Fields 106
 - Add or Edit Extension Web Page Fields 109
 - Terminal Web Page Fields 112
 - Servers Web Page Fields 114
 - Network Web Page Fields 122
 - Management Web Page Fields 126

Firmware Update Web Page Fields	133
Country Web Page Fields	135
Security Web Page Fields	137
Central Directory Web Page Fields	141
Dual Cell Web Page Fields	144
Multi Cell Web Page Fields	146
LAN Sync Web Page Fields	150
Star Codes Web Page Fields	151
Call Progress Tones Web Page Fields	152
Dial Plans Web Page Fields	153
Local Call Groups	153
Repeaters Web Page Fields	155
Add or Edit Repeaters Web Page Fields	157
Alarm Web Page Fields	157
Statistics Web Page Fields	158
Generic Statistics Web Page Fields	161
Diagnostics Web Page Fields	165
Configuration Web Page Fields	167
Syslog Web Page Fields	167
SIP Log Web Page Fields	168
Web Pages for Previous Firmware Releases	168
Extensions Web Page Fields for Firmware Release V450 and V460	168
Terminal Web Page Fields for Firmware Release V450 and V460	170
View the Handset Status	172
Perform a Site Survey	173

CHAPTER 6
Maintenance 175

Reboot the Base Station from the Web Pages	175
Reboot the Base Station Remotely	176
Remove the Handset from the Web Page	176
Remove the Handset Remotely	177
Reset the Base Station to Factory Defaults	177
Reset the Handset to Factory Defaults	177
Verify the System Configuration	178

Back Up the System Configuration	178
Restore the System Configuration	179
System Upgrades and Downgrades	179
Upgrade or Downgrade Workflow	180
Prepare TFTP, HTTP, or HTTPS Server for Upgrades or Downgrades	180
Set Up the Firmware Update Parameters	181
Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server	181
Upgrade the Base Stations	183
Upgrade the Handsets	184
Downgrade the Base Stations	186
Downgrade the Handsets	187
View Base Statistics	188
Base Station States	189

CHAPTER 7**Troubleshooting 191**

Base Station Installation Problems	191
Base Station LED is Solid Red	191
Repeater Installation Problems	192
Can't Set Up a Repeater - LED is Red	192
Handset Installation Problems	192
Handset Won't Register (Automatic Configuration)	192
Handset Won't Register (Manual Configuration)	193
Handset Can't Register	193
Operational Problems with the Base Station	194
Base Station LED Flashes Red and Handset Displays "No SIP Reg" Message	194
Operational Problems with the Handset	194
Handset Won't Turn On	194
Handset Won't Stay On	195
Handset Doesn't Ring	195
Handset Doesn't Respond to Key Presses	196
Handset Beeps Continuously While in the Charger	196
Handset Screen Displays "Searching"	196
No Audio on Your Handsets with a Single Base Station System	197
Dualcell Troubleshooting	197

Multicell Troubleshooting	197
Base Station Shows Searching in DECT Property	198
Troubleshooting Procedures	198
Collect Troubleshooting Logs for a General Problem	198
Collect Troubleshooting Logs for a Repeatable Problem	199
Change the Debug Log Level	200
Turn On Dualcell Debug Logs	201
Turn on Multicell Debug Logs	201
Generate PCAP Logs	202

APPENDIX A

Cisco IP DECT 6800 Series with Cisco Unified Communications Manager	205
Deployment of DECT 6800 on Cisco Unified Communication Manager (CUCM)	205
Create a User	205
Add IP DECT 6825 on CUCM	206
Add a Line to the Device	207
Associate the Device to the User	207
Configure the Base Station	208

APPENDIX B

Technical Details	211
Base Station Specifications	211
Logging of Configuration Changes of Base Station	212
Reporting of Configuration Changes	212
Handset Specifications	212
Network Protocols	213
Reset the Network VLAN	216
SIP Configuration	216
SIP and the Cisco IP DECT Phone	216
SIP over TCP	217
SIP Proxy Redundancy	217
Failover and Recovery Registration	220
External Devices	220

APPENDIX C

Worksheets	221
Worksheets	221

Server Configuration Parameters Worksheet 221

Base Station Worksheet 222

Handset Configuration Parameters Worksheet 223



CHAPTER 1

Cisco IP DECT 6800 Series

- [Cisco IP DECT 6800 Series Overview, on page 1](#)
- [New and Changed Information, on page 4](#)
- [Set Up the Cisco IP DECT 6800 Series \(Workflow\), on page 16](#)
- [Set Up a 110 Repeater in Your Network, on page 18](#)
- [Base Station Accounts, on page 19](#)
- [System Behavior During Times of Network Congestion, on page 19](#)
- [Power Outage, on page 19](#)
- [Terminology Differences, on page 20](#)
- [Supported Characters, on page 20](#)
- [Cisco IP DECT 6800 Series Documentation, on page 21](#)

Cisco IP DECT 6800 Series Overview

The Cisco IP DECT 6800 Series is designed for small and medium businesses. The series is made up of:

- Cisco IP DECT 110 Single-Cell Base Station
- Cisco IP DECT 210 Multi-Cell Base Station
- Cisco IP DECT 110 Repeater
- Cisco IP DECT Phone 6823 Handset
- Cisco IP DECT Phone 6825 Handset
- Cisco IP DECT Phone 6825 Ruggedized Handset

The base stations and repeater look the same. But each has a different function.



Note This document covers the Cisco IP DECT 6800 Series only. This series is different from the Cisco IP Phone 6800 Series Multiplatform Phones. For information on the Cisco IP Phone 6800 Series Multiplatform Phones, see <https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-phone-6800-series-multiplatform-firmware/series.html>

Figure 1: Cisco IP DECT Phone 6823 Handset, Cisco IP DECT Phone 6825 Handset, Cisco IP DECT Phone 6825 Ruggedized Handset, Cisco IP DECT 110 Repeater, Cisco IP DECT 210 Multi-Cell Base Station, and Cisco IP DECT 110 Single-Cell Base Station



The orange Cisco IP DECT Phone 6825 Ruggedized Handset is IP65-rated. IP65 means that the handset is dust tight and protected against water projected from a nozzle. The orange color makes the handset easier to locate.

The following table gives the main differences between the Cisco IP DECT Phone 6825 Handset and the Cisco IP DECT Phone 6823 Handset.

Feature	Cisco IP DECT Phone 6825 Handset	Cisco IP DECT Phone 6823 Handset
Screen	Display: 2 inches Resolution: 240 x 320 pixels	Display: 1.7 inches Resolution: 128 x 160 pixels
Emergency button	Present	Not present
Bluetooth	Supported	Not supported
Charging cradle	USB port and LED	No USB port or LED

The handsets use Digital Enhanced Cordless Telecommunications (DECT) to communicate with a base station. The base station communicates with the call control system for call control functions.

You can set up the system in these configurations:

- One Cisco IP DECT 110 Single-Cell Base Station with up to six 110 Repeaters
- Two Cisco IP DECT 110 Single-Cell Base Stations with up to twelve 110 Repeaters
- One or more Cisco IP DECT 210 Multi-Cell Base Station with up to three 110 Repeaters per base station.

Multiple base stations extend radio coverage for larger office spaces.

Each Cisco IP DECT 210 Multi-Cell Base Station can have up to 30 handsets configured to use the base station. Each 110 Single-Cell Base Station can have up to 20 handsets configured to use the base station. The number of active calls on a base station is limited. For more information, see [Installation Requirements, on page 23](#).

This document discusses the installation, configuration, and administration of the system. For information about using the handset, see the *Cisco IP DECT 6800 Series User Guide*.

The following table lists some common terms and their meanings used in this document.

Table 1: Terms

Term	Meaning
<i>Handset or phone</i>	6823 Handset 6825 Handset
<i>Base station</i>	110 Single-Cell Base Station 210 Multi-Cell Base Station
<i>Repeater</i>	110 Repeater
<i>System</i>	The set of handsets, repeaters, and base stations at a customer site.



Note Not all features may be supported on your system. Contact your service provider for the supported features.

Base Station and Repeater Identification

You can identify the Cisco IP DECT 6800 Series devices by the symbol on the top of the device.

Device	Symbols
110 Single-Cell Base Station	
210 Multi-Cell Base Station	
110 Repeater	

You can also identify the base stations and repeaters in these ways:

- The product identification label on the back of the devices.
- Repeaters don't have a LAN port.

New and Changed Information

New and Changed Information for Firmware Release 5.1(2)

Features	New or Changed Information
Updated the topic for LLDP and CDP	Network Protocols , on page 213
Technical Details	New section: Reset the Network VLAN , on page 216
A new topic added to base station now allows to download complete XML config file from Cisco EDOS server	EDOS Profile and XML Parameters , on page 58
A new topic added to record configuration changes that users make to the base station using the configuration changes logging function	Logging of Configuration Changes of Base Station , on page 212
A new topic added to the base station requests DECT locked handsets for changelogs	Reporting of Configuration Changes , on page 212
New topics added for DECT on CUCM support	Cisco IP DECT 6800 Series with Cisco Unified Communications Manager , on page 205
Added a new topic to support on-device firewall	Configure On-Device Firewall , on page 63 Firewall Default Port Settings , on page 64
Added new parameters in Web page fields to support on-device firewall	Firewall Section Fields in Security Web Page Fields , on page 137

New and Changed Information for Firmware Release 5.1(1)

Features	New or Changed Information
Automatic Handset Registration in HEBU Mode	<p>New sections:</p> <ul style="list-style-type: none"> • Configure the HEBU Mode in the Base Station, on page 92 • Configure the HEBU Username and Password in the Base Station, on page 93 <p>Updated sections:</p> <ul style="list-style-type: none"> • Management Web Page Fields, on page 126 • Terminal Web Page Fields, on page 112

Features	New or Changed Information
Base Station Status File Export	New section: Export the Base Station's Status File, on page 102
Call Groups Addition for Intercom Calls	New sections: <ul style="list-style-type: none">• Add or Edit Local Call Groups, on page 78• Configure Handsets to the Call Group, on page 79• Configure Handset Intercom Function, on page 80• Local Call Groups, on page 153
Caller ID Display Enhancement	New sections: <ul style="list-style-type: none">• Add or Edit the Caller ID on IP DECT Phone, on page 99• Configure Caller ID for the Handset, on page 100
	Updated section: Dial Plans Web Page Fields, on page 153

Features	New or Changed Information
Dial Plan Enhancements	<p>New sections:</p> <ul style="list-style-type: none"> • Dial Plan, on page 85 • Dial Plan Overview, on page 85 • Digit Sequences, on page 85 • Digit Sequence Examples, on page 86 • Acceptance and Transmission of the Dialed Digits, on page 88 • Interdigit Long Timer (Incomplete Entry Timer), on page 89 • Syntax for the Interdigit Long Timer, on page 89 • Example for the Interdigit Long Timer, on page 89 • Interdigit Short Timer (Complete Entry Timer), on page 89 • Syntax for the Interdigit Short Timer, on page 89 • Examples for the Interdigit Short Timer, on page 90 • Add or Edit the Dial Plan on IP DECT Phone, on page 90 • Configure Dial Plan for the Handset, on page 91 • DTMF Wait and Pause Parameters, on page 91
Handset Settings Enhancements	<p>New section: Modification to Handset Settings, on page 83</p>
Language and Texts Changes in a Handset	<p>Updated section: Management Web Page Fields, on page 126</p>
Location Server Configuration for Emergency Calls	<p>New section: Configure Language and Text Settings for a Handset, on page 60</p> <p>Updated section: Firmware Update Web Page Fields, on page 133</p>
Location Server Configuration for Emergency Calls	<p>New section: Configure the Location Server for Emergency Calls, on page 77</p> <p>Updated section: Management Web Page Fields, on page 126</p>

Features	New or Changed Information
Media Security and Call Handling Enhancements	New sections: <ul style="list-style-type: none"> • Configure the SIP Transport, on page 52 • SIP Configuration, on page 216 Updated sections: <ul style="list-style-type: none"> • Set Up the Media Security, on page 63 • Security Web Page Fields, on page 137
Report Upload to Problem Report Server	New section: Configure Problem Report Tool Server , on page 101 Updated section: Management Web Page Fields , on page 126

New and Changed Information for Firmware Release 5.0

Features	New or Changed Information
Base Station Default Password Change	Updated sections: <ul style="list-style-type: none"> • Sign in to the administration web page, on page 46 • Sign in to the User Web Page, on page 47 • Change the Web Page Administrator or User Password, on page 65 • Security Web Page Fields, on page 137
Call Quality Statistics to Call Server	New section: Set Up Call Quality Statistics to Call Server , on page 76 Updated section: Servers Web Page Fields , on page 114

Features	New or Changed Information
Dual Cell Network	<p data-bbox="922 289 1073 317">New sections:</p> <ul data-bbox="954 338 1442 506" style="list-style-type: none"> <li data-bbox="954 338 1442 401">• Add an Additional Base Station to Make a Dualcell Network (Workflow), on page 93 <li data-bbox="954 405 1442 432">• Dual Cell Web Page Fields, on page 144 <li data-bbox="954 436 1442 464">• Dualcell Troubleshooting, on page 197 <li data-bbox="954 468 1442 506">• Turn On Dualcell Debug Logs, on page 201 <p data-bbox="922 527 1114 554">Updated sections:</p> <ul data-bbox="954 575 1484 1262" style="list-style-type: none"> <li data-bbox="954 575 1484 638">• Cisco IP DECT 6800 Series Overview, on page 1 <li data-bbox="954 642 1484 705">• Set Up the Cisco IP DECT 6800 Series (Workflow), on page 16 <li data-bbox="954 709 1484 737">• Handset Registrations, on page 25 <li data-bbox="954 758 1484 821">• Single Cell, Dualcell, and Multicell Networks, on page 26 <li data-bbox="954 842 1484 905">• Mount the base station or repeater on the ceiling, on page 30 <li data-bbox="954 909 1484 972">• Mount the base station or repeater on a desk, on page 34 <li data-bbox="954 976 1484 1039">• Mount the base station or repeater on the wall, on page 35 <li data-bbox="954 1043 1484 1071">• Set the Base Station Country, on page 51 <li data-bbox="954 1075 1484 1138">• Add Additional Base Stations to Make a Multicell Network (Workflow), on page 97 <li data-bbox="954 1142 1484 1169">• Home/Status Web Page Fields, on page 105 <li data-bbox="954 1190 1484 1253">• Handset Screen Displays "Searching", on page 196
Firmware Filename Modification	<p data-bbox="922 1287 1073 1314">New sections:</p> <ul data-bbox="954 1335 1442 1419" style="list-style-type: none"> <li data-bbox="954 1335 1442 1362">• Downgrade the Base Stations, on page 186 <li data-bbox="954 1383 1442 1419">• Downgrade the Handsets , on page 187 <p data-bbox="922 1451 1114 1478">Updated sections:</p> <ul data-bbox="954 1499 1484 1583" style="list-style-type: none"> <li data-bbox="954 1499 1484 1526">• Firmware Update Web Page Fields, on page 133 <li data-bbox="954 1547 1484 1583">• System Upgrades and Downgrades, on page 179
SIP Notification of Handset Removal	<p data-bbox="922 1623 1484 1686">New section: Configure the SIP Notify Authentication, on page 53</p> <p data-bbox="922 1707 1484 1764">Updated section: Servers Web Page Fields, on page 114</p>

Features	New or Changed Information
UI Enhancements	<ul style="list-style-type: none">• New fields SIP Session Timers and Supported 100rel in the Servers Web Page Fields, on page 114• New fields Mode, Via DHCP priority, LLDP-MED Send, and LLDP-MED Send Delay in the Network Web Page Fields, on page 122• New field Protocol in the Management Web Page Fields, on page 126• New fields Current local RTP connections, Current local relay RTP connections, Current remote relay RTP connections, Current recording RTP connections, Current Blackfin DSP status, and Total number of Blackfin DSP restarts in the Generic Statistics Web Page Fields, on page 161• New field Info in the Diagnostics Web Page Fields, on page 165
General Changes	<p>New maintenance procedures:</p> <ul style="list-style-type: none">• Reboot the Base Station Remotely, on page 176• Remove the Handset from the Web Page, on page 176• Remove the Handset Remotely, on page 177

New and Changed Information for Firmware Release 4.8

Feature	New or Changed Content
110 Single-Cell Base Station	<p>New section: Base Station and Repeater Identification, on page 3</p> <p>Updated sections:</p> <ul style="list-style-type: none"> • Cisco IP DECT 6800 Series Overview, on page 1 • Set Up the Cisco IP DECT 6800 Series (Workflow), on page 16 • Installation Requirements, on page 23 • Mount the base station or repeater on the ceiling, on page 30 • Mount the base station or repeater on a desk, on page 34 • Mount the base station or repeater on the wall, on page 35 • Set the Base Station Country, on page 51 • Add Additional Base Stations to Make a Multicell Network (Workflow), on page 97 • Handset Screen Displays "Searching", on page 196 • Automatic Configuration, on page 47 • Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server, on page 181
110 Repeater	<p>New sections:</p> <ul style="list-style-type: none"> • Base Station and Repeater Identification, on page 3 • Set Up a 110 Repeater in Your Network, on page 18 • Repeater Package Contents, on page 28 • Add a Repeater, on page 57 • Repeaters Web Page Fields, on page 155 • Repeater Installation Problems, on page 192

Feature	New or Changed Content
110 Repeater	<p>Updated sections:</p> <ul style="list-style-type: none"> • Cisco IP DECT 6800 Series Overview, on page 1 • Set Up the Cisco IP DECT 6800 Series (Workflow), on page 16 • Installation Requirements, on page 23 • Install the Base Station, on page 29 • Mount the base station or repeater on the ceiling, on page 30 • Mount the base station or repeater on a desk, on page 34 • Mount the base station or repeater on the wall, on page 35 • Extensions Web Page Fields, on page 106 • Statistics Web Page Fields, on page 158 • Diagnostics Web Page Fields, on page 165 • Perform a Site Survey, on page 173 • Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server, on page 181 • Handset Installation Problems, on page 192
6823 Handset	<p>Updated sections:</p> <ul style="list-style-type: none"> • Cisco IP DECT 6800 Series Overview, on page 1 • Installation Requirements, on page 23 • Set Up the charging cradle, on page 42 • Configure Alarms, on page 76 • Firmware Update Web Page Fields, on page 133 • System Upgrades and Downgrades, on page 179 • Handset Specifications, on page 212
Access Code Addition to Handsets	<p>Updated the sections:</p> <ul style="list-style-type: none"> • Assign handsets to users, on page 55 • Start handset registration, on page 56 • Connect the handset to the base station, on page 56 • Country Web Page Fields, on page 135
Certificate Time Validation Enhancement	<p>Updated the section Set the Base Station Country, on page 51</p>

Feature	New or Changed Content
Paging	New sections: <ul style="list-style-type: none"> • Configure Paging, on page 74 • The table Multiple Paging Group Parameters in Management Web Page Fields, on page 126 • The field Page Tone in Call Progress Tones Web Page Fields, on page 152
Password Enhancements	New sections: <ul style="list-style-type: none"> • Set a Password Rule, on page 66. • The table Web password constraints Section Fields in Security Web Page Fields, on page 137
Multicell Provisioning Enhancement	Updated section: Automatic Configuration, on page 47
Security for Media	New section: Set Up the Media Security, on page 63 Updated sections: <ul style="list-style-type: none"> • Security, on page 61 • The field Secure RTP, and new fields Media Security and Media Security only for TLS in Servers Web Page Fields, on page 114
Shared Call Enhancements	New field BroadWorks Busy Lamp Field List URI in Add or Edit Extension Web Page Fields, on page 109
Temporary Handset Addition to Base Station	New sections: <ul style="list-style-type: none"> • Set Up a Handset Automatically with the Username and Password, on page 48 • Set Up a Handset Automatically with a Short Activation Code, on page 49 • Temporary Handset Addition to the Base Station, on page 80 • The table Promiscuous Mode Section Fields in Management Web Page Fields, on page 126
UI Enhancements	New fields Status and Extension in the Extensions Web Page Fields, on page 106
Troubleshooting Changes	New section: Handset Can't Register, on page 193.

Feature	New or Changed Content
General Changes	<p>Addition of handset package details in Handset package contents, on page 28</p> <p>Update of default password in Sign in to the User Web Page, on page 47</p> <p>Addition of static IP details in Configure the Network Settings, on page 51</p> <p>Addition of local text folder details in Central Directory Setup, on page 69</p> <p>Addition of information about an alarm server configuration in Configure Alarms, on page 76</p> <p>Addition of multicell system prerequisite requirements in Set Up a Multicell System on the Primary Base Station, on page 97</p> <p>Update of headset support information in Audio Quality, on page 104</p> <p>Addition of description details in various web page field tables</p> <p>Addition of values for auto resync in Management Web Page Fields, on page 126</p> <p>Addition of LED pattern and upgrade time in Upgrade the Base Stations, on page 183 and Upgrade the Handsets, on page 184</p> <p>New troubleshooting procedure in Handset Beeps Continuously While in the Charger, on page 196</p>

New and Changed Information for Firmware Release 4.7

Starting with this release:

- The release number scheme changes to conform to the standard Cisco release numbers. Internally, the previous number scheme will display. Firmware Release 4.7 and Firmware Release V470 B6 are the same firmware release.
- All document updates related to the release are clearly marked. For example, if there is a new field added or a field removed, the documentation indicates the type of change and what release the change applies to.

Feature	New or Changed Information
210 Multi-Cell Base Station	<p>Cisco IP DECT 6800 Series Overview, on page 1</p> <p>Set Up the Cisco IP DECT 6800 Series (Workflow), on page 16</p> <p>Installation Requirements, on page 23</p> <p>Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server, on page 181</p> <p>Upgrade the Handsets, on page 184</p> <p>Handset Specifications, on page 212</p>
DNS NAPTR Support	<p>Add information to the SIP Transport field to Servers Web Page Fields, on page 114.</p>
Opus Codec Support	<p>Add OPUS to the Codec Priority field in Servers Web Page Fields, on page 114.</p>
UI Enhancements	<p>The Extensions web page and its subpages have been changed. This impacts the following content:</p> <ul style="list-style-type: none"> • Extensions Web Page Fields, on page 106 The previous section is available here: Extensions Web Page Fields for Firmware Release V450 and V460, on page 168. • Terminal Web Page Fields, on page 112 The previous section is available here: Terminal Web Page Fields for Firmware Release V450 and V460, on page 170 • Add or Edit Extension Web Page Fields, on page 109 <p>Add the Extension Info, Terminal Position, Battery Level, RSSI, and Measurement Time [mm:ss] fields in Extensions Web Page Fields, on page 106.</p> <p>Add the maximum length of the Authentication User Name, Authentication Password, XSI User Name and XSI Password fields in Add or Edit Extension Web Page Fields, on page 109.</p> <p>Add Failover Reconnect Time to Network Web Page Fields, on page 122.</p> <p>Add Emergency calls, Call drops due to emergency call, and Emergency calls rejected fields to Calls view in Statistics Web Page Fields, on page 158.</p> <p>Some fields no longer display in the web pages for Firmware Release 4.7. They have been marked as removed.</p>

Feature	New or Changed Information
General changes	<p>Updates to Set Up the Cisco IP DECT 6800 Series (Workflow), on page 16 to reorder the tasks.</p> <p>Clarifications about country information in Set the Base Station Country, on page 51.</p> <p>Perform a Site Survey, on page 173 was rewritten.</p> <p>New troubleshooting procedures Handset Won't Turn On, on page 194 and Handset Won't Stay On, on page 195.</p>

New and Changed Information for Firmware Release V460

Feature	New or Updated Sections
Base station web page enhancements	<p>New Base Station Accounts, on page 19</p> <p>New Sign in to the User Web Page, on page 47</p> <p>Updated Base Station Web Pages, on page 105</p> <p>Updated New and Changed Information for Firmware Release V460, on page 15</p> <p>Updated Terminal Web Page Fields for Firmware Release V450 and V460, on page 170</p> <p>Updated Servers Web Page Fields, on page 114</p> <p>Updated Management Web Page Fields, on page 126</p> <p>Updated Central Directory Web Page Fields, on page 141</p> <p>Updated Generic Statistics Web Page Fields, on page 161</p>
Broadsoft All directory	Updated Central Directory Web Page Fields , on page 141
CDP support	Updated Network Web Page Fields , on page 122 and Network Protocols , on page 213
Handset out-of-box enhancements	Updated Handset Won't Register (Automatic Configuration) , on page 192
PCAP logs	<p>Updated Diagnostics Web Page Fields, on page 165</p> <p>New task Generate PCAP Logs, on page 202</p>

Feature	New or Updated Sections
General changes	New tasks: <ul style="list-style-type: none"> • Add a Second Line to a Handset, on page 82 • Share a Line Between Handsets, on page 82 • Handset Won't Register (Automatic Configuration), on page 192 • Handset Won't Register (Manual Configuration), on page 193 • Base Station LED Flashes Red and Handset Displays No SIP Reg Message, on page 194

Set Up the Cisco IP DECT 6800 Series (Workflow)

Use the following workflow to guide you through the setup of the 110 Single-Cell Base Station or 210 Multi-Cell Base Station in your system.



Note This workflow is a plan for a single-base system. If you need to add another 110 Single-Cell Base Station or Cisco IP DECT 210 Multi-Cell Base Station, or additional 210 Multi-Cell Base Stations, the additional base stations require additional knowledge.

Installation can take two approaches:

- **Automatic:** In this scenario, the base station and handsets are preconfigured by the service provider.
- **Manual:** In this scenario, the base station and handsets must be configured with the administration web pages. The service provider needs to provide information to enable the system to communicate with the call control service.

After you complete this workflow, you can configure directories, security, and additional features. For more information, see [Phone Administration, on page 45](#).

Procedure

	Command or Action	Purpose
Step 1	Installation Requirements, on page 23	Prepare for system installation.
Step 2	Install the Base Station, on page 29	Check that the base station and network can communicate. If the system uses automatic configuration, the system automatically downloads its configuration.
Step 3	Perform a Site Survey, on page 173	Temporarily place the base station in the planned locations and ensure that the

	Command or Action	Purpose
		placement gives good coverage before you permanently install the hardware. For more information, see the <i>Cisco IP DECT Phone 6800 Series Deployment Guide</i> .
Step 4	Perform one of these tasks: <ul style="list-style-type: none"> • Mount the base station or repeater on the ceiling, on page 30 • Mount the base station or repeater on a desk, on page 34 • Mount the base station or repeater on the wall, on page 35 	Mount the base station in the desired location.
Step 5	Sign in to the administration web page, on page 46	Connect to the base station web page from your browser.
Step 6	Configure the Base Station, on page 50	(Manual configuration only) Configure the base station to communicate with the SIP server for call processing.
Step 7	Set the Base Station Country, on page 51	(Manual configuration only) Configure the country and time for the base station. The country determines ringtones and in-band tones. The country also helps with time setup. The time is displayed on the handsets and in the base station log files.
Step 8	Configure the Network Settings, on page 51	(Manual configuration only) Set up the network so that you can make calls.
Step 9	Add Handsets to the Base Station, on page 54	(Manual configuration only) Configure handsets on the base station. You can set up one handset or multiple handsets.
Step 10	Assign handsets to users, on page 55	(Manual configuration only) In the multiple handset setup scenario, assign handsets to specific users.
Step 11	Start handset registration, on page 56	Prepares the base station to expect the handsets to register and complete the communication loop.
Step 12	Connect the handset to the base station, on page 56	Set up communication between the handset and the base station.
Step 13	Verify the System Configuration, on page 178	Check that you can place calls.
Step 14	(Optional) Perform a Site Survey, on page 173	Check that the base stations are correctly placed for communication with the handsets.

	Command or Action	Purpose
Step 15	(Optional) Back Up the System Configuration, on page 178	Perform a backup to save the configuration.

What to do next

If you need to set up a 110 Repeater, go to [Set Up a 110 Repeater in Your Network, on page 18](#).

Related Topics

[Manual Configuration, on page 50](#)

[Automatic Configuration, on page 47](#)

Set Up a 110 Repeater in Your Network

Use the following workflow to configure a 110 Repeater to work with your 110 Single-Cell Base Station.



Note Do not connect the repeater to power until instructed to in [Add a Repeater, on page 57](#).

Before you begin

The base station must be installed and active.

At least one handset must be installed and active.

Procedure

	Command or Action	Purpose
Step 1	Installation Requirements, on page 23	Prepare for system installation.
Step 2	Perform a Site Survey, on page 173	Temporarily place the repeaters in the planned locations and ensure that the placement gives good coverage before you permanently install the hardware. For more information, see the <i>Cisco IP DECT Phone 6800 Series Deployment Guide</i> .
Step 3	Perform one of these: <ul style="list-style-type: none"> • Mount the base station or repeater on the ceiling, on page 30 • Mount the base station or repeater on a desk, on page 34 • Mount the base station or repeater on the wall, on page 35 	Mount the repeater in the desired location.
Step 4	Sign in to the administration web page, on page 46	Connect to the base station web page from your browser.

	Command or Action	Purpose
Step 5	Add a Repeater, on page 57	Add the repeater to the system.
Step 6	Verify the System Configuration, on page 178	Check that you can place calls.
Step 7	Perform a Site Survey, on page 173	Check that the base station and repeater are correctly placed for communication with the handsets.
Step 8	(Optional) Back Up the System Configuration, on page 178	Perform a backup to save the configuration.

Base Station Accounts

You can sign into the base station as an administrator or as a user. Your service provider gives you the IDs and passwords.

The administrator ID gives you access to all the web pages and all fields described in this document.

The user ID gives you access to a subset fields in these web pages only:

- Home/Status
- Extensions
- Terminal

Related Topics

[Base Station Web Pages](#), on page 105

System Behavior During Times of Network Congestion

Anything that degrades network performance can affect phone system voice quality, and in some cases, can cause a call to drop. Sources of network degradation can include, but are not limited to, the following activities:

- Administrative tasks, such as an internal port scan or security scan
- Attacks that occur on your network, such as a Denial of Service attack

Power Outage

Your access to emergency service through the phone requires that the base station receive power. If a power interruption occurs, service or emergency calling service dialing does not function until power is restored. If a power failure or disruption occurs, you may need to reset or reconfigure the equipment before you can use service or emergency calling service dialing.

Your access to emergency service also requires that the handset has sufficient battery power. If the battery doesn't have enough power, service or emergency calling service dialing does not function until the battery is sufficiently charged.

Terminology Differences

The following table highlights some of the terminology differences in the *Cisco IP DECT 6800 Series User Guide* and the *Cisco IP DECT 6800 Series Administration Guide*.

Table 2: Terminology Differences

User Guide	Administration Guide
Message Indicators	Message Waiting Indicator (MWI) or Message Waiting Lamp
Voicemail System	Voice Messaging System

Supported Characters

When you input information, the base stations and handsets support the following characters:

Figure 2: Supported Characters

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0			0	@	P	`	p	€	ı	°	À	Đ	à	đ		
1		!	1	A	Q	a	q	ı	'	ı	±	Á	Ñ	á	ñ	
2		"	2	B	R	b	r	,	'	φ	Č	Â	Ò	â	ò	
3		#	3	C	S	c	s	f	"	£	č	Ă	Ó	ă	ó	
4		\$	4	D	T	d	t	"	"	¤	'	Ä	Ô	ä	ô	
5		%	5	E	U	e	u	...	•	¥	µ	Å	Õ	å	õ	
6		&	6	F	V	f	v	†	-	ı	¶	Æ	Ö	æ	ö	
7		'	7	G	W	g	w	‡	—	Š	·	Ç	×	ç	÷	
8		(8	H	X	h	x	^	~	"	„	È	Ø	è	ø	
9)	9	I	Y	i	y	Ř	ř	Û	Ǿ	É	Ù	é	ù	
A		*	:	J	Z	j	z	Š	š	û	d'	Ê	Ú	ê	ú	
B		+	;	K	[k	{	<	>	«	»	Ë	Û	ë	ü	
C		,	<	L	\	l		œ	œ	Ë	Ť	İ	Ü	ı	ü	
D		-	=	M]	m	}	Š	š	ě	ł'	Í	Ý	í	ý	
E		.	>	N	^	n	~	Ž	ž	Ň	ň	İ	ı	ı	ı	
F		/	?	O	_	o	ö	ÿ	ˉ	ı	ı	ı	ı	ı	ı	



Note You can press the center softkey in the 6823 Handset to access the special characters.

Cisco IP DECT 6800 Series Documentation

See the publications that are specific to your language and firmware release. Navigate from the following Uniform Resource Locator (URL):

<https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-dect-6800-series-multiplatform-firmware/tsd-products-support-series-home.html>



CHAPTER 2

Hardware Installation

- [Installation Requirements, on page 23](#)
- [Install the Base Station, on page 29](#)
- [Mount the base station or repeater on the ceiling, on page 30](#)
- [Mount the base station or repeater on a desk, on page 34](#)
- [Mount the base station or repeater on the wall, on page 35](#)
- [Install the battery in the handset, on page 39](#)
- [Set Up the charging cradle, on page 42](#)
- [Charge the handset battery, on page 42](#)

Installation Requirements

The Cisco IP DECT 6800 Series is made up of the following hardware:

- 6825 Handset
- 6825 Ruggedized Handset
- 6823 Handset
- 110 Single-Cell Base Station
- 210 Multi-Cell Base Station
- 110 Repeater



Note The 110 Single-Cell Base Station can't be used in the multicell system.

Before you begin to set up the Cisco IP DECT 6800 Series system:

- Determine the number of users (handsets) that are required.
- Determine the number of phone lines (numbers) that are required. Each user can have up to 2 lines and 2 concurrent calls, if the supported total number of concurrent calls on the system aren't reached.
- Given the number of handsets, determine the number of base stations required, based on:

- Estimated simultaneous handset usage: For more information, see [Handset Registrations, on page 25](#).
- Size of the space covered.
- Range of the base stations. Each base station has a range of up to 984 feet (300 meters) outdoors and a range of 164 feet (50 meters) indoors.
- If required, you can add repeaters to the base station to extend the range of the system:

Table 3: Maximum Number of Repeaters for the Base Stations

Base Stations	Repeaters
110 Single-Cell Base Station	6
210 Multi-Cell Base Station	3

Range of the repeaters. Each repeater has a range of up to 984 feet (300 meters) outdoors and a range of 164 feet (50 meters) indoors.

For more information to determine the number of base stations, repeaters and handsets for the coverage area, see *Cisco IP DECT Phone 6800 Series Deployment Guide*.

- The call control system must be set up and operational. Obtain the call control system information, including server addresses, user ids, and passwords. You may find [Worksheets, on page 221](#) useful when you collect the information.
- Plan the location to install each base station.
 - Determine if you need to mount the base stations on walls or on the ceiling.
We provide wall plugs and screws to mount the base station on drywall (plasterboard).
 - Ensure that there's a LAN connection close to the planned location of each base station. The Ethernet cable included with the base is 78.5 inches (200 cm) but you can use up to 3937 inches (10,000 cm) length of straight-through CAT5e cable.
 - If you don't use Power over Ethernet (PoE), install the base station near the electrical outlet located in an area that provides a good coverage for the base station. The length of the power cord with the adapter is 82 inches (208 cm).
 - Determine that the base stations are placed so that handsets can communicate. Make sure that the coverage is optimal for your users.
With the 110 Single-Cell Base Station, you can add repeaters to improve the coverage.
With the 210 Multi-Cell Base Station, you can add additional base stations or repeaters to improve coverage.
- If repeaters are required:
 - Determine if you need to mount the repeaters on walls or on the ceiling.
We provide wall plugs and screws to mount the repeater on drywall (plasterboard). See the mounting procedures for further information.

- Ensure that there's an electrical outlet close to the planned location of each repeater. The length of the power cord with the adapter is 82 inches (208 cm).
- Ensure that the repeater is within the range of the base station. Each base station has a range of up to 984 feet (300 meters) outdoors and a range of 164 feet (50 meters) indoors.

Handset Registrations

You can have up to 20 handsets registered on a 110 Single-Cell Base Station and 30 handsets registered on a 210 Multi-Cell Base Station. However, the number of active calls the base station can handle is limited by the codec.

Table 4: Number of Active Calls Supported for one 110 Single-Cell Base Station and one 210 Multi-Cell Base Station

Band	110 Single-Cell Base Station	210 Multi-Cell Base Station
Concurrent Narrowband	10	10
Concurrent Secure Narrowband	10	8
Wideband	5	5

Table 5: Number of Active Calls Supported for two 110 Single-Cell Base Stations and two 210 Multi-Cell Base Stations

Band	110 Single-Cell Base Station	210 Multi-Cell Base Station
Concurrent Narrowband	20	16
Concurrent Secure Narrowband	20	16
Wideband	10	10

Table 6: Maximum Number of Active Calls Supported for many 210 Multi-Cell Base Stations

Band	Multicell System
Concurrent Narrowband	2000
Concurrent Secure Narrowband	2000
Wideband	1250



Note If a user turns on Push to Talk, the base station may reduce the supported number of active calls.



Note If you use repeaters, the base supports less active handsets.

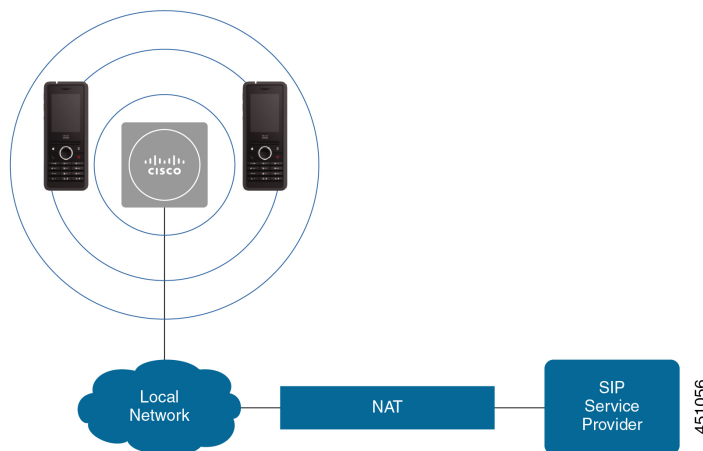
The single cell, dualcell, and multicell deployments have different maximum numbers of handsets and base stations. For more information, see [Single Cell, Dualcell, and Multicell Networks, on page 26](#).

Single Cell, Dualcell, and Multicell Networks

You can set up either a single cell system, a dualcell system, or a multicell system.

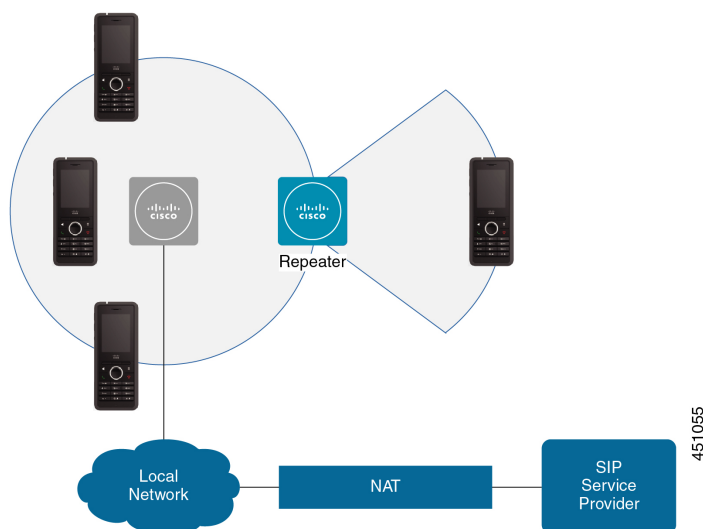
A single cell system consists of either one 110 Single-Cell Base Station with up to 20 handsets or 210 Multi-Cell Base Station with up to 30 handsets. You can also use up to 6 of the 110 Repeaters with 110 Single-Cell Base Station and up to 3 of the 110 Repeaters with 210 Multi-Cell Base Station for improved radio coverage. The following diagram shows a single cell network with one base station.

Figure 3: Single Cell Network



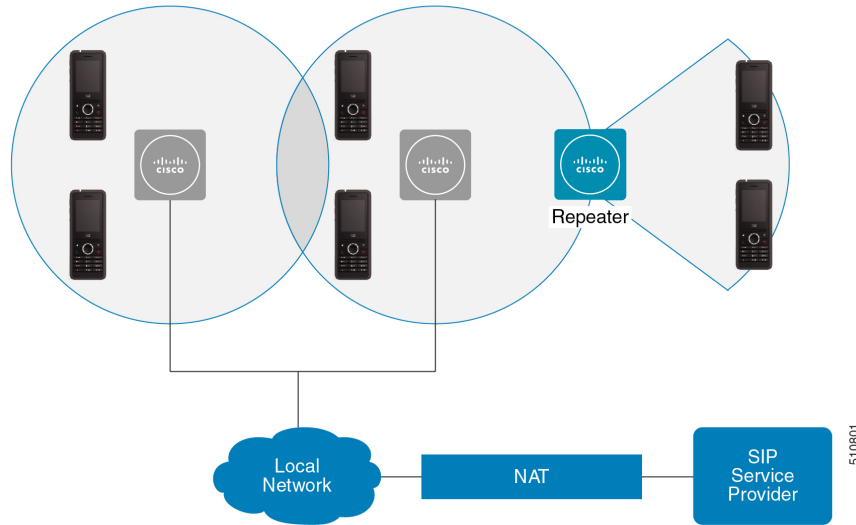
The following diagram shows a single cell base station with one repeater.

Figure 4: Single Base Station with One Repeater



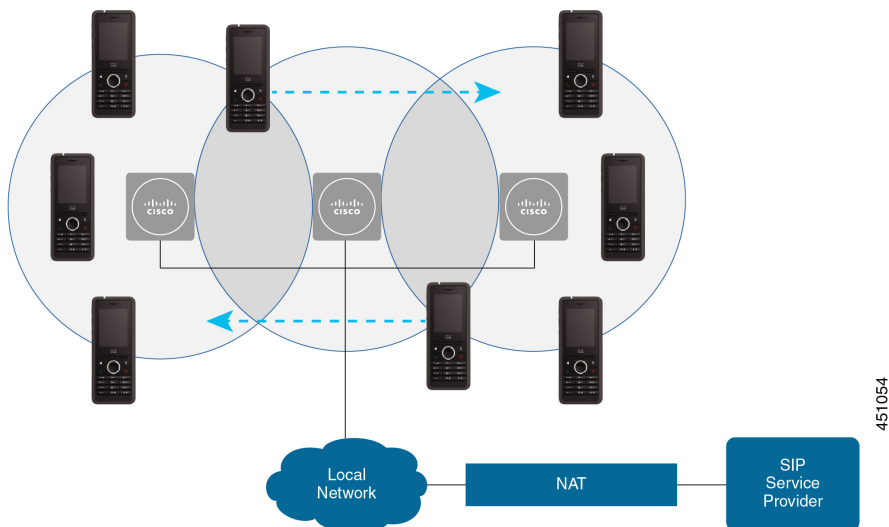
A dualcell system consists of two of the 110 Single-Cell Base Stations with up to 30 handsets. In this system, you can also use up to 12 of the 110 Repeaters for improved radio coverage. The following diagram shows two base stations with one repeater.

Figure 5: Dualcell Network



A multicell system consists of two of the 210 Multi-Cell Base Stations with up to 60 handsets or up to 250 of the 210 Multi-Cell Base Stations with up to 1000 handsets. In this system, you can also use up to 6 of the 110 Repeaters with two base stations or 100s of the 110 Repeaters with 250 of the base stations for improved radio coverage. The following diagram shows a multicell network with 3 base stations.

Figure 6: Multicell Network



Related Topics

- [Add Additional Base Stations to Make a Multicell Network \(Workflow\)](#), on page 97
- [Add an Additional Base Station to Make a Dualcell Network \(Workflow\)](#), on page 93

Base Station Package Contents

Your base station package has the following contents:

- Base station
- Base station stand
- Ethernet cable
- Regional power adapter
- USB-to-power jack cable
- Mounting screws and plugs
- Printed compliance document

If you want to mount the base station on the ceiling, you need to order a separate ceiling mount kit.

Repeater Package Contents

Your repeater package has the following contents:

- Repeater
- Repeater stand
- Regional power adapter
- USB-to-power jack cable
- Mounting screws and plugs
- Printed compliance document

If you want to mount the repeater on the ceiling, you need to order a separate ceiling mount kit.

Handset package contents

Your handset package has the following contents:

- Handset with attached belt clip. Inside the handset is the battery, with a piece of plastic over the battery contacts.



Note You need to remove the plastic over the battery contacts. For more information, see [Install the battery in the handset, on page 39](#).

- Charging cradle with attached USB cable.
- Regional power adapter for the charging cradle.
- Plastic cover to replace the belt clip on the handset.



Note Make sure that you save this small plastic cover, in case you want to use the handset without the belt clip.

- Printed compliance document.

You need the label on the box during handset registration.

Power Requirements

The base station requires one of these power sources:

- Power over Ethernet (PoE) - minimum IEEE 802.3: Power class 2 (3.84 – 6.49W)
- Power adapter specific to your region with a USB-to-power jack cable. The power adapter is plugged into an electrical outlet.

The handset is powered by a 3.7V, 1000mAh, 4.1Wh, Lithium ion battery.

The handset charger power cable plugs into the regional power adapter, and the power adapter must be plugged into an electrical outlet.

Install the Base Station

When the base station connects to the network, the LEDs light to indicate the network status:

- Green—Connected.
- Amber—Connection in progress.
- Red, flashing—Can't connect to the network.
- Red, solid—Network connection resetting.

Use this procedure to check that the base station and the network can communicate with each other, before you mount the base station in the chosen location.

Before you begin

The base station requires:

- Power over Ethernet (PoE) or a power adapter
- LAN connection
- An IP address assigned by DHCP in the network

Procedure

- Step 1** Plug one end of the Ethernet cable into the base station.

- Step 2** Plug the other end of the Ethernet cable into the LAN port.
- Step 3** If you don't use PoE, plug the power adapter into the base station and then into the electrical outlet.
- Step 4** If the LED flashes red after a few minutes, do these steps:
- Locate the **Reset** button on the bottom edge of the base station.
 - Press and hold **Reset** until the LED is a solid red.
 - Release **Reset**.

The LED should flash amber and then try to connect. If the LED doesn't light green, then the base station can't get an IP address. See [Base Station LED is Solid Red, on page 191](#) for further help.

What to do next

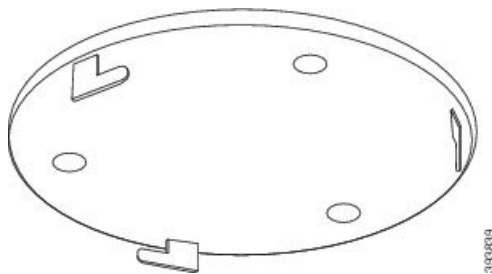
Mount the base station with one of these procedures:

- [Mount the base station or repeater on the ceiling, on page 30](#)
- [Mount the base station or repeater on a desk, on page 34](#)
- [Mount the base station or repeater on the wall, on page 35](#)

Mount the base station or repeater on the ceiling

You can mount the base station or repeater on a ceiling. They use a custom ceiling mount bracket that you can install on the ceiling. You need to order the ceiling mount bracket.

Figure 7: Ceiling Mount Bracket



The base station and repeater have a range of up to 984 feet (300 meters) outdoors and a range of 164 feet (50 meters) indoors.

In this task, the term *device* means the base station or repeater.

Before you begin

You need:

- Ceiling mount bracket
- Pencil
- Mounting hardware (screws and plugs) suitable for the ceiling construction.

- Base station: LAN connection close to the mounting location.
- Base station: If you do not use PoE, a power outlet close to the mounting location.
- Repeater: A power outlet close to the mounting location.
- Ensure that the base station can communicate with the network (see [Install the Base Station, on page 29](#)). After it can communicate and the LED is green, you can unplug the cables.

Determine the best placement, taking into account the coverage area and the building construction materials.

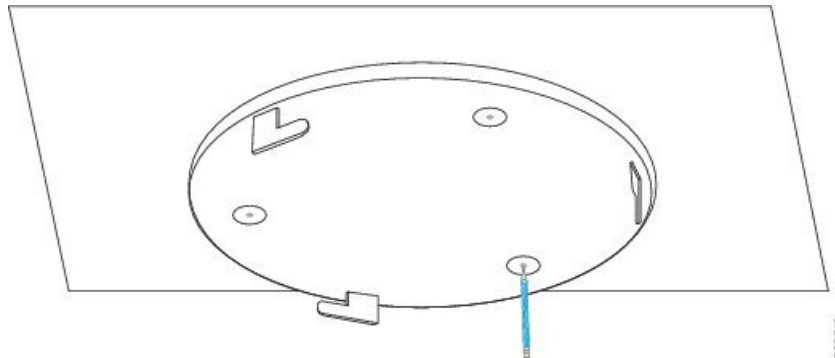
- If you have a 110 Single-Cell Base Station, you may need to add another 110 Single-Cell Base Station or additional 110 Repeaters.
- If you have a 210 Multi-Cell Base Station, you may need to add additional base stations or repeaters.

You can use the site survey tool on the handset to plan placement.

Procedure

Step 1 Hold the ceiling mount bracket in the desired location.

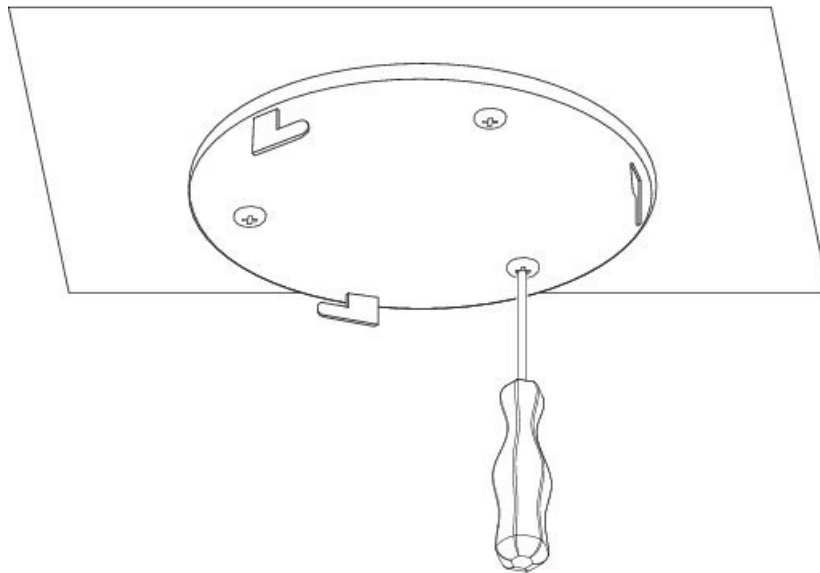
Step 2 Mark the screw placement.



Step 3 Install the plugs as described by the manufacturer.

Step 4 Install the screws through the bracket and into the plugs.

Mount the base station or repeater on the ceiling



393841

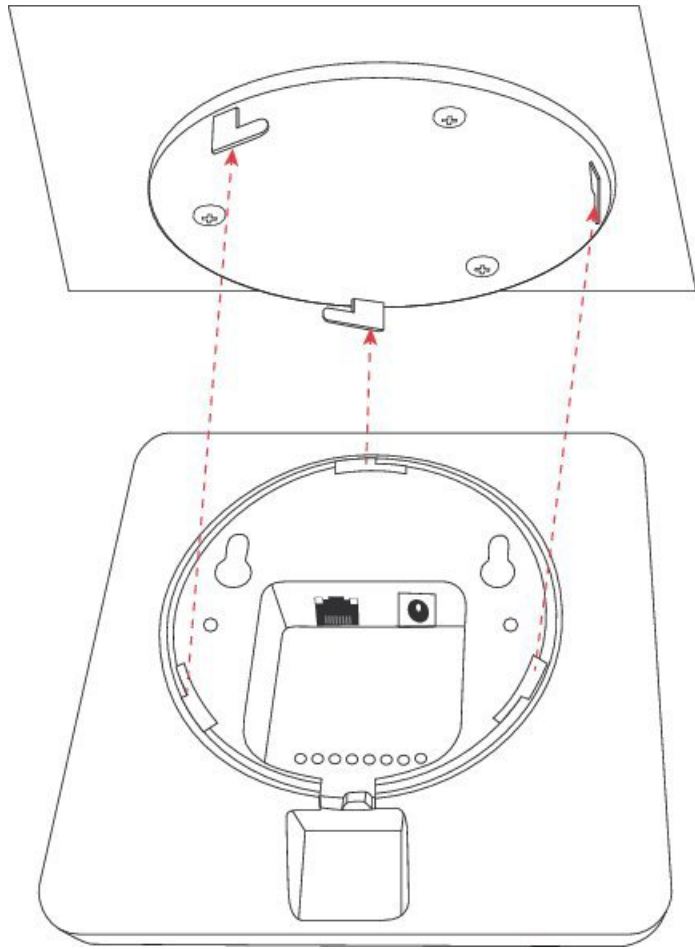
Step 5 Base station only: Connect the Ethernet cable to the device and route the cable through the slot in the device.

Step 6 Provide power to the device:

- Base station with PoE on the LAN: Additional power is not required.
- Base station without PoE: Plug the power adapter into the base station and route the cable through the slot in the base station.
- Repeater: Plug the power adapter into the repeater and route the cable through the slot in the repeater.

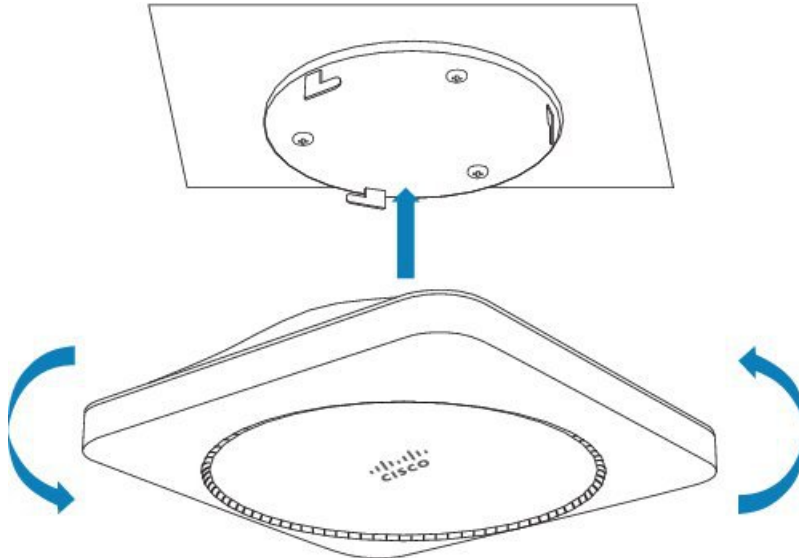
Step 7 Align the slots in the bracket with the slots in the device and turn left until the device locks in place.

This graphic shows the alignment of the mounting bracket to the base station. The back of the repeater is similar to the base station.



393843

This diagram shows the way you turn the device to lock it into the mounting bracket.



393842

Step 8 Base station only: Plug the Ethernet cable into the LAN port.

Step 9 If required, plug the power adapter into the electrical outlet.

What to do next

Do one of these:

- Base station installation:
 - Manual configuration: [Sign in to the administration web page, on page 46](#) and [Configure the Base Station, on page 50](#)
 - Automatic configuration: [Sign in to the administration web page, on page 46](#) and [Start handset registration, on page 56](#)
- Repeater installation: [Add a Repeater, on page 57](#)

Mount the base station or repeater on a desk

You can place the base station or repeater on a desk or other horizontal surface (for example, a book shelf). Select a location where the base station or repeater won't be easily knocked off.

The base station and repeater have a range of up to 984 feet (300 meters) outdoors and a range of 164 feet (50 meters) indoors.

In this task, the term *device* means the base station or repeater.

Before you begin

You need:

- Base station: LAN connection close to the mounting location.
- Base station: If you do not use PoE, a power outlet close to the mounting location.
- Repeater: A power outlet close to the mounting location.
- Ensure that the base station can communicate with the network (see [Install the Base Station, on page 29](#)). After it can communicate and the LED is green, you can unplug the cables if you haven't tested the base station in the final location.

Determine the best placement, taking into account the coverage area and the building construction materials.

- If you have a 110 Single-Cell Base Station, you may need to add another 110 Single-Cell Base Station or additional 110 Repeaters.
- If you have a 210 Multi-Cell Base Station, you may need to add additional base stations or repeaters.

You can use the site survey tool on the handset to plan placement.

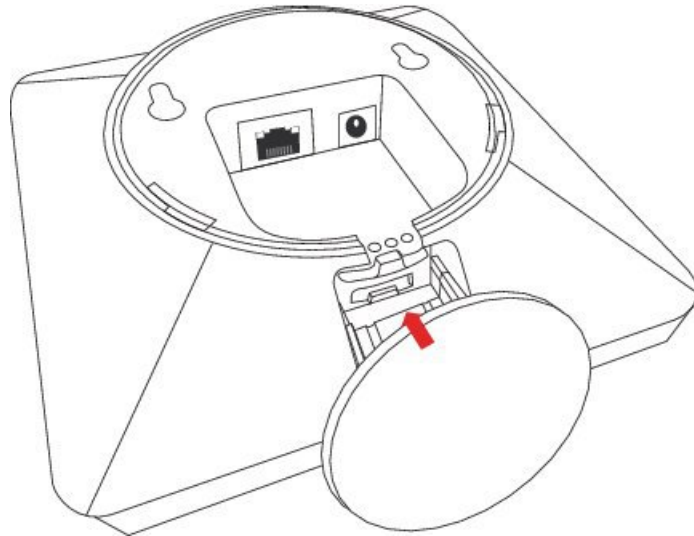
Procedure

Step 1 Base station only: Connect the Ethernet cable to the device and route the cable through the slot in the device.

- Step 2** Provide power to the device:
- Base station with PoE on the LAN: Additional power is not required.
 - Base station without PoE: Plug the power adapter into the base station and route the cable through the slot in the base station.
 - Repeater: Plug the power adapter into the repeater and route the cable through the slot in the repeater.

- Step 3** Slide the stand into the device and press it until it clicks into place.

This graphic shows the stand connection to the base station. The back of the repeater is similar to the base station.



- Step 4** Base station only: Plug the Ethernet cable into the LAN port.

- Step 5** If required, plug the power adapter into the electrical outlet.

What to do next

Do one of these:

- Base station installation:
 - Manual configuration: [Sign in to the administration web page, on page 46](#) and [Configure the Base Station, on page 50](#)
 - Automatic configuration: [Sign in to the administration web page, on page 46](#) and [Start handset registration, on page 56](#)
- Repeater installation: [Add a Repeater, on page 57](#)

Mount the base station or repeater on the wall

You can mount the base station or repeater on a wall. You put two screws into the wall and slip the base station or repeater onto the screw heads or you can use the ceiling mount bracket.

We recommend that you mount the base station or repeater as high as possible on a wall. If possible, mount it at a downward facing angle for better radio coverage.

The base station and repeater have a range of up to 984 feet (300 meters) outdoors and a range of 164 feet (50 meters) indoors.

In this task, the term *device* means the base station or repeater.

Before you begin

You need:

- Pencil
- Level
- Tape measure
- Mounting hardware (screws and wall plugs) suitable for the wall construction. You can also use the ceiling mount bracket.
- Base station: LAN connection close to the mounting location.
- Base station: If you do not use PoE, a power outlet close to the mounting location.
- Repeater: A power outlet close to the mounting location.
- Ensure that the base station can communicate with the network (see [Install the Base Station, on page 29](#)). After it can communicate and the LED is green, you can unplug the cables.

Determine the best placement, taking into account the coverage area and the building construction materials.

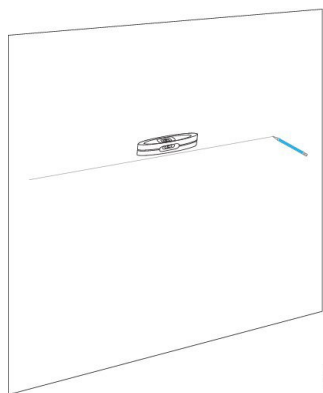
- If you have a 110 Single-Cell Base Station, you may need to add another 110 Single-Cell Base Station or additional 110 Repeaters.
- If you have a 210 Multi-Cell Base Station, you may need to add additional base stations or repeaters.

You can use the site survey tool on the handset to plan placement.

Procedure

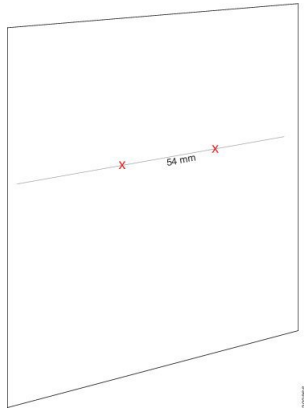
Step 1

Hold the level in the desired location and at least 2.25 inches (5.7 cm) below the ceiling, and draw a level line.



Step 2 Mark the placement of the screws.

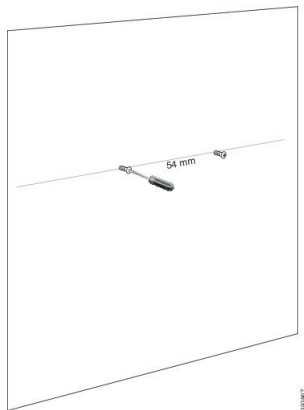
- Without the ceiling mount bracket: Mark the line so that the screws are 2.126 inches (54 mm) apart (center to center).



- With the ceiling mount bracket: Hold the bracket so that two of the holes intersect the line. Mark the holes.

Step 3 Install the wall plugs as described by the manufacturer.**Step 4** Insert the screws.

- Without the ceiling mount bracket: Screw in the screws until there is about 0.375 inches (9.52 mm) between the screw head and the wall.



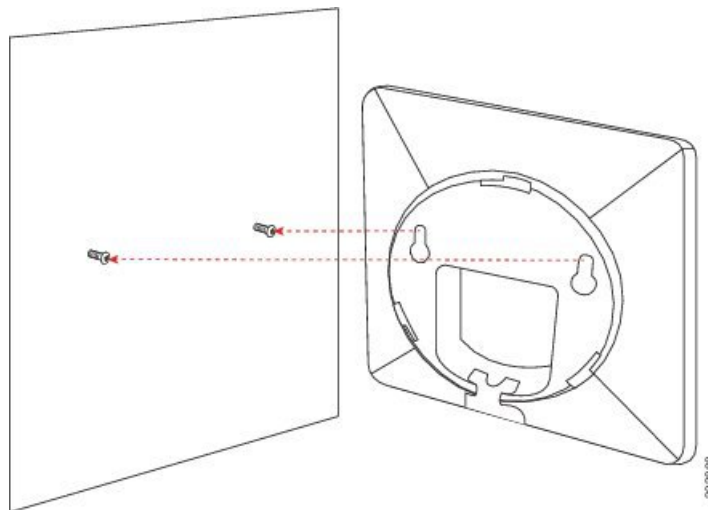
- With the ceiling mount bracket: Hold the bracket over the holes and screw in the screws until the bracket doesn't move.

Step 5 Base station only: Connect the Ethernet cable to the base station and route the cable through the slot in the base station.**Step 6** Provide power to the device:

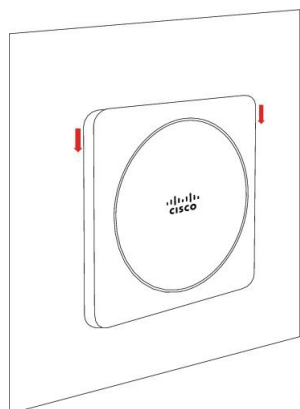
- Base station with PoE on the LAN: Additional power is not required.
- Base station without PoE: Plug the power adapter into the base station and route the cable through the slot in the base station.
- Repeater: Plug the power adapter into the repeater and route the cable through the slot in the repeater.

Step 7 Put the device on the wall.

- Without the ceiling mount bracket: This diagram shows the alignment of the screw heads and the device.



This diagram shows how you seat the device on the screw heads.



- With the ceiling mount bracket: Hold the device with the lettering in the Cisco logo on the bottom and turn slightly right. Align the slots on the underside of the device with the hooks on the bracket, press the device into the bracket, and turn it left until the device is attached.

Step 8 Base station only: Plug the Ethernet cable into the LAN port.

Step 9 If required, plug the power adapter into the electrical outlet.

What to do next

Do one of these:

- Base station installation:
 - Manual configuration: [Sign in to the administration web page, on page 46](#) and [Configure the Base Station, on page 50](#)

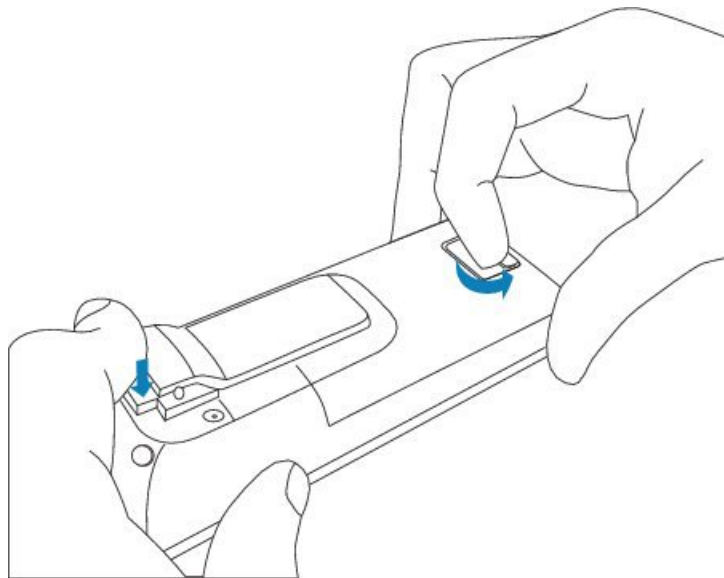
- Automatic configuration: [Sign in to the administration web page, on page 46](#) and [Start handset registration, on page 56](#)
- Repeater installation: [Add a Repeater, on page 57](#)

Install the battery in the handset

The handset battery is shipped inside the handset, but there's a plastic tab over the battery contacts. You need to remove the plastic tab.

Procedure

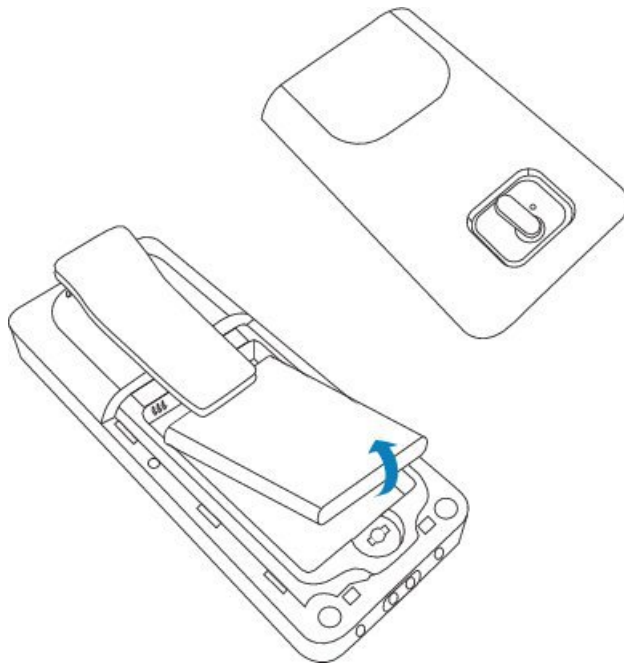
- Step 1** On the back of the handset, turn the latch counterclockwise to unlock the back, lift the clip, and lift the cover to remove the battery cover.



35081

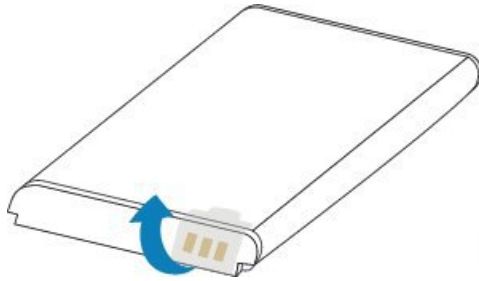
- Step 2** Remove the battery from the handset.

Install the battery in the handset



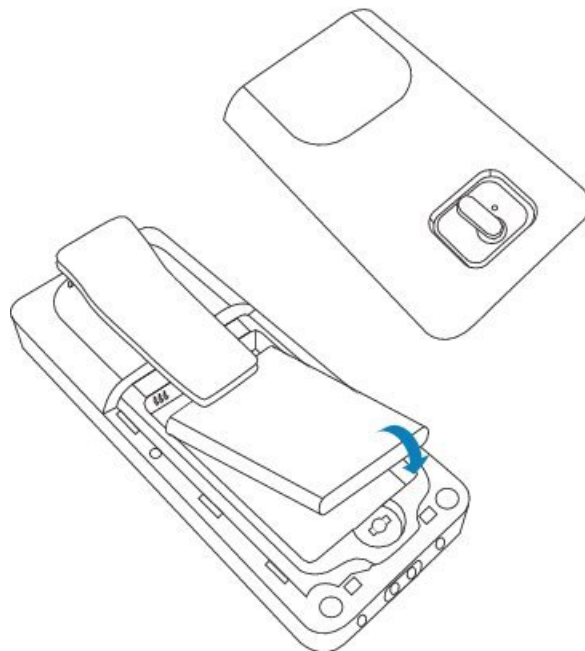
38128108

Step 3 Remove the plastic over the contacts.



3830009

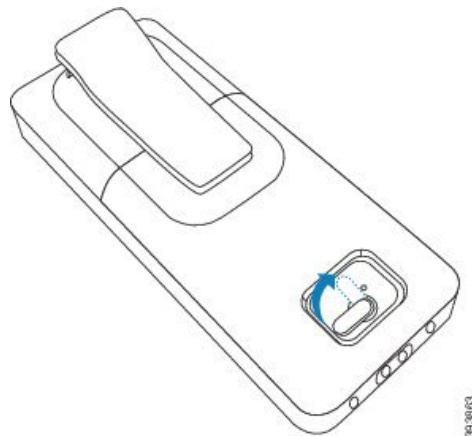
Step 4 Place the battery under the clip and drop it into the compartment.



The battery contacts are on the top left edge of the battery and the top left edge of the battery compartment. Ensure that the contacts meet and that the battery is seated in the compartment.

Note The battery fits only one way in the compartment. Don't force the battery in the wrong way in the battery compartment.

- Step 5** Replace the battery cover, make sure that the cover is closed, and turn the latch clockwise to the locked position.
- Don't force the cover closed. If it doesn't close easily, take it off and check that the battery is completely seated in the battery compartment.



What to do next

Before you use the handset, you need to charge it. See [Charge the handset battery, on page 42](#).

Set Up the charging cradle

You use the charging cradle to charge the handset. The cradle has a built-in USB cable that plugs into the power adapter. The power adapter is designed for your country's electrical outlet configuration and power rating.

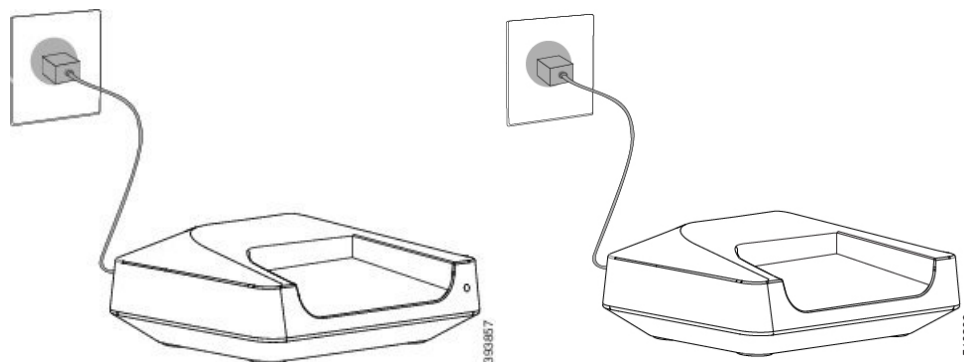
The charging cradle with 6825 Handset and 6825 Ruggedized Handset has a USB port on the side of the cradle and an LED indicator in the front of the cradle. The side USB port doesn't have supported use at this time. The LED indicator is lit when the handset is charging.

The charging cradle shipped with 6823 Handset doesn't have the USB port and the LED indicator. You can also use the charging cradle of 6825 Handset to charge this handset.

Procedure

-
- Step 1** Place the cradle on a level surface.
 - Step 2** Plug the USB connector of the power cord into the power adapter.
 - Step 3** Plug the power adapter into the electrical outlet.

Figure 8: 6825 Handset and 6823 Handset Charging Cradle



Charge the handset battery

You use the handset charger to charge the handset battery.



Note The battery comes partially charged, but you should charge it for a *minimum of 10 hours* before you use it for the first time. If you don't fully charge it, you may decrease the life of the battery.

If you remove and replace the battery from the handset, you need to fully discharge and then fully charge the battery so that the battery indicator is accurate.



Caution Charge the battery with the handset charger provided. If you use another method, you can damage the battery, the handset, or your surrounding area.

Only charge the battery in environments where the temperature is between 32°F (0°C) and 104°F (40°C).



Caution Don't charge the battery in hazardous environments or where there's explosion danger.

When you place the handset into the charger, it turns on (if not already on) and displays a message that the handset is charging. The handset screen dims and turns off at the configured time.

If the LED on the handset starts to flash, the handset is updating its firmware.

Before you begin

Set up the cradle as described in [Set Up the charging cradle, on page 42](#).

Ensure that your handset charger is plugged into the electrical outlet.

Procedure

Place the handset in the charger so that the contacts in the handset and the contacts in the charger match.

The handset beeps, screen turns on, and displays a message that the handset is charging. If this doesn't happen, remove the handset from the charger and try again.

If the handset beeps continuously while on the charger, try the troubleshooting solution available in the section [Handset Beeps Continuously While in the Charger, on page 196](#).

Charge the handset battery



CHAPTER 3

Phone Administration

- [Find the base station IP address, on page 45](#)
- [Sign in to the administration web page, on page 46](#)
- [Sign in to the User Web Page, on page 47](#)
- [Automatic Configuration, on page 47](#)
- [Manual Configuration, on page 50](#)
- [EDOS Profile and XML Parameters , on page 58](#)
- [Change the Handset Information, on page 59](#)
- [Change the Extension, on page 60](#)
- [Configure Language and Text Settings for a Handset, on page 60](#)
- [Security, on page 61](#)
- [Local Contacts Setup, on page 67](#)
- [Central Directory Setup, on page 69](#)
- [Feature Setup, on page 72](#)
- [Configure the HEBU Mode in the Base Station, on page 92](#)
- [Add an Additional Base Station to Make a Dualcell Network \(Workflow\), on page 93](#)
- [Add Additional Base Stations to Make a Multicell Network \(Workflow\), on page 97](#)
- [Add or Edit the Caller ID on IP DECT Phone, on page 99](#)
- [Configure Problem Report Tool Server, on page 101](#)
- [Export the Base Station's Status File, on page 102](#)

Find the base station IP address

You use the handset to find the IP address of the base stations in your network. The handset displays the IP address of every base station within range.

If you have access to your router administration page, you can also use it to find the IP address.


You may find the [Base Station Worksheet, on page 222](#) useful to track your configuration.

Before you begin

You need these:

- The base station needs to be connected into the network.
- A handset needs to be available with a charged battery.

Procedure

- Step 1** Press and hold **Power/End**  until the screen turns on.
- Step 2** Press **Menu** .
- Step 3** Enter ***47***.
-

Sign in to the administration web page

You use the base station web page to configure the base station and handsets.



Note Contact your service provider to determine if you connect to the base station with HTTP or HTTPS. This procedure assumes that you use HTTP.

The web page signs you out after five minutes of inactivity.

Before you begin

You need the IP address of the base station.

The base station needs to be connected to the network and the green LED lit.

Procedure

- Step 1** Find the IP address of the base station with [Find the base station IP address, on page 45](#).
- Step 2** In a browser, enter the address of the base station.

Format:

`http://<address>/main.html`

where:

- **address** is the IPv4 address of the base station.

Example

`http://xxx.xxx.xxx.xxx/main.html` where xxx.xxx.xxx.xxx is the IPv4 address.

- Step 3** Sign in to the base station as the administrator.

Note We strongly recommend that you change the default administrator and user password. For more information, see [Change the Web Page Administrator or User Password, on page 65](#).

Sign in to the User Web Page

You use the base station web page as a user to view system status and to perform limited configuration tasks.



Note Contact your service provider to determine if you connect to the base station with HTTP or HTTPS. This procedure assumes you use HTTP.

The web page signs you out after five minutes of inactivity.

Before you begin

You need the MAC of the base station.

The base station needs to be connected to the network and the green LED lit.

Procedure

Step 1 Find the IP address of the base station with [Find the base station IP address, on page 45](#).

Step 2 In a browser, enter the address of the base station.

Format:

`http://<address>/main.html`

where:

- **address** is the IPv4 address of the base station.

Example

`http://xxx.xxx.xxx.xxx/main.html` where xxx.xxx.xxx.xxx is the IPv4 address.

Step 3 Sign in to the base station as the user.

Automatic Configuration

Your system may be set up so that when you plug the base station into the LAN, it automatically looks for a server to get its configuration. The configuration server sends configuration information to set up the base station and the handsets. The handset information includes phone numbers, but doesn't map the phone numbers to a particular handset.



Note If you automatically get the configuration file from Customer Device Activation (CDA), you can only set the profile rule (<Profile_Rule>). CDA was previously known as Enablement Data Orchestration System (EDOS).

Typically, the system configuration is set up and maintained by your service provider, including multicell systems. In Firmware Release 4.8, you can configure a multicell system automatically without a primary base station. The multicell system uses one base station configuration file for all base stations.

After the base is configured, you pair the handsets with the base station to get the phone line to map to the handset:

- Temporary: You can register handsets temporarily to the base station which is in promiscuous mode and update the handsets. See these tasks:
 - [Set Up a Handset Automatically with the Username and Password, on page 48](#)
 - [Set Up a Handset Automatically with a Short Activation Code, on page 49](#)
- Automatic: You use the handset to pair with the base station. This task allocates the handset with a phone number from the configured pool of numbers. See this task:
 - [Set Up the Handset Automatically, on page 49](#)
- Manual: You manually match a handset to a phone number, then pair the handset with the base station. See these tasks:
 - [Assign handsets to users, on page 55](#)
 - [Start handset registration, on page 56](#)
 - [Connect the handset to the base station, on page 56](#)

If the handsets need more than one line (private or shared), you can use automatic configuration for the first line, then manually configure the other lines. See:

- [Add a Second Line to a Handset, on page 82](#)
- [Share a Line Between Handsets, on page 82](#)

Related Topics

[Set Up the Cisco IP DECT 6800 Series \(Workflow\), on page 16](#)

Set Up a Handset Automatically with the Username and Password

When you power on a new handset, it automatically registers itself with the base station which is in promiscuous mode. If the server requests authorization, you enter the username and password. When you need to register multiple handsets, we recommend that you power on one handset to enter the credentials. The other handsets don't receive the authorization request when they register.


The username and password can be a combination of letters, numbers, and symbols. The username can be between 1 and 24 characters and password can be between 1 and 128 characters.

If you enter a wrong username or password, an error message displays. You have three attempts to enter the correct username and password. If you fail all the attempts, the handset deregisters from the base station. Restart the handset and enter the correct username and password, or contact your administrator.

Before you begin

Your administrator or service provider gives you the username and password.

Procedure

- Step 1** Press and hold **Power/End**  until the screen turns on.
- Step 2** Enter the **Username** and **Password** in the **Sign in** screen.
- Step 3** Press **Submit**.
-

Set Up a Handset Automatically with a Short Activation Code

When you power on a new handset, it automatically registers itself with the base station which is in promiscuous mode. If the server requests the short activation code, you enter the short activation code. After the short activation code input, if the server requires authentication, you enter the username and password. When you need to register multiple handsets, we recommend that you power on one handset to enter the short activation code. The other handsets won't receive the authorization request when they register.


The short activation code starts with the # and varies between 3 to 16-digit number. The username and password can be a combination of letters, numbers, and symbols. The username can be between 1 and 24 characters and password can be between 1 and 128 characters.

If you enter a wrong short activation code, an error message screen displays. You have three attempts to enter the correct short activation code. If you fail all the attempts, the handset deregisters from the base station. Restart the handset and enter the correct short activation code, or contact your administrator.

Before you begin

Your administrator or service provider gives you the short activation code, username, and password.

Procedure

- Step 1** Press and hold **Power/End**  until the screen turns on.
- Step 2** Enter the short activation code in the **Enter activation code** screen.
- Step 3** Press **Submit**.
- Step 4** (Optional) Enter the **Username** and **Password** in the **Sign in** screen.
- Step 5** Press **Submit**.
-

Set Up the Handset Automatically

You complete steps 1 to 3 to start the deployment and either you or your users complete steps 4 and 5. If your users complete steps 4 and 5, make sure you tell them the access code available in the **AC** field.

Before you begin

[Sign in to the administration web page, on page 46](#)

Procedure

- Step 1** Click **Extensions**.
- Step 2** Make note of the content in the **AC** field.
The page also contains the list of phone numbers.
- Step 3** Click **Logout**.
- Step 4** Power on the handsets.
- Step 5** At the PIN entry message on the handset, enter the information captured in Step 2.
The handsets complete the connection to the base station and download their configuration. The handsets are assigned phone numbers from the pool of numbers available.
-

Manual Configuration

If your system does not use automatic configuration, you need to configure the base station and handsets manually.

Related Topics

[Set Up the Cisco IP DECT 6800 Series \(Workflow\)](#), on page 16

Configure the Base Station

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

The base station needs to be connected to the network and the green LED lit.

Procedure

- Step 1** Click **Servers**.
- Step 2** Click **Add Server**.
- Step 3** Set the **Server Alias** field.
- Step 4** Set the **Registrar** field to the address given by your service provider.
- Step 5** Set the **Outbound Proxy** field to the address given by your service provider.
- Step 6** Configure the remaining fields, as described in [Servers Web Page Fields, on page 114](#).
- Step 7** Click **Save**.
-

What to do next

[Set the Base Station Country, on page 51](#)

Set the Base Station Country

You must set the country and time for your base station. The base station uses the time information to control the synchronization of the multicell or dualcell system configuration. You don't require this information for the 110 Single-Cell Base Station in single cell. The handsets display the system time.



Note The base station is preprogrammed for the specific DECT frequency range for your location. The country information on this page is only used to identify the date and time zone of the system.

You can either use a network time server or set the time to the time on your PC. However, if you set up a dualcell or multicell system, you must use a network time server. During TLS authentication, this time is used for certificate time validation. If the base station doesn't receive the time from the server or the time on your PC, the certificate time validation is ignored.

If you set or change the country or time, you must reboot your base stations. A single base station can take up to 1 minute and multiple base stations in a system can take several minutes to reboot.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

The base station needs to be connected to the network and the green LED lit.

Procedure

- Step 1** Click **Country**.
 - Step 2** Choose your country in the **Select country** list.
 - Step 3** If applicable, set your **State/Region**.
 - Step 4** Select your language in the **Set Language** list.
 - Step 5** Select your time server method:
 - If you don't use a network time server, click **Time PC** to use the current time of your PC.
 - If you use a network time server, enter the address in the **Time Server** field.

An example of a network time server address is `0.us.pool.ntp.org`.
 - Step 6** Configure the remaining fields, as described in [Country Web Page Fields, on page 135](#).
 - Step 7** Click **Save and Reboot**.
-

What to do next

[Configure the Network Settings, on page 51](#)

Configure the Network Settings

The system uses DHCP by default to obtain the IP address. If DHCP isn't available, the base station uses the predefined static IP address of 169.254.xx.xx after a delay of 5 minutes. Use the handset to obtain the IP

address of the base station so that you can sign in and change the settings. You can change the predefined static IP address to another static IP address.

You may need to change these specific fields, as instructed by your service provider:

- VLAN
- Use Different SIP Ports
- RTP Port

For information on the fields, see [Network Web Page Fields, on page 122](#).

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

- Step 1** Click **Network**.
- Step 2** If your network doesn't use DHCP, set the **DHCP/Static IP** field to **Static IP**.
If you select **Static IP**, you must configure these additional fields:
- **IP Address**
 - **Subnet Mask**
 - **Default Gateway**
 - **DNS (Primary)**
 - **DNS (Secondary)**
- Step 3** If you are setting up a single-base system, set **Use Different SIP Ports** to **Enabled**.
- Step 4** Set the **RTP Port** field, as instructed by your service provider.
- Step 5** Configure the remaining network fields, as described in [Network Web Page Fields, on page 122](#).
- Step 6** Click **Save**.
-

What to do next

[Add Handsets to the Base Station, on page 54](#)

Configure the SIP Transport

For SIP messages, you can configure each extension to use:

- A specific protocol
- The protocol that the base station automatically selects

When you set up automatic selection, the base station determines the transport protocol that is based on the Name Authority Pointer (NAPTR) records on the DNS server. The base station uses the protocol with the highest priority in the records.

You can configure the SIP transport in the **Servers** web page or in the configuration file (.xml).

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

-
- Step 1** Click **Servers**.
 - Step 2** Click **Add Server**.
 - Step 3** Select any of the protocols from the list in the **SIP Transport** field.

You can also configure this parameter in the configuration file (.xml) by entering a string in this format:

```
<SIP_Transport_1_>n</SIP_Transport_1_>
```

Where, n is the protocol.

Options: UDP (default), TCP, TLS, and Auto. The option **AUTO** allows the base station to select the appropriate protocol automatically, based on the NAPTR records on the DNS server.

- Step 4** Click **Save**.

After you save the change, you must reboot the base station.

Configure the SIP Notify Authentication

When the base station receives the SIP Notify, you can configure the base station to request credentials for the SIP notification.

The base station uses TCP, UDP, or TLS to receive the SIP Notify from the system. When the SIP transport is TCP or UDP, the base station requests authorization. The credentials from the system should match the credentials of the handset extension. If the credentials don't match, the base station sends an authorization error to the system.

You can enable the authorization and enter the domain name for the system in the **Servers** web page or in the configuration file (.xml). For information about the fields, see [Servers Web Page Fields, on page 114](#).

Configure the notification fields this way in the configuration file (.xml).

```
<Auth_Resync_reboot_1_>enable</Auth_Resync_reboot_1_>  
<Reversed_Auth_Realm_1_>n</Reversed_Auth_Realm_1_>
```

Where, n indicates the domain name for the system.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

- Step 1** Click **Servers**.
 - Step 2** Set **Auth Resync reboot** to **Enabled**.
 - Step 3** In the **Reversed Auth Realm** field, enter the domain name.
 - Step 4** Click **Save**.
-

What to do next

The SIP Notify can contain the events to reset IPEI number of the handset or reboot the base station.

For more information, see [Remove the Handset Remotely, on page 177](#) or [Reboot the Base Station Remotely, on page 176](#).

Add Handsets to the Base Station

You need to configure the handsets on the base station so that they can connect and communicate.

You can add and register handsets one at a time, or you can set up multiple handsets.

- **Single handset setup:** At the end of this procedure, the base station has the information about the handset set up, but the handset is not registered to the base station and able to make calls.
- **Multiple handset setup:** At the end of this procedure, the base station is set up, but you need to complete user-specific configuration to assign the handset to the correct person.

You may find the [Handset Configuration Parameters Worksheet, on page 223](#) helpful.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

The base station needs to be connected to the network and the green LED lit.

Procedure

- Step 1** Click **Extensions**.
- Step 2** (Optional) Change the Access Code (AC).
We recommend that you change the AC to prevent users from deregistering the handset.
- Step 3** Click **Add extension**.
- Step 4** Set the **Line name**. Typically, this is the name of the user.
- Step 5** For a new handset, set **Terminal** to **New Terminal**.
- Step 6** Set the **Extension** field to the telephone number assigned to the user.
- Step 7** Set the **Authentication User Name** field to the user ID assigned to the user.
- Step 8** Set the **Authentication Password** field to the user's assigned password..
- Step 9** Set the **Display Name** field to the name you want to be displayed on the handset screen.

- Step 10** Set the **Server** field to the **Server Alias** you configured when you added the base station.
- Step 11** Configure the remaining extension fields, as described in [Add or Edit Extension Web Page Fields, on page 109](#).
- Step 12** Click **Save**.
- Step 13** (Optional) Repeat steps 2 to 10 to add more handsets.

What to do next

- If you are setting up your system one handset at a time, perform [Start handset registration, on page 56](#).
- If you are setting up multiple handsets, perform [Assign handsets to users, on page 55](#).

Assign handsets to users

When you set up multiple handsets, you need to assign each handset to a specific user. Each user has a unique phone number and voicemail box, and may have different features. You can assign individual access code to each handset with the **Terminal** web page fields or in the configuration file (.xml). You can set the access code this way in the configuration file:

```
<Subscr_Dect_Ac_Code_x_>nnnn</Subscr_Dect_Ac_Code_x_>
```

Where, x is the handset number and nnnn is the access code.

If the access code is more than 4 digits, only the first 4-digits are accepted.

To assign the handset to the user, you assign the International Portable Equipment Identity (IPEI) number of the handset to the correctly configured extension. The IPEI number for the handset is located in these locations:

- On the label of the box that contained the handset
- Under the handset battery

You may find the [Handset Configuration Parameters Worksheet, on page 223](#) helpful.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

The base station needs to be connected to the network and the green LED lit.

The handsets need to be set up as described in [Add Handsets to the Base Station, on page 54](#).

Procedure

- Step 1** Click **Extensions**.
- Step 2** Click the link in the **Extension Info** column for the handset for a specific user.
The IPEI link shows the null IPEI number FFFFFFFF.
- Step 3** In the **Terminal** page, set the **IPEI** field to the IPEI for the user's new handset.
- Step 4** Set the **AC** field.

- Step 5** (Optional) Configure the other fields, as described in [Terminal Web Page Fields, on page 112](#).
- Step 6** Click **Save**.
- Step 7** (Optional) Repeat steps 3 to 7 to set up more handsets.
-

What to do next

[Start handset registration, on page 56](#).

Start handset registration

After you have one or more handsets configured on the base station, you tell the base station to start the registration process. The base station waits to receive registration messages from the handsets to complete the communication loop.

You can register all the handsets at the same time or register them one by one.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

The base station needs to be connected to the network and the green LED lit.

- Single handset configured: The handset must be configured as described in [Add Handsets to the Base Station, on page 54](#)
- Multiple handsets configured: The handsets must be assigned to users as described in [Assign handsets to users, on page 55](#)

Procedure

- Step 1** In the **Extensions** page, check the check boxes beside the new handsets to be registered.
- Step 2** Click **Register Terminal**.
- Step 3** Check the check boxes for the handsets in the **Extension** column.
- Step 4** Click **Start SIP Registration(s)**.
-

What to do next

- On each handset, perform [Connect the handset to the base station, on page 56](#).

Connect the handset to the base station


After you configure the handset to connect to the base station, it registers. You can make calls when the registration is complete.

If your users perform this procedure, then you need to give them the procedure and the access code.

Before you begin

- The handset battery must be installed. See [Install the battery in the handset, on page 39](#).
- The handset battery must be charged. See [Charge the handset battery, on page 42](#).
- The handset must be configured on the base station as described in [Add Handsets to the Base Station, on page 54](#) and you need the base station access code (AC).

Procedure

- Step 1** Turn on the handset. See [Turn on your handset, on page 57](#).
- Step 2** Press **Menu** .
- Step 3** Select **Connectivity > Register**.
- Step 4** Press **Select**.
- Step 5** (Optional) Enter the access code in the **AC** field.
- Step 6** Press **Ok**.
-

Turn on your handset

Procedure

Press and hold **Power/End**  until the screen turns on.

Add a Repeater

If you have a 110 Single-Cell Base Station, you can extend coverage in your location with 110 Repeaters. You can have up to 6 repeaters.

If you have a 210 Multi-Cell Base Station, you can extend coverage in your location with 110 Repeaters. You can have up to 3 repeaters per base station.



Note Do not connect the repeater to power until Step 6.

When you power on a new repeater, it tries to register with the base station, and this registration needs to happen within 5 minutes.

The repeater reboots at the end of its configuration. This is normal because it has set up encrypted communications. After the reboot, it is ready to use.

You can add a repeater in the **Repeaters** web page or in configuration file (.xml).

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

-
- Step 1** Click **Repeaters**.
- Step 2** Click **Add Repeater**.
- Step 3** Set the **DECT sync mode** field.
- **Manual:** You need to manually assign parameters.
 - **Local Automatic:** The repeater detects the base signal and automatically configures.
 - **Chaining Automatically:** All base stations and repeaters send a RSSI report to the primary base station. The primary base station uses the report to create a new DECT synchronization tree with all the selected base stations and repeaters to use this setting.

In the configuration file(.xml), enter a string in this format:

```
<Repeater_Auto_Config_Mode_1_>n</Repeater_Auto_Config_Mode_1_>
```

Where, n is the value 0 (Manual), 1 (Local Automatic), or 2 (Chaining Automatically)

- Step 4** For manual configuration, select a Repeater RPN from the dropdown menu.
- Each repeater needs a unique RPN.
- Single cell systems: The base is always RPN000. The first repeater is RPN01, the second RPN02, and so on.
 - Multicell systems: The base numbers increment by 4 (RPN00, RPN04, and so on). The first repeater for the first base station is RPN01, the second RPN02. The first repeater for the second base station is RPN05, the second RPN06.
- Step 5** Click **Save**.
- Step 6** Power on the repeater.

The repeater LED will flash green (two short flashes) to indicate registration mode. When registration completes, the repeater and base station reboot to set up encrypted communications.

If you powered on the repeater before you completed step 5 and the repeater LED is red, the repeater won't register. You must follow the information in [Can't Set Up a Repeater - LED is Red, on page 192](#) to get the repeater into registration mode.

EDOS Profile and XML Parameters

The base station now allows to download complete XML config file from Cisco EDOS server. It handles EDOS in the following way:

- When the base boots up and no configuration server is set, then configuration file is downloaded from the EDOS server.

- When the base boots up and there is no DHCP options present on the network, Then the base will reach out to CDA (EDOS) and look for its configuration file. Then the base downloads it from the EDOS server:

```
https://activate.cisco.com/software/edos/callhome/rc?id=$MAU:$SN:$PN&sw=$SWVER
```

After successful download, the configuration file is parsed as any other configuration file.

- If there is no <profile_rule> set in the downloaded configuration file, then it will not store any server that provides the configuration file to the base station. In this situation, when the base restarts the EDOS config file will download again.
- If there is a <profile_rule> set in the downloaded configuration file, then it is stored in the the base memory and the base reboots. This is the current behavior of the base.

When the download fails, the base tries downloading at retry intervals (in minutes) of 30, 60, 120, 240, 480, 960, 1440 (24h) 1440, 1440. If the retry reaches to 1440 minutes, then it will continue to try and download at every 1440 minutes until the base reboots. After the base reboots (normal reboot or factory default), the base will try and download from EDOS again when no configuration server is set or no server is received from a DHCP option.



Note

- If a DHCP option such as 66, 160, 150 is present on the network, then the base will stop its process and never reaches out to CDA (EDOS).
- If download from the server provided from the DHCP fails, the EDOS configuration will not download.
- If there is no filename in the DHCP, then no address is stored in the **Configuration Server Address** (profile rule) on the base (server or filename). Hence, every time the base starts, it will first search for DBS-210-3PC.xml (DBS-110-3PC.xml for Dual cell) followed by \$MA.cfg only if there is a server mentioned in the DHCP.

Change the Handset Information

You can configure common handset information like the access code, alarm information, shared lines, and the phone book.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

The base station needs to be connected to the network and the green LED lit.

Procedure

-
- Step 1** Click **Extensions**.
 - Step 2** In the IPEI column, click the link for the phone.
 - Step 3** Configure the terminal fields, as described in [Terminal Web Page Fields, on page 112](#).
 - Step 4** Click **Save**.
-

Change the Extension

You can configure each extension on the handset. Extension information includes the user's name and password, the phone number, voicemail, and some features.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

The base station needs to be connected to the network and the green LED lit.

Procedure

-
- Step 1** Click **Extensions**.
 - Step 2** In the **Extension** column, click the link for the phone.
 - Step 3** Configure the server fields, as described in [Extensions Web Page Fields, on page 106](#).
 - Step 4** Click **Save**.
-

Configure Language and Text Settings for a Handset

You can change the language and text settings in the language file (.xml) to update these settings in the handset. Define these elements in the language file (.xml) to change the settings:

- **CustomTexts:** Define the attributes `Locked` to change the language and `Version` attribute to display the language pack version on the handset. If you set `Locked` to `enabled`, you can't change the language on your handset.
- **Language:** Define the attributes `BaseLanguage` for the current language, `Name` for the display, and `CustomInput Language` to change to another active language on the handset.
- **Text:** Define the attribute `ID` for the name of the text identifier on the handset, `Text` for the original text in the Firmware, and `CustomText` with the new text to display on the handset. You can add only one `CustomText` attribute to each text element.

The base station converts this file an accepted format and sends the file to the handset. This file updates the settings in the handset. You must place the handset on the charging station for the update. When the update begins, you can view the status or errors on the **Extensions** or **Syslog** web page. After the update, restart the handset. The handset displays the language pack version on the **Status** screen, after the restart.

You can reset these settings in the base station or handsets if the update fails, reset to different settings or return to default settings. In the base station, you can erase the filename to reset to default settings or enter a new filename to replace with new settings.

For more information to reset the handset to default settings, see the section **Reset Language and Text to Default in the Handset** in *Cisco IP DECT 6800 Series User Guide*.

You can set the language file (.xml) in the **Firmware Update** web page or in the configuration file (.xml).

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

Step 1 Click **Firmware Update**.

Step 2 Enter the filename in the **Language pack** field for each handset.

In the configuration file (.xml), enter a string in this format:

```
<Language_Rule>https://www.server.com/path/[handsettype]_[name].xml</Language_Rule>
```

Where, [handsettype]_[name] is the handset type (example, 6825) with the language filename.

Step 3 Click **Start/Save Update**.

Accept the messages that display during the update.

What to do next

Confirm the language and the text displays on your handset.

Security

The system hardware has Manufacturing Installed Certificates (MIC) already installed. But you may want to increase the security of your system.

To increase security, you need custom certificates that have been generated by a Certificate Authority (CA).

You can also increase the media security. For more information, see [Set Up the Media Security, on page 63](#).

Set Up a Device Certificate and Key Pair

The base station uses the device identity certificate and key pair when the base station acts as a server, or when the server requires client SSL authentication.

Certificates can be installed on the system in the factory or by your service provider. You can also buy your own certificates. If you buy and install your own certificates, the certificates must be in DER encoded binary X.509 (.cer) format.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Obtain a custom certificate.

Procedure

Step 1 Click **Security**.

- Step 2** In the **Device Identify** section, click **Choose Files**.
For information on field requirements, see [Security Web Page Fields, on page 137](#).
- Step 3** Select the certificate and click **OK**.
- Step 4** Click **Load**.
- Step 5** Click **Save**.
-

Set Up a Trusted Server Certificate

The base station may need a trusted server certificate to validate a certificate chain.

Certificates can be installed on the system in the factory or by your service provider. You can also buy your own certificates. If you buy and install your own certificates, the certificates must be in DER encoded binary X.509 (.cer) format.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).
Obtain a custom certificate.

Procedure

- Step 1** Click **Security**.
- Step 2** In the **Trusted Server Certificates** section, click **Choose File**.
For information on field requirements, see [Security Web Page Fields, on page 137](#).
- Step 3** Select the certificate and click **OK**.
- Step 4** Click **Load**.
- Step 5** Click **Save**.
-

Set Up a Trusted Root Certificate

The base station uses trusted root certificates from the server to authenticate the SSL handshake.

Certificates can be installed on the system in the factory or by your service provider. You can also buy your own certificates. If you buy and install your own certificates, the certificates must be in DER encoded binary X.509 (.cer) format.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).
Obtain a custom certificate.

Procedure

- Step 1** Click **Security**.
 - Step 2** In the **Trusted Root Certificates** section, click **Choose File**.
For information on field requirements, see [Security Web Page Fields, on page 137](#).
 - Step 3** Select the certificate and click **OK**.
 - Step 4** Click **Load**.
 - Step 5** (Optional) Set the **Use Only Optional Certificates** field.
 - Step 6** Click **Save**.
-

Set Up the Media Security

The base station uses the media security to protect media sessions. You can enable the media security feature and use it only if the SIP transfer protocol is TLS or the NAPTR can choose TLS as the SIP transport. You can change the media protocol to RTP or SRTP. For information about the fields, see [Servers Web Page Fields, on page 114](#).

Configure the media security in the **Servers** web page or configuration file.

You configure the feature this way in the configuration file (.xml):

```
<MediaSec_Request_n_>enabled</MediaSec_Request_n_>  
<MediasSec_Over_TLS_Only_n_>disabled</MediasSec_Over_TLS_Only_n_>
```

Where, n indicates the server number.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

- Step 1** Click **Servers**.
 - Step 2** In the **Media Security** field, select **Enabled**.
 - Step 3** In the **Media Security only for TLS** field, select **Enabled**.
 - Step 4** In the **Secure RTP** field, select **Auto**.
 - Step 5** Click **Save**.
-

Configure On-Device Firewall

You can enable stateful firewall to control incoming network traffic for Cisco IP DECT 110 Single-Cell Base Station and Cisco IP DECT 210 Multi-Cell Base Station as outgoing traffic is considered as trusted. When the firewall is enabled, incoming traffic is blocked, and silently discarded by default on all listening ports (excludes Web server, SRTP, and the ports used for inter-base communication). When you configure the base

station to unblock traffic for a specific port or range of ports, the base station does not block the traffic from the specified port range. However, incoming traffic is always blocked on the ports which are not opened.

This feature disables incoming traffic on existing ports or services. The firewall unblocks normally blocked ports. The outgoing TCP connection or UDP flow unblocks the port for return and continued traffic. The port is kept unblocked although the flow is active. The port reverts to blocked state after an interval with no activity.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

-
- Step 1** Click **Security**.
- Step 2** In the **Firewall** section, set the fields **Firewall**, **No ICMP Ping**, **No ICMP unreachable**, **No non-default TFTP**, **Trusted TCP port range**, **Trusted UDP port range**. For information on field requirements, see the table **Firewall Section Fields** in [Security Web Page Fields, on page 137](#).
- Step 3** Click **Save**.
-

Firewall Default Port Settings

The firewall is enabled by default with the settings in following table. Services listening on ports that are blocked by default, might not operate as expected, before firewall is configured with trusted port(s).

Table 7: Firewall Default Port Settings

Usage	Port	Protocol	Description	Blocked
DHCP/DHCPv6	68 / 546	UDP	To be able to get IP address.	No
RTP / SRTP	Configurable start port and range: (Default: 16384:16424)	UDP		No
Sync	Based on chain-id Port range: 49200:50000	UDP	Inter-base data synchronization (Multicast or peer-to-peer)	No
SIP	Configurable start port: (default: 5060)	UDP	Only relevant when SIP configured for UDP. In case each SIP extensions uses different port, the trusted port range will start from configured base port and next 1000 for DBS-210 / 30 for DBS-110.	No
Trel	10010:10011	UDP	Inter-base communication	No

Usage	Port	Protocol	Description	Blocked
Latency Stats	12285	UDP	Inter-base latency statistic	No
Web Server	80 / 443	TCP	Web interface	No
ICMP	-	ICMP	Diagnostic network	No
ARP	-	ARP	Address resolution protocol	No
PTP (IEEE1588)	Configurable event port: (default: 319) General port: Event port +1 (default: 320)	UDP	Radio LAN synchronization might be operational, even though the used ports are not trusted by firewall. This is due to the concept of trusting ports for outgoing traffic and keep it open for responses. However, it is still recommended to configure firewall to explicit trust the ports, if IEEE1588 LAN Sync is used instead of DECT Sync.	Yes
PTT	Control port: 42000 RTP port: 52000	UDP	Push-to-talk requires at least two handsets has enabled the feature. Base station automatic starts the service, but firewall blocks incoming data until both ports are explicit trusted	Yes

Change the Web Page Administrator or User Password

We recommend that you change the administrator and user password when you set up the system.

You can change the administrator or user password in the **Security** web page or in the configuration file (.xml).

Change the password this way in the configuration file (.xml).

- Administrator password:

```
<Admin_Password>xxxxxxx</Admin_Password>
```

Where, xxxxxxxx is the new admin password.

- User password:

```
<User_Password>xxxxxxx</User_Password>
```

Where, xxxxxxxx is the new user password.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

-
- Step 1** Click **Security**.
- Step 2** In the **Password** section, set the password fields.
For information on field requirements, see [Security Web Page Fields, on page 137](#).
- Step 3** Click **Save**.
-

Set a Password Rule

You can define the minimum password length and restrict the use of ASCII characters in the password in the **Security** web page or the configuration file (.xml).

The default password length is 4 and maximum is 127.

You configure the feature this way in the configuration file (.xml):

```
<Web_Min_Pass_Len>4</Web_Min_Pass_Len>
<Web_Pass_Constraint_To_Ascii>0</Web_Pass_Constraint_To_Ascii>
```

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

-
- Step 1** Click **Security**.
- Step 2** In the **Web password constraints** section, set these fields:
- **Minimum length (min 1)**: Enter the value for the minimum password length.
 - **Only ASCII characters**: Select **Yes** to restrict the use of characters in the password.
- Step 3** Click **Save**.
-

Set Up the Web Server for HTTP or HTTPS

To make your base station more secure, you can set it up to communicate with HTTPS only. The default is to allow HTTP or HTTPS.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

- Step 1** Click **Security**.
- Step 2** In the **Secure Web Server** section, enable or disable the requirement for HTTPS.
For information on field requirements, see [Security Web Page Fields, on page 137](#).
- Step 3** Click **Save and Reboot**.
-

Cisco Product Security Overview

This product contains cryptographic features and is subject to U.S. and local country laws that govern import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations can be found at <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>.

Local Contacts Setup

You can manage contact lists for your users. For example, you might set up a contact list for all members of a team or department. You have these options:

- Create a contact list on a handset, export it from the handset, and import it into another handset.
- Create a contact list with a text editor and import it into another handset.



Note When you import a contact list, it overwrites the existing contact list. If the user has created custom contacts, then these custom contacts are lost.

Import a Contact List

You can import a standard contact list to a handset. For example, you might set up a contact list for all members of a team or department.



Note When you import a contact list, it overwrites the existing contact list. If the user has created custom contacts, then these custom contacts are lost.

Before you begin

You can export a contact list from a handset or you can create a contact list using a text editor, such as Notepad. Other programs may insert additional information that can't be parsed correctly. Set the file extension to `.csv` or `.txt`.

The list is created in comma separated value (CSV) format. Here is an example.

```
John Smith,+2345678901,+2345678901,,+2345678911
Ann Jones,+2345678902,+2345678902,,+2345678912
Fred Brown,+2345678903,+2345678903,,
```

The format of each line of the file is

<name>,<work number>,<mobile number>,<home number>,<other number>

Where:

- **<name>** is the name of the user. The constraints to the name are:
 - Can be up to 23 characters long. Names longer than 23 characters are truncated.
 - Can't contain a comma (,).
 - Only uses the letters listed in [Supported Characters, on page 20](#).
- **<work number>,<mobile number>,<home number>,<other number>** are the phone numbers. The constraints to each number are:
 - Can be left empty. There shouldn't be a space between two commas(,). For example, if the contact doesn't have a mobile number, the line becomes **<name>,<work number>,,<home number>,<other number>**
 - Can be up to 21 digits long (including +). If the number is longer than 21 digits, the entry is discarded with no warning.
 - Can only contain these characters: +0123456789
 - Can't be a SIP URI.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Click Extensions . |
| Step 2 | In the Extension column, click the link for the phone. |
| Step 3 | In the Import Local Phonebook area, click Choose File . |
| Step 4 | Browse to the file, select it, and click OK . |
| Step 5 | Click Load . |
| Step 6 | Click OK . |
-

Export a Contact List

You can export the local contacts list from a handset.

You may find it useful to create a contact list on a handset, export it, then import it into other handsets.

Procedure

- Step 1** Click **Extensions**.
 - Step 2** In the **Extension** column, click the link for the phone.
 - Step 3** In the **Export Local Phonebook** area, click **Export**.
 - Step 4** Choose a location to save the file and click **OK**.
-

Central Directory Setup

A central directory is a directory on the handset that allows your users to look up and call people easily. The type of directory you use depends on a number of factors.

- If you administer a small network, you can do any of the following:
 - Create a local directory as a text file and upload it to the base station.
 - Create a local directory text file and save in the folder `Directory` in the server. The base station locates the file in this directory when it uses the http protocol.
-
- If your organization already has a Lightweight Directory Access Protocol (LDAP) phone directory (for example, for desk phones), you can configure the same directory on the base station.

Set Up a Text Central Directory

Before you begin

You create a text file for the directory. The text file is in the following format:

`<name> , <number>`

Where:

- `<name>` is the name of the user. The constraints to the name are:
 - Can be up to 23 characters long. Names longer than 23 characters are truncated.
 - Can't contain a comma (,).
 - Only uses these characters:
 - A–Z
 - a–z
 - 0–9
 - -

- `<number>` is the phone number. The constraints to the number are:
 - Can be up to 21 digits long (including +). If the number is longer than 21 digits, the entry is discarded with no warning.
 - Can only contain these characters: +0123456789
 - Can't be a SIP URI.



Note Don't put a space between the comma and the phone number, or the entry is discarded.

Here is a sample txt file.

```
John Smith,+2345678901
Ann Jones,+2345678902
Fred Brown,+2345678903
```

The file size must be less than 100 Kb.

You create this list with a text editor such as Notepad. Other programs may insert additional information that can't be parsed correctly. Set the file extension to `.csv` or `.txt`.



Note If you have a directory uploaded and then upload a new directory, the new directory overwrites the old directory.

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

- Step 1** Click **Central Directory**.
 - Step 2** Set the **Location** field to **Local**.
 - Step 3** Click **Save**.
 - Step 4** Locate and import the CSV file. For more information, see “Local Directory Fields” and “Import Central Directory Section Fields” tables in [Central Directory Web Page Fields, on page 141](#).
 - Step 5** Click **Save**.
-

Set Up an LDAP Central Directory

Before you begin

You need the information about the LDAP directory.

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

- Step 1** Click **Central Directory**
- Step 2** Set the **Location** field to **LDAP Server**.
- Step 3** Click **Save**.
- Step 4** Configure the LDAP fields, as described in the “LDAP Central Directory Fields” and “LDAP Central Directory: Handset Identity Section Fields” tables in [Central Directory Web Page Fields, on page 141](#).
- Step 5** Click **Save**.
-

Set Up an XML Central Directory



Note This type is currently not supported.

You can create an XML file with the directory entries and then upload the XML file to the base station.

You create this file with a text editor such as Notepad. Other programs may insert additional information that can't be parsed correctly. Set the file extension to `.xml`.



Note If you have a directory uploaded and then upload a new directory, the new directory overwrites the old directory.

Before you begin

You need to create an XML directory file. The requirements are:

- The file must have the `.xml` file extension.
- Names longer than 23 characters will be truncated to 23 characters.
- Only uses the letters listed in [Supported Characters, on page 20](#).
- Phone numbers can be up to 21 digits long, including the plus (+).
- Phone numbers can only contain `+0123456789` characters.
- Phone numbers can't be a SIP URI.
- Each `<DirectoryEntry>` tag needs a `<Name>` and `<Telephone>` tag. The Telephone tag identifies the main telephone number.

The schema for the XML file is:

```
<IPPhoneDirectory>
<DirectoryEntry>
<Name>x</Name>
<Telephone>x</Telephone>
<Office>x</Office>
<Mobile>x</Mobile>
```

```
<Fax>x</Fax>
</DirectoryEntry>
</IPPhoneDirectory>
```

You add as many `<DirectoryEntry>` tags as you need. Remember to close the tags (for example, `</DirectoryEntry>`).

Here is a sample XML file.

```
<IPPhoneDirectory>
<DirectoryEntry>
<Name>John Smith</Name>
<Telephone>1001</Telephone>
<Office>+2345678901</Office>
<Mobile>+2345678901</Mobile>
<Fax>+2345678911</Fax>
</DirectoryEntry>
<DirectoryEntry>
<Name>Ann Jones</Name>
<Telephone>1002</Telephone>
<Office>+2345678902</Office>
<Mobile>+2345678902</Mobile>
<Fax>+2345678912</Fax>
</DirectoryEntry>
<DirectoryEntry>
<Name>Fred Brown</Name>
<Telephone>1003</Telephone>
<Office>+2345678903</Office>
<Mobile>+2345678903</Mobile>
</DirectoryEntry>
</IPPhoneDirectory>
```

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

-
- Step 1** Click **Central Directory**
 - Step 2** Set the **Location** field to **XML Server**.
 - Step 3** Click **Save**.
 - Step 4** Configure the XML fields, as described in the “XML Central Directory Fields” and “XML Central Directory:Directory Name Fields” tables in [Central Directory Web Page Fields, on page 141](#).
 - Step 5** Click **Save**.
-

Feature Setup

You may need to change some of the features that impact the user experience. Make sure that you tell your users if you change any of these features.

Set Up Management Settings

The **Management** page controls some internal system features and some features that impact users.

- **Settings** area: controls some communication requirements and features.

- **Configuration** area: controls how the base and handset handle configuration changes.
- **Text Messaging** area: controls the ability for users to send and receive text messages. For more information, see [Configure Text Messaging, on page 73](#).
- **Syslog/SIP Log** area: controls the storage of system messages and other information.
- **Emergency Numbers**: controls the emergency numbers for users. For more information, see [Configure Emergency Numbers, on page 78](#).

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

-
- Step 1** Click **Management**.
- Step 2** Configure the **Settings**, **Configuration**, and **Syslog/SIP Log** fields, as described in the **Settings** table in [Management Web Page Fields, on page 126](#).
- At minimum, you must configure this field:
- **Emergency Numbers**
- Step 3** Do one of these actions:
- If you changed the **VLAN** field, click **Save and Reboot**.
 - For all other changes, click **Save**.
-

Configure Text Messaging

You may want to change the settings in the Text Messaging area in the **Management** web page. These fields control the ability of the handset to send and receive text messages. By default, text messages are disabled.

After being enabled, you can set up the system to allow messages only within your system or to allow messages to and from other systems.



Note If you enable text messaging, make sure that you tell your users.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

-
- Step 1** Click **Management**.

- Step 2** Configure the text message fields, as described in the Text Messaging table in [Management Web Page Fields, on page 126](#).
- Step 3** Click **Save**.
-

Configure Paging

You can configure a paging group to page a group of handsets. You send a page to a group of handsets in the same network.

You can add a handset to up to three paging groups. Each paging group has a unique multicast port and number. The phones within a paging group must subscribe to the same multicast IP address, port, and multicast number.

You configure the priority for the incoming page from a specific group. The priority level ranges between 0 and 3. The priority level indicates:

- 0: The incoming page places the active call on hold. The call resumes after the page is played.
- 1: The incoming page and the active call play at the same time.
- 2: The incoming page alerts with a tone. The paging plays when the active call is put on hold or the call ends.
- 3: The incoming page doesn't alert during an active call.

When multiple paging sessions occur, they are answered in chronological order. The active page must end to answer the next page. When do not disturb (DND) is enabled, the phone ignores incoming page.

The audio codec is set to G.711u.

Before you begin

- Make sure that all the handsets in a paging group are in the same multicast network.
- Access the phone administration web page.

Procedure

- Step 1** Click **Management**.
- Step 2** In the **Multiple Paging Group Parameters** section, set values for **Group (n) Paging Script** fields.

Enter a string to configure the phone to listen and initiate multicast paging. Each string can have a maximum length of 128 characters. You can add a phone to up to 3 paging groups. Enter the script in this format:

```
pggrp:multicast-address:port;[name=xxxx;]num=yyy;[listen={yes|no}]];pri=n
```

Where,

- `multicast-address`—Indicates the multicast IP address the base stations listen and receive the pages.
- `port`—Indicates the port to page. You use different ports for each paging group. Port must be between 0 and 65534, and have an equal value.
- `name=xxxx` (optional)—Indicates the name of the paging group. The maximum length of the name is 35 characters.

- `num=yyy`—Indicates a unique number to dial to access the paging group. The number is 3 or 4 digits.
- `listen={yes|no}`—Indicates whether the phone listens on the page group. Only the first two enabled groups can listen. If the field isn't defined, the default value is `no`.
- `pri=n`—Indicates the priority level of the paging. Priority level ranges 0–3.

For example:

```
pggrp=224.168.168.168:34560;name=All;num=500;listen=yes;pri=0
```

You can configure this parameter with configuration XML file (`cfg.xml`) by entering a string in this format:

```
<Group_Paging_Script_1_>pggrp=224.168.168.169:34560;name=All;num=500;listen=yes;pri=0</Group_Paging_Script_1_>
```

Step 3 Click **Save**.

Change Star Codes

The base station is set up with a series of star codes. Star codes enable users to access some functions quickly. The *Cisco IP DECT 6800 Series User Guide* contains a list of the standard star codes.



Note If you change a star code, make sure that you tell your users about the changes.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

- Step 1** Click **Star Codes**.
- Step 2** Change the star code fields, as described in [Star Codes Web Page Fields, on page 151](#).
- Step 3** Click **Save**.
-

Change Call Progress Tones

The base station is set up with a series of call progress tones. Call progress tones are tones that you hear during call setup and progression.

The default call progress tones depend on the country and region you set up for the base station. You can change the tones from the default values.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

-
- Step 1** Click **Call Progress Tones**.
 - Step 2** Configure the fields, as described in [Call Progress Tones Web Page Fields, on page 152](#).
 - Step 3** Click **Save**.
-

Set Up Call Quality Statistics to Call Server

You can send the call quality statistics to call control system after the call ends. The statistics is sent from the RTP media unit to the SIP control unit after each call ends in a Multicell system. You can view the statistics log in the **SIP Log** web page.

You enable the data collection with the **Servers** web page or in the configuration file (.xml).

Where, *n* is the server number.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

-
- Step 1** Click **Servers**.
 - Step 2** Set **Call Statistics in SIP** to **Enabled**.
Enable the call statistics this way in the configuration file (.xml):
`<Call_Statistics_In_SIP_n_>Yes</Call_Statistics_In_SIP_n_>`
 - Step 3** Click **Save**.
-

Configure Alarms

You can set up the handsets to raise an alarm when the **Emergency** button on the top of the 6825 Handset or 6825 Ruggedized Handset is pressed.



Note The 6823 Handset doesn't have an **Emergency** button.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

You can configure an alarm server in the **Management Settings** page. See [Set Up Management Settings, on page 72](#) and [Management Web Page Fields, on page 126](#). If you don't configure an alarm server, you can make calls to the defined number.

Procedure

- Step 1** Click **Alarm**.
- Step 2** Configure the alarm fields, as described in [Alarm Web Page Fields, on page 157](#).
- Step 3** Click **Save**.
-

What to do next

After you set up the alarm profile alias, go to [Change the Handset Information, on page 59](#) and assign the alarms to each handset that requires the alarm. You need to set the **Alarm Profile** and configure the **Alarm Line** and **Alarm Number** fields. After you set up alarms on a handset, you need to reboot the handset.

Configure the Location Server for Emergency Calls

You can define the HTTP Enabled Location Delivery (HELD) company ID, primary, and secondary server in the base station to receive the location information for emergency calls. The location information is sent to the Public Safety Answering Point (PSAP). The handset has a retry timeout of 120 seconds to receive the valid location token.

You can enter the HELD company ID and server details in the base station's **Management** web page or configuration file (.xml).

Configure the notification fields this way in the configuration file (.xml).

```
<Held_Company_Id>n</Held_Company_Id>, where n is the HELD company account ID.
```

```
<Held-Token_Srv1>n</Held-Token_Srv1>, where n is the primary server address.
```

```
<Held-Token_Srv2>n</Held-Token_Srv2>, where n is the secondary server address.
```

Before you begin

- Connect to the base station web page as described in *Sign in to the Administration Web Page*.
- Ensure that the network supports LLDP or CDP protocols and configured on the HELD (RedSky) server. If the network uses CDP, configure the advertisements between 5–900 seconds to get the valid token.
- Ensure that the location information server database is mapped to civic addresses.
- Ensure that both the configured dial plans and emergency numbers can exist.
- Set the company ID as a server setting and not a global setting. The extensions connected to a defined server refers to specific company ID during an emergency call.

Procedure

- Step 1** Click **Management**.
- Step 2** Set the fields in the **HELD (RedSky)** section as described in [Management Web Page Fields, on page 126](#).

Step 3 Click **Save**.

Configure Emergency Numbers

You may want to change the settings in the **Emergency Numbers** table in the **Management** web page. These fields control the numbers that are associated with emergency calls.

Make sure that your users are familiar with the emergency numbers. Your users can dial these numbers even if the keypad is locked.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

Step 1 Click **Management**.

Step 2 Configure the emergency numbers, as described in the **Emergency Numbers** table in [Management Web Page Fields, on page 126](#).

Step 3 Click **Save**.

Add or Edit Local Call Groups

You can add or edit a local call group and associate multiple handsets to a group. You register the extension to the SIP server. The registered handsets in the group can receive incoming calls within the group, make new calls, transfer calls, and make three-way conference calls.

You can create up to 32 call groups for 210 Multi-Cell Base Station and 10 call groups for 110 Single-Cell Base Station.

You add or edit the call group with the base station's **Local Call Groups** web page or in the configuration file (.xml).

You can add or edit a call group and configure the handset extension in the configuration file (.xml) by entering a string in this format:

```
<Call_Group_Sip_Account_n_x></Call_Group_Sip_Account_n_x>
```

Where, n is the call group ID and x is the extension.

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

Step 1 Click **Local Call Groups**.

The **Local Call Groups** page displays the list of the call groups.

- Step 2** Click **Add Call Group**.
The **Local Call Groups** page displays.
- Step 3** Set the fields as described in [Local Call Groups, on page 153](#).
- Step 4** Click **Save**.
-

What to do next

[Configure Handsets to the Call Group, on page 79](#)

Configure Handsets to the Call Group

After you add or edit a call group, you configure the handset to the group. You can configure the handsets to none, one, or up to 32 call groups with bit mapping. The following are the bit mapping details:

- 0x0—No Call Group is associated.
- 0x1—Call Group 1 is associated with this Terminal (bitmap 1, decimal 1).
- 0x3—Call Groups 1 and 2 are associated with this Terminal (bitmap 11, decimal 3).
- 0x6—Call Groups 2 and 3 are associated with this Terminal (bitmap 110, decimal 6).
- 0x20080001—Call Groups 1, 20 and 30 are associated with this terminal (bitmap 00100000000010000000000000000001, decimal 537395201).

You configure the handset to the call group with the base station's **Terminal** web page or in the configuration file (.xml).

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Ensure that the handset is registered to the base station.

Procedure

- Step 1** Click **Terminal**.
- Step 2** Enter the group number as the bit map number in the **Call Group(s)** field.
You can also configure this parameter in the configuration file (.xml) by entering a string in this format:
`<Subcsr_Call_Group_Subscribed_>x</Subcsr_Call_Group_Subscribed_>`
Where, x is the call group bit map number.
- Step 3** Click **Save**.
-

What to do next

[Configure Handset Intercom Function, on page 80](#)

Configure Handset Intercom Function

You can enable the intercom feature for the handset in a call group. The intercom function allows the handsets in the group to make new calls, calls within the group, transfer calls to the handsets within the group, and make three-way conference calls.

On 210 Multi-Cell Base Station, there is no call group.

You can set up the intercom with the base station's **Terminal** web page or in the configuration file (.xml).

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Ensure that the extension registers successfully with the SIP server.

Procedure

Step 1 Click **Extensions**.

Step 2 Click the link in the **Extension Info** column for the handset for a specific user. The **Terminal** page displays.

Step 3 Select the option **Enabled** in the **Intercom** field.

You can also configure this parameter in the configuration file (.xml) by entering a string in this format:

```
<Subscr_Intercom_Enabled_>x</Subscr_Intercom_Enabled_>
```

Where, x is the value to enable the intercom feature.

Step 4 Click **Save**.

Temporary Handset Addition to the Base Station

You can register a handset temporarily to the base station in promiscuous mode. The base station can be in promiscuous mode when it's factory reset. The promiscuous mode is active for 255 minutes when enabled from the **Management** web page or configuration file (.xml), or 5 minutes when you press the base station **Reset** button. You can add the unregistered handsets to the base station and update the handsets.

The base station downloads the configuration file from the CDA or DHCP server to update the handsets. If the server requests authorization, you enter the username and password with the handset. If the base station doesn't have the <profile_rule> set in the configuration file, the CDA server requests the short activation code that you enter with your handset.

The handsets deregister when the promiscuous mode times out. If any handset update is in progress, the timer is reset.

You can enable the promiscuous mode in these ways:

- Configuration file or Management web page. For more information, see [Turn On Promiscuous Mode from the Firmware, on page 81](#).
- **Reset** button. For more information, see [Turn On Promiscuous Mode with the Base Station Reset Button, on page 81](#)

Turn On Promiscuous Mode from the Firmware

You can set up promiscuous mode to enable temporary handset registration. When the base station is in promiscuous mode, the LED blinks in this order: red, amber, and green. The base station is in promiscuous mode for 255 minutes. You can register up to 30 handsets to the base station in this mode.

You set the mode this way in the configuration file (.xml):

```
<Promiscuous_mode>n</Promiscuous_mode>
```

Where, n is the time in minutes to enable the mode.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

Step 1 Click **Management**.

Step 2 Configure **Enable in (min)** to indicate the number of minutes until promiscuous mode starts.

The **Promiscuous mode timeout in** field displays the number of minutes until promiscuous mode ends. Refresh the page to view the remaining time.

For more information, see the **Promiscuous Mode** table in [Management Web Page Fields, on page 126](#)

Step 3 Click **Save**.

What to do next

- [Set Up a Handset Automatically with the Username and Password, on page 48](#)
- [Set Up a Handset Automatically with a Short Activation Code, on page 49](#)

Turn On Promiscuous Mode with the Base Station Reset Button

You enable promiscuous mode manually with the **Reset** button on the base station. If the option `Promiscuous_button_enabled` in the configuration file (.xml) is set to `No`, press the button for 15 seconds to reset the base station to the factory defaults and then enable the promiscuous mode. When you enable promiscuous mode, the base station LED flashes from red to amber in 2 seconds and then to green in 6 seconds. The base station is in promiscuous mode for 5 minutes.

Before you begin

Locate the **Reset** button on the bottom edge of the base station.

Procedure

Press and hold the **Reset** button for 6 seconds.

What to do next

- [Set Up a Handset Automatically with the Username and Password, on page 48](#)
- [Set Up a Handset Automatically with a Short Activation Code, on page 49](#)

Add a Second Line to a Handset

You can add another line to a handset.

Procedure

-
- Step 1** Click **Extensions**.
- Step 2** Identify the index number in the left column for the handset.
- Step 3** Click **Add extension**.
- Step 4** Set the **Line name**.
- Give the line a different name from other lines to avoid confusion.
- Step 5** In the **Terminal** field, select the handset for the second extension.
- For example, if you are adding the line to the handset with index 2 from step 2, then select **Terminal Idx 2**.
- Step 6** Set the **Extension** field to the telephone number assigned to the user.
- Step 7** Set the **Authentication User Name** field to the user ID assigned to the user.
- Step 8** Set the **Authentication Password** field to the user's assigned password..
- Step 9** Set the **Display Name** field to the name you want to be displayed on the handset screen.
- Step 10** Set the **Server** field to the **Server Alias** you configured when you added the base station.
- Step 11** Configure the remaining extension fields, as described in [Add or Edit Extension Web Page Fields, on page 109](#).
- Step 12** Click **Save**.
- Step 13** In the **Extensions** page, check the associated VoIP Idx box.
- Step 14** Click **Start SIP Registration(s)**.
- Step 15** Turn the handset off, then back on again.
- Step 16** Start to enter a number in the handset, and press **Line**.
- Step 17** Verify that the new extension is listed.
-

What to do next

If this extension is to be shared, see [Share a Line Between Handsets, on page 82](#)

Share a Line Between Handsets

You can set up a line to be available on two or more handsets.

On the handset, the shared line displays in the line list when the user makes a call. The user also sees an icon immediately below the handset header row. The icon displays the status of the shared line.

Procedure

- Step 1** Add the same extension to each handset. See [Add a Second Line to a Handset, on page 82](#).
For example:
- Configure the extension to **Terminal Idx 1** and register it.
 - Configure the extension to **Terminal Idx 2** and register it.
- Step 2** In the **Extensions** page, click the handset link (IPEI number) for the first handset that will share the extension.
- Step 3** In the **Shared Call Appearance Settings**, set the **Idx** to the extension to be shared.
- Step 4** Click **Save**.
- Step 5** Repeat steps 2-4 for the second handset to share the number.
-

Modification to Handset Settings

You can update alarm, various settings, and connectivity for a handset when the handset is SIP registered to a base station. You can also update the settings at once for multiple handsets in a system.

There are various options to update settings on a handset. You can download the handset settings configuration file directly from the server for example, via a browser. The server may request authentication to download the file. Once downloaded, you can do either of the following:

- Upload the file in the handset section of the base station on the **Configuration** page.
- Send a SIP NOTIFY event from the server to the base to update the handset settings.

For more details, see [Configure the Handset Server , on page 83](#) and [Update Handset Settings, on page 84](#).

Configure the Handset Server

You can define the server, protocol, and credentials to download the handset settings configuration file.

You configure server in the base station's **Management** web page or in the configuration file (.xml). The server may request login credentials to download the file.

Logs for the download is available in the **Syslog** web page.

If configuring via XML, configure the server in the base station the following way in the configuration file (.xml):

- `<Hs_Config_Server>n </Hs_Config_Server>`, where `n` is the server address to the file. If the protocol isn't specified in the URL, TFTP is used.
- `<Hs_Config_Protocol>n</Hs_Config_Protocol>`, where `n` is the protocol.
- `<Hs_Config_Server_Username>n</Hs_Config_Server_Username >`, where `n` is the username to access the server.

- `<Hs_Config_Server_Password>n</Hs_Config_Server_Password>`, where `n` is the password to access the server.

Before you begin: Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

-
- Step 1** Click **Management**.
- Step 2** Configure the fields in the section **Configuration -handset (retrieved on SIP NOTIFY request)** as described in [Management Web Page Fields, on page 126](#)
- Step 3** Click Save.
-

What to do next

[Update Handset Settings, on page 84](#)

Update Handset Settings

You use the handset settings configuration that you downloaded to update the handset settings. This file can update one handset or multiple handsets in a system.

You can update the handset settings either by uploading the handset settings configuration file in the base station's **Configuration** web page or by sending a SIP notification event `Event:check-sync-handset;hs=all` or `Event:check-sync-handset;hs=1,3,5,900,30` to the server. The handset must be SIP registered to a base station and power must be on to update the settings.

Example: `hs=all` means all registered handsets and `hs=1,3,5,900,30` means handset indexes 1,3,5,900 and 30. A maximum of 10 handset indexes can be defined.

You can view the update details in the handset's **Settings** menu or the base station's **Terminal** web page. If a base station or multiple base stations in a system restarts, the update details aren't available.



Note To know more about XML tags description used for handset settings, see *XML Tags for Handset Settings* section in *XML Reference Guide for Cisco IP DECT 6800 Series*.

The base station attempts 3 times to update the handsets. If all the attempts fail, the handset doesn't update the settings and the message saves in the syslog.

Before you begin:

- Connect to the base station web page as described in *Sign in to the Administration Web Page*.
- Ensure that the handset or handsets power is on.
- Ensure that the handset or handsets in a system is SIP registered to the base station.

Procedure

-
- Step 1** Click **Configuration**.
- Step 2** Click **Choose File** in the **Load Configuration** field to upload the handset configuration file.
- Step 3** Click **Load**.
-

Dial Plan

Dial Plan Overview

Dial plans determine how digits are interpreted and transmitted. They also determine if the number you dial is accepted or rejected. You can use a dial plan to facilitate dialing or block certain types of calls such as long distance or international.

Use the base station's **Dial Plans** web page or the configuration file (.xml) to configure dial plans.

This section includes information about dial plans, and procedures to configure the dial plans.

The Cisco IP DECT Phone has various degrees of dial plans and process the digits sequence.

When you press the speaker button on the handset, the following sequence begins:

1. The base station begins to collect the dialed digits. The interdigit timer starts to track the time that elapses between digits.
2. If the interdigit timer value is reached, or if another terminating event occurs, the base station compares the dialed digits with the dial plan.

Digit Sequences

A dial plan contains a series of digit sequences, separated by the | character. The entire collection of sequences is enclosed within parentheses. Each digit sequence within the dial plan consists of a series of elements that are individually matched to the keys that you press on the handset.

White space is ignored, but can be used for readability.

Digit Sequence	Function
0 1 2 3 4 5 6 7 8 9 * #+	Characters that represent a key that you must press on the handset.
x	Any key from 0-9 on the handset keypad.
[sequence]	<p>Characters within square brackets create a list of accepted key presses. You can press any one of the keys in the list.</p> <p>A numeric range, for example, [2-9] allows you to press any one digit from 2 through 9.</p> <p>A numeric range can include other characters. For example, [35-8*] which allows you to press 3, 5, 6, 7, 8, or *.</p>

Digit Sequence	Function
.	(period) A period indicates element repetition. The dial plan accepts 0 or more entries of the digit. For example, 01. allows you to enter 0, 01, 011, 0111, and so forth.
<dialled:substituted>	This format indicates that certain <i>dialed</i> digits are replaced by the <i>substituted</i> characters when the sequence is transmitted. The <i>dialed</i> digits can be zero to 9. For example: <8:1650>xxxxxxxx When you press 8 followed by a seven-digit number, the system automatically replaces the dialed 8 with the sequence 1650. If you dial 85550112 , the system transmits 1650550112 . If the <i>dialed</i> parameter is empty and there is a value in the <i>substituted</i> field, no digits are replaced and the <i>substituted</i> value is always attached to the transmitted string. For example: <:1>xxxxxxxxxxxx When you dial 972550112 on your handset, the number 1 is added at the beginning of the sequence; the system transmits 1972550112 .
!	(exclamation point) Prohibits a dial sequence pattern. For example: 1900xxxxxxxx! Rejects any 11-digit sequence that begins with 1900.
*xx	Allows to enter a 2-digit star code.
S0 or L0	For Interdigit Timer Master Override, enter S0 to reduce the short interdigit timer to 0 seconds, or enter L0 to reduce the long interdigit timer to 0 seconds.

Digit Sequence Examples

The following examples show digit sequences that you can enter in a dial plan.

In a complete dial plan entry, sequences are separated by a pipe character (|), and the entire set of sequences is enclosed within parentheses:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

- Extensions on your system:

```
( [1-8]xx | 9, xxxxxxx | 9, <:1>[2-9]xxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxx | 9, 1 900 xxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11 )
```

[1-8]xx Allows to dial any three-digit number that starts with the digits 1 to 8. If your system uses four-digit extensions, enter the following string: [1-8]xxx

- Local dialing with seven-digit number:


```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]111 )
```

9, xxxxxxxx After you press 9, you can enter any seven-digit number, as in a local call.

- Local dialing with 3-digit area code and a 7-digit local number:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )
```

9, [2-9]xxxxxxxxxx This example is useful where a local area code is required. After you press 9, you must enter a 10-digit number that begins with a digit 2 through 9. The system automatically inserts the 1 prefix before it transmits the number to the carrier.

- Local dialing with an automatically inserted 3-digit area code:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )
```

8, xxxxxxxx This example is useful where a local area code is required by the carrier but most calls go to one area code. After you press 8, you can enter any seven-digit number. The system automatically inserts the 1 prefix and the 212 area code before it transmits the number to the carrier.

- U.S. long-distance dialing:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )
```

9, 1 [2-9] xxxxxxxxxx After you press 9, you can enter any 11-digit number that starts with 1 and is followed by a digit 2 through 9.

- Blocked number:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )
```

9, 1 900 xxxxxxxx ! This digit sequence prevents from dialing numbers that are associated with high tolls or inappropriate content, such as 1-900 numbers in the U.S. After you press 9, if you enter a 11-digit number that starts with the digits 1900, the call is rejected.

- U.S. international dialing:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )
```

9, 011xxxxxxx After you press 9, you can enter any number that starts with 011 for an international call from the U.S.

- Informational numbers:

```
( [1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxx
| 9, 1 900 xxxxxxxx ! | 9, 011xxxxxxx. | 0 | [49]11 )
```

0 | [49]11 This example includes two-digit sequences, separated by the pipe character. The first sequence allows you to dial 0 for an operator. The second sequence allows you to enter 411 for local information or 911 for emergency services.

Acceptance and Transmission of the Dialed Digits

When you dial a series of digits, each sequence in the dial plan is tested as a possible match. The matching sequences form a set of candidate digit sequences. When you enter more digits, the set of candidates diminish until only one or none is valid. When a terminating event occurs, the server either accepts the dialed sequence and initiates a call, or else rejects the sequence as invalid. You hear the reorder (fast busy) tone if the dialed sequence is invalid.

The following table explains how terminating events are processed.

Terminating Event	Processing
Dialed digits have not matched any sequence in the dial plan. Example: Dial plan: (xx) Digits: 123 - Rejected	The number is rejected.
Pressing hook off/call and dialed digits partially matches one sequence in the dial plan. Example: Dial plan: (xx) Digits: 1 – Allowed Digits: 12 – Allowed Digits: *3 - Rejected	If the dial plan allows the partial sequence, the number is accepted and transmitted according to the dial plan.
Dialed digits exactly match one sequence in the dial plan. Example: Dial plan: (xx) Digits: 12 - Allowed	If the dial plan allows the sequence, the number is accepted and is transmitted according to the dial plan. If the dial plan blocks the sequence, the number is rejected.
A timeout occurs.	The number is rejected if the dialed digits are not matched to a digit sequence in the dial plan within the specified time. The Interdigit Long Timer applies when the dialed digits do not match any digit sequence in the dial plan. The default time is 10 seconds. The Interdigit Short Timer applies when the dialed digits match one or more candidate sequences in the dial plan. The default time is three seconds.

Terminating Event	Processing
You press the # key hook off.	<p>If # is in the dial plan, it is accepted as an input. Otherwise, the key is used as a hook off.</p> <p>If the sequence is complete and is allowed by the dial plan, the number is accepted and is transmitted according to the dial plan.</p> <p>If the sequence is incomplete or is blocked by the dial plan, the number is rejected.</p>

Interdigit Long Timer (Incomplete Entry Timer)

The Interdigit Long Timer measures the interval between dialed digits. It applies until the dialed digits don't match any digit sequences in the dial plan. Unless you enter another digit within the specified number of seconds, the entry is evaluated. If the entry is valid, the call proceeds. If the entry is invalid, the call is rejected.

Default: 10 seconds

Syntax for the Interdigit Long Timer

SYNTAX: L:s, (dial plan)

- **s:** The number of seconds. If a number isn't entered after L:, the default timer is 10 seconds. When the timer is set to 0 seconds, the call is transmitted automatically to the specified extension when the handset goes off hook.

The maximum number of timer is always one second less than the time specified in power save setting. For example, if the power save time is 60 seconds and the timer is 60 seconds (or even more,) then timer expires after the 59 seconds.

- The timer sequence appears to the left of the initial parenthesis for the dial plan.

Example for the Interdigit Long Timer

```
L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)
```

L:15 means this dial plan allows you to pause for up to 15 seconds between digits before the Interdigit Long Timer expires. This setting is helpful to sales people who read the numbers from business cards and other printed materials while dialing.

Interdigit Short Timer (Complete Entry Timer)

The Interdigit Short Timer measures the interval between dialed digits. The timer applies when the dialed digits match at least one digit sequence in the dial plan. Unless you enter another digit within the specified number of seconds, the entry is evaluated. If the entry is valid, the call proceeds. If the entry is invalid, the call is rejected.

Default: 3 seconds.

Syntax for the Interdigit Short Timer

SYNTAX 1: S:s, (dial plan)

Use this syntax to apply the new setting to the entire dial plan within the parentheses.

SYNTAX 2: *sequence Ss*

Use this syntax to apply the new setting to a particular dialing sequence.

s: The number of seconds. If a number isn't entered after S, the default timer of 3 seconds applies.

The maximum number of timer is always one second less than the time specified in power save setting. For example, if the power save time is 60 seconds and the timer is 60 seconds (or even more,) then timer expires after the 59 seconds.

Examples for the Interdigit Short Timer

To set the timer for the entire dial plan:

```
S:6, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.[1-8]xx)
```

S:6 means when you enter a number with the handset off hook, you can pause for up to 6 seconds between digits before the Interdigit Short Timer expires.

Set an instant timer for a particular sequence within the dial plan:

```
(9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxxS0 | 9,8,011xx. | 9,8,xx.[1-8]xx)
```

9,8,1[2-9]xxxxxxxxxxS0 means with the timer set to 0, the call is transmitted automatically when you dial the final digit in the sequence.

Add or Edit the Dial Plan on IP DECT Phone

You can delete digit sequences, add digit sequences, or replace the entire dial plan with a new dial plan. You can configure up to ten dial plans in the base station's **Dial Plans** web page or in the configuration file (.xml).

After you add or edit a dial plan, you must subscribe a dial plan for the handset.

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

Step 1 Click **Dial Plans**.

Step 2 Enter or edit the dial plan digits in the field **Dial Plan**.

You can also configure this parameter in the configuration file (.xml) by entering a string in this format:

```
<Dial_Plan_n_>*xx|#xx|xx.|+x.</Dial_Plan_n_>
```

Where, n is the index number of the dial plan.

Step 3 Click **Save**.

What to do next

[Configure Dial Plan for the Handset, on page 91](#)

Configure Dial Plan for the Handset

The handset subscribes to a dial plan. After you add or edit the dial plan, you must set the dial plan ID for the handset.

You can set the dial plan ID for the handset in the **Terminal** web page or in the configuration file (.xml).

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

Step 1 Click **Extensions**.

Step 2 Click the link in the **Extension Info** column for the handset for a specific user.

Step 3 In the **Terminal** page, set the **Dial Plan ID** for the handset.

You can also configure this parameter in the configuration file (.xml) by entering a string in this format:

```
<Dial_Plan_Subscription_n_> x</Dial_Plan_Subscription_n_>
```

Where, *n* is the handset index and *x* is the dial plan index.

Step 4 Click **Save**.

DTMF Wait and Pause Parameters

Speed dial, directory, extended function, and other strings configured in the phone can include *wait* (;) and *pause* (,) characters. These characters allow manual and automatic DTMF (Dual-Tone Multi-Frequency) signal transmission.

You can add the wait and pause character with speed-dial, extended function, or directory strings in this format:

```
NumberToCall(, or ;)Digits(, or ;)Digits(, or ;)Digits
```

where:

- **NumberToCall**—is the extension of the handset to call. For example, 8537777 or 14088537777.
- **, (comma)**—is a 2-second pause that is inserted for each comma in the string. The number after the , (comma) dials after a pause.

If there are multiple ,(comma) in a contact, the digits dialed is until the next ,(comma).

- **;(wait)**—indicates that the handset displays a message and waits for your confirmation.

When you manually enters the DTMF signal with the key pad, you see a message to acknowledge that the transmission of the manual entry is complete. On confirmation, the handset sends any DTMF signals defined by the *Digits*. The handset runs the next parameter. If there are no more parameters in the dial string to run, the handset exits to the main screen.

The wait prompt window does not disappear until you confirm the wait prompt. If you don't confirm, you need to end the call or the remote device ends the call.

If there are multiple ;(wait) in a contact, the digits dialed is until the next ;(wait).

- **Digits**—is the DTMF signals that your handset sends to a remote device after the call connects. The handset can't send signals other than valid DTMF signals.

Example:

95556,1234,,9876;56789#

A speed dial entry triggers the handset to dial 95556. There is a pause for 2 seconds and then dials 1234. The handset pauses for 4 seconds before it dials 9876. There is wait period before the handset displays a confirmation message to dial 56789#. After you confirm, the handset dials these digits.

Usage Guidelines

You can dial the digits any time on your handset during an active call.

The maximum length of the string is 24 digits.

If only the first part of a dial string matches a dial plan when you dial a call, the portion of the dial string that doesn't match the dial string is ignored. For example: 85377776666,,1,23

Configure the HEBU Mode in the Base Station

You can set the base station in Handset Extension by Username (HEBU) mode and register a handset. A base station can't be set in promiscuous mode and HEBU mode simultaneously. The first mode that is enabled in the base station is available.

You can enable the HEBU mode in the **Management** web page or in the configuration file (.xml).

Before you begin

- Connect to the base station web page as described in *Sign in to the Administration Web Page*.
- The base station must be connected to the network and the green LED light indicates if the base is connected.

Procedure

Step 1 Click **Management**.

Step 2 Select **Enabled** in the **Assing HS to Ext by Credentials (HEBU)** field.

You can also configure this parameter in the configuration file (.xml) by entering a string in this format:

```
<Hebu_Mode>enabled</Hebu_Mode>
```

Step 3 Click **Save**.

What to do next

[Configure the HEBU Username and Password in the Base Station, on page 93](#)

Configure the HEBU Username and Password in the Base Station

You can set the HEBU username and password in the base station to authorize the handset registration.

The username and password you enter in the login screen on your handset should match the HEBU username and password in the base station. You may need to enter the access code before this screen displays. If the username and password are valid, the handset registers with the base station. If you enter a wrong username or password in three attempts or a timeout occurs, the handset will reboot.

You can set the HEBU username and password in the **Terminal** web page or in the configuration file (.xml).

Configure the HEBU username and password way in the configuration file (.xml).

```
<Subscr_Hebu_Username_1_>Abcd</Subscr_Hebu_Username_1_>, where n is the username.
```

```
<Subscr_Hebu_Password_1_>Testpwd1@</Subscr_Hebu_Password_1_>, where n is the password.
```

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

The base station must be connected to the network and the green LED light indicates if the base station is connected.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Click Extensions . |
| Step 2 | Click the link in the Extension Info column for the handset for a specific user.
The IPEI link shows the IPEI number as FFFFFFFF. |
| Step 3 | In the Terminal page, set the fields HEBU Username and HEBU Password . |
| Step 4 | Click Save . |
-

Add an Additional Base Station to Make a Dualcell Network (Workflow)

If you have a 110 Single-Cell Base Station, you can add another 110 Single-Cell Base Station to the network if some handsets have connection problems. For example, the handset may be too far from the base station, or the base station may be too busy. When you set up two base stations, you have a dualcell system, which improves the coverage. You can also add repeaters to enhance the radio coverage.

Two 110 Single-Cell Base Station base stations in the same network form the dualcell network automatically.

For information on setting up two 210 Multi-Cell Base Station, see [Add Additional Base Stations to Make a Multicell Network \(Workflow\)](#), on page 97.



Note The 110 Single-Cell Base Station supports only single cell and dualcell configurations. The 210 Multi-Cell Base Station supports single cell, dualcell, and multicell configurations.

Here are the constraints for a dualcell system:

- Maximum number of 110 Single-Cell Base Stations in a dualcell system: 2
- Maximum number of handsets in a dualcell system is: 30

If you need to replace a base station in the system, configure the replacement timeout before you add the base station. For more information, see [Set Up Base Station Replace Timeout in Dualcell Network, on page 96](#).

The base stations synchronize their data regularly in a dualcell system. All the registered handsets can communicate with any base station in the dualcell system. If the primary base station becomes unresponsive, the other base station in the dualcell system automatically becomes the primary base station.



Note For 110 Single-Cell Base Station, the handsets register only with the primary base station.

For information about the workflow to set up a dualcell or multicell system for 210 Multi-Cell Base Station, see [Add Additional Base Stations to Make a Multicell Network \(Workflow\), on page 97](#)

Use this workflow to set up a dualcell system for 110 Single-Cell Base Station:

Before you begin

Set up the first base station and add at least one handset. For more information see, [Set Up the Cisco IP DECT 6800 Series \(Workflow\), on page 16](#).

Procedure

	Command or Action	Purpose
Step 1	Set Up a Dualcell System on the Primary Base Station, on page 94	Set up the first base station as the primary base station for a dualcell system.
Step 2	Set Up a Dualcell System on the Secondary Base Station, on page 95	Set up a secondary base station.
Step 3	(Optional) Back Up the System Configuration, on page 178	Perform a backup to save the configuration.

Set Up a Dualcell System on the Primary Base Station

For the base stations to work together, the System chain ID of both the base stations must be the same. Use this procedure to set up the existing base station for dualcell. You will do this procedure only once.



Note You can't change the System chain ID of 110 Single-Cell Base Station.

Before you begin

- The time server must be configured on the base station.
- At least one extension must be added to the base station.

Procedure

-
- Step 1** Access the existing base station web page. See [Sign in to the administration web page, on page 46](#).
- Step 2** Click **Dual cell**.
- Step 3** Make sure that **Dual cell system** is set to **Enabled** (default).
- Step 4** Set the rest of the fields as described in [Dual Cell Web Page Fields, on page 144](#).
- Step 5** Click **Save and Reboot**.
- Step 6** After the base station reboots, reconnect to the administration web page. See [Sign in to the administration web page, on page 46](#).
- Step 7** Refresh the browser until the **Home/Status** page displays Dual cell Unchained(Setup Socket) Allowed to join as Primary in the **System Information** field.
-

What to do next

[Set Up a Dualcell System on the Secondary Base Station, on page 95](#)

Set Up a Dualcell System on the Secondary Base Station

After you set up your primary base station for a dualcell system, you can add one more base station with this procedure. Both base stations in the dualcell system use the same System chain ID.

The primary base station connects with the secondary base station in 5 to 8 minutes. After the connection, the primary base station automatically synchronizes the data.



-
- Note** If you changed the administration password on the primary base station before you started the dualcell configuration, the password automatically changes on the secondary base station during the synchronization phase.
-

Before you begin

- You must complete [Set Up a Dualcell System on the Primary Base Station, on page 94](#).
- The **Home/Status** page of the primary base station must display Allowed to join as Primary in the **System Information** field.

Procedure

-
- Step 1** Set up the new base station hardware with [Install the Base Station, on page 29](#).

- Step 2** Mount the new base station with one of these options:
- [Mount the base station or repeater on the ceiling, on page 30](#)
 - [Mount the base station or repeater on a desk, on page 34](#)
 - [Mount the base station or repeater on the wall, on page 35](#)
- Step 3** Access the new base station web page. See [Sign in to the administration web page, on page 46](#) and use the MAC address of the new base station.
- Make a note of the IP address for this base station, as displayed in the browser.
- The **Home/Status** page displays `Unchained Allowed to Join as Primary`.
- Step 4** Connect to the administration web page of the new base station. See [Sign in to the administration web page, on page 46](#) and use the IP address you made note of in Step 3.
- After the successful connection, the **System Information** field displays `Keep Alive`. A new System chain ID is automatically assigned to both the base stations. The **Base Station Group** section displays the details of both the base stations.

What to do next

After you have your dualcell system set up, [Back Up the System Configuration, on page 178](#).

Set Up Base Station Replace Timeout in Dualcell Network

After you set up the dualcell system, the connections between the base stations verify every 30 seconds. If the base stations lose connection within 30 seconds, the message `Connection lost!` displays on the **Dual Cell** web page. If any of the base stations loses connection for a longer duration, the message `Replace the other base` displays on the **Home/Status** web page.

You can set the replacement timeout in the Dual Cell web page of the configuration file (`.xml`).

Set the replacement timeout this way in the configuration file (`.xml`).

```
<Dual_Cell_Replacement_Timeout>n</Dual_Cell_Replacement_Timeout>
```

Where, `n` is the time in minutes. The default time is 15 minutes and the maximum time to enter is 255 minutes.

Before you begin

- The time server must be configured on the base station.
- The data sync mode must be configured on the base station, if required.

Procedure

- Step 1** Access the base station web page as described in [Sign in to the administration web page, on page 46](#).
- Step 2** Click **Dual Cell**.
- Step 3** Enter the time in minutes in the field **Base Replacement Timeout (15-255 Min)**.
- Step 4** Click **Save and Reboot**.
- Step 5** After the base station reboots, reconnect to the administration web page. See

- Step 6** Refresh the browser until the Home/Status page displays `Dual Cell Unchained (Unchained) Allowed to Join as Secondary` in the **System Information** field.

Add Additional Base Stations to Make a Multicell Network (Workflow)

If you have a 210 Multi-Cell Base Station, you can add additional base stations to the network if some handsets have connection problems. For example, the handset may be too far from the base station, or the base station may be too busy. When you have two or more than two base stations, you have a multicell system.

The 110 Single-Cell Base Station supports a dualcell configuration and not a multicell configuration. For more information on dualcell system with 110 Single-Cell Base Station, see [Add an Additional Base Station to Make a Dualcell Network \(Workflow\)](#), on page 93.

Here are the constraints for a multicell system:

- Maximum number of 210 Multi-Cell Base Stations in a multicell system: 250
 - Maximum number of handsets with two base stations in the system: 60
- Maximum number of handsets in a multicell system: 1000

After you set up the multicell system, the base stations synchronize their data on a regular basis. All registered handsets can communicate with any base station in the multicell system. If the primary base station becomes unresponsive, another base station in the multicell system automatically becomes the primary base station.

Use this workflow to set up a multicell system.

Procedure

	Command or Action	Purpose
Step 1	Set Up the Cisco IP DECT 6800 Series (Workflow) , on page 16	Set up the first base station.
Step 2	Set Up a Multicell System on the Primary Base Station , on page 97	Set up the first base station as the primary base station for a multicell system.
Step 3	Set Up a Multicell System on a Secondary Base Station , on page 98	Set up a secondary base station. You repeat this step for each additional base station.
Step 4	(Optional) Back Up the System Configuration , on page 178	Perform a backup to save the configuration.

Set Up a Multicell System on the Primary Base Station

To make the base stations work together, you assign the same System chain ID to each base station in the multicell network. Use this procedure to set up the existing base station for multicell. You will do this procedure only once.

Before you begin

- The time server must be configured on the base station.
- At least one extension must be added to the base station.

Procedure

-
- Step 1** Access the existing base station web page. See [Sign in to the administration web page, on page 46](#).
- Step 2** Click **Multi Cell**.
- Step 3** Set **Multi cell system** to **Enabled**.
- Step 4** Set a **System chain ID**.
- We recommend that you set the **System chain ID** to a number that doesn't look like an extension number. For example, if you use 4-digit extension numbers, set the **System chain ID** to be more than 4 digits.
- Step 5** Set the rest of the fields as described in [Multi Cell Web Page Fields, on page 146](#).
- Step 6** Click **Save and Reboot**.
- Step 7** After the base station reboots, reconnect to the administration web page. See [Sign in to the administration web page, on page 46](#).
- Step 8** Refresh the browser until the **Home/Status** page displays `Multi cell Unchained (Unchained) Allowed to join as primary` in the **System Information** field.
-

What to do next

[Set Up a Multicell System on a Secondary Base Station, on page 98](#)

Set Up a Multicell System on a Secondary Base Station

After you set up your primary base station for multicell, you add one or more base stations with this procedure. All the base stations in the multicell configuration use the same System chain ID.

When the secondary base station has multicell enabled and reboots, the primary base station automatically starts the process of synchronizing the data.



Note If you changed the administration password on the primary base station before you started the multicell configuration, the password automatically changes on the secondary base station during the synchronization phase.

Before you begin

- You must complete [Set Up a Multicell System on the Primary Base Station, on page 97](#).
- The **Home/Status** page of the primary base station must display `Allowed to join as primary` in the **System Information** field.
- You need the **System chain ID** setting from the primary base station.

- You need to know the MAC address of your new base station.

Procedure

- Step 1** Set up the new base station hardware with [Install the Base Station, on page 29](#).
- Step 2** Mount the new base station with one of these options:
- [Mount the base station or repeater on the ceiling, on page 30](#)
 - [Mount the base station or repeater on a desk, on page 34](#)
 - [Mount the base station or repeater on the wall, on page 35](#)
- Step 3** Access the new base station web page. See [Sign in to the administration web page, on page 46](#) and use the MAC address of the new base station.
- Make a note of the IP address for this base station, as displayed in the browser.
- The **Home/Status** page displays `Multi cell Disabled`.
- Step 4** Click **Multi Cell**.
- Step 5** Set **Multi cell system** to **Enabled**.
- Step 6** Set the **System chain ID** to match the field on the primary base station.
- Step 7** Set the rest of the fields as described in [Multi Cell Web Page Fields, on page 146](#).
- Step 8** Click **Save and Reboot**.
- Step 9** Connect to the administration web page of the new base station. See [Sign in to the administration web page, on page 46](#) and use the new IP address you made note of in Step 3.
- Step 10** Refresh the browser until the **Home/Status** page displays `Multi cell Unchained(Initial sync 1) Allowed to join as secondary` in the **System Information** field.
- After the message displays, the base stations start to synchronize their data. It can take up to 5 minutes to synchronize the existing and new base station. You see that the message changes to `Multi cell Unchained(Initial sync 1) Secondary Waiting for Primary`,
- Step 11** Refresh the browser until the **Home/Status** page displays `Multi cell Ready (Keep Alive) Secondary` in the **System Information** field.
- If you look at the administration web page for the primary base station, the **Home/Status** page displays `Multi cell Ready (Keep Alive) Primary` in the **System Information** field.
-

What to do next

After you have your multicell system set up, [Back Up the System Configuration, on page 178](#).

Add or Edit the Caller ID on IP DECT Phone

You can add or edit the caller Identification (ID) to match the incoming call with the local contacts and display the contact details on the handset screen. The caller ID helps to facilitate accepting or rejecting certain types of calls such as long distance or international.

The caller ID string contains a series of digit sequences, which are separated by the | character. For more information about the allowed digit sequences and their functions, see *Digit Sequences*. The caller ID sequence can include up to three substitutions. You can add ten caller IDs and each caller ID can be up to 64 characters.

After you add or edit the caller ID, you must set the caller ID index for each handset.

You can add or edit the caller ID in the **Dial Plans** web page or in the configuration file (.xml).

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

Step 1 Click **Dial Plans**.

Step 2 Enter the caller ID in the **Call ID Map** field for each **Idx**.

You can also configure this parameter in the configuration file (.xml) by entering a string in this format:

```
<Call_Id_Map_n_>x</Call_Id_Map_n_>
```

Where, n is the index number of the caller ID and x is the caller ID digit substitution.

Step 3 Click **Save**.

What to do next

[Configure Caller ID for the Handset, on page 100](#)

Configure Caller ID for the Handset

You configure the caller ID index for the handset after you add or edit the caller ID.

You can set the caller ID index for the handset in the **Terminal** web page or in the configuration file (.xml).

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

Step 1 Click **Extensions**.

Step 2 Click the link in the **Extension Info** column for the handset for a specific user.

Step 3 In the **Terminal** web page, set the **Caller ID Map** for the handset.

You can also configure this parameter in the configuration file (.xml) by entering a string in this format:

```
<Call_ID_Map_Subscription_n_> x</ Call_ID_Map_Subscription_n_>
```

Where, n is the handset index and x is the caller ID index.

Step 4 Click **Save**.

Configure Problem Report Tool Server

You can configure the Problem Report Tool (PRT) server to upload system messages. In a multicell system, you must configure the PRT server in each base station in the system. You can check the status of the report upload in the **Syslog** web page.

You can request the report upload in these ways:

- You can send a SIP notification `Event: prt-gen` to the base station. If the SIP transport is TCP or UDP, the base station requests authorization. The report uploads if the credentials match between the server and the handset extension. If you disable the SIP notification, an unregistered handset can send the SIP notification `PIAxxx`, to the base station. The `PIA` is the provisioning identity account and `xxx` is the system chain ID of the base station.
- You can use an action URL `https://<xx.xx.xxx.xx>/admin/prt-gen` and define the base station IP address in the URL.
- If the base station experiences an unexpected reboot, it triggers an event to upload a report to the defined PRT server.

If you define an invalid server, the connection with the server fails, or an error occurs during the problem report generation, a message saves in the system logs.

You can configure the PRT server in the **Management** web page or in the configuration file (.xml).

Configure the notification fields this way in the configuration file (.xml).

`<PRT_upload_server>n</PRT_upload_server>`, where `n` is the protocol, domain name, and port.

`<PRT_upload_filename>n</PRT_upload_filename>`, where `n` is the filename.

`<PRT_http_header>n</PRT_http_header>`, where `n` is the header text.

`<PRT_http_header_value>n</PRT_http_header_value>`, where `n` is the value to add to the header.

Before you begin

Connect to the base station web page as described in *Sign in to the Administration Web Page*.

Procedure

Step 1 Click **Management**.

Step 2 Configure the fields as described in the **Problem Report Tool** section in [Management Web Page Fields, on page 126](#).

Step 3 Click **Save**.

Export the Base Station's Status File

You can export the `status.xml` file which contains the system information, registered device information, and the statistics for a base station. You can also export the `status.xml` files for multiple base stations in a system.

You can export the file in the following ways:

- Use the **Export Status** link on the base station's **Home/Status** web page.
- Use the options on the base station's **Diagnostics** page for the current base station or all the base stations in the system.
- Use an action URL: `<protocol>://<ip>/admin/status.xml` and define the base station IP address in the URL.
- Send the SIP notification event `prt-gen` to the registered handset. In this way, the Problem Report Tool (PRT) server will have the `status.xml` files. Ensure that the PRT server is configured correctly, see the section *Configure Problem Report Tool Server* for details.

You can export the file this way with the **Diagnostics** web page.

Before you begin

- Connect to the base station web page as described in *Sign in to the Administration Web Page*.
- Ensure that the PRT server is available.
- Ensure that the handsets are registered to the base station.

Procedure

- Step 1** Click **Diagnostics**.
- Step 2** Click **All Basestations** or **Current Basestations** in the **Logging** view of the web page.
-

What to do next

Download the file that you export.



CHAPTER 4

Headsets

- [Supported Headsets, on page 103](#)
- [Important Headset Safety Information, on page 103](#)
- [Audio Quality, on page 104](#)

Supported Headsets

You can use these types of headsets with your handset:

- Headset with a 3.5 mm audio plug
- Bluetooth LE headset



Note The 6823 Handset doesn't support Bluetooth.

Important Headset Safety Information



High Sound Pressure—Avoid listening to high volume levels for long periods to prevent possible hearing damage.

When you plug in your headset, lower the volume of the headset speaker before you put the headset on. If you remember to lower the volume before you take the headset off, the volume will start lower when you plug in your headset again.

Be aware of your surroundings. When you use your headset, it may block out important external sounds, particularly in emergencies or in noisy environments. Don't use the headset while driving. Don't leave your headset or headset cables in an area where people or pets can trip over them. Always supervise children who are near your headset or headset cables.

Audio Quality

Beyond physical, mechanical, and technical performance, the audio portion of a headset must sound good to the user and to the party on the far end. Sound quality is subjective, and we cannot guarantee the performance of any third-party headset. However, various headsets from leading headset manufacturers are reported to perform well with Cisco IP Phones.

Cisco doesn't recommend or test any third-party headsets with their products. For information about third-party headset support for Cisco products, go to the manufacturer's web site.

Cisco does test the Cisco headsets with the Cisco IP Phones. For information about Cisco Headsets and Cisco IP Phone support, see <https://www.cisco.com/c/en/us/products/collaboration-endpoints/headsets/index.html>.



CHAPTER 5

Monitoring

- [Base Station Web Pages](#), on page 105
- [View the Handset Status](#), on page 172
- [Perform a Site Survey](#), on page 173

Base Station Web Pages

You can use the base station web pages to configure the base station and to get status and statistics.

All pages are available in the admin view. To access the base station web pages in admin view, see [Sign in to the administration web page](#), on page 46.

Some pages are available in the user view. To access the base station web pages in user view, see [Sign in to the User Web Page](#), on page 47.

Unless otherwise specified, web pages display in the admin view only.

Related Topics

[Base Station Accounts](#), on page 19

Home/Status Web Page Fields

These are the fields displayed on the **Home/Status** web page of the base station. These fields are read-only.

The page displays in admin and user views.

Table 8: Home/Status Web Page Fields

Field	Description
System Information	Identifies if Dual Cell or Multi cell mode is enabled or disabled. The dual cell information only displays on the 110 Single-Cell Base Station. The multi cell information only displays on the 210 Multi-Cell Base Station.
Phone Type	Identifies the base station hardware version (IPDECT-Vx) and type (DBS-110-3PC or DBS-210-3PC).
System Type	Identifies the protocol enabled.

Field	Description
RF Band	Identifies the radio frequency (RF) band used by the system. RF bands are specific to the country where the equipment is installed.
Current local time	Identifies the current date and time of the system.
Operation time	Identifies the amount of time (in days, hours, minutes, and seconds) since the last reboot.
RFPI Address	Identifies the Radio Fixed Part Identity (RFPI) of the base station.
MAC Address	Identifies the MAC address of the base station.
IP Address	Identifies the assigned IP address of the base station.
Product Configuration	Reserved for future use.
Firmware Version	Identifies the firmware version and firmware date currently operational on the base station.
Firmware URL	Identifies the firmware update server IP address and the firmware path on the server.
Reboot	Displays entries for the last 6 reboots, with the date, time, type of reboot, and firmware version. Type of reboot includes: Normal Reboot, Forced Reboot, Power Loss, Unexpected Reboot
Base Station Status	Identifies the current status: <ul style="list-style-type: none"> • Idle—No active calls • In use—One or more active calls
SIP Identity Status on this Base Station	Identifies the extensions configured on the base station and the status of the extension: <ul style="list-style-type: none"> • OK—Handset is OK. • SIP Error—Handset has a SIP registration error.

Extensions Web Page Fields

These are the fields displayed on the **Extensions** web page of the base station.

The page displays in admin and user views.



This section is applicable to Firmware Release 4.7 and later. For the page for Firmware Release V450 and V460, see [Extensions Web Page Fields for Firmware Release V450 and V460, on page 168](#).


Table 9: General Section

Field	Contents	Description
AC	4-digit numerical code	Identifies the access code (AC) for the base station. This field can only be changed in admin view.

Table 10: Extensions Section

Field	Contents	Description
Idx	This field is read-only.	Identifies the index of the handset.
Extension, Info	This field is read-only.	<p>Indicates the International Portable Equipment Identity (IPEI), the unique DECT identification number for the handset.</p> <p>This field is a link to further information about the handset in the Terminal page.</p> <p>Below the IPEI link is the status of the handset and the extension.</p> <ul style="list-style-type: none"> • Status: a colored dot indicates the status: <ul style="list-style-type: none"> • Green: the handset is registered. Red: the handset is removed. • Extension: the name of the extension <p>The handset can appear in the list twice if it has 2 lines assigned to it.</p>
Terminal Position	This field is read-only	<p>This field is new for Firmware Release 4.7.</p> <p>Indicates RPN number and name of the base station.</p>
Terminal State	This field is read-only	<p>Indicates the current status of the handset:</p> <ul style="list-style-type: none"> • Present@RPNxx: Handset is connected to the base station RPNxx. • Detached: Handset is not connected (for example, powered off or not registered). • Located: Handset is configured to communicate with a specific base station, but can't connect. For example, this displays if the handset is powered on but the base station is powered off. • Removed: Handset has not connected to the base station (out of sight) for a specific amount of time, typically one hour.

Field	Contents	Description
Terminal Type, FW Info	This field is read-only	Identifies the handset model number and the firmware version.
FWU Progress	This field is read-only	Identifies the firmware update (FWU) state: <ul style="list-style-type: none"> • Off: Identifies that the sw version field is set to 0 in the Firmware Update page. • Initializing: Identifies that the update process is starting. • X%: Identifies the progress of the download, where X is the amount of progress (0–100). • Verifying X%: Identifies that the firmware verification is in progress before it is used. • Waiting for charger: Identifies that the firmware download is complete and the handset needs to be put into the charger to install the new firmware. • Conn.term.wait: Identifies that the repeater firmware update is complete and the repeater reset is in progress. • Complete: Identifies that the firmware update is complete. • Error: Identifies that the update was not successful. Possible reasons included: <ul style="list-style-type: none"> • File can't be found. • File isn't valid.
Battery Level	This field is read-only	This field is new for Firmware Release 4.7. Displays a snapshot of the current charge level of the handset battery. To refresh the Battery Level, RSSI, and Meas. time fields, click Refresh  to the left of the IPEI check box.
RSSI	This field is read-only.	This field is new for Firmware Release 4.7. Displays a snapshot of the Received Signal Strength Indicator (RSSI) for the connected base station or repeater. To refresh the Battery Level, RSSI, and Meas. time fields, click Refresh  to the left of the IPEI check box.

Field	Contents	Description
Measurement Time [mm:ss]	This field is read-only	This field is new for Firmware Release 4.7. Displays the time in minutes and seconds since the battery and RSSI information was captured from the handset. To refresh the Battery Level, RSSI, and Meas. time fields, click Refresh  to the left of the IPEI check box.

Add or Edit Extension Web Page Fields

These are the fields displayed on the **Add Extension** and **Edit Extension** web pages of the base station.

Table 11: Add Extension Web Page Fields

Field	Contents	Description
Line name	String Length: 1 to 7 characters	Indicates the name of the line for incoming and outgoing calls.
Terminal	Choice: <ul style="list-style-type: none"> • New Terminal • Terminal Idx 1 • Terminal Idx 2 	Identifies how to assign the extension. <ul style="list-style-type: none"> • New Terminal—A new handset is being configured. • Terminal Idx x—Identifies the index of an existing handset (from the Servers page). Used when you assign a second extension to a handset.
Extension	Digit string	Identifies the telephone number. The extension must be configured on the SIP server before the handset can make and receive calls. The extension displays on the main screen of the handset.
Authentication User Name	String	Identifies the user name assigned to the handset on the call control system. In Firmware Release 4.7, the name can be up to 128 characters long.
Authentication Password	String	Identifies the user's password on the call control system. In Firmware Release 4.7, the password can be up to 128 characters long.

Field	Contents	Description
Display Name	String	Identifies the name to display for the extension. This name displays on the main screen immediately under the date and time.
XSI Username	String	Identifies the username for the BroadSoft XSI phone book. In Firmware Release 4.7, the name can be up to 128 characters long.
XSI Password	String	Identifies the password for the BroadSoft XSI phone book. In Firmware Release 4.7, the password can be up to 128 characters long.
Mailbox Name	String	Identifies the username for the voicemail system.
Mailbox Number	Digit string Valid contents are 0–9, *, #	Identifies the number to be dialed to the voicemail system. This number needs to be enabled on the SIP server.
Server	Drop-down list of IP addresses	Identifies the SIP server address of the call control system.
Call waiting feature	Feature status: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Identifies if the call waiting is available on the phone.
BroadWorks Busy Lamp Field List URI	Feature status: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Identifies the URL to use for busy lamp field (BLF) information Only applicable to BroadSoft SIP servers.
BroadWorks Shared Call Appearance	Feature status: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Identifies if the line is shared. Only applicable to BroadSoft SIP servers. Must be enabled on the SIP server.
BroadWorks Feature Event Package	Feature status: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Identifies if the BroadWorks package is available. Features include: do not disturb, call forward (all, busy, no answer). Only applicable to BroadSoft SIP servers. Must be enabled on the SIP server.

Field	Contents	Description
Forwarding Unconditional Number (2 fields)	Digit string: <ul style="list-style-type: none"> Valid contents are 0–9, *, # Feature status: <ul style="list-style-type: none"> Disabled (default) Enabled 	Identifies: <ul style="list-style-type: none"> If call forward unconditional is available. What number to dial when an incoming call arrives for the handset. Applies to all incoming calls.
Forwarding No Answer Number (3 fields)	Digit string: <ul style="list-style-type: none"> Valid contents are 0–9, *, # Feature status: <ul style="list-style-type: none"> Disabled (default) Enabled Time in seconds: <ul style="list-style-type: none"> Range 0 to 255 Default 90 	Identifies: <ul style="list-style-type: none"> If call forward no answer is available. What number to dial when an incoming call arrives for the handset and isn't answered. How long to wait, in seconds, before the call is considered unanswered. Applies to all unanswered calls.
Forwarding on Busy Number (2 fields)	<ul style="list-style-type: none"> Valid contents are 0–9, *, # Feature status: <ul style="list-style-type: none"> Disabled (default) Enabled 	Identifies: <ul style="list-style-type: none"> If call forward busy is available. What number to dial when the handset is busy. A handset is busy when it already has 2 calls (one active and one on hold). Applies when the handset is on an existing call.
Reject anonymous calls	Values: <ul style="list-style-type: none"> Disabled (default) Enabled 	Indicates if the handset should reject calls that don't have a caller IC.
Hide Number	Values: <ul style="list-style-type: none"> Off On for next call Always on 	Indicates if the handset can make a call without the caller ID.

Field	Contents	Description
Do Not Disturb	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the user can turn on do not disturb (DND) mode.


Terminal Web Page Fields

These are the fields displayed on the **Terminal** web page of the base station. You click on the IPEI number of the handset in the **Extensions** page to see this screen.

The page displays in admin and user views. Not all fields are available in user view.

This section is applicable to Firmware Release 4.7. For the page for Firmware Release V450 and V460, see [Terminal Web Page Fields for Firmware Release V450 and V460, on page 170](#).

Table 12: Terminal Web Page Fields

Field	Contents	Description
IPEI	10 character string	Identifies the International Portable Equipment Identity (IPEI) of the handset. Each handset has a unique IPEI number, and the number is displayed on the label under the handset battery and on the label of the handset box. If you change this field, the handset deregisters.
Paired Terminal	Values: <ul style="list-style-type: none"> • No Paired Terminal • Handset ID 	Identifies the terminal paired with the handset.
AC	4 digit code	Identifies the access code that was used to register the handset. After the handset registers, this code is not used. Note We recommend that you change this from the default when you start to set up your system to increase security.
Alarm Line	Values: <ul style="list-style-type: none"> • No Alarm Line Selected • Telephone number 	Identifies the line to be used for alarm calls.
Alarm Number	Phone number	Identifies the number to be dialed when a user presses and holds the Emergency  button on the handset for 3 seconds or more.

Field	Contents	Description
Dial Plan ID	Values: 1 to 10	Admin view only This field is new for Firmware Release 5.1(1). Identifies the index of the dial plan, configured in Dial Plans Web Page Fields, on page 153 .
HEBU Username	String up to 40 characters	This field is new for Firmware Release 5.1(1). Indicates the username for the handset registration in HEBU mode.
HEBU Password	String up to 40 characters	This field is new for Firmware Release 5.1(1). Indicates the password for the handset registration in the HEBU mode.
Extensions		
VoIP Idx	This field is read-only.	Identifies the index of the handset.
Extension	This field is read-only.	Identifies the configured extension name. The extension must be configured on the SIP server before the handset can make and receive calls. Admin view only: This field is a link to further information about the handset in the Edit extension page.
Display Name	This field is read-only.	Identifies the telephone number. This information displays on the main screen of the handset.
Server	This field is read-only.	Identifies the SIP server address of the call control system.
Server Alias	This field is read-only.	Identifies the name of the call control system.
State	This field is read-only.	Identifies the SIP registration state. If the field is empty, the handset isn't SIP-registered.
Beacon Settings		
Receive Mode		Admin view only Reserved for future use.
Transmit Interval		Admin view only Reserved for future use.
Alarm Profiles		

Field	Contents	Description
Profile 0 to 7		Admin view only Indicates the list of alarms.
Alarm Type	Name of the alarm	Admin view only Indicates which alarm type is configured for the particular profile. When no alarms are configured, the field displays <code>Not configured</code> .
Alarm Type check box	Check box (default unchecked)	Admin view only Identifies the alarm type that is active on the handset.
Shared Call Appearance Settings		
Idx 1 to 8		Admin view only Index of the extensions
Extension	Extension number	Admin view only Identifies the handset lines that support Shared Call Appearances. When no lines support the feature, the field displays <code>Not configured</code> .
Import Local Phonebook	Filename	Used to upload a local directory from a computer to the phone in comma separated value (CSV) format. For more information, see Local Contacts Setup, on page 67 .
Export Local Phonebook		Used to export a local directory from a phone to the computer in CSV format. For more information, see Local Contacts Setup, on page 67 .

Servers Web Page Fields

These are the fields displayed on the **Servers** web page of the base station or on the **Add Server** web page when you start the setup.

Table 13: Servers Web Page Fields

Field	Contents	Description
Server Alias	String	Identifies the short name for the call control server.

Field	Contents	Description
NAT Adaption	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates how SIP messages are handled in a SIP-aware router. <ul style="list-style-type: none"> • Enabled—When the system receives a SIP response to a REGISTER request with a <i>Via</i> header that includes the <i>received</i> parameter, the base adapts its contact information to the IP address from the received parameter. For example, “Via: SIP/2.0/UDP 10.1.1.1:4540;received=68.44.20.1”. The base issues another REGISTER request with the updated contact information. • Disabled—The received parameter is ignored.
Registrar	IP address, DNS address, or URL	Identifies the SIP Server (call control system) proxy server. The port number in the address is optional.
Outbound Proxy	IP address, DNS address or URL	Identifies the Session Border Controller or SIP server outbound proxy. Set the outbound proxy to the address and port of the private NAT gateway, so that SIP messages are sent through the NAT gateway.
Enable Conference Server	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Controls the use of the external conference server. <ul style="list-style-type: none"> • Disabled: No external conference server is configured. When the user starts a conference, the handset starts a conference with the internal three-party conference feature. • Enabled: An external conference server is configured. When the user starts a conference, the handset starts a conference on the conference server configured in the Conference Server field.
Conference Server	IP address	Identifies the IP address of the service provider's conference server, if available.
Call Log Server	IP address	Indicates the XSI Call Log Server. When set, the handset logs calls on the call log server. If left blank, the handset uses the local call log.
Reregistration time (s)	Integer Default: 3600	Indicates the time in seconds for a valid SIP registration and represents the maximum time between SIP registrations for the SIP account. <p>Note We recommend that you don't set this below 60 seconds.</p>

Field	Contents	Description
Registration Retry Interval	Integer Default: 30	Identifies the time in seconds to wait before the handset retries registration after a failed registration. This is used when the registration failure message is <code>Retry Reg RSC</code> .
Registration Retry Interval High Rnd	Integer Default: 30	This field is new in Firmware Release 5.1. Identifies the high value of random interval to wait before registration retry after failing during the last registration. If the value of this field is greater than the value in Registration Retry Interval field, a random value between these two values is chosen.
Registration Retry Interval Long	Integer Default: 1200	Identifies the time in seconds to wait before the handset retries registration after a failed registration. This is used when the registration failure message is something other than <code>Retry Reg RSC</code> . If the field is set to 0, the handset doesn't retry the registration. This field needs to be a larger interval than the value in Registration Retry Interval .
Registration Retry Long Interval High Rnd	Integer Default: 1200	This field is new in Firmware Release 5.1. Indicates the high value of random long interval to wait before registration long interval retry. If the value of this field is greater than the value in the field <code>RegistrationRetry Interval Long</code> , a random value between these two values is chosen. If the value in this field is less than or equal to the value in the field <code>Registration Retry Interval Long</code> , the value in the field <code>Registration Retry Interval Long</code> is chosen. The allowed value is from 1 to 2147483.
Registration Retry RSC		Identifies the Response SIP Code (RSC) that triggers a retry. You can set up to 4 comma-delimited values and use the wildcard character (?). For example, you could enter <code>5??, 6??</code> .
Deregister After Failback	Values <ul style="list-style-type: none"> • Disabled (default) • Enabled 	This field is new in Firmware Release 5.0. Indicates if the failover should start when the time expires and the corresponding SIP transaction fails.
Supported 100rel	Values <ul style="list-style-type: none"> • Disabled • Enabled (default) 	This field is new in Firmware Release 5.0.

Field	Contents	Description
SIP Session Timers	Values <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates the keep alive mechanism for calls. This specifies the maximum time between session refresh signals. When the phone is on a call and it doesn't send a session refresh signal in the configured time, the call terminates. If disabled, session timers aren't used.
Session Timer Value(s)	Integer Default: 1800	Indicates the length of time in seconds for the SIP Session Timer.
SIP Transport	Values: <ul style="list-style-type: none"> • UDP (default) • TCP • TLS • Auto 	Indicates the protocol for SIP transport. <ul style="list-style-type: none"> • UDP: Enforce the use of SIP over UDP. If an NAPTR lookup succeeds and returns entries, then only SIP/UDP entries are used. • TCP: Enforce the use of SIP over TCP. If an NAPTR lookup succeeds and returns entries, then only SIP/TCP entries are used. • TLS: Enforce the use of TLS over TCP. If an NAPTR lookup succeeds and returns entries, then only SIPS/TCP entries are used. • Auto: A NAPTR lookup must succeed. The order (normally TLS, TCP, UDP) of the entries from the DNS NAPTR lookup is taken into account. TLS, TCP, and UDP are all accepted. SCTP is not accepted.
Signal TCP Source Port	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates if the source port needs to be explicitly signaled in the SIP messages. When SIP Transport is set to TCP or TLS, a connection is established for each SIP extension. The source port of the connection is chosen by the TCP stack, and the local SIP port parameter is not used.
Use One TCP Connection per SIP Extension	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates how TCP or TLS connections are used. When TCP or TLS is used for SIP transport, there are two choices for connections: <ul style="list-style-type: none"> • Disabled—Each base station has a single TCP or TLS connection that the handsets share. • Enabled—Each line has an individual TCP or TLS connection. <p>Note You should set this field to Enabled to handle multiple responses to a NAPTR or SRV lookup.</p>

Field	Contents	Description
RTP from own base station	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates that the RTP stream is sent. This field displays only on the Cisco IP DECT 210 Multi-Cell Base Station. <ul style="list-style-type: none"> • Disabled—The RTP stream is sent from the base station associated with the handset. • Enabled—The RTP stream is sent from the base station where the SIP registration is located. Set this field to Enabled for single-base systems.
Keep Alive	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates if the port of the relevant NAT-aware router is kept open for 30 seconds.
Show Extension on Handset Idle Screen	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates if the handset idle screen displays the extension.
Hold Behaviour	Values: <ul style="list-style-type: none"> • RFC 3264 • RFC 2543 (default) 	Indicates the way hold works on the handset. <ul style="list-style-type: none"> • RFC 3264—The connection information part of the SDP contains the IP address of the endpoint, and based on the context the direction attribute is send only, recvonly, or inactive. • RFC 2543—The connection information part of the SDP is set to 0.0.0.0, and based on the context the direction attribute is send only, recvonly, or inactive.
Local Ring Back Tone	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Controls whether the ring tone is generated locally by the handset. <ul style="list-style-type: none"> • Disabled—The handset doesn't generate the ringtone. • Enabled (default)—The handset generates the ringtone.
Remote Ring Tone Control	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the call control system can choose ringtones for the handset. <ul style="list-style-type: none"> • Disabled (default)—The call control system can't choose ringtones. • Enabled—The call control system can choose ringtones.

Field	Contents	Description
Attended Transfer Behaviour	Values: <ul style="list-style-type: none"> • Hold 2nd Call • Do Not Hold 2nd Call 	Indicates if the second call is put on hold during an attended transfer. When you have two calls, and one call is on hold, it is possible to perform attended transfer. When you press Transfer softkey, traditionally the active call is on hold before the SIP REFER request is sent. Some PBX systems do not expect that the second call is put on hold, and therefore attended transfer fails. <ul style="list-style-type: none"> • Hold 2nd Call—The second call is put on hold. • Do Not Hold 2nd Call—The second call is not put on hold.
Use Own Codec Priority	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates the codec priority for incoming calls. <ul style="list-style-type: none"> • Disabled—Uses the calling party priority. • Enabled—Uses the system codec priority. For example, if enabled and the base has G722 as the top codec and the calling party has Alaw on top and G722 further down the list, the G722 codec is chosen for the call.
DTMF Signalling	Values: <ul style="list-style-type: none"> • SIP INFO • RFC 2833 (default) • RFC 2833 and SIP INFO 	Controls how to handle DTMF. <ul style="list-style-type: none"> • SIP INFO—DTMF tones are handled in the same layer as the voice stream. • RFC 2833—DTMF tones are sent in data packets in different internet layers from the voice stream. • RFC 2833 and SIP INFO—DTMF tones are handled in the same or different layers.
DTMF Payload Type	Integer Default: 101	Indicates the type of DTMF payload when the DTMF Signaling field is set to RFC 2833.
Remote Caller ID Source Priority	Values: <ul style="list-style-type: none"> • PAI - FROM (default) • FROM • ALERT_INFO - PAI - FROM 	Contains SIP information used for the Caller ID source.
Enable Blind Transfer	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if you can use direct transfer.

Field	Contents	Description
Call Statistics in SIP	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	This field is new in Firmware Release 5.0. Indicates whether the call quality is sent to the call control system.
Codec Priority Max number of codecs is 5	Values, one or more of: <ul style="list-style-type: none"> • G711A • G711U • G722 • G726 • G729 • OPUS 	Identifies the code priority that base stations use for audio compression and transmission. You can change the order of the codecs. To get OPUS to display in the list, click Reset Codecs . Note If you change the list in any way, you must press Reset Codecs on this page and Reboot chain on the Multi cell page. Starting in Firmware Release 4.7, only the first five codecs in the list are used.
G729 Annex B	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the G729 Annex B is used.
Use ptime	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates if the RTP Packet Size parameter is used.
RTP Packet Size	Values: <ul style="list-style-type: none"> • 20 ms (default) • 40 ms • 60 ms • 80 ms 	Indicates the preferred RTP packet size when the packet size is negotiated.
RTCP	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates if RTCP is used.

Field	Contents	Description
Secure RTP	Values: <ul style="list-style-type: none"> • Optional • Required • Auto 	Indicates the type of RTP to use. <ul style="list-style-type: none"> • Optional: Indicates that the system can send and receive with SRTP and RTP. • Required: Indicates if RTP is encrypted with AES-128 using the key negotiated in the SDP protocol at call setup. • Auto: Indicates media security to use RTP or SRTP. If SRTP is in use, RTP is blocked. When system uses SRTP, call capacity reduce. If SIP Transport field is set to Auto, it is recommended to set this field to this option. This option is added for Firmware Release 4.8.
Secure RTP Auth	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if secure RTP uses authentication of RTP packets. <p>Note When enabled, a base can support a maximum of 4 concurrent calls.</p>
SRTP Crypto Suites	Values: <ul style="list-style-type: none"> • AES_CM_128_HMAC_SHA1_32 • AES_CM_128_HMAC_SHA1_80 	Indicates the list of supported SRTP Crypto Suites. Each device starts with two suites. You can change the order of the suites. <p>Note If you change the list in any way, you must press Reset Crypto Suites on this page.</p>
Media Security	Values: <ul style="list-style-type: none"> • Enabled • Disabled 	This field is new for Firmware Release 4.8. <p>Controls the media security.</p> <ul style="list-style-type: none"> • Enabled: Client-initiated Mode—The phone initiates media security negotiations. • Disabled: Server-initiated Mode—The server initiates media security negotiations. The phone doesn't initiate negotiations, but can handle negotiation requests from the server to establish secure calls.
Media Security only for TLS	Values: <ul style="list-style-type: none"> • Enabled • Disabled 	This field is new for Firmware Release 4.8. <p>Controls the media security only if the SIP transfer protocol is TLS.</p>
Auth Resync reboot	Values: <ul style="list-style-type: none"> • Enabled (default) • Disabled 	This field is new for Firmware Release 5.0. <p>Enabled: Indicates that the authentication is required for SIP notification if the event is <code>reset-ipei-for-handset</code> or <code>check-sync</code> and the protocol isn't TLS.</p>

Field	Contents	Description
Reversed Auth Realm	String Maximum up to 64 characters	This field is new for Firmware Release 5.0. Indicates the server that the handset extension uses.

Network Web Page Fields

These are the fields displayed on the **Network Settings** web page of the base station.

Table 14: IP Settings Section Fields

Field	Contents	Description
DHCP/Static IP	Values: <ul style="list-style-type: none"> • DHCP (default) • Static 	Indicates the method that the device gets the TCP/IP parameters. <ul style="list-style-type: none"> • DHCP—Automatically allocated from a pool of addresses. If DHCP is used, the other IP settings or options can't be set. • Static—Manually set.
IP Address		Indicates the IPv4 address of the device. Can only be changed if DHCP is not enabled.
Subnet Mask		Indicates the 32-bit subnet mask of the device. Can only be changed if DHCP is not enabled.
Default Gateway		Indicates the IPv4 address of the default network router or gateway. Can only be changed if DHCP is not enabled.
Via DHCP priority	IPv4	
DNS (Primary)		Indicates the IPv4 address of the main server used for Domain Name System (DNS) queries. Mandatory when DHCP is not used. Can only be changed if DHCP is not enabled.
DNS (Secondaries)		Indicated the alternate DNS server. Can only be changed if DHCP is not enabled.
MDNS	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if Multicast Domain Name System (MDNS) is available. Can only be changed if DHCP is not enabled.

Table 15: NAT Settings Section Fields

Field	Contents	Description
Enable STUN	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if RFC3489 Session Traversal UDP for NAT (STUN) is used.
STUN Server	IPv4 address or URL	Identifies the location of the STUN server.
STUN Bindtime Determine	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Determines if the base station detects the STUN bindtime from the NAT bindings. <ul style="list-style-type: none"> • Disabled: NAT bindings can't be used • Enabled: NAT bindings can be used.
STUN Bindtime Guard	Integer Range: 0–65535 Default: 80	Identifies the lifetime of the STUN binding.
Enable RPORT	Value: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the RPORT is used in SIP messages.
Keep alive time	Integer Range: 0-65535 Default: 90	Determines the frequency of keep alive messages (in seconds) to the server to maintain NAT bindings

Table 16: VLAN Settings Section Fields

Field	Contents	Description
ID	Integer Range: 0–4094 Default: 0	Identifies the 802.1Q VLAN.
User Priority	Integer Range: 0–7 Default: 0	Defines the user priority. These values can be used to prioritize different classes of traffic (voice, video, data). <ul style="list-style-type: none"> • 0—best effort • 1—lowest priority • 7—highest priority

Field	Contents	Description
Synchronization	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates if the VLAN ID automatically synchronizes between the base stations in the chain. This field only displays on the Cisco IP DECT 210 Multi-Cell Base Station.

Table 17: SIP/RTP Settings Section Fields

Field	Contents	Description
Use Different SIP Ports	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates SIP signaling ports. <ul style="list-style-type: none"> • Disabled—The Local SIP Port field specifies the source port used for SIP signaling in the system. • Enabled—The Local SIP Port field specifies the source port used for the first user agent (UA) instance. Succeeding UAs get successive ports. Set this field to Enabled for single-base systems.
RTP Collision Detection	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	<ul style="list-style-type: none"> • Disabled—When two sources have the same SSRC, the second source is discarded. • Enabled—The device accepts all sources.
Always reboot on check-sync	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the base station reboots when a new configuration is loaded.
Outbound Proxy Mode	Values: <ul style="list-style-type: none"> • Use Always (default) • Only Initial Request 	Indicates the outbound proxy use. <ul style="list-style-type: none"> • Use always—All outbound calls as sent to the outbound proxy. • Only initial request—Only use the outbound proxy for initial SIP requests.
Failover SIP Timer B	Integer Default: 5	Indicates the time to wait for a response from an INVITE message from the SIP server before failover is triggered.
Failover SIP Timer F	Integer Default: 5	Indicates the time to wait for a response from a non-INVITE message from the SIP server before failover is triggered.

Field	Contents	Description
Failover Reconnect Timer	Integer Default: 60	Controls the delay, in seconds, between queries from the base station to locate the primary server during failover. This field is new for Firmware Release 4.7.
Local SIP port	Integer Range: 0–65535 Default: 5060	Indicates the SIP signaling source port.
SIP ToS/QoS	Integer Range: 0–65535 Default: 0x68	Indicates the priority of call control signaling traffic, based on the IP layer Type of Service (ToS) byte. ToS is the same as Quality of Service (QoS) in packet-based networks.
RTP port	Integer Range: 0–65535 Default: 16384	Indicates the first RTP port to use for RTP audio streaming.
RTP port range	Integer Range: 0–65535 Default: 40	Indicates the number of ports to use for RTP audio streaming.
RTP ToS/QoS	Integer Range: 0–65535 Default: 0xB8	Indicates the priority of RTP traffic, based on the IP layer ToS byte. For more information, see RFC 1349. <ul style="list-style-type: none"> • Bits 7–5 define precedence • Bits 4–2 define ToS • Bits 1–0 are ignored. <p>Note The cost bit is not supported.</p>
Reject anonymous calls	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the call should be rejected if it is made anonymously.

Table 18: DHCP Options Section Fields

Field	Contents	Description
Plug-n-Play	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates if the base automatically receives PBX IP addresses under DHCP option 66.

Table 19: TCP Options Section Fields

Field	Contents	Description
TCP Keep Alive Interval	Integer Range: 0–65535 Default: 75	Identifies the length of time, in seconds, that the client waits before it sends a keep-alive message on a TCP connection.

Table 20: Discovery Section Fields

Field	Contents	Description
LLDP-MED Send	Values: <ul style="list-style-type: none"> • Enabled (default) • Disabled 	This field is new in Firmware Release 5.0. Controls the use of Link Layer Discovery Protocol (LLDP) on the base. If enabled, the base station sends 5 LLDP-MED messages after it starts.
LLDP-MED Send Delay	Integer Range: Default: 30	This field is new in Firmware Release 5.0. Identifies the length of time, in seconds, that the device waits between LLDP-MED messages. Note The option LLDP-MED must be enabled to use this option.
CDP Send	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Controls the use of Cisco Discovery Protocol (CDP) on the base. For more information about CDP, see Network Protocols, on page 213 . <ul style="list-style-type: none"> • Disabled—The base station doesn't send CDP messages. • Enabled—The base station sends CDP messages.
CDP Send Delay	Integer Range: 1–255 Default: 60	Identifies the length of time, in seconds, that the device waits between CDP messages.

Management Web Page Fields

These are the fields displayed on the **Management Settings** web page of the base station.

Table 21: Management Settings Web Page Fields

Field	Contents	Description
Base Station Name	1-35 characters	Indicates the name of the base station.

Table 22: Settings Section Fields

Field	Contents	Description
Management Transfer Protocol	Values: <ul style="list-style-type: none"> • TFTP (default) • HTTP • HTTPS 	Indicates the transfer protocol assigned for the configuration file and central directory.
HTTP Management upload script	folder or path	Indicates the location for the configuration files on the configuration server. This field must start with slash (/) or backslash (\). This field is available only when the Management Transfer Protocol is set to HTTP or HTTPS.
HTTP Management username	8-character string	Indicates the user name for access to the configuration server. This field is available only when the Management Transfer Protocol is set to HTTP or HTTPS.
HTTP Management password	8-character string	Indicates the password for access to the configuration server. This field is available only when the Management Transfer Protocol is set to HTTP or HTTPS.
Factory reset from button	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Indicates if the reset button on the base station can be used. When set to Disabled, nothing happens when the reset button is pressed.

Table 23: Text Messaging Section Fields

Field	Contents	Description
Text Messaging	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled • Enabled Without Server 	Indicates if users can send text messages to other devices that support text messages. <ul style="list-style-type: none"> • Disabled: Users can't send text messages. • Enabled: Users can send text messages to anyone. This requires the rest of the fields in this area to be set. • Enabled Without Server: Users can only send text messages to other members of the system.

Field	Contents	Description
Text Messaging & Alarm Server	IP address or URL	Indicates the IP address or URL of the Messaging and Alarm server. Set the address to allow users to exchange text messages with people outside your system. If you leave this field empty, users can only communicate inside the system.
Text Messaging Port	Default: 1300	Indicates the Messaging and Alarm server port used for messages. Set the port to allow users to exchange text messages with people outside your system. The value of this field depends on the message server. If you leave this field empty, users can only communicate inside the system.
Text Messaging Keep Alive (m)	Range: 0–65535 Default: 30	Indicates the frequency of keep alive messages in minutes.
Text Messaging Response (s)	Range: 0–65535 Default: 30	Indicates the timeout if the system doesn't receive a response from the message server. This field is in seconds.
Text Messaging TTL	Range: 0–65535 Default: 0	Indicates the text message time to live (TTL) in seconds. If set, the message only displays for the configured amount of time. After that time, the message is automatically deleted. A default of 0 means the message doesn't expire.

Table 24: Terminal Section Fields

Field	Contents	Description
Keep Alive (m)	Integer Default: 0	Indicates the length of time in minutes that the handset waits before sending an automatic emergency notification message to the server. When set to 0, the handset doesn't send notifications.
Auto Stop Alarm	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the handset should stop the automatic emergency notification. <ul style="list-style-type: none"> • Disabled: The handset doesn't stop notification. • Enabled: The handset stops the notification after the number of seconds set in Auto Stop Alarm Delay.
Auto Stop Alarm Delay (s)	Integer Default: 30	Indicates the time (in seconds) before the handset stops automatic emergency notification.

Table 25: Configuration Section Fields

Field	Contents	Description
Configuration File Download	Values: <ul style="list-style-type: none"> • Disabled • Base Specific File (default) • Multi Cell specific File • Base and Multi Cell Specific File 	Indicates the type of configuration file for the base station. <ul style="list-style-type: none"> • Disabled: no file expected • Base Specific File: base station expects a filename in this format: <mac address>.cfg • Multi Cell specific File: base station expects a filename in this format: <chain id>.cfg • Base and Multi Cell Specific File: base station expects a filename in these formats: <ul style="list-style-type: none"> • <mac address>.cfg • <chain id>.cfg
Configuration Server Address	https://ciscoserver.com	Identifies the server or device that provides the configuration file to the base station. <p>Note The configuration server and the base-specific file, multi-cell-specific file or the dual-cell-specific file of these profile rule. For instance, if the configuration server is https://cisco.sipflash.com and the file specific to M\$MA.xml, the result should be <Profile_Rule>https://cisco.sipflash.com/\$MA.xml. You will be able to view this profile rule in its form in the Configuration tab on the base web UI.</p>
Base Specific File	[macaddress].xml	Identifies the base configuration file name.
Multi Cell Specific File	MultiCell_[chainid].cfg	Identifies the configuration file for the multicell system. The filename is the chain id. <p>This field only displays on the 210 Multi-Cell Base Station.</p>
Dual Cell Specific File	MultiCell_[chainid].cfg	This field is new in Firmware Release 5.0. <p>Identifies the configuration file for the dualcell system. The filename is the chain id.</p> <p>This field only displays on the 110 Single-Cell Base Station.</p>

Field	Contents	Description
Auto Resync Polling	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Controls the ability to look for new configuration files for the automatic synchronization. <ul style="list-style-type: none"> • Disable—No automatic sync • Enable—Automatic sync enabled.
Auto Resync Time	hh:mm Default: 00:00 Maximum: 23:59	Indicates the time (24-hour clock) that the base station looks to resync the configuration file. This field is available when Auto Resync Polling is enabled.
Auto Resync Days	Minimum: 0 Maximum: 364	Indicates the number of days between resync operations. This field is available when Auto Resync Polling is enabled.
Auto Resync Max Delay (Min)	Default: 15 Minimum: 0 Maximum: 1439	Indicates the time delay, in seconds. Set different delay times for each base station to prevent them from asking for new configuration files at the same time. This field is available when Auto Resync Polling is enabled.
DHCP Controlled Config Server		Identifies the configuration server.
DHCP option priority	Default: 66, 160, 159, 150, 60	Identifies the priority of the DHCP options.

Table 26: Syslog/SIP Log Section Fields

Field	Contents	Description
Upload of SIP Log	Values <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if low-level SIP debug messages are to be saved to the server. SIP logs are saved in the file format: <MAC_address><Time_stamp>SIP.log

Field	Contents	Description
Syslog Level	Values <ul style="list-style-type: none"> • Off • Normal Operation (default) • System Analyze • Debug 	Identifies the level of system-level log messages to be saved on the syslog server. <ul style="list-style-type: none"> • Off—No messages saved • Normal Operation—Normal message for: operational events, incoming calls, outgoing calls, handset registration, DECT location, call lost due to busy, critical system errors, and general system information. • System Analyze—Captures logs for handset roaming, handset firmware updates status. The system analyze level also contains the messages from normal operation. • Debug—Captures logs for debugging problems <p>Note Don't enable Debug logs during normal operation. These logs can result in system slowdown.</p>
TLS security	Values <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Controls TLS 1.2 security. <ul style="list-style-type: none"> • Disabled: system doesn't use TLS 1.2. • Enabled: system uses TLS 1.2.
Syslog Server IP Address	IP address or URL	Indicates the address of the Syslog server.
Syslog Server Port	0-xx Default: 514	Indicates the port of the Syslog server.

The Configuration -handset (retrieved on SIP NOTIFY request) section is new in Firmware Release 5.1(1).

Table 27: Handset Settings Fields

Field	Contents	Description
Configuration Server and File	String up to 256 characters	Defines the server and the handset settings configuration file to download. If the protocol isn't specified in the URL, TFTP is used.
Protocol	Values: <ul style="list-style-type: none"> • IPv4 • IPv6 	Indicates the protocol to download the handset settings configuration file.

Field	Contents	Description
Username	String up to 40 characters	Indicates the username to access the handset configuration server.
Password	String up to 40 characters	Indicates the password to access the handset configuration server.

The Problem Report Tool section is new in Firmware Release 5.1(1).

Table 28: Problem Report Tool

Field	Contents	Description
PRT Upload Server	String up to 127 characters	Specifies the target server to upload the problem report. You can enter the protocol (optional), server domain, and port (optional) in the field. The default protocol is HTTP. The default port is 80 for HTTP and 443 for HTTPS.
PRT Upload Filename	String up to 63 characters	Specifies the problem report filename. The file extension is <code>tar.gz</code> . You can use <code>\$MAC</code> in the filename which uses the base station's MAC address to generate the filename automatically in the format <code>MAC-%d%m%Y-%H%M%S.tar.gz</code> .
PRT Upload HTTP Header	String up to 63 characters	This field is optional. Specifies a header for the HTTP upload request. If you specify the header, you must enter the HTTP header value in the field PRT Upload HTTP Header Value .
PRT Upload HTTP Header Value	String up to 127 characters	Specifies the header field value for HTTP upload request. You must specify the header text to enter this value.

The Promiscuous Mode section is new in Firmware Release 4.8.

Table 29: Promiscuous Mode Section Fields

Field	Contents	Description
Enable in (min)	Number	Indicates the time for the base station in promiscuous mode.
Promiscuous mode timeout in	This field is read-only.	Indicates the remaining time to deregister the handsets.

Table 30: Emergency Numbers Section Fields

Field	Contents	Description
list of numbers		Indicates the available emergency numbers.
HELD company ID	String up to 48 characters	This field is new for Firmware Release 5.1(1). Specifies the HELD company account ID.
Primary HELD server	String up to 128 characters	This field is new for Firmware Release 5.1(1). Specifies the primary server for location token requests.
Secondary HELD server	String up to 128 characters	This field is new for Firmware Release 5.1(1). Specifies the secondary server for location token requests.

The Assign HS to Ext by Credentials (HEBU) section is new in Firmware Release 5.1(1).

Table 31:

Field	Contents	Description
Assign HS to Ext by Credentials (HEBU)	Values: <ul style="list-style-type: none"> • Enabled • Disabled (default) 	Indicates if the HEBU mode is enabled. The base station can't be set in promiscuous mode and HEBU mode simultaneously.

The Multiple Paging Group Parameters section is new in Firmware Release 4.8.

Table 32: Multiple Paging Group Parameters

Field	Contents	Description
Group 1-3 Paging Script	String up to 128 characters	For more information, see Configure Paging, on page 74

Firmware Update Web Page Fields

These are the fields displayed on the **Firmware Update** web page of the base station.



Note We recommend that you update the base station first, then update the handsets after the base station update completes.

Table 33: Firmware Update Web Page Fields

Field	Contents	Description
Firmware update server address	IP address or URL	Indicates the location of the update server (TFTP server address).
Firmware path	String	Indicates the path on the update server where the firmware update files are stored. For example, set this field to Cisco .
Terminal file path	String	This field is new in Firmware Release 5.1(1). Indicates the server settings and name of the language pack file.
Enable legacy firmware naming	Check box Default: unchecked	This field is new in Firmware release 5.0. Identifies Firmware downgrade to latest branch of Firmware version 4.8(1) SR1.
Type	Update Base Stations 6823 6825 RPT-110-3PC	Indicates the hardware: Update Base Stations: The Firmware field indicates the firmware version to update the base station. 6823: The Firmware field indicates the firmware version to update the handset. The Language field indicates the language file to update the settings in the handset. 6825: The Firmware field indicates the firmware version to update the handset. The Language field indicates the language file to update the settings in the handset. RPT-110-3PC: The Firmware field indicates the firmware version to update the repeater.
Required version	8-character string	Indicates the firmware version to be updated. When the field contains zero (0), the firmware upgrade is disabled. When you update this field, the version number doesn't require the leading zeros. That is, if the version is "v0445", you can input the version as 445 .
Required branch	8-character string	Indicates the branch of firmware . When you update this field, the branch doesn't require the leading zeros. That is, if the branch is "b003", you can input the version as 3 .

Country Web Page Fields

These are the fields displayed on the **Country/Time Settings** web page of the base station.

Table 34: Country/Time Settings Web Page Fields

Field	Contents	Description
Select country	List of countries	Identifies the country where the base station is located.
State / Region	List of states or regions, based on the country selected.	Identifies the state or region where the base station is located.
Notes	Text	Contains notes about the settings.
Select Language	List of languages	Identifies the language for the base station web pages.
Time Service	Text	Displays the defined time service.
Time Server	Text	Identifies the DNS name or the IP address of the network time server. Note Only IPv4 addresses are supported
Allow broadcast NTP	Check box Default: checked	Identifies if the time server should be used for all devices.
Refresh time (h)	Integer (1-24) Default: 24	Identifies the frequency that the base station syncs its time (in hours) with the time server.
Set timezone by country/region	Check box Default: checked	Indicates that the base station uses the timezone setting from the country and state/region fields in this screen. When this box is checked, you can't update some of the other fields in this table.
Timezone	0 or hh:mm	Indicates the time zone in GMT or UTC format. Minimum: -12:00 Maximum: +13:00
Set DST by country/region	Check box Default: checked	Identifies if the daylight savings time (DST) for the state or region can be used.
Daylight Saving Time (DST)	Values <ul style="list-style-type: none"> • Automatic (default) • Disabled • Enabled 	Indicates how DST is configured. <ul style="list-style-type: none"> • Automatic: Uses the settings associated with the country. • Enabled: you need to set the rest of the DST fields. • Disabled: No DST required.

Field	Contents	Description
DST Fixed by Day	Values: <ul style="list-style-type: none"> • Use Month and Day of Week • Use Month and Date 	Identifies how DST is managed: <ul style="list-style-type: none"> • Use Month and Day of Week: DST starts on a particular month and day of the week. Use this if DST starts on a different date every year. • Use Month and Date: DST starts on a specific month and day. Use this if DST starts on the same day of the month every year.
DST Start Month	List of months	Identifies the month that DST starts.
DST Start Date	Integer 0–31	Identifies the specific day of the month that DST starts. If set to 0, the DST Start Day of Week entry is used.
DST Start Time	Integer 0–23	Identifies the hour that DST starts.
DST Start Day of Week	Days of the week	Identifies the day of the week that DST starts.
DST Start Day of Week Last in Month	Values: <ul style="list-style-type: none"> • First in Month • Last in Month • Second First in Month • Second Last in Month • Third First in Month 	Identifies which day in the month that DST starts. <ul style="list-style-type: none"> • First in Month: DST starts on the first DST Start Day of Week of the month. • Last in Month: DST starts on the last DST Start Day of Week of the month. • Second First in Month: DST starts on the second DST Start Day of Week of the month. • Second Last in Month: DST starts on the second-last DST Start Day of Week of the month. • Third First in Month: DST starts on the third DST Start Day of Week of the month.
DST Stop Month	List of months	Identifies the month that DST stops.
DST Stop Date	Integer 0–31	Identifies the specific day of the month that DST starts. If set to 0, the DST Stop Day of Week entry is used.
DST Stop Time	Integer 0–23	Identifies the hour that DST stops.
DST Stop Day of Week	Days of the week	Identifies the day of the week that DST stops.

Field	Contents	Description
DST Stop Day of Week Last in Month	Values: <ul style="list-style-type: none"> • First in Month • Last in Month • Second First in Month • Second Last in Month • Third First in Month 	Identifies which day in the month that DST stops. <ul style="list-style-type: none"> • First in Month: DST stops on the first DST Stop Day of Week of the month. • Last in Month: DST stops on the last DST Stop Day of Week of the month. • Second First in Month: DST stops on the second DST Stop Day of Week of the month. • Second Last in Month: DST stops on the second-last DST Stop Day of Week of the month. • Third First in Month: DST stops on the third DST Stop Day of Week of the month.

Security Web Page Fields

These are the fields displayed on the **Security** web page of the base station.

Table 35: Device Identity Section Fields

Field	Contents	Description
Idx		Indicates the index of the certificate.
Issued To	String	Indicates the name of the Certificate Authority (CA) for the certificate. The name is part of the certificate file.
Issued By	String	Indicates the organization or company that the certificate is created for. This name is part of the certificate file.
Valid Until	mm/dd hh:mm:ss yyyy	Indicates the date that the certificate expires. This date is part of the certificate file.
Import Device Certificate and Key Pair: Filename	String	Displays the filename of the imported file.

Table 36: Trusted Server Certificates Section Fields

Field	Contents	Description
Idx		Indicates the index of the certificate.
Issued To	String	Indicates the name of the CA for the certificate. The name is part of the certificate file.

Field	Contents	Description
Issued By	String	Indicates the organization or company that the certificate is created for. This name is part of the certificate file.
Valid Until	mm/dd hh:mm:ss yyyy	Indicates the date that the certificate expires. This date is part of the certificate file.
Import Trusted Certificates: Filename		Displays the filename of the imported file.

Table 37: Trusted Root Certificates Section Fields

Field	Contents	Description
Idx		Indicates the index of the certificate.
Issued To	String	Indicates the name of the CA for the certificate. The name is part of the certificate file.
Issued By	String	Indicates the organization or company that the certificate is created for. This name is part of the certificate file.
Valid Until	mm/dd hh:mm:ss yyyy	Indicates the date that the certificate expires. This date is part of the certificate file.
Import Root Certificate: Filename		Indicates the name of the root certificate to import.

Table 38: Strict Certificate Validation Section Fields

Field	Contents	Description
Use Only Trusted Certificates	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	<ul style="list-style-type: none"> • Disabled: Accepts all the certificates from the server. • Enabled: Validates the certification from the server and loads it into the system. When a matching certificate isn't found, the TLS connection fails.

Table 39: Secure Web Server Section Fields

Field	Contents	Description
Secure HTTP	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates the type of security for the web server. <ul style="list-style-type: none"> • Disabled: You can use HTTP or HTTPS. • Enabled: You use HTTPS only.

The Web password constraints section is new in Firmware Release 4.8

Table 40: Web password constraints Section Fields

Field	Contents	Description
Minimum length (min 1)	Default value: 4	Indicates the minimum length of the password. The minimum length is 1 character and maximum length is 127 characters.
Only ASCII characters	Values: <ul style="list-style-type: none"> • Yes • No 	Defines the usage of ASCII characters in the password. <ul style="list-style-type: none"> • Yes: Password can contain capital letters, small letters, and special characters. For more information, see Supported Characters, on page 20. Password can't contain a space character. • No: Password can contain unicode characters.

Table 41: Password Section Fields

Field	Contents	Description
Username	Values: <ul style="list-style-type: none"> • user • admin (default) 	Indicates username to update the password.
Admin Password	String, up to 128 characters	Input the current administrator password to authorize password changes.
New Password	String, up to 128 characters	Valid characters are: <ul style="list-style-type: none"> • 0–9 • a–z, A–Z • @ / < > - _ : . ? * + #
Confirm Password	String, up to 128 characters	This field and the previous field must match.

Table 42: Firewall Section Fields

Field	Contents	Description
Firewall	Values: <ul style="list-style-type: none"> • Enabled (default) • Disabled 	Enables stateful firewall and blocks incoming unintended traffic. If disabled, accepts traffic on all open ports.
No ICMP Ping	Check box	When selected, the firewall blocks for incoming ICMP echo requests (Ping).
No ICMP unreachable	Check box	When selected, firewall prevents base station to send ICMP destination unreachable for UDP ports except (S)RTP port range. This setting is only relevant when the port is trusted. For untrusted port, the firewall always prevents sending ICMP destination unreachable.
No non-default TFTP	Check box	When selected, firewall blocks TFTP traffic to all other destination ports than default port 69. If not selected, TFTP client uses port range 53240:53245.
Trusted TCP port range	Decimal format. Supports upto five trusted elements. Each element can be a port or a port range. Blank spaces are not allowed. Multiple settings are separated by comma. Format: <port> or <port-from>:<port-to> Example: 1000:2000,5000,42000:43000	Specifies trusted TCP port or the range of IPv4 ports defined for incoming connections.
Trusted UDP port range	Decimal format. Supports upto five trusted elements. Each element can be a port or a port range. Blank spaces are not allowed. Multiple settings are separated by comma. Format: <port> or <port-from>:<port-to> Example: 1000:2000,5000,42000:43000	Specifies trusted UDP port or the range of IPv4 ports defined for incoming connections.

Field	Contents	Description
Note	If any field is blank, any firewall configurations will be cleared. The firewall will have default settings. For default settings, see Firewall Default Port Settings , on page 64.	

Central Directory Web Page Fields

These are the fields displayed on the **Central Directory** web page of the base station. The **Location** field determines the rest of the fields displayed.

Table 43: Central Directory Web Page Fields

Field	Contents	Description
Central Directory Location	Values: <ul style="list-style-type: none"> • Local • LDAP Server • XML Server 	Identifies the type of central directory: <ul style="list-style-type: none"> • Local—Indicates that an imported comma separated value (CSV) file is to be used. See “Local Directory” below. • LDAP Server—Indicates that an LDAP directory is used. See “LDAP Directory” below. • XML Server—Indicates that an XML directory is used (for example, a BroadSoft directory). See “XML Directory” below. <p>Note When you change this field, the screen updates to display different fields, based on the directory type.</p>

Local Directory

Table 44: Local Directory Fields

Field	Contents	Description
Server	IP address or URL	Identifies the server that contains the directory.
Filename		Identifies the name of the directory file on the server.
Phonebook reload interval (s)	0–xx	Controls how often the base station refreshes the phonebook contents in seconds. The refresh doesn't happen when the field is set to 0. Specify a time that is frequent enough for the users but not so frequent that the base station is overloaded.

Table 45: Import Central Directory Section Fields

Field	Content	Description
Filename	string	Displays the name of the imported central directory.

LDAP Directory

Table 46: LDAP Central Directory Fields

Field	Content	Description
Server	IP address or URL	Identifies the server that contains the directory file.
TLS security	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Identifies the TLS 1.2 security. <ul style="list-style-type: none"> • Disabled: The system doesn't use TLS 1.2 when it accesses the LDAP server. • Enabled: The system uses TLS 1.2 when it accesses the LDAP server.
Port		Identifies the server port number that is open for LDAP connections
Sbase		Identifies the search base criteria. Example: CN=Users, DC=number, DC=loc
LDAP Filter		Identifies the search filter. Example: if the field is set to ((givenName=%*) (sn=%*)) , the system uses this filter when it requests entries from the LDAP server. % is replaced with the content entered by the user during the search operation. So if a user enters "J" for the search criteria, the string sent to the server is ((givenName=J*) (sn=J*)) and server sends the matches for given names or surnames that start with the letter "J".
Bind		Identifies the user name that is used when the phone connects to the server.
Password		Contains the LDAP Server password.
Virtual List	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Controls if virtual list search is possible. <ul style="list-style-type: none"> • Disabled: All search results are loaded. • Enabled: Only 25 contacts are loaded at a time.

Table 47: Terminal Identity

Field	Content	Description
Name	Values: <ul style="list-style-type: none"> • cn • sn+givenName 	Indicates whether the common name or surname with the given name returns in the LDAP search results.
Work	Default: telephoneNumber	Indicates LDAP work number attribute which is mapped to the handset work number.
Home	Default: homePhone	Indicates LDAP home number attribute which is mapped to the handset home number.
Mobile	Default: mobile	Indicates LDAP mobile number attribute which is mapped to the handset mobile number.

XML Server

Table 48: XML Central Directory Fields

Field	Content	Description
Server	string	Identifies the XML server.

Table 49: XML Central Directory: Directory Names Fields

Field	Content	Description
Enterprise	String and check box	Allows you to change the Enterprise string to another label. For example, if you set this field to “Company”, the handset displays “Company” instead of “Enterprise”. When you check the check box, the directory displays on the Central directory page.
EnterpriseCommon	String and check box	Allows you to change the EnterpriseCommon string to another label. When you check the check box, the directory displays on the Central directory page.
Group	String and check box	Allows you to change the Group string to another label. For example, if you set this field to “Department”, the handset displays “Department” instead of “Group”. When you check the check box, the directory displays on the Central directory page.

Field	Content	Description
GroupCommon	String and check box	Allows you to change the GroupCommon string to another label. When you check the check box, the directory displays on the Central directory page.
Personal	String and check box	Allows you to change the Personal string to another label. For example, if you set this field to “Home”, the handset displays “Home” instead of “Personal”. When you check the check box, the directory displays on the Central directory page.

Dual Cell Web Page Fields

These are the fields displayed on the **Dual Cell** web page of the base station.

This page only displays on the 110 Single-Cell Base Station.

Table 50: Dual Cell Status

Field	Description
System Information	Indicates the status of the base station in the dualcell configuration.
Last packet received from IP	Indicates the IP address of the last communicator to the base station.

Table 51: Settings for this unit

Field	Contents	Description
Dual cell system	Values: <ul style="list-style-type: none"> • Enabled (default) • Disabled 	Indicates if the base station is part of a dualcell configuration. If you change this field, you must press Save and Reboot .
System chain ID	Up to 10 digits	Identifies the dualcell chain. The chain ID is generated automatically and can't be modified. Each base station in the chain uses the same ID.

Field	Contents	Description
Data Sync	Values: <ul style="list-style-type: none"> • Multicast (default) • Peer-to-peer 	Indicates the type of data synchronization. <ul style="list-style-type: none"> • Multicast—Requires Multicast/IGMP to be enabled on the call control system. <ul style="list-style-type: none"> • The multicast port range and IP addresses used is calculated from the chain ID. • The multicast feature uses the port range: 49200 to 49999. • The multicast feature IP range: 224.1.0.0 to 225.1.0.0. • Multicast uses UDP. • Peer-to-peer—Use this mode when the network doesn't allow Multicast. For multicast operation, enable the Multicast/IGMP on your switches. Otherwise, use Peer-to-peer mode.
Primary Data Sync IP	IP address	Indicates the base station data synchronization IP address. <p>When Data Sync is set to multicast, this base IP is selected automatically.</p> <p>The data sync feature uses the port range of 49200 to 49999.</p> <p>When Data Sync is set to Peer-to-peer, you must define the IP of the base used for the data sync source.</p>
Base Replacement Timeout (15-255 Min)	Default: 60 minutes	Indicates the timeout to replace a base station.

Field	Contents	Description
Dual cell debug	<ul style="list-style-type: none"> • None • Data Sync • Auto Tree • Both (default) 	<p>Indicates the level of the dualcell system debugging information stored in the logs.</p> <ul style="list-style-type: none"> • None (default)—No debugging information. • Data Sync—Writes header information for all packets received and sent to be used to debug any special issues. <p>Note This setting generates many logs, so use it for a short period when you debug the issues.</p> <ul style="list-style-type: none"> • Auto Tree—Writes states and data related to the Auto Tree Configuration feature. • Both—Both Data Sync and Auto Tree are enabled. <p>Note This setting generates many logs, so use it for a short period when you debug the issues.</p>

After you set the **Dual cell system** field to **Enabled**, and reboot the base station, a message displays on the page.

Multi Cell Web Page Fields

These are the fields displayed on the **Multi Cell** web page of the base station.

This page only displays on the 210 Multi-Cell Base Station.

Table 52: Multi Cell Status Section Fields

Field	Description
System Information	Indicates the current status of the base station in the multi cell configuration.
Last packed received from IP	Indicates the IP address of the last communicator to the base station.

Table 53: Settings for this Unit Section Fields

Field	Contents	Description
Multi cell system	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the base station is part of a multicell configuration. If you change this field, you must press Save and Reboot .
System chain ID	512 (default) Up to 5 digits	Identifies the multi cell chain. Each base station in the chain uses the same ID. Note We recommend that you do not use a chain ID that is similar to an extension number.
Synchronization time (s)	Values: <ul style="list-style-type: none"> • 30 • 60 (default) • 90 • 120 • 150 • 180 • 240 • 270 • 300 	Indicated the period in seconds between synchronization requests by the base stations in the chain.
Data Sync	Values: <ul style="list-style-type: none"> • Multicast (default) • Peer-to-peer 	Indicates the type of data synchronization. <ul style="list-style-type: none"> • Multicast—requires Multicast/IGMP to be enabled on the call control system. <ul style="list-style-type: none"> • The multicast port range and IP addresses used is calculated from the chain id. • The multicast feature uses the port range: 49200 to 49999 • The multicast feature IP range: 224.1.0.0 to 225.1.0.0 • Multicast uses UDP. • Peer-to-peer—Use this mode when the network doesn't allow Multicast. See LAN Sync Web Page Fields, on page 150.

Field	Contents	Description
Primary Data Sync IP	IP address	<p>Indicates the base station data synchronization IP address.</p> <p>Using multicast, this base IP is selected automatically.</p> <p>The data sync feature uses the port range 49200 to 49999</p> <p>Note Using Peer to Peer mode, the IP of the base used for data sync source MUST be defined.</p> <p>Note Using Peer to Peer mode with version below V306 limits the system automatic recovery feature. There is no automatic recovery of the data sync source in Peer to Peer mode.</p>
Multi cell debug	<p>Values:</p> <ul style="list-style-type: none"> • None (default) • Data Sync • Auto Tree • Both 	<p>Indicates the level of multicell debugging information is stored in the logs.</p> <ul style="list-style-type: none"> • None (default)—No d • Data Sync—Writes header information for all packets received and sent to be used to debug any special issues. <p>Note This setting generates many logs, so use it for a short period of time when debugging.</p> <ul style="list-style-type: none"> • Auto Tree—Writes states and data related to the Auto Tree Configuration feature. • Both—Both Data Sync and Auto Tree are enabled. <p>Note This setting generates many logs, so use it for a short period of time when debugging.</p>

After you set the Multi cell system field to **Enabled**, and reboot the base station, a message displays on the page.

Table 54: DECT system settings

Field	Contents	Description
RFPI System		Displays the radio identity that all the base stations use for the multicell system.

Field	Contents	Description
Auto configure DECT sync source tree	Values <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Controls the ability to synchronize the multicell system. <ul style="list-style-type: none"> • Disabled: If the original primary base station can't be reached, the system continues without a primary to sync to. • Enabled: If the original primary base station can't be reached, another base station takes over as the primary base station.
Allow multi primary	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Allows the setup of systems in multiple locations.
Auto create multi primary	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	

Table 55: Base station settings

Field	Contents	Description
Number of SIP accounts before distributed load		
SIP Server support for multiple registrations per account	Values <ul style="list-style-type: none"> • Disabled (default) • Enabled 	
System combination (Number of base stations/Repeaters per base station)		

Table 56: Base Station Group

Field	Contents	Description
ID		A read-only index number.
RPN		Indicates the Radio Fixed Part Number (RPN) of the base station. Each base station RPN is unique.
Version		Indicates the firmware version.

Field	Contents	Description
MAC Address		Contains the base station MAC address.
IP Address		Contains the base station IP address.
IP Status	Values: <ul style="list-style-type: none"> • Connected • Connection Loss • This Unit 	Indicates the base station status. <ul style="list-style-type: none"> • Connected: the base station is online. • Connection Loss: the base station is not on the network • This Unit: the base station that you are viewing information about.
DECT sync source		Contains information about the multicell chain.
DECT property	Values <ul style="list-style-type: none"> • Primary • Locked • Searching • Free Running • Unknown • Assisted lock • Sync. Lost 	Indicates the status of the base station. <ul style="list-style-type: none"> • Primary: The base station is the primary base station and that all other base stations synchronize to this base station. • Locked: The base station is synchronized with the primary base station. • Searching: The base station is trying to synchronize with the primary base station. • Free Running: The base station has lost its synchronization with the primary base station. • Unknown: There is no connection information. • Assisted lock: The base station can't sync with the primary base station using DECT, and that it is using the Ethernet to sync. • Sync. Lost: Indicates that the base station has lost synchronization, but there is an active call on an associated handset. When the call completes, the base will attempt to sync.
Base Station Name		Indicates the base station name assigned in the Management page.

The DECT Chain section displays the hierarchy of base stations in a graphical form.

LAN Sync Web Page Fields

These are the fields displayed on the **LAN Sync** web page of the base station.

This page only displays on the 210 Multi-Cell Base Station.

Table 57: IEEE1588 LAN Synchronization Settings

Field	Contents	Description
IEEE1588	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Enabled: Indicates the use of LAN synchronization. The following are the network requirements for LAN synchronization: <ul style="list-style-type: none"> • The Sync Master and Sync Slave base stations support a maximum of 3 cascaded Ethernet switches. • We recommend and support only the switches which meet the IEEE1588 Ethernet synchronization requirements. • All base stations must connect to a dedicated DECT VLAN. • The DECT VLAN in all the switches which connect to the DECT infrastructure must be configured to the highest priority. • The backbone network load should not exceed 50 percent of the total link capacity. • The Ethernet switch must use DSCP as QoS parameter. • The network must support multicast datagrams from IEEE1588.

Star Codes Web Page Fields

These are the fields displayed on the **Star Codes** web page of the base station.

Table 58: Star Codes Web Page Fields

Field	Code	Description
Call Return	Default: 69	Dial this star code to return a call.
Blind Transfer	Default: 88	Dial this star code to transfer a call without consultation.
Call Forward All Activate	Default: 72	Dial this star code to forward all calls.
Call Forward All Deactivate	Default: 73	Dial this star code to stop make calls ring on the phone again.
Call Wait Activate	Default: 56	Dial this star code to enable the call waiting tone.
Call Wait Deactivate	Default: 57	Dial this star code to disable the call waiting tone.

Field	Code	Description
Block Caller Id On Outgoing Calls Activate	Default: 67	Dial this star code to not send the caller ID on an outgoing call.
Block Caller ID On Outgoing Calls Deactivate	Default: 68	Dial this star code to send the caller ID on an outgoing call.
Block Anonymous Incoming Calls Activate	Default: 77	Dial this star code to block calls that don't have a caller ID.
Block Anonymous Incoming Calls Deactivate	Default: 87	Dial this star code to all the phone to receive calls that don't have a caller ID.
Do Not Disturb Activate	Default: 78	Dial this star code to stop calls ringing on the phone.
Do Not Disturb Deactivate	Default: 79	Dial this star code to allow calls to ring on the phone.

Call Progress Tones Web Page Fields

These are the fields displayed on the **Call Progress Tones** web page of the base station.

Standard call progress tones differ by region. When you set the country for your system, this page displays the default tones for your country.

Table 59: Call Progress Tones Section Fields

Field	Description
Dial Tone	Prompts the user to enter a phone number.
Outside Dial Tone	Alternative to the Dial Tone. It prompts the user to enter an external phone number, as opposed to an internal extension. It is triggered by a comma (,) character encountered in the dial plan.
Prompt Tone	Prompts the user to enter a call forwarding phone number.
Busy Tone	Played when a 486 RSC is received for an outbound call.
Reorder Tone	Played when an outbound call has failed or after the far end hangs up during an established call. Reorder Tone is played automatically when Dial Tone or any of its alternatives times out.
Off Hook Warning Tone	Played when the phone receiver has been off hook after a period of time.
Ring Back Tone	Played during an outbound call when the far end is ringing.
Call Waiting Tone	Played when a call is waiting.
Confirm Tone	Brief tone to notify the user that the last input value has been accepted.
Holding Tone	Informs the local caller that the far end has placed the call on hold.

Field	Description
Conference Tone	Played to all parties when a three-way conference call is in progress.
Page Tone	This field is new for Firmware Release 4.8. Played to all handsets when the base station receive a page.

Dial Plans Web Page Fields

These are the fields displayed on the **Dial Plans** web page of the base station.

Table 60: Dial Plans Fields

Field	Description
Idx	Indicates the index number of the dial plan (used in the Terminal Web Page Fields, on page 112 page).
Dial Plan	Contains the definition of a dial plan.
Idx	This field is new for Firmware Release 5.1(1). Indicates the index number of the caller ID.
Call Id Map	This field is new for Firmware Release 5.1(1). Contains the definition of a caller ID.

Local Call Groups

These are the fields displayed to add or edit local call groups.

This web page is new for Firmware Release 5.1(1)

Table 61: Local Call Groups Web Page Fields

Field	Contents	Description
Line name	String Length: 1 to 7 characters	Indicates the name of the line for incoming and outgoing calls.
Extension	Digit string	Identifies the telephone number. The extension must be configured on the SIP server before the handset can make and receive calls. The extension displays on the main screen of the handset.
Authentication User Name	String	Identifies the user name assigned to the handset on the call control system. The name can be up to 128 characters long.

Field	Contents	Description
Authentication Password	String	Identifies the user's password on the call control system. The password can be up to 128 characters long.
Display Name	String	Identifies the name to display for the extension. This name displays on the main screen immediately under the date and time.
XSI Username	String	Identifies the username for the BroadSoft XSI phone book. The name can be up to 128 characters long.
XSI Password	String	Identifies the password for the BroadSoft XSI phone book. The password can be up to 128 characters long.
Mailbox Name	String	Identifies the username for the voicemail system.
Mailbox Number	Digit string Valid contents are 0–9, *, #	Identifies the number to be dialed to the voicemail system. This number needs to be enabled on the SIP server.
Server	Drop-down list of IP addresses	Identifies the SIP server address of the call control system.
Call waiting feature	Feature status: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Identifies if the call waiting is available on the phone.
BroadWorks Shared Call Appearance	Feature status: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Identifies if the line is shared. Only applicable to BroadSoft SIP servers. Must be enabled on the SIP server.
BroadWorks Feature Event Package	Feature status: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Identifies if the BroadWorks package is available. Features include: do not disturb (DND), call forward (all, busy, and no answer). Only applicable to BroadSoft SIP servers. Must be enabled on the SIP server.
Forwarding Unconditional Number (2 fields)	Digit string: <ul style="list-style-type: none"> • Valid contents are 0–9, *, # Feature status: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Identifies: <ul style="list-style-type: none"> • If call forward unconditional is available. • What number to dial when an incoming call arrives for the handset. Applies to all incoming calls.

Field	Contents	Description
Forwarding No Answer Number (3 fields)	Digit string: <ul style="list-style-type: none"> Valid contents are 0–9, *, # Feature status: <ul style="list-style-type: none"> Disabled (default) Enabled Time in seconds: <ul style="list-style-type: none"> Range 0 to 255 Default 90 	Identifies: <ul style="list-style-type: none"> If call forward no answer is available. What number to dial when an incoming call arrives for the handset and isn't answered. How long to wait, in seconds, before the call is considered unanswered. Applies to all unanswered calls.
Forwarding on Busy Number (2 fields)	<ul style="list-style-type: none"> Valid contents are 0–9, *, # Feature status: <ul style="list-style-type: none"> Disabled (default) Enabled 	Identifies: <ul style="list-style-type: none"> If call forward busy is available. What number to dial when the handset is busy. A handset is busy when it already has 2 calls (one active and one on hold). Applies when the handset is on an existing call.
Reject anonymous calls	Values: <ul style="list-style-type: none"> Disabled (default) Enabled 	Indicates if the handset should reject calls that don't have a caller ID.
Hide Number	Values: <ul style="list-style-type: none"> Off On for next call Always on 	Indicates if the handset can make a call without the caller ID.
Do Not Disturb	Values: <ul style="list-style-type: none"> Disabled (default) Enabled 	Indicates if the user can turn on do not disturb mode.

Repeaters Web Page Fields

These are the fields displayed on the **Repeaters** web page of the base station.

Table 62: Repeaters Web Page Fields

Field	Contents	Description
Idx	This field is read-only	Identifies the index of the repeater
RPN	This field is read-only	Identifies the repeater number.
Name/IPEI	This field is read-only	Indicates the configured name and IPEI of the repeater.
DECT sync source	This field is read-only	Indicates the base station the repeater communicates with.
DECT sync mode	This field is read-only	Indicates the type of synchronisation with the base station.
State	This field is read-only	Indicates the state of the repeater. <ul style="list-style-type: none"> • Disabled: The repeater isn't configured to communicate with the base. • Enabled: The repeater is configured to communicate with the base.
Type/FW Info	This field is read-only	Indicates the firmware version of the repeater.
FWU Progress	This field is read-only	Identifies the firmware update (FWU) state: <ul style="list-style-type: none"> • Off—Identifies that the sw version field is set to 0 in the Firmware Update page. • Initializing—Identifies that the update process is starting. • X%—Identifies the progress of the update, where X is the amount of progress (0–100) • Verifying X%—Identifies that the firmware verification is in progress before it is used. • Conn.term.wait—Identifies that the repeater firmware update is complete and the repeater reset is in progress. • Complete—Identifies that the firmware update is complete. • Error—Identifies that the update was not successful. Possible reasons included: <ul style="list-style-type: none"> • File can't be found. • File isn't valid.

Add or Edit Repeaters Web Page Fields

These are the fields displayed on the **Repeater** web page of the base station. This page displays when you add or change the configuration of a repeater.

Table 63: Repeater Web Page Fields

Field	Contents	Description
Name	String	Identifies the repeater name. You might want to set the name to a location
DECT Sync mode	Choice: <ul style="list-style-type: none"> • Manual • Local Automatic 	Indicated the registration type for the repeater. <ul style="list-style-type: none"> • Manual: You need to manually assign parameters. • Local Automatic: The repeater detects the base signal and automatically configures.
RPN	Choice: <ul style="list-style-type: none"> • ERROR • RPNxx 	Indicates the RPN for the repeater <ul style="list-style-type: none"> • ERROR: The repeater selects the first available base station slot. • RPNxx: The repeater selects the configured base station slot.
DECT sync source	List of RPNs available	Identifies the RPNs that are available on the base stations.

Alarm Web Page Fields

These are the fields displayed on the **Alarm** web page of the base station.

Table 64: Alarm Web Page Fields

Field	Contents	Description
Idx	digit	Indicates the index number of the alarm.
Profile Alias	String	Identifies the name of the alarm.
Alarm Type	Values: <ul style="list-style-type: none"> • Alarm Button • Disabled (default) 	Identifies the type of alarm from the Emergency button.

Field	Contents	Description
Alarm Signal	Values: <ul style="list-style-type: none"> • Message • Call • Beacon Message 	Indicates how the alarm signals when the handset activates the alarm (Emergency) button. <ul style="list-style-type: none"> • Message—A text message is sent to the alarm server. • Call—An outgoing call is placed to the specified emergency number.
Stop Alarm from Handset	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Identifies if the handset can cancel the alarm.
Trigger Delay	Digit 0–255	Identifies the delay in seconds before the handset displays a pre-alarm warning. <ul style="list-style-type: none"> • 0—No pre-alarm warning; the alarm is sent immediately. • Other—The amount of time that the pre-alarm warning displays. When the number of seconds passes, the alarm is sent. It may take a few seconds for the alarm to be sent to the configured location.
Stop Pre-Alarm from Handset	Values: <ul style="list-style-type: none"> • Disabled • Enabled (default) 	Identifies if the user can stop an alarm.
Pre-Alarm Delay	Digit 0–255	Indicates the delay between the time the pre-alarm is displayed and the time that the alarm is signalled.
Howling	Values: <ul style="list-style-type: none"> • Disabled (default) • Enabled 	Indicates if the handset should start the howling signal. If disabled, only the call or message signal is sent.

Statistics Web Page Fields

The **Statistics** web page has a number of statistics views:

- System
- Calls
- Repeater (not used)

Each page has information to help you understand how your system is being used and helps you identify problems early.

System Web Page Fields

These are the fields displayed on the **System** link of the **Statistics** web page of the base station.

Table 65: Statistics: System Web Page Fields

Field	Description
Base Station Name	Contains the base IP address and name. The last row of the table contains the sum of all the preceding rows in the table. If there's only one base station in the system, then only the summary (Sum) row displays.
Operation/Duration D-H:M:S	Displays the time since the last reboot and the cumulative up-time since the last reset of statistics or the last firmware upgrade.
DECT Operation D-H:M:S	Identifies the time that the DECT protocol was active.
Busy	Contains the number of times that the base was busy (can't handle more active calls).
Busy Duration D-H:M:S	Displays the cumulative time that the base was busy.
SIP Failed	Displays the number of times that a SIP registration failed.
Terminal Removed	Displays the number of times that a handset was marked as removed.
Searching	Displays the number of times that the base was searching for its sync source. This field only displays on the 210 Multi-Cell Base Station.
Free Running	Displays the number of times that a base hasn't synchronized its data from the sync source. If this state is triggered often, you may need to make changes to your base station configuration. For more information, see Base Station States, on page 189 . This field only displays on the 210 Multi-Cell Base Station.
Source Changed	Displays the number of times that the base changed its sync source. This field only displays on the 210 Multi-Cell Base Station.

Calls Web Page Fields

These are the fields displayed on the **Calls** link of the **Statistics** web page of the base station.

Table 66: Calls Web Page Fields

Field	Description
Base Station Name	Contains the base IP address and name. The last row of the table contains the sum of all the preceding rows in the table. If there's only one base station in the system, then only the summary (Sum) row displays.
Operation/Duration D-H:M:S	Displays the time since the last reboot and the cumulative up-time since the last reset of statistics or the last firmware upgrade.
Count	Displays the number of calls handled on the base.
Dropped	Displays the number of active calls that were dropped. Each dropped call results in a syslog entry. An example of a dropped call is when a user is on an active call and then walks out of range of the base station.
Emergency calls	Displays the total number of emergency calls. This field is new for Firmware Release 4.7.
Call drops due to emergency call	Displays the number of calls dropped due to emergency calls. This field is new for Firmware Release 4.7.
Emergency calls rejected	Displays the number of rejected emergency calls. This field is new for Firmware Release 4.7.
No Response	Displays the number of calls that didn't respond to an incoming call because of hardware issues. Each calls results in a syslog entry. An example of a no response calls is if an external user tries to call a handset that isn't in range of the base station.
Duration D-H:M:S	Displays the total time that calls were active on the base.
Active	Displays the number of handsets that are active on the base at the present time.
Max Active	Displays the maximum number of calls that were active at the same time.
Codec G711U:G711A:G729:G722:G726:OPUS	Displays the number of times each codec was used in the calls.
Handover Attempt Success	Displays the number of successful handovers. This field only displays on the 210 Multi-Cell Base Station.
Handover Attempt aborted	Displays the number of failed handovers. This field only displays on the 210 Multi-Cell Base Station.

Field	Description
Audio Not Detected	Displays the number of times that an audio connection was not established.

Repeater Web Page Fields

These are the fields displayed on the **Repeater** link of the **Statistics** web page of the base station.

Table 67: Repeater Web Page Fields

Field	Description
IDX/Name	Contains the repeater index and name. The last row of the table contains the sum of all the preceding rows in the table. If there is only one repeater in the system, then only the summary (Sum) row displays.
Operation D-H:M:S	Displays the time since the last reset of statistics or the last firmware upgrade.
Busy	Displays the number of times that the repeater was busy.
Busy Duration D-H:M:S	Displays the time that the repeater was busy.
Max Active	Displays the maximum number of calls that were active at the same time.
Searching	Displays the number of times that the repeater searched for the sync source.
Recovery	Displays the number of times that the repeater couldn't connect to its sync source and synced to a different base or repeater.
Source Changed	Displays the number of times the repeater changed its sync source.
Wide Band	Displays the number of wide band calls.
Narrow Band	Displays the number of narrow band calls.

Generic Statistics Web Page Fields

These are the fields displayed on the **Generic Statistics** web page of the base station.

Each row gives a value and a graph of the data for the last 24 hours.

Table 68: DECT Statistics Fields

Field	Description
Total number of DLC instances	The life time total count of instantiated Data Link Control (DLC) instances.

Field	Description
Max concurrent DLC instances	The life time highest concurrent count of instantiated DLC instances.
Current number of DLC instances	The current count of instantiate DLC instances.
Total number of times in max DLC instances in use	The number of times we reach the currently highest count of DLC instances.
Total Time spend in max DLC instances in use (H:M:S)	The time spent in the highest concurrent number of instantiated DLC instances.
Average frequency x usage this hour (max 100 per slot) (where x is 0 to 9)	The average use of the frequency number x. The value is 100 if the frequency is used fully by a slot in the measured time frame.
Average even slot usage this hour (max 100 per slot)	The average use of the even-numbered slots.
Average odd slot usage this hour (max 100 per slot)	The average use of the odd-numbered slots.
Percentage time of x slots used this hour (where x is 0 to 12)	The percentage time usage of the x number of DECT slots for the current hour. The percentual time that X number of dect slots are used during the given hour (compared to other slot counts).
Total Codec usage (G.711A, G.711U, G.726, G.729)	This shows what codec, that have been used. The number of times we instantiate RTP stream using either codec. This field isn't available for Firmware Release 4.7.
Total CHO success	The number of times the connection handover is successful.
Total number of forced PP moves	The life time total count that this base forces PP moves.

The DECT Synchronization Statistics only display on the 210 Multi-Cell Base Station.

Table 69: DECT Synchronization Statistics Fields

Field	Description
Current synchronization state	The current DECT sync state. For example, Master, Searching, Free Running, and so on.
Current synchronization chain	The current DECT sync source Fp Id of this base.
Timestamp for last changed synchronization chain	Timestamp of the last time the DECT sync source changed for this base.
Hourly number of synchronization chain changes	The number of times the DECT sync source changed for this base in the current hour.

Field	Description
Total number of synchronization chain changes	The life time total count of times this base changed DECT sync source.
Total time in sync state: Master (H:M:S)	The time in the current hour when the base station's sync state was Master.
Total time in sync state: Locked (H:M:S)	The time in the current hour when the base station's sync state was Locked.
Total time in sync state: Free Running (H:M:S)	The time in the current hour when the base station's sync state was Alien Free Running.
Total time in sync state: Locked Assisted	The time in the current hour when the base station's sync state was Lock Assisted.
Total time in sync state: Sync Lost (H:M:S)	The time in the current hour when the base station's sync state was lost.
Total time in sync state: Searching (H:M:S)	The time in the current hour when the base station was searching for the source.
Total time in sync state: Unknown (H:M:S)	The time in the current hour when the base station's sync state wasn't Unknown.
Last reported sync information to this base	The time when the system last received the base station's sync information.

Table 70: RTP Statistics Fields

Field	Description
Total RTP connections (including connection type information, e.g. external, relay, recording)	The life time total count of instantiated RTP streams.
Max concurrent RTP connections (including connection type information, e.g. external, relay, recording)	The life time highest concurrent count of instantiated RTP streams.
Total Time spent in max RTP connections in use (H:M:S)	The time we have spent in the highest concurrent count of instantiated RTP streams.
Current RTP connections (including connection type information, e.g. external, relay, recording)	The current count of instantiated RTP streams.
Current local RTP connections	This field is new in Firmware Release 5.0. Indicates the use of number of active local RTP streams.

Field	Description
Current local relay RTP connections	This field is new in Firmware Release 5.0. Indicates the use of number of active local RTP relay streams.
Current remote relay RTP connections	This field is new in Firmware Release 5.0. Indicates the use of number of active remote RTP relay streams.
Current recording RTP connections	This field is new in Firmware Release 5.0. Indicates the current count of RTP recording streams.
Current Blackfin DSP status	This field is new in Firmware Release 5.0. This field only displays on the 210 Multi-Cell Base Station.
Total number of Blackfin DSP restarts	This field is new in Firmware Release 5.0. This field only displays on the 210 Multi-Cell Base Station.

Table 71: IP - Stack Statistics Fields

Field	Description
Total connections open	The life time total count of used sockets.
Max concurrent connections open	The life time highest concurrent count of used sockets.
Current connections open	The current count of the used sockets.
Total number of tx messages	The life time total count of transmitted IP packets.
Total number of rx messages	The life time total count of received IP packets.
Total number of tx errors	The life time total count of errors occurred during IP packet transmission.

Table 72: System Statistics Fields

Field	Description
Up time (H:M:S)	The time the base has been running consecutively.
Current CPU load	The current load percentage of the CPU. This information refreshes every 5 seconds.
Current Heap usage	The current use of heap in bytes.
Max Heap usage (%)	The peak usage of heap in percentage.
Mail queue ROS_SYSLOG	The size of the internal mail queue for syslogs.
Mail queue ROS_x (where x is 0 to 5)	The size of the internal mail queue.

Diagnostics Web Page Fields

The **Diagnostics** web page has these views:

- Base stations
- Extensions
- Logging

Each page has information to help you understand how your system is being used and helps you identify problems early.

Base Station

These are the fields displayed on the **Base stations** link of the **Diagnostics** web page of the base station.

Table 73: Base Stations Web Page Fields

Field	Description
Base Station Name	Indicates the IP address and name of the base station from the management settings. The last row of the table contains the sum of all the preceding rows in the table. If there is only one base station in the system, then only the summary (Sum) row displays.
Active DECT Ext (Mm/Ciss/CcOut/CcIn)	Indicates the number of active connections to extensions in the base station. <ul style="list-style-type: none"> • Mm—Mobility Management • Ciss—Call Independent Supplementary Service • CcOut—Call Control Out • CcIn—Call Control In
Active DECT Rep (Mm/Ciss/CcOut/CcIn)	Indicates the number of connections to repeaters in the base station. <ul style="list-style-type: none"> • Mm—Mobility Management • Ciss—Call Independent Supplementary Service • CcOut—Call Control Out • CcIn—Call Control In
Active RTP (Lcl/Rx BC)	Indicates the number of active RTP streams in use. <ul style="list-style-type: none"> • Lcl—local RTP stream • Rx BC—broadcast receive RTP stream

Field	Description
Active Relay RTP (Lcl/Remote)	Indicates the number of active relay streams. <ul style="list-style-type: none"> • Lcl—Local RTP relay stream • Remote—remove RTP relay stream
Latency [ms] (Avg.Min/Average/Avg.Max)	Indicates the latency of ping between the base station. <ul style="list-style-type: none"> • Avg.Min—average minimum delay • Average—average delay • Avg.Max—average maximum delay

Extensions

These are the fields displayed on the Extension view of the **Diagnostics** web page.

Table 74: Extensions Web Page Fields

Field	Descriptoin
Idx	Indicates the extension index number
No of HS restarts	Indicates the number of times that the handset has restarted.
Last HS restart(dd/mm/yyyy hh:mm:ss)	Indicates the date and time of the last handset restart.

Logging

These are the fields displayed on the Logging view of the **Diagnostics** web page.

Table 75: Logging Web Page Fields

Field	Descriptoin
RSX internal tracing	Indicates if internal tracing is Disabled or Enabled
PCAP internal tracing	
Trace packets to/from this base (except Audio)	
Trace audio packets to/from this base	
Trace received broadcast packets	
Trace received IPv4 multicast packets	

Field	Descriptoin
Trace received packet with destination MAC between (compare between each byte)	6 pairs
Trace received Ethertype	3 fields
Trace received IPv4 protocol	3 fields
Trace received TCP/UDP port	3 fields
Info	This field is new in Firmware release 5.0. This field is read only. This field displays The traces are stored in ring buffers, so please download the traces immediately after the incident has happened.
Download traces from	Click the All Basestations or Current Basestations button.

Configuration Web Page Fields

The **Configuration** web page of the base station displays a read-only version of the base station configuration file. The file is stored in the /Config folder TFTP server. Each base station has a unique configuration file, based on the MAC address.

You can make changes to a file in these ways:

- **[Recommended method]** Change the settings in the base station web pages and export the file for a backup.
- Export the file, make changes, and then upload the file.



Note If you choose to make manual changes, you must ensure that you retain all formatting. Otherwise, the phone may not be set up correctly.

Syslog Web Page Fields

The **Syslog** web page displays a live feed of system-level messages of the current base station. The Syslog level field in the **Management** web page controls the messages that are logged.



Note When the base station reboots, a new syslog starts and the previous information is lost. If you have a problem and plan to reboot, save the syslog file to your computer before you do the reboot.

If the **Syslog level** field is set for debug logs, additional information is written to the syslog. You should only capture debug logs for a short amount of time to minimize system congestion.



Note You will see frequent messages like this:

Sent to udp:xxx.xxx.xxx.xxx:xxxx at mm/dd/yyyy hh:mm:ss (4 bytes), where xxx.xxx.xxx.xxx:xxxx is the IP address and port, mm/dd/yyyy is the date, and hh:mm:ss is the time.

These are the keep alive messages and you can ignore them.

SIP Log Web Page Fields

The **SIP Log** web page displays a live feed of SIP server messages of the system (single cell, dualcell or multicell). The information is also saved as a file on the TFTP server. Logs are saved in 2 blocks of 17 KB, and when one block is full, the other one is used (it will overwrite previous content).

Filename: <MAC_address><time_stamp>SIP.log

Web Pages for Previous Firmware Releases

Extensions Web Page Fields for Firmware Release V450 and V460

These are the fields displayed on the **Extensions** web page of the base station.

The page displays in admin and user views. Not all fields are available in user view.

This section is applicable to Firmware Release V450 and V460. For Firmware Release 4.7, see [Extensions Web Page Fields, on page 106](#).

Table 76: General Section

Field	Contents	Description
AC	4-digit numerical code	Identifies the access code (AC) for the base station.

Table 77: Extensions Section

Field	Contents	Description
Idx	This field is read-only.	Identifies the index of the handset.
IPEI		Indicates the International Portable Equipment Identity (IPEI), the unique DECT identification number for the handset. This field is a link to further information about the handset in the Terminal page. The handset can appear in the list twice if it has 2 lines assigned to it.

Field	Contents	Description
Terminal State	This field is read-only	Indicates the current status of the handset: <ul style="list-style-type: none"> • Present@RPNxx—Handset is connected to the base station RPNxx; where xx is the number of the base station. • Detached—Handset is not connected (for example, powered off). • Located—Handset is powered on but can't connect to the base station. • Removed@RPNxxx—Handset has not connected to the base station (out of sight) for a specific amount of time, typically one hour.
Terminal Type, FW Info	This field is read-only	Identifies the handset model number and the firmware version.
FWU Progress	This field is read-only	Identifies the firmware update (FWU) state: <ul style="list-style-type: none"> • Off—Identifies that the sw version field is set to 0 in the Firmware Update page. • Initializing—Identifies that the update process is starting. • X%—Identifies the progress of the update, where X is the amount of progress (0–100) • Verifying X%—Identifies that the firmware verification is in progress before it is used. • Waiting for charger—Identifies that the firmware update is complete and the handset needs to be put into the charger to install the new firmware. • Conn.term.wait—Identifies that the repeater firmware update is complete and the repeater reset is in progress. • Complete—Identifies that the firmware update is complete. • Error—Identifies that the update was not successful. Possible reasons included: <ul style="list-style-type: none"> • File can't be found. • File isn't valid.
VoIP Idx	This field is read-only	Identifies the index of the configured SIP extension.

Field	Contents	Description
Extension		Identifies the telephone extension assigned to the handset. (Admin view only) This field is a link to further information about the handset in the Extension page.
Display Name	This field is read-only	Identifies the name assigned to the handset.
Server	This field is read-only	Identifies the Server IP Address or URL.
Server Alias	This field is read-only	Identifies the server alias, if configured.
State	This field is read-only	Identifies the SIP registration state and the base station that the handset is registered to. If the field is empty, the handset isn't SIP-registered.

Terminal Web Page Fields for Firmware Release V450 and V460


These are the fields displayed on the **Terminal** web page of the base station. You click on the IPEI number of the handset in the **Extensions** page to see this screen.

The page displays in admin and user views. Not all fields are available in user view.

This section is applicable to Firmware Release V450 and V460. For Firmware Release 4.7, see [Terminal Web Page Fields, on page 112](#).

Table 78: Terminal Web Page Fields

Field	Contents	Description
IPEI	10 character string	Identifies the International Portable Equipment Identity (IPEI) of the handset. Each handset has a unique IPEI number, and the number is displayed on the label under the handset battery and on the label of the handset box. If you change this field, the handset deregisters.
Paired Terminal	Values: <ul style="list-style-type: none"> • No Paired Terminal • Handset ID 	Identifies the terminal paired with the handset.
AC	4 digit code	Identifies the access code that was used to register the handset. After the handset registers, this code is not used. Note We recommend that you change this from the default when you start to set up your system to increase security.

Field	Contents	Description
Alarm Line	Values: <ul style="list-style-type: none"> No Alarm Line Selected Telephone number 	Identifies the line to be used for alarm calls.
Alarm Number	Phone number	Identifies the number to be dialed when a user presses and holds the Emergency  button on the handset for 3 seconds or more.
Dial Plan ID	Values: 1 to 10	Admin view only Identifies the index of the dial plan, configured in Dial Plans Web Page Fields , on page 153.
Battery and RSSI Status		
Battery level	Percentage	Read-only field Displays the current charge level of the handset battery.
RSSI		Read-only field Displays the Received Signal Strength Indicator (RSSI) for the connected base station or repeater.
Measured time [mm:ss]		Read-only field Displays the time in minutes and seconds since the battery and RSSI information was captured from the handset.
Located		Read-only field Identifies the connected base station or repeater with which the handset communicates.
Beacon Settings		
Receive Mode	Values: <ul style="list-style-type: none"> Disabled (default) Enabled 	Admin view only Reserved for future use.
Transmit Interval	Values: <ul style="list-style-type: none"> Disabled (default) Enabled 	Admin view only Reserved for future use.
Alarm Profiles		

Field	Contents	Description
Profile 0 to 7		Admin view only Indicates the list of alarms.
Alarm Type	Name of the alarm	Admin view only Indicates which alarm type is configured for the particular profile. When no alarms are configured, the field displays <code>Not configured</code> .
Alarm Type check box	Check box (default unchecked)	Admin view only Identifies the alarm type that is active on the handset.
Shared Call Appearance Settings		
Idx 1 to 8		Admin view only Index of the extensions
Extension	Extension number	Admin view only Identifies the handset lines that support Shared Call Appearances. When no lines support the feature, the field displays <code>Not configured</code> .
Import Local Phonebook	Filename	Used to upload a local directory from a computer to the phone in comma separated value (CSV) format. For more information, see Local Contacts Setup, on page 67 .
Export Local Phonebook		Used to export a local directory from a phone to the computer in CSV format. For more information, see Local Contacts Setup, on page 67 .

View the Handset Status

You can see the status of your handset to assist in troubleshooting problems. Information includes the firmware version installed on the handset as well as information about the connected base station.

Procedure

-
- Step 1** Press **Menu** .
- Step 2** Select **Settings**  > **Status**.
-

Perform a Site Survey

You do a site survey to check that you have your base stations placed so that the handsets can connect easily. Each base station has radio coverage of about 164 feet (50 meters) indoors and up to 984 feet (300 meters) outdoors. However, there can be interference with other equipment as well as poor coverage because of wall and door construction (for example, fire doors).

You perform a site survey:

- During initial setup: you can place your base stations in temporary locations and power them on. They don't need to be connected to the LAN. You perform the survey to check that the handsets can communicate with the base.
- After setup is complete: you can perform a survey to ensure that the system is working correctly and to troubleshoot user connection problems.

You use the handset to check that coverage is good for your users in all the areas to be covered.





Note In the handset, you can adjust the signal strength for the handset radio. However, we recommend that you speak to your service provider or Cisco TAC to discuss the signal strength change.

Perform this task when you set up your system and when there are changes to the area (for example, changes to walls, or new areas added).

Before you begin

You need at least one handset fully charged.

Procedure




- Step 1** On the handset, press and hold **Power/End**  until the screen turns on.
- Step 2** Press **Menu** .
- Step 3** Enter ***47*** to get a list of base stations and repeaters within range.
- Step 4** (Optional) Press **Settings** to view the dBm threshold for the ranges.
- **Green to yellow:** identifies the threshold value for the yellow indication. For example, if this field contains -70dBm, a reading of -69 dBm will display green and -70 dBm will display yellow. The default is -70 dBm.
 - **Yellow to red:** identifies the threshold value for the red indication. For example, if this field contains -80dBm, a reading of -79 dBm will display yellow and -80 dBm will display red. The default is -80 dBm.

To change the range,

- Highlight one of the entries and press **Select**.
- Highlight a new value from the list and press **Select**.

Step 5 Highlight a MAC address and IP address pair in the **IP Search** list and press **Select**.

The screen displays this information about the selected base station or repeater:

- Signal strength icon:
 - Green check mark : the handset has very good DECT contact with the base station or repeater in the current location.
 - Amber triangle icon : the handset has adequate DECT contact with the base station or repeater in the current location.
 - Red circle icon : the handset has poor or no DECT contact with the base station or repeater in the current location. In this situation, you need to either move the base station to get better coverage, add another base station, or add a repeater.
- MAC: the MAC address of the base station.
- IP: the IP address of the base station.
If the base station is powered on but isn't connected to the LAN, the handset displays 0.0.0.0.
- RFPI: the Radio Fixed Part Identity (RFPI) of the base station.
- RSSI: the Received Signal Strength Indicator of the signal from the base station to the handset.

Step 6 Press **Power/End**  until you return to the main screen.

Step 7 Move to a different location and repeat Steps 2, 3, and 5 to check the coverage.



CHAPTER 6

Maintenance

- [Reboot the Base Station from the Web Pages, on page 175](#)
- [Reboot the Base Station Remotely, on page 176](#)
- [Remove the Handset from the Web Page, on page 176](#)
- [Remove the Handset Remotely, on page 177](#)
- [Reset the Base Station to Factory Defaults, on page 177](#)
- [Reset the Handset to Factory Defaults, on page 177](#)
- [Verify the System Configuration, on page 178](#)
- [Back Up the System Configuration, on page 178](#)
- [Restore the System Configuration, on page 179](#)
- [System Upgrades and Downgrades, on page 179](#)
- [View Base Statistics, on page 188](#)

Reboot the Base Station from the Web Pages

When you need to reboot the base station, you have two reboot choices:

- **Reboot**—The reboot takes place when the base station has no active connections, such as active calls, directory access, or firmware update activity.
- **Forced Reboot**—The reboot takes place within 1 minute. Activity on the base station immediately stops.



Note When the base station reboots, a new syslog starts and the previous information is lost. If you have a problem and plan to reboot, save the syslog file to your computer before you do the reboot.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

The base station needs to be connected to the network and the green LED lit.

Procedure

- Step 1** Access the **Home/Status** page.
 - Step 2** Click **Reboot** or **Forced Reboot**.
-

Reboot the Base Station Remotely

You may receive the SIP Notify to reboot the base station from the call control system. The SIP Notify contains the event `Event:check-sync`. If the parameter `Sip_Check_Sync_Always_Reboot` is set to `On`, the base station initiates a reboot.

For more information about SIP Notify authentication, see [Configure the SIP Notify Authentication, on page 53](#).

You can reboot the base station remotely in this way.

Before you begin

Ensure that the base station is idle.

Procedure

Send SIP notify from the call control system.

The base station reboots automatically.

Remove the Handset from the Web Page

You may need to remove the handset, if the handset is faulty or there are problems with the handset. You can remove the handset this way from the **Extensions** web page.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

- Step 1** Click **Extensions**.
 - Step 2** Click the link in the **Extension Info** column for the handset.
 - Step 3** Set the IPEI number to `FFFFFFFFF`.
 - Step 4** Click **Save**.
-

Remove the Handset Remotely

You may receive the SIP Notify to reset the handset's IPEI number from the call control system. The notification contains the handset index number. For example, `Event:reset-ipei-for-handset;hs=1`.

For more information about SIP Notify authentication, see [Configure the SIP Notify Authentication, on page 53](#).

You can reset the handset's IPEI number remotely in this way.

Before you begin

Ensure that the handset and the extensions aren't used.

Procedure

Send SIP Notify from the call control system.

The handset's IPEI number is reset as `FFFFFFFF` and the handset isn't configured to the extension.

Reset the Base Station to Factory Defaults

The reset button is located on the bottom edge of the base station.

Before you begin

The **Factory reset from button** field in the **Management** Settings page must be enabled. For more information, see [Set Up Management Settings, on page 72](#) and [Management Web Page Fields, on page 126](#).

Procedure

Press and hold the reset button for 10 seconds.

You can release the button when the LED turns red.

Reset the Handset to Factory Defaults

Occasionally, you need to reset a handset to factory defaults. The reset deletes any information you stored in the handset (for example, ringtones). Any content that is controlled by the base station (for example, system configuration) is not deleted.

Procedure

- Step 1** Press **Menu** .
- Step 2** Select **Settings**  > **Reset settings**.
-

Verify the System Configuration

After you set up the system, check that you can make calls and receive calls from within the system and from external numbers. For each of the steps below, the called device rings and you are able to hear and talk from both devices.

If you have problems, the [Troubleshooting, on page 191](#) chapter may help you.

Before you begin

You need these devices to be configured and active:

- One base station
- Two handsets

Procedure

- Step 1** Call from one handset to the other and ensure that you have a two-way audio path.
- Step 2** Call from one of the handsets to an external number (for example, a mobile phone) and ensure that you have a two-way audio path.
- Step 3** Call to one of the handsets from an external number and ensure that you have a two-way audio path.
-

Back Up the System Configuration

You should back up your system configuration. Export the configuration as a file, and save it in a secure location. Remember that the export file may contain sensitive text.

For information on the configuration, see [Configuration Web Page Fields, on page 167](#).

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

Step 1 Click **Configuration**.

Step 2 Click **Export**.

If your browser displays the configuration in a new browser window, you have encountered a known browser problem. Return to the administration screen, right-click on **Export** and select **Save link as**.

Step 3 Set the filename and location for the export, and click **OK**.

Related Topics

[Restore the System Configuration](#), on page 179

Restore the System Configuration

If your base station loses its configuration, you can load the backed-up configuration file to restore the system.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

You need a configuration file, for example, a file created from [Back Up the System Configuration, on page 178](#).

Procedure

Step 1 Click **Configuration**.

Step 2 Click **Choose File**.

Step 3 Navigate to the location and exported filename, and click **OK**.

Step 4 Click **Load**.

Related Topics

[Back Up the System Configuration](#), on page 178

System Upgrades and Downgrades

You can upgrade the Cisco IP DECT 6800 Series base stations, handsets, and repeaters with the updated software.

You can downgrade the Cisco IP DECT 6800 Series base stations, handsets, and repeaters to an earlier Firmware version. The base stations, handsets, and repeaters can't be downgraded lower than Firmware version 4.8(1) SR1. If you attempt to downgrade to a Firmware from version lower than 4.8(1) SR1, the secured data can't be decrypted and a message is saved in the system log.

For the procedure to downgrade the base station and handsets, see [Downgrade the Base Stations, on page 186](#) and [Downgrade the Handsets , on page 187](#).

The software is available on cisco.com at <https://software.cisco.com/download/home/286323307>.

Each software release has release notes available here: <https://www.cisco.com/c/en/us/support/collaboration-endpoints/ip-dect-6800-series-multiplatform-firmware/products-release-notes-list.html>.

The software from the release is loaded onto a TFTP, HTTP, or HTTPS server. You upgrade or downgrade the base station first, then upgrade or downgrade the handsets. After the base station upgrades or downgrades, it automatically reboots. After the handsets upgrades or downgrades, they automatically reboot.

Upgrade or Downgrade Workflow

The following workflow describes the steps you take to prepare the TFTP, HTTP, or HTTPS server and upgrade or downgrade the system. Some steps you typically only do once, during the initial setup.



Note We recommend that you upgrade or downgrade the base station first, then upgrade or downgrade the handsets after the base station upgrade completes.

Before you begin

You need to have a TFTP, HTTP, or HTTPS server available.

Procedure

	Command or Action	Purpose
Step 1	(Do this one time) Prepare TFTP, HTTP, or HTTPS Server for Upgrades or Downgrades, on page 180	Sets up the required TFTP server directory structure.
Step 2	(Do this one time) Set Up the Firmware Update Parameters, on page 181	Identifies the TFTP server and directory.
Step 3	Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server, on page 181	Places the firmware files in the TFTP directory structure
Step 4	Upgrade the Base Stations, on page 183 or Downgrade the Base Stations, on page 186	Instructs the base station to transfer the firmware file from the TFTP server and install the firmware in memory.
Step 5	Upgrade the Handsets, on page 184 or Downgrade the Handsets, on page 187	Instructs the handsets to transfer the firmware file from the TFTP server and install the firmware in memory.

Prepare TFTP, HTTP, or HTTPS Server for Upgrades or Downgrades

Before you download the firmware, set up the required directory structure on your TFTP, HTTP, or HTTPS server. The base station, handset, and repeater firmware must go into specific folders.

You only need to do this task once.

Before you begin

You need a TFTP, HTTP, or HTTPS server configured and active.

Configure the TFTP, HTTP, or HTTPS server timeout for at least 3 seconds.

Procedure

-
- Step 1** Open the root folder of the TFTP, HTTP, or HTTPS server file system.
- Step 2** Create a subdirectory. For example, `Cisco`.
-

What to do next

[Set Up the Firmware Update Parameters, on page 181](#)

Set Up the Firmware Update Parameters

Typically, you only do this task once.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

You need the IP address or fully-qualified directory name (FQDN) of the TFTP, HTTP, or HTTPS server.

Procedure

-
- Step 1** Click **Firmware Update**.
- Step 2** Enter the TFTP, HTTP, or HTTPS server IP address or FQDN into the **Firmware update server address** field.
- Step 3** Enter `Cisco` into the **Firmware path** field.
- Step 4** Click **Save/Start Update**.
-

Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server

You access the Cisco Software Download page to get the firmware in zip files. The zip files contain these firmware files:

- For the base station, the zip filename starts with:
 - `IPDect-DBS110` for Cisco IP DECT 110 Single-Cell Base Station
 - `IPDect-DBS210` for Cisco IP DECT 210 Multi-Cell Base Station
- From Firmware Release 5.0, the zip filename for the repeater starts with `IPDect-RPT-110` for Cisco IP DECT 110 Repeater.

For the Firmware Release earlier than 5.0, the zip filename for the repeater starts with `IPDect-RPT110` for Cisco IP DECT 110 Repeater.

- For the handsets, the zip filename starts with:
 - `IPDect-PH6823` for Cisco IP DECT Phone 6823 Handset
 - `IPDect-PH6825` for Cisco IP DECT Phone 6825 Handset
 - `IPDect-PH6825RGD` for Cisco IP DECT Phone 6825 Ruggedized Handset



Note For Firmware Release earlier than 5.0, when the Cisco IP DECT Phone 6825 Handset and Cisco IP DECT Phone 6825 Ruggedized Handset have the same version and branch, you only need the `IPDect-PH6825` file.

Before you begin

You need the TFTP, HTTP, or HTTPS server information.

Procedure

- Step 1** From your browser, go to <https://software.cisco.com/download/home/286323307>.
- Step 2** If required, sign in with your user ID and password.
- Step 3** Click **IP DECT 210 Multi-Cell Base-Station**.
- Step 4** Select the release.
- Step 5** Download the zip file for the required version.
- Step 6** Return to <https://software.cisco.com/download/home/286323307>.
- Step 7** (Optional) Click **IP DECT 110 Repeater with Multiplatform Firmware**.
- Select the release.
 - Download the zip file for the required version.
 - Return to <https://software.cisco.com/download/home/286323307>.
- Step 8** (Optional) Click **IP DECT 210 Multi-Cell Base Station with Multiplatform Firmware**.
- Select the release.
 - Download the zip file for the required version.
 - Return to <https://software.cisco.com/download/home/286323307>.
- Step 9** Click **IP DECT 6825 with Multiplatform Firmware**.
- Step 10** Select the release.
- Step 11** Download the zip file for the required version.
- Step 12** (Optional) Click **IP DECT 6825 with Multiplatform Firmware**.
- Select the release.
 - Download the zip file for the required version.
- Step 13** On your PC, unzip the files.
- Step 14** Access the TFTP, HTTP, or HTTPS server file system.

- Step 15** If not available, create a `Cisco` directory.
 - Step 16** Open the `Cisco` directory.
 - Step 17** Copy the new base station firmware file to the `Cisco` folder.
 - Step 18** Copy the new repeater firmware file to the `Cisco` folder.
 - Step 19** Copy the new handset firmware file to the `Cisco` folder.
-

What to do next

[Upgrade the Base Stations, on page 183](#) or [Downgrade the Base Stations, on page 186](#)

[Upgrade the Handsets, on page 184](#) or [Downgrade the Handsets, on page 187](#)

Upgrade the Base Stations

The Firmware filename is available in a new format from the Firmware Release 5.0. For example, DBS-210-3PC.04-80-01-0001-02.fwu. You must enter the complete filename with the extension into the upgrade page.

The filename of the Firmware versions earlier than 5.0 contains the version (v) and branch number (b). For example, DBS-210_v0470_b0001.fwu is version 470 and branch 1. When you upgrade to Firmware versions earlier than 5.0, you can enter the firmware version and branch number without the leading zeros.



Note You should upgrade the base station when it's inactive. All the active calls drop when the upgrade starts. During the upgrade, the base station LED flashes in the order green, red, green, and amber. Don't power off the base station while the LED flashes. The upgrade may take about 30 minutes to 1 hour to complete and reboot the base station.



Note We recommend that you upgrade the base station first, then upgrade the handsets after the base station upgrade completes.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#). If you have multiple base stations, you should sign into the primary base station.

You need to have completed [Set Up the Firmware Update Parameters, on page 181](#) and [Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server, on page 181](#).

Procedure

- Step 1** Click **Firmware Update**.
- Step 2** Enter the Firmware filename with the extension in the **Firmware** version field for the base station.
- Step 3** Click **Save/Start Update**.

Step 4 Click **Save** in the pop-up window.

Step 5 In the warning window, click the browser **Back** arrow.

Step 6 Wait a few seconds, then click **Syslog**.

Step 7 Verify that you see the message based on the Firmware version:

- Firmware Release 5.0: Example `DBS-110-3PC 0c:75:bd:33:f8:ca -- Requesting upgrade betaware.rtx.net/MPE/test/bin/DBS-110-3PC-05-00-01-0001-12.fwu`
- Firmware Release earlier than 5.0: `Firmware update started to version vvvv branch bbbb`

Where:

- vvvv is the version number.
- bbbb is the branch number.

After a few minutes, the base station will automatically reboot and you need to sign into the administration page. When the handsets register with the base station, the base station upgrade is complete.

Upgrade the Handsets

The Firmware filename is available in a new format from the Firmware release 5.0. For example, 6825-05-00-01-0002-14.fwu. You must put the complete filename with the extension into the upgrade page.

The filename of the Firmware versions earlier than 5.0 contains the version (v) and branch number (b). For example, 6825-210_v0470_b0001.fwu is version 470 and branch 1. When you upgrade to Firmware versions earlier than 5.0, you can enter the firmware version and branch number without the leading zeros.

The 6823 Handset, 6825 Handset, and the 6825 Ruggedized Handset have different firmware file from the Firmware release 5.0.

After you start the upgrade from the web page, all handsets download and load the new firmware file. The upgrade may take 20-30 minutes to download and verify, and an extra few minutes to load the new firmware file on the handset. The handset must be placed in the charger and not removed until the handset loads the firmware file and reboots. While the handset loads the new firmware, the LED flashes in the order green, red, green, and amber. The handsets automatically reboot at the end of the upgrade.

The **Extensions** page shows the upgrade progress in the **FWU Progress** column.

- During the download, the column shows the download progress as a percentage. For example, 41%.
- After the file is downloaded, it's verified and the column shows the verification progress as a percentage. For example, `Verifying 23%`.
- If the verification is complete and the handset isn't on the charger, the column shows `Waiting for charger`.
- If the verification is complete and the handset is placed in the charger, the column shows `Waiting for charger` before it shows `Restarting`.
- When the upgrade is complete, the column shows `Complete`.

If the **FWU Progress** shows `Off`, the version and branch in the Firmware Update page are set to 0.



Note We recommend that you update the base station first, then update the handsets after the base station update completes.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

You need to have completed [Set Up the Firmware Update Parameters, on page 181](#) and [Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server, on page 181](#).

Procedure

- Step 1** Click **Firmware Update**.
- Step 2** Enter the Firmware filename with the extension in the **Firmware** version field for all the handsets.
- Step 3** Click **Save/Start Update**.
- Step 4** Click **Save** in the pop-up window.
- Step 5** In the warning window, click the browser **Back** arrow.
- Step 6** Wait a few seconds, then click **Syslog**.
- Step 7** Verify that you see the message based on the Firmware version: .
- Firmware Release 5.0: `Example Firmware update started to Version 05-00-01-0001-11 for Handset: 0`
 - Firmware Release earlier than 5.0: `Firmware update started to version vvvv branch bbbb for handset: x`
- Where:
- vvvv is the version number.
 - bbbb is the branch number.
 - x is the handset number.
- You should see one message for each handset registered to the base station. If you don't see this message, there may be error messages.
- Step 8** Click **Extensions**.
- The **FWU Progress** column displays the upgrade status. Refresh your browser to monitor the progress.
- Step 9** If you see the message `Waiting for charger`, put the handset in the charging cradle.
- Caution** Don't remove the handset from the charger until the upgrade completes. At the end of the upgrade, the handset reboots before it can be used.
-

Downgrade the Base Stations



Note You can downgrade the base stations running Firmware version 5.0(1) only to the latest branch of Firmware version 4.8(1) SR1.

The firmware filename contains the version (v) and branch number (b). For example, DBS-210_v0480_b0001.fwu is version 480 and branch 1. When you put the firmware version and branch number into the **Firmware Update** page, you don't need the leading zeros.



Note During the downgrade, the base station LED flashes in the order green, red, green, and amber. Don't power off the base station while the LED flashes. The downgrade may take about 30 minutes to 1 hour to complete and reboot the base station.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#). If you have multiple base stations, you should sign into the primary base station.

You need to have completed [Set Up the Firmware Update Parameters, on page 181](#) and [Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server, on page 181](#).

Procedure

- Step 1** Click **Firmware Update**.
- Step 2** Check the check box for the option **Enable legacy firmware naming**.
- Step 3** Enter the new firmware version in the **Required version** field for the base station.
- Step 4** Enter the branch number in the **Required branch** field for the base station.
- Step 5** Click **Save/Start Update**.
- Step 6** Click **Save** in the pop-up window.
- Step 7** In the warning window, click the browser **Back** arrow.
- Step 8** Wait a few seconds, then click **Syslog**.
- Step 9** Verify that you see the message `Firmware upgrade started to version vvvv branch bbbb`.

Where:

- vvvv is the version number.
- bbbb is the branch number.

After a few minutes, the base station will automatically reboot and you need to sign into the administration page. When the handsets register with the base station, the base station downgrade is complete.

Downgrade the Handsets



Note You can downgrade the base stations running Firmware version 5.0(1) only to the latest branch of Firmware version 4.8(1) SR1.

The firmware filename contains the version (v) and branch number (b). For example, 6825-210_v0480_b0001.fwu is version 480 and branch 1. When you put the firmware version and branch number into the **Firmware Update** page, you don't need the leading zeros.

The 6825 Handset, 6825 Ruggedized Handset, and 6823 Handset have their own firmware file.

After you start the downgrade from the web page, all handsets download and load the new firmware file. The downgrade may take 20-30 minutes to download and verify, and an extra few minutes to load the new firmware file on the handset. The handset must be placed in the charger and not removed until the handset loads the firmware file and reboots. While the handset loads the new firmware, the LED flashes in the order green, red, green, and amber. The handsets automatically reboot at the end of the downgrade.

The **Extensions** page shows the downgrade progress in the **FWU Progress** column.

- During the download, the column shows the download progress as a percentage. For example, 41%.
- After the file is downloaded, it's verified and the column shows the verification progress as a percentage. For example, *Verifying 23%*.
- If the verification is complete and the handset isn't on the charger, the column shows *Waiting for charger*.
- If the verification is complete and the handset is placed in the charger, the column shows *Waiting for charger before it shows Restarting*.
- When the downgrade is complete, the column shows *Complete*.

If the **FWU Progress** shows *Off*, the version and branch in the Firmware Update page are set to 0.



Note We recommend that you download the base station first, then download the handsets after the base station update completes.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

You need to have completed [Set Up the Firmware Update Parameters, on page 181](#) and [Download and Copy the Firmware Files to the TFTP, HTTP, or HTTPS Server, on page 181](#).

Procedure

- Step 1** Click **Firmware Update**.
- Step 2** Enter the new firmware version in the **Required version** field for all the handsets.
- Step 3** Enter the branch number in the **Required branch** field for all the handsets.

- Step 4** Click **Save/Start Update**.
- Step 5** Click **Save** in the pop-up window.
- Step 6** In the warning window, click the browser **Back** arrow.
- Step 7** Wait a few seconds, then click **Syslog**.
- Step 8** Verify that you see the message `Firmware upgrade started to version vvvv branch bbbb for handset: x`.
- Where:
- vvvv is the version number.
 - bbbb is the branch number.
 - x is the handset number.
- You should see one message for each handset registered to the base station. If you don't see this message, there may be error messages.
- Step 9** Click **Extensions**.
- The **FWU Progress** column displays the downgrade status. Refresh your browser to monitor the progress.
- Step 10** If you see the message `Waiting for charger`, put the handset in the charging cradle.
- Caution** Don't remove the handset from the charger until the downgrade completes. At the end of the downgrade, the handset reboots before it can be used.
-

View Base Statistics

You should check the statistics stored in the base station on a regular basis. If you see problems, you can proactively identify and address any issues. The page contains statistics for:

- System
- Calls
- DECT

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

The base station needs to be connected to the network and the green LED lit.

Procedure

- Step 1** Click **Statistics**.
- Step 2** Click the links to view the different base station statistics, as described in [Statistics Web Page Fields, on page 158](#).

Step 3 (Optional) Click **Export** to export the data on the displayed page in comma separated value (CSV) format.

Step 4 (Optional) Click **Clear** to reset all the statistics to zero (0).

All statistics page statistics are set to 0.

Base Station States

The base station is normally in the *Locked* state. If there are problems, the base station can automatically change to *Free running* state.

Free running state is when a base station has not synchronized its data from the sync source after a period of time. When this happens, the base station will change to a new state after two minutes:

- If the base station is idle, the state changes to *Searching*.
- If the base station has an active call, the state changes to *Sync lost*. When the call completes, the status changes to *Searching*.

Reasons for the *Free running state* can include:

- There are two bases using the same DECT slots and therefore can't see each other.
- There were many simultaneous voice or data calls.
- There was a sudden change of environment (for example, a fire door closed).
- There was a distortion of DECT frequency (around 1.8MHz) either by other DECT systems or other equipment.

When the base station goes into *Free running* state, you can do one or both of these things:

- Change the DECT slot. This may enable the base station to connect to its synchronization source.
- Change the state to *Assisted lock*. This enables the base station to use information from other base stations.

If the *Assisted lock* state is stable for a long time, you can change the state back to *Locked*. The *Free running* state may also change back to *Locked*.



CHAPTER 7

Troubleshooting

- [Base Station Installation Problems, on page 191](#)
- [Repeater Installation Problems, on page 192](#)
- [Handset Installation Problems, on page 192](#)
- [Operational Problems with the Base Station, on page 194](#)
- [Operational Problems with the Handset, on page 194](#)
- [Dualcell Troubleshooting, on page 197](#)
- [Multicell Troubleshooting, on page 197](#)
- [Troubleshooting Procedures, on page 198](#)

Base Station Installation Problems

Base Station LED is Solid Red

Problem

The LED on the base station doesn't change to green.

Cause

The base station can't get an IP address.

Solution

- Test the Ethernet cable with another device to check for signal.
- Ensure that the Ethernet cable is connected on the switch.
- Check that the DHCP server is available on the network.
- Replace the Ethernet cable with one that you know is working.

Repeater Installation Problems

Can't Set Up a Repeater - LED is Red

Problem

The repeater LED is red and registration of fails.

Cause

The repeater is not in registration mode.

Solution

Reset the repeater with one of these options:

- Unplug the repeater. Wait 30 seconds, then plug the repeater in again.
- Press and hold the reset button on the bottom edge of the repeater for 5 seconds.

Handset Installation Problems

Handset Won't Register (Automatic Configuration)

Problem

The initial setup of a handset is complete, but the handset won't register with a base station or repeater.

Cause

The base station isn't working, the base station isn't in range, or the base station is not trying to connect with the handset.

Solution

Check the following items:

- If the handset displays the message `Can't locate a base station`, check that the base station is working. If it is working, move the handset close to the base station. You may need to extend the network with an additional multicell base station. If you have a single cell base station, you may need to change to a multicell system.

If the handset displays the message `Can't locate a base station`, check that the base station is working. If it is working, move the handset close to the base station. You may need to extend the network with an additional multicell base station or repeater. If you have a single cell base station, you may need to change to a multicell system or add a repeater.

- If the handset displays the message `Sign in error`. Contact your administrator., there is a problem with the user's configuration or authentication. Contact your service provider.
- If the handset displays the message `Device error`. Contact your administrator, contact your service provider. This message indicates that you have reached the maximum number of handsets you can configure.
- If the handset displays the message `Registration timeout`. Contact your administrator, check that the base station is working and within range of the handset. If the timeout continues, contact your service provider.
- If the handset displays the message `Access Code error`. Enter the code or contact your administrator:
 - If there are multiple base stations within range, check that the user is trying to access the correct base station.
 - Verify that you have given the correct access code for the selected base station.

Handset Won't Register (Manual Configuration)

Problem

The initial setup of a handset is complete, but the handset won't register with a base station or repeater.

Cause

The configuration is incomplete or incorrect, the base station isn't working, the base station isn't in range, or the base station is not trying to connect with the handset.

Solution

Check the following items:

- If the IPEI number of the handset is configured in the **Extensions** web page, ensure that the IPEI is correct. If it isn't correct, change it.
- Check that the base station LED is green and that the handset is in range of a base station or a repeater. If the base station isn't in range, you may need to add a repeater to the system.
- Access the **Extensions** web page, check the **VoIP Idx** check box associated with the handset, and click **Start SIP Registration(s)**.

Handset Can't Register

Problem

The handset displays `Deregistered`. When you try to register the handset in the **Extensions** web page, the handset doesn't register.

Solution

1. In the **Extensions** web page, click the **Refresh** button.
2. You may be prompted to reconnect the handset to the base station.
3. If the handset doesn't register, contact your service provider.

Operational Problems with the Base Station

Base Station LED Flashes Red and Handset Displays "No SIP Reg" Message

Problem

The LED on the base station flashes red. One or more handsets display the message No SIP Reg. In the base station administration **Extensions** web page, the handset status doesn't say SIP Registered.

Cause

The base station can't communicate with the call control system.

Solution

1. Sign into the base station administration web page.
2. Click **Extensions**.
3. In the **VoIP Idx** column, check the check box for each handset that is not registered.
4. Click **Start SIP Registration(s)**.

Operational Problems with the Handset

This section contains troubleshooting information for common handset problems.

Handset Won't Turn On



Problem

The handset has a battery installed but won't turn on.

Cause

The battery doesn't have sufficient charge, the plastic tab over the battery contacts aren't removed, or the battery has failed.

Solution

1. Place the handset in the charger and monitor it. If the screen turns on after a few minutes, the battery was depleted and needs to be fully charged. You can confirm the battery level from the **Menu**  > **Settings**  > **Status** screen while the handset is in the charger.
This happens if the handset hasn't been used for a long period of time.
2. If the handset won't turn on after 10 minutes on the charger, remove the battery and replace it with a battery that you know is charged. If the handset now works, the battery may have failed.

Handset Won't Stay On

Problem

The handset won't stay powered on when not in the charging cradle. When in the charging cradle, the handset turns on.

Solution

Check:


- Does the handset have a battery installed? You can use the handset in the cradle with no battery, but it needs the battery as soon as you remove it from the cradle.
- If the handset is new, has the plastic tab over the battery contacts been removed?
- Have you tried to use the handset with a charged battery from another handset?

Handset Doesn't Ring


Problem

The phone can receive calls but no ringtone is heard.

Cause

The phone may be in silent mode and the silent mode icon  is displayed in the screen header.

Solution

- Increase the volume from the **Settings**  menu.
- Press and hold the pound (#) key for two seconds while the phone is idle to disable silent mode.

Handset Doesn't Respond to Key Presses

Problem

Nothing happens when you press a key on the handset.

Cause

The keypad is probably locked.

Solution

Press and hold the star (*) key for 2 seconds to unlock the keypad.

Handset Beeps Continuously While in the Charger

Problem

The handset beeps continuously when placed in the charger.

Solution

Check these scenarios:

- The handset wasn't placed in the charger so that the contacts on the handset and charger touched.
- The handset is new and this is the first time it has been placed on the charger. Check that the plastic on the battery has been removed.

If none of the scenarios apply, the battery may be defective. Put a battery that you know works into the handset and place the handset in the charger. If the handset doesn't beep, then the original battery is defective.

Handset Screen Displays "Searching"

Problem

The handset displays the message *Searching*.

Cause

The handset is too far from the closest base station or the base station isn't active.

Solution

- If the handset has been stationary, the base station may be rebooting or inactive.
 1. Wait a couple of minutes to see if the handset can communicate with the base station.
 2. If the problem persists, check that the base station has power and the LED is green. If the handset power was off while searching for the base station, it takes more time to register after the handset power is on.

- If the handset has been carried around, it may be out of range of the base station.
 - Short term solution: Move the handset closer to the base station.
 - Long term solution for system with one single cell base station:
 - Add another 110 Single-Cell Base Station to set up a dualcell system.
 - Add repeaters to improve coverage.
 - Long term solution for system with one multi-cell base station: Add additional 210 Multi-Cell Base Stations or repeaters to improve coverage.
 - Long term solution for dualcell system: Change the base stations to 210 Multi-Cell Base Station or add repeaters to improve coverage.
 - Long term solution for multicell system: Add one or more 210 Multi-Cell Base Stations or repeaters to improve coverage.

No Audio on Your Handsets with a Single Base Station System

Problem

You have one base station and two or more handsets. But when you try to call from one handset to the other, you don't hear anything on either phone.

Solution

1. Sign into the base station web page.
2. Click **Network Settings**.
3. Verify that the field **Use Different SIP Ports** is set to **Enabled**.

Dualcell Troubleshooting

If you have problems with a dualcell system, you may need to turn on extra logs to debug the problem. For more information, see [Turn On Dualcell Debug Logs, on page 201](#).

Multicell Troubleshooting

If you have problems with a multicell system, you may need to turn on extra logs to debug the problem. For more information, see [Turn on Multicell Debug Logs, on page 201](#).

Base Station Shows Searching in DECT Property

Problem

You have set up a multicell system, but the **Multi cell** web page shows **Searching!** in the **DECT property** column.

Cause

The base stations can't communicate.

Solution

Check these things:

- The base station that can't connect is too far from the other base stations. Move the base station closer, or add another base station between the one that can't communicate and the base stations already set up.

Look at the field **DECT sync source** in the **Multi cell** page. Each base station in the system shows the signal strength it receives in decibels per milliwatt (dBm).

- -75 dBm or lower is recommended.
 - -76 to -85 dBm is acceptable.
 - -86 to -90 dBm is acceptable but you should consider adding another base station.
 - -91 dBm and above, you must add another base station.
- There is something interfering with the radio signal. For example, there may be a door or equipment that disrupts the radio communications. You may need to move the base station.
 - On the **Home/Status** web page for each base station, compare the **RF Band** fields to ensure that they have the same band configured. You must have all base stations on the same RF band for the base stations to communicate. You also must have all base stations on the RF band for your country. The RF band is configured on the base station in the factory.

Troubleshooting Procedures

These procedures can be used to identify and correct problems.

Collect Troubleshooting Logs for a General Problem

When you have problems with your system, the SIP logs and syslogs may help to identify the problem. Your service provider may need this information to fix the problem.

The sections [SIP Log Web Page Fields, on page 168](#) and [Syslog Web Page Fields, on page 167](#) give you some information about the contents of the logs.

Use this procedure if the problem is not repeatable. If you can recreate the problem, use [Collect Troubleshooting Logs for a Repeatable Problem, on page 199](#).

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#)

Procedure

-
- Step 1** Click **Syslog**.
- Step 2** Click at the beginning of the log.
- Step 3** Scroll to the end of the log, hold Shift and then click at the end of the log.
- Step 4** Press **Ctrl+C**.
- Step 5** Go to the text editor and click in the top of the file body
- Step 6** Press **Ctrl+V**.
- Step 7** Save the file to a known location on your PC.
- Name the file with the log type, date, and time. For example, syslog_20181212.txt.
- Step 8** Click **SIP Log**.
- Step 9** Click at the beginning of the log.
- Step 10** Scroll to the end of the log, hold Shift and then click at the end of the log.
- Step 11** Press **Ctrl+C**.
- Step 12** Go to the text editor and click in the top of the file body.
- Step 13** Press **Ctrl+V**.
- Step 14** Save the file to a known location on your PC.
- Name the file with the log type, date, and time. For example, siplog_20181212.txt.
-

Collect Troubleshooting Logs for a Repeatable Problem

When you have problems with your system, the SIP logs and syslogs may help to identify the problem. Your service provider may need this information to fix the problem.

The sections [SIP Log Web Page Fields, on page 168](#) and [Syslog Web Page Fields, on page 167](#) give you some information about the contents of the logs.

Use this procedure if the problem is repeatable. If you can't recreate the problem, use [Collect Troubleshooting Logs for a General Problem, on page 198](#).

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Open Notepad or a similar test editor and open a new file.

Procedure

-
- Step 1** Use [Change the Debug Log Level, on page 200](#) to change the debug level to Debug.

- Step 2** Click **Syslog**.
- Step 3** Click **Clear**.
- Step 4** Click **Syslog**.
- Step 5** Click **Clear**.
- Step 6** Recreate the problem.
- Step 7** Click **Syslog**.
- Step 8** Click at the beginning of the log.
- Step 9** Scroll to the end of the log, hold **Shift** and then click at the end of the log.
- Step 10** Press **Ctrl+C**.
- Step 11** Go to the text editor and click in the top of the file body.
- Step 12** Press **Ctrl+V**.
- Step 13** Save the file to a known location on your PC.
Name the file with the log type, date, and time. For example, syslog_20181212.txt.
- Step 14** Click **SIP Log**.
- Step 15** Click at the beginning of the log.
- Step 16** Scroll to the end of the log, hold **Shift** and then click at the end of the log.
- Step 17** Press **Ctrl+C**.
- Step 18** Go to the text editor and click in the top of the file body.
- Step 19** Press **Ctrl+V**.
- Step 20** Save the file to a known location on your PC.
Name the file with the log type, date, and time. For example, siplog_20181212.txt.
- Step 21** Use [Change the Debug Log Level, on page 200](#) to change the debug level to Normal Operation.
-

Change the Debug Log Level

When you have problems with your system, detailed SIP logs and syslogs may help to identify the problem. Use this procedure only when requested by your service provider. The amount of information gathered with increased debug levels may degrade system performance.



Note After you get the required logs, make sure you return the debug level to **Normal Operation**.

For more information about the fields, see [Management Web Page Fields, on page 126](#).

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

Procedure

- Step 1** Click **Management**.
 - Step 2** In the Syslog/SIP Log section, change the **Upload of SIP Log** to Enabled.
 - Step 3** In the Syslog/SIP Log section, change the **Syslog Level** to the required level.
 - Step 4** Click **Save**.
 - Step 5** After you capture logs, click **Management**.
 - Step 6** (Optional) In the Syslog/SIP Log section, change the **Upload of SIP Log** to Enabled.
 - Step 7** In the Syslog/SIP Log section, change the **Syslog Level** to Normal Operation.
 - Step 8** Click **Save**.
-

Turn On Dualcell Debug Logs

To debug dualcell system problems, enable debugging. This causes the log files to contain extra log messages about dualcell.



Note After you get the required logs, make sure you set the debug level to **Disabled**.

Procedure

- Step 1** Access a base station web page. See [Sign in to the administration web page, on page 46](#).
 - Step 2** Click **Dual Cell**.
 - Step 3** Set **Dual cell debug** to **Both**.
 - Step 4** Click **Save**.
-

Turn on Multicell Debug Logs

In order to debug multicell problems, you need to turn multicell debugging. This causes the log files to contain extra log messages about multicell.



Note After you get the required logs, make sure you return the debug level to **Disabled**.

Procedure

- Step 1** Access a base station web page. See [Sign in to the administration web page, on page 46](#).
- Step 2** Click **Multi Cell**.

Step 3 Set **Multi cell debug** to **Both**.

Step 4 Click **Save**.

Generate PCAP Logs

You can create a Packet Capture (PCAP) from the base station web page to assist in troubleshooting problems. You can select a number of trace options.



Note Some of the trace options can quickly fill the limited buffer. Use these with caution.

Some trace options should only be used by experienced personnel.

PCAP logs are stored in the base station RAM. If the base station loses power or resets before you download the logs to your computer, the logs are lost. After you download the logs, you can open them in a packet capture tool (for example, WireShark) for further analysis.

Until the memory fills up, call performance is not impacted by the capture. But memory can fill up quickly, so limit the capture.

Packet traces are done with Ethernet II. Other traces, like Novell raw IEEE 802.3, IEEE 802.2 LLC, and IEEE 802.2 SNAP, are not available.

The packets are filtered based on MAC addresses, for example, 00:08:7B:17:80:39.

Before you begin

Connect to the base station web page as described in [Sign in to the administration web page, on page 46](#).

You need to be using one of the following browsers:

- Microsoft Edge, version 42 or later
- Firefox, version 61 or later
- Chrome, version 68 or later

Procedure

Step 1 Click **Diagnostics**.

Step 2 Click **Logging**.

Step 3 Check one or more check box:

- **Trace packets to/from this base (except Audio)**: All Ethernet packets to and from the base station are traced. This includes broadcast packets but does not include audio.
- **Trace audio packets to/from this base**: All RTP streams to and from the base station are traced. The trace uses the **RTP port** and **RTP port range** from the **Network Settings** web page.

Note Audio packets can quickly fill the log buffer. Use this setting with caution.

- **Trace received broadcast packets:** All broadcast packets received by the base station are traced.
Note Broadcast packets can quickly fill the log buffer. Use this setting with caution.
- **Trace received IPv4 multicast packets:** All IPv4 multicast packets received by the base station are traced.
Note Multicast packets can quickly fill the log buffer. Use this setting with caution.
- **Trace received packet with destination MAC between (compare between each byte):** You set up the MAC address range to be monitored with the 6 pairs of fields. Each byte of the received destination MAC is checked to determine if it is in the trace range.
Note For expert use only.
- **Trace received Ethertype:** You can select up to three received Ethertypes to trace.
Note For expert use only.
- **Trace received IPv4 protocol:** You can select up to 3 received IPv4 protocols to trace.
Note For expert use only.
- **Trace received TCP/UDP port:** You can set up to 3 TCP/UDP ports to trace. The packet is logged if the select port is the destination port or the source port for a packet.
Note For expert use only.

- Step 4** Click **Save** to start the packet capture.
 - Step 5** If you are trying to troubleshoot a specific problem, reproduce the problem.
 - Step 6** Click **Cancel** to stop the packet capture.
 - Step 7** (Optional) Click **Reset traces** to start the packet capture again. The existing capture is deleted.
 - Step 8** Click **All Basestations** or **Current Basestation** to download the packet capture to your computer.
-



APPENDIX **A**

Cisco IP DECT 6800 Series with Cisco Unified Communications Manager

- [Deployment of DECT 6800 on Cisco Unified Communication Manager \(CUCM\), on page 205](#)
- [Create a User, on page 205](#)
- [Add IP DECT 6825 on CUCM, on page 206](#)
- [Add a Line to the Device, on page 207](#)
- [Associate the Device to the User, on page 207](#)
- [Configure the Base Station, on page 208](#)

Deployment of DECT 6800 on Cisco Unified Communication Manager (CUCM)

The Cisco IP DECT 6800 Series uses Digital Enhanced Cordless Telecommunications (DECT), a wireless technology. DECT operates at or near the 1.9 GHz frequency and does not interfere with other wireless technologies such as Bluetooth (operates at 2.5 GHz or 5 GHz). The Cisco IP DECT 6800 base station converts IP to DECT. The CUCM has no knowledge of the DECT operations. From the CUCM perspective, the DECT handsets appear as VoIP endpoints.



Note You must configure DECT base station for TCP. You must not use base station MAC address when you add the DECT to the CUCM. Each Cisco IP DECT Phone 6825 is a separate Third-party SIP device (advanced) on CUCM. For example, if you have 100 6825 handsets, then you will need 100 Third-Party SIP Device (Advanced) devices in CUCM.

Currently, few basic features such as make a call, answer a call, hold, transfer a call, conference are supported.

Create a User

The Cisco IP DECT Phone 6825 handset uses DECT to communicate to a base station. The base station converts DECT to IP. The base station acts as a relay between the 6825 and Cisco Unified Communications Manager. In Cisco Unified Communications Manager, you add 6825 as a Third-Party SIP device (Advanced). You must not add the base station directly to the CUCM.

Before you begin

Log in to Cisco Unified Communications Manager Administration.

Procedure

-
- Step 1** In Cisco Unified Communications Manager Administration, choose **User Management > End User**.
The **Find and List Users** window appears.
- Step 2** To select an existing user, specify the appropriate filters in the **Find User Where** field, click **Find** to retrieve a list of users, and then select the user who is synchronized with LDAP from the list. You can also create a new user.
- Step 3** In the **End User Configuration** window, the **User ID** fields populates the SIP digest username. The directory number configured for the user is displayed in the **Telephone Number** field.
- Step 4** In the **Digest Credentials** field, you need to populate the value and the value is the SIP digest password that is set in the headset.
- Step 5** Click **Save**.
-

Add IP DECT 6825 on CUCM

You can add an IP DECT 6825 on the CUCM and each device adds as a separate device enter. The device does not equal a base station. A device in this case is a line in conjunction with a digest user selection.

Before you begin

Log in to Cisco Unified Communications Manager Administration.

Procedure

-
- Step 1**
- Step 2** In Cisco Unified Communications Manager Administration, choose **User Management > End User**.
The **Find and List Users** window appears.
- Step 3** In the **Find and List Users** window, click **Add New**.
- Step 4** In the **Add a New Phone** window, select **Phone Type** as **Third-party SIP Device (Advanced)**.
- Step 5** Click **Next**.
- Step 6** In the **Phone Configuration** window, add value in the **MAC Address** field.
- Note** You must not enter the base station MAC address in this field. You can enter any value in this field as the profiles are not synchronized to MAC addresses. You can also enter IPEI value of the base station and add some other digits as suffix.
- Step 7** Select the **Device Pool** as appropriate for the device environments. For example, you can select **Default**.
- Step 8** From the **Phone Button Template** field, select **Third-party SIP Device (Advanced)**.

- Step 9** In the **Owner User ID** field, add the owner that you want to register with the device.
- Step 10** In the **Protocol Specific Information** section, select the value **Third-party SIP Device Advanced** from the list **Device Security Profile**.
- Step 11** From the **SIP Profile** field, select **Standard SIP Profile**.
- Step 12** From the **Digest User** field, select the same end user for who you want to register the device.
- Step 13** Set the rerouting CSS.
- Step 14** Click **Save**.
-

Add a Line to the Device

Before you begin

Log in to Cisco Unified Communications Manager Administration.

Procedure

- Step 1** In the **Phone Configuration** window, select **Directory Number (Line 1)**.
- Step 2** In the **Directory Number** field, enter the directory number of the same end user for who you want to register the device.
- Step 3** Select the **Route Partition**, for example, **Everyone**.
- Step 4** In the **Directory Number Settings** section, select a value from the **Calling Search Space** field.
If you set a value for the **Calling Search Space** field, you must set the value for **Rerouting Calling Search Space**.
- Step 5** Click **Save**.
-

Associate the Device to the User

After you add the device to the CUCM, you must associate the device to the user.

Before you begin

- Log in to Cisco Unified Communications Manager Administration.
- Create a user.
- Add the device to CUCM.
- Add a directory number, partition, CSS to the device.

Procedure

- Step 1** In the **End User Configuration** section, click **Device Association**.
- Step 2** In the **User Device Association** section, specify the appropriate filters in the **Find User Device Association where** field, click **Find** to retrieve a list of users.
- Step 3** Select the user and click **Save Selected/Changes**.

If you want to associate other devices, you can follow all the procedures but use a new directory number and new user.

Configure the Base Station

When you associate the device with the user, you need to configure the base station.

Procedure

- Step 1** On the IP DECT device, press Menu button. Then type *47* on the keypad.
You will be able to fetch the IP address of the base station. The device should be kept at the proximity of the base station.
- Step 2** On a Web browser, enter the IP address of the base station.
Setup a username and password when you log into the base station for the first time as a security measure. If you cannot access the base station, in the web browser, type https:// and then the IP address reported by the device.
- Step 3** In the base station Administration web page, click **Servers** and then click **Add Server**.
- Step 4** Set the **Server Alias** field. For example, **CUCM**.
- Step 5** Set the **Registrar** field to the address given by your service provider.
This address is the actual DNS name of the Cisco Unified Communication Manager. For example, **cucm1.dcloud.cisco.com**. This the subscriber that registers to the CUCM server group.
- Step 6** Set the **SIP Transport** field to **TCP**.
- Step 7** Click **Save**.
- Step 8** Click **Extensions** to add an extension.
- Step 9** In the **Line name** field, add the directory number of the user for who the device is associated.
- Step 10** Set the **Extension** field. You can enter the same value as the value of **Line name** field.
- Step 11** In the **Authentication User Name**, enter the user that is specified in the CUCM.
- Step 12** Set the **Authentication Password** as the digest password.

Clear any password from the XSI Password field and set the Server same as Registrar field. For example, as

- Step 13** Clear any password from the **XSI Password** field and set the **Server** same as **Registrar** field, such as **cucm1.dcloud.cisco.com**.

Step 14 Click **Save**.

For any new device, you can repeat all the steps.

Step 15 On the base station web page, navigate to **Extensions** and validate the entries appears on the page. The green circle indicates successful registration.

You can enable both single-cell and multi-cell base station on CUCM. For details, on multi-cell base station, see *Cisco IP DECT 6800 Series Administration Guide*.



APPENDIX **B**

Technical Details

- [Base Station Specifications, on page 211](#)
- [Handset Specifications, on page 212](#)
- [Network Protocols, on page 213](#)
- [SIP Configuration, on page 216](#)
- [External Devices, on page 220](#)

Base Station Specifications

The following table shows the physical and operating environment specifications for the base station.

Table 79: Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 113°F (0° to 45°C)
Operating relative humidity	10% to 90% (noncondensing)
Storage temperature	14° to 140°F (-10° to 60°C)
Storage relative humidity	10% to 95% (noncondensing)
Height	4.75 in. (120 mm)
Width	4.75 in. (120 mm)
Depth	1.25 in (30 mm)
Weight	6 oz. (167 g)
Cables	<ul style="list-style-type: none"> • Category 3/5/5e/6 for 10-Mbps cables with 4 pairs • Category 5/5e/6 for 100-Mbps cables with 4 pairs
Distance Requirements	As supported by the Ethernet Specification, it is assumed that the maximum cable length between each base station and the switch is 100 meters (330 feet).

Specification	Value or Range
Power	Power adapter for local power Ethernet PoE (Ethernet adaptor for normal power); IEEE 802.3: Power class 2 (3.84 – 6.49W)
Radio Frequency (RF) Bands	Bands are set in the factory and cannot be changed by customers. <ul style="list-style-type: none"> • 1880 - 1895 (Taiwan) • • 1880 – 1900 MHz (Australia and New Zealand – reduced power 22 dBm) • 1880 – 1900 MHz (E.U. and APAC) • 1910 – 1930 MHz (LATAM and Argentina) • 1910 – 1920 MHz (Brazil and Uruguay) • 1910 – 1920 MHz (Uruguay – reduced power 140 mW) • 1910 – 1930 MHz (Chile – reduced power 22 dBm) • 1920 – 1930 MHz (U.S. and Canada)

For detailed technical information about the base station, see the datasheet at:

<https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-dect-6800-series-multiplatform-firmware/datasheet-listing.html>

Logging of Configuration Changes of Base Station

You can record configuration changes that users make to the base station using the configuration changes logging function. In a similar manner, you may track configuration changes of a handset. In the changelog, the basic memory stores the information about which parameters is changed. However, this information does not contain the actual details of the changes; rather, it just stores specific changes made to the configuration. The changelog is cleared after the changes have been successfully reported.

Reporting of Configuration Changes

When base station configuration changes are reported, the base station requests DECT locked handsets for changelogs. The base station sends three requests, one every five seconds, for each locked handset. Once requests for all handsets are complete, the changelogs of the base and the handsets are collected, processed, transformed to the correct XML tags. Then these tags are sent to the configuration server. If a handset doesn't respond, the syslog records this behavior. The handset changelogs from the device are cleared only after successful delivery of it to a base station.

Handset Specifications

The following table shows the physical and operating environment specifications for the handsets.

Table 80: Physical and Operating Specifications

Specification	Value or Range
Operating temperature	32° to 113°F (0° to 45°C)
Operating relative humidity	10% to 90% (noncondensing)
Storage temperature	14° to 140°F (-10° to 60°C)
Storage relative humidity	10% to 95% (noncondensing)
Height	6825 Handset: 4.6 in. (117 mm) 6825 Ruggedized Handset: 4.6 in. (117 mm) 6823 Handset: 4.82 in. (122 mm)
Width	6825 Handset: 1.8 in. (46 mm) 6825 Ruggedized Handset: 1.8 in. (46 mm) 6823 Handset: 1.99 in. (51 mm)
Depth	6825 Handset: 0.78 in. (20 mm) 6825 Ruggedized Handset: 0.78 in. (20 mm) 6823 Handset: 0.91 in. (23 mm)
Weight	6825 Handset: 3 oz. (86 g) 6825 Ruggedized Handset: 3 oz. (86 g) 6823 Handset: 3.17 oz. (90 g)
Power	Rechargeable Lithium ion battery.

For detailed technical information about the handsets, see the datasheet at:

<https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-dect-6800-series-multiplatform-firmware/datasheet-listing.html>

Network Protocols

Cisco handsets and base stations support several industry-standard and Cisco network protocols that are required for voice communication. The following table provides an overview of the network protocols that the handsets and base stations support.

Table 81: Supported Network Protocols

Network Protocol	Purpose	Usage Notes
Bootstrap Protocol (BootP)	BootP enables a network device, such as the handset, to discover certain startup information, such as its IP address.	—

Network Protocol	Purpose	Usage Notes
Cisco Discovery Protocol (CDP)	<p>CDP is a device-discovery protocol that runs on all Cisco-manufactured equipment.</p> <p>A device can use CDP to advertise its existence to other devices and receive information about other devices in the network.</p> <p>The Native VLAN type of the CDP can be used to obtain the VLAN network information.</p>	The device uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.
Domain Name Server (DNS)	DNS translates domain names to IP addresses.	The base station has a DNS client to translate domain names into IP addresses.
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP dynamically allocates and assigns an IP address to network devices.</p> <p>DHCP enables you to connect a base station into the network and have the base station become operational without the need to manually assign an IP address or to configure additional network parameters.</p>	<p>DHCP is enabled by default. If disabled, you must manually configure the IP address, subnet mask, and gateway on each base station locally.</p> <p>We recommend that you use the DHCP custom option 160, 159.</p>
Hypertext Transfer Protocol (HTTP)	HTTP is the standard protocol for transfer of information and movement of documents across the Internet and the web.	The base station uses HTTP for XML services, provisioning, upgrade, and for troubleshooting purposes.
Hypertext Transfer Protocol Secure (HTTPS)	HTTPS is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of servers.	<p>Web applications with both HTTP and HTTPS support have two URLs configured. Base stations that support HTTPS choose the HTTPS URL.</p> <p>A lock icon is displayed to the user if the connection to the service is via HTTPS.</p>
Internet Protocol (IP)	IP is a messaging protocol that addresses and sends packets across the network.	<p>To communicate with IP, network devices must have an assigned IP address, subnet, and gateway.</p> <p>IP addresses, subnets, and gateways identifications are automatically assigned if you are using the base station with Dynamic Host Configuration Protocol (DHCP). If you are not using DHCP, you must manually assign these properties to each base station locally.</p>

Network Protocol	Purpose	Usage Notes
Link Layer Discovery Protocol (LLDP)	VLAN network information can be collected from the LLDP from numerous subtypes of the type 127. In this implementation, the information will be taken from one of two subtypes, which are prioritised as follows: <ol style="list-style-type: none"> 1. IEEE – PORT VLAN ID 2. Network Policy 	
Network Time Protocol (NTP)	NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.	The base station uses NTP to communicate with the time server.
Real-Time Transport Protocol (RTP)	RTP is a standard protocol for transporting real-time data, such as interactive voice and video, over data networks.	The base station uses the RTP protocol to send and receive real-time voice traffic from other devices and gateways.
Real-Time Control Protocol (RTCP)	RTCP works in conjunction with RTP to provide QoS data (such as jitter, latency, and round trip delay) on RTP streams.	RTCP is disabled by default.
Session Description Protocol (SDP)	SDP is the portion of the SIP protocol that determines which parameters are available during a connection between two endpoints. Conferences are established by using only the SDP capabilities that all endpoints in the conference support.	SDP capabilities, such as codec types, DTMF detection, and comfort noise, are normally configured on a global basis by a Third-Party Call Control System or a Media Gateway in operation. Some SIP endpoints may allow configuration of these parameters on the endpoint itself.
Session Initiation Protocol (SIP)	SIP is the Internet Engineering Task Force (IETF) standard for multimedia conferencing over IP. SIP is an ASCII-based application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more endpoints.	Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.
Secure Real-Time Transfer protocol (SRTP)	SRTP is an extension of the Real-Time Protocol (RTP) Audio/Video Profile and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets providing authentication, integrity, and encryption of media packets between two endpoints.	Handsets and base stations use SRTP for media encryption.
Transmission Control Protocol (TCP)	TCP is a connection-oriented transport protocol.	—

Network Protocol	Purpose	Usage Notes
Transport Layer Security (TLS)	TLS is a standard protocol for securing and authenticating communications.	When security is implemented, the base station uses the TLS protocol when securely registering with the third-party call control system.
Trivial File Transfer Protocol (TFTP)	TFTP allows you to transfer files over the network. On the base station, TFTP enables you to obtain a configuration file specific to the phone type.	TFTP requires a TFTP server in your network, which can be automatically identified from the DHCP server.
User Datagram Protocol (UDP)	UDP is a connectionless messaging protocol for delivery of data packets.	UDP is used only for RTP streams. SIP uses UDP, TCP, and TLS.

Reset the Network VLAN

When the advertisement discovery packages arrive, they are monitored and analysed, and the network information contained in them is compared to previous packages. If the VLAN changes, the DECT base must reboot and reconnect to complete a new network initialization.

SIP Configuration

SIP and the Cisco IP DECT Phone

The Cisco IP DECT Phone use Session Initiation Protocol (SIP), which allows interoperation with all IT service providers that support SIP. SIP is an IETF-defined signaling protocol that controls voice communication sessions in an IP network.

SIP handles signaling and session management within a packet telephony network. *Signaling* allows call information to be carried across network boundaries. *Session management* controls the attributes of an end-to-end call.

In typical commercial IP telephony deployments, all calls go through a SIP Proxy Server. The receiving handset is called the SIP user agent server (UAS), while the requesting handset is called the user agent client (UAC).

SIP message routing is dynamic. If a SIP proxy receives a request from a UAS for a connection but cannot locate the UAC, the proxy forwards the message to another SIP proxy in the network. When the UAC is located, the response routes back to the UAS, and the two user agents connect using a direct peer-to-peer session. Voice traffic transmits between user agents over dynamically assigned ports using Real-time Protocol (RTP).

RTP transmits real-time data such as audio and video; RTP does not guarantee real-time delivery of data. RTP provides mechanisms for the sending and receiving applications to support streaming data. Typically, RTP runs on top of UDP.

SIP over TCP

To guarantee state-oriented communications, the Cisco IP DECT Phone can use TCP as the transport protocol for SIP. This protocol provides *guaranteed delivery* that assures that lost packets are retransmitted. TCP also guarantees that the SIP packages are received in the same order that they were sent.

SIP Proxy Redundancy

An average SIP Proxy Server can handle tens of thousands of subscribers. A backup server allows an active server to be temporarily switched out for maintenance. The base station supports the use of backup servers to minimize or eliminate service disruption.

A simple way to support proxy redundancy is to specify a SIP Proxy Server in the base station configuration profile. The base station sends a DNS NAPTR or SRV query to the DNS server. If configured, the DNS server returns SRV records that contain a list of servers for the domain, with their hostnames, priority, listening ports, and so on. The base station tries to contact the servers in the order of the priority. The server with a lower number has a higher priority. Up to six NAPTR records and twelve SRV records are supported in a query.

When the base station fails to communicate with the primary server, the base station can failover to a lower-priority server. If configured, the base station can restore the connection back to the primary. Failover and fallback support switches between servers with different SIP transport protocols. The base station doesn't perform fallback to the primary server during an active call until the call ends and the fallback conditions are met.

Example of Resource Records from the DNS Server

```

sipurash      3600      IN NAPTR 50   50 "s"  "SIPS+D2T"  ""  _sips._tcp.tlstest
              3600      IN NAPTR 90   50 "s"  "SIP+D2T"   ""  _sip._tcp.tcptest
              3600      IN NAPTR 100  50 "s"  "SIP+D2U"   ""  _sip._udp.udptest

_sips._tcp.tlstest  SRV 1 10 5061 srv1.sipurash.com.
                   SRV 2 10 5060 srv2.sipurash.com.
_sip._tcp.tcptest  SRV 1 10 5061 srv3.sipurash.com.
                   SRV 2 10 5060 srv4.sipurash.com.
_sip._udp.udptest  SRV 1 10 5061 srv5.sipurash.com.
                   SRV 2 10 5060 srv6.sipurash.com.

srv1      3600      IN      A      1.1.1.1
srv2      3600      IN      A      2.2.2.2
srv3      3600      IN      A      3.3.3.3
srv4      3600      IN      A      4.4.4.4
srv5      3600      IN      A      5.5.5.5
srv6      3600      IN      A      6.6.6.6
    
```

The following example shows the priority of the servers from the perspective of the base station.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	UP
2nd	2.2.2.2	TLS	UP
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

The base station always sends SIP messages to the available address with the top priority and with the status UP in the list. In the example, the base station sends all the SIP messages to the address 1.1.1.1. If the address 1.1.1.1 in the list is marked with the status DOWN, the base station communicates with 2.2.2.2 instead. The base station can restore the connection back to 1.1.1.1 when the specified fallback conditions are met. For

more details about failover and fallback, see [SIP Proxy Failover, on page 218](#) and [SIP Proxy Fallback, on page 219](#).

SIP Proxy Failover

The base station performs a failover in any of these cases:

- **Fast Response Timer expiry:** In RFC3261 the two transactions timers, TIMER B and TIMER F defines when an INVITE transaction and a Non-INVITE transaction has expired respectively. These are configurable with a default value of 5 sec. When one of these timers expires, and the corresponding SIP transaction fails, failover is triggered. In-dialog requests does not trigger failover.
- **SIP 5xx Response Codes:** If the server responds with a 5xx response to a SIP request, failover is triggered.
- **TCP disconnect:** If the remote server disconnects the TCP connection (ex. TCP RST or TCP FIN), failover is triggered.

We strongly recommend that you set the **Failback before Failover** to **Enabled** when **SIP Transport** is set to **Auto**.

You can also configure this extension-specific parameters in the configuration file (.xml):

```
<SIP_Transport_n>Auto</SIP_Transport_n>
<Srv_Failback_Before_Failover_n>Yes</Srv_Failback_Before_Failover_n>
```

Where, n is the extension.

Base Station Failover Behavior

When the base station fails to communicate with the currently connected server, it refreshes the server list status. The unavailable server is marked with the status DOWN in the server list. The base station tries to connect to the top-priority server with the status UP in the list.

In the following example, the addresses 1.1.1.1 and 2.2.2.2 aren't available. The base station sends SIP messages to 3.3.3.3, which has the top priority among the servers with the status UP.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	DOWN
2nd	2.2.2.2	TLS	DOWN
3rd	3.3.3.3	TCP	UP
4th	4.4.4.4	TCP	UP
5th	5.5.5.5	UDP	UP
6th	6.6.6.6	UDP	UP

In the following example, there are two SRV records from the DNS NAPTR response. For each SRV record, there are three A records (IP addresses).

Priority	IP Address	SIP Protocol	Server	Status
1st	1.1.1.1	UDP	SRV1	DOWN
2nd	1.1.1.2	UDP	SRV1	UP
3rd	1.1.1.3	UDP	SRV1	UP
4th	2.2.2.1	TLS	SRV2	UP
5th	2.2.2.2	TLS	SRV2	UP
6th	2.2.2.3	TLS	SRV2	UP

Let's assume that the base station failed to connect to 1.1.1.1 and then registered to 1.1.1.2. When 1.1.1.2 goes down, base station behavior depends on the setting of **Proxy Fallback Intvl**.

- When **Failover SIP Timer B** is set to **0**, the base station tries with the addresses in this order: 1.1.1.1, 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.
- When **Failover SIP Timer B** is set to a value other than zero, the base station tries with the addresses in this order: 1.1.1.3, 2.2.2.1, 2.2.2.2, 2.2.2.3.

SIP Proxy Fallback

The proxy fallback requires that the field **Failback before Failover** in the **Server** web page is set to **Enabled**. If you set this field to **Disabled**, the SIP proxy fallback feature is disabled. You can also configure this extension-specific parameter in the configuration file (.xml) in this format:

```
<Srv_Failback_Before_Failover_n_>yes</Srv_Failback_Before_Failover_n_>
```

Where, *n* is the extension number.

The time when the base station triggers a fallback depends on the configuration and the SIP transport protocols in use.

To enable the base station to perform fallback between different SIP transport protocols, set **SIP Transport** to **Auto** on the **Servers** web page. You can also configure this extension-specific parameter in the configuration file (.xml) with the following XML string:

```
<SIP_Transport_@SRVIDX_>AUTO</SIP_Transport_@SRVIDX_>
```

Where, *n* is the server index.

Failback from a UDP Connection

The failback from a UDP connection is triggered by SIP messages. In the following example, the base station first failed to register to 1.1.1.1 (TLS) at the time T1 since there's no response from the server. When SIP Timer F expires, the base station registers to 2.2.2.2 (UDP) at the time T2 (T2=T1+SIP Timer F). The current connection is on 2.2.2.2 via UDP.

Priority	IP Address	SIP Protocol	Status	
1st	1.1.1.1	TLS	DOWN	T1 (Down time)
2nd	2.2.2.2	UDP	UP	
3rd	3.3.3.3	TCP	UP	

The base station has the following configuration:

```
<Proxy_Fallback_Intvl_n_ ua="na">60</Proxy_Fallback_Intvl_n_>
<Register_Expires_n_ ua="na">3600</Register_Expires_n_>
<SIP_Timer_F ua="na">16</SIP_Timer_F>
```

where *n* is the extension number.

The base station refreshes the registration at time T2 (T2=(3600-16)*78%). The base station checks the address list for the availability of the IP addresses and the down time. If T2-T1 >= 60, the failed server 1.1.1.1 resumes back to UP and the list is updated to the following. The base station sends SIP messages to 1.1.1.1.

Priority	IP Address	SIP Protocol	Status
1st	1.1.1.1	TLS	UP
2nd	2.2.2.2	UDP	UP
3rd	3.3.3.3	TCP	UP

Failover and Recovery Registration

- **Failover**—The base station performs a failover when transport timeout/failure or TCP connection failures; if **Failover SIP Timer B** and **Failover SIP Timer F** values are datafilled.
- **Recovery**—The base station attempts to reregister with the primary proxy while registered or actively connected to the secondary proxy.

Auto register when failover parameter controls the failover behavior when there is an error. When this parameter is set to yes, the base station re-registers upon failover or recovery.

Fallback Behavior

The fallback occurs when the current registration expires or Proxy Fallback Intvl fires.

If the Proxy Fallback Intvl is exceeded, all the new SIP messages go to primary proxy.

For example, when the value for Register Expires is 3600 seconds and Proxy Fallback Intvl is 600 seconds, the fallback triggers 600 seconds later.

When the value for Register Expires is 800 seconds and Proxy Fallback Intvl is 1000 seconds, the fallback triggers at 800 seconds.

After successful registration back to the primary server, all SIP messages go to the primary server.

External Devices

We recommend that you use good-quality external devices that are shielded against unwanted radio frequency (RF) and audio frequency (AF) signals. External devices include headsets, cables, and connectors.

Depending on the quality of these devices and their proximity to other devices, such as mobile phones or two-way radios, some audio noise may still occur. In these cases, we recommend that you take one or more of these actions:

- Move the external device away from the source of the RF or AF signals.
- Route the external device cables away from the source of the RF or AF signals.
- Use shielded cables for the external device, or use cables with a better shield and connector.
- Shorten the length of the external device cable.
- Apply ferrites or other such devices on the cables for the external device.

Cisco cannot guarantee the performance of external devices, cables, and connectors.



Caution

In European Union countries, use only external speakers, microphones, and headsets that are fully compliant with the EMC Directive [89/336/EC].



APPENDIX C

Worksheets

- [Worksheets, on page 221](#)

Worksheets

You may find these worksheets useful when you gather the information you need to configure your system. You can print this chapter if you need a paper record. You could also set up a spreadsheet or document and recreate the worksheets for an electronic record.

Server Configuration Parameters Worksheet

The following table contains the mandatory information you need to configure the base station. You can use the Data column to gather your information if you print the chapter.

Field name	Description	Data
Registrar	The IP address or FQDN of the call control system.	
Outbound proxy	Session Border Controller or SIP server outbound proxy.	
Time Server	The IP address or FQDN of the network time server.	
MAC address of the base station	The MAC address is on the label under the LAN port and also on the cardboard box that contained the base station.	
IP address of the base station	When the base station is plugged in, it uses DHCP to get an IP address. You can get the IP address of the base station with this task: Find the base station IP address, on page 45	
MAC address of the second base station	The MAC address is on the label under the LAN port and also on the cardboard box that contained the base station.	

Field name	Description	Data
IP address of the second base station	When the base station is plugged in, it uses DHCP to get an IP address. You can get the IP address of the base station with this task: Find the base station IP address, on page 45	
-		
-		

Base Station Worksheet

You find most of this information on the box label or the label on the base station.

Primary Base Station

Description	Data
PID/VID	
Serial number	
MAC address	
IPv4 address	
RFPI address	
Installed location	

Secondary Base Station 1

Description	Data
PID/VID	
Serial number	
MAC address	
IPv4 address	
RFPI address	
Installed location	

Secondary Base Station 2

Description	Data
PID/VID	
Serial number	
MAC address	
IPv4 address	
RFPI address	
Installed location	

Handset Configuration Parameters Worksheet

The following table contains the mandatory information you need to configure the handsets on the base station.

You can have up to 30 handsets configured on a base station, but the maximum number of handsets that can be active at one time is limited. For more information, see [Add Handsets to the Base Station, on page 54](#).

The handset's International Portable Equipment Identity (IPEI) identifies the exact handset that the user is allocated.

User name	Phone Number and Handset IPEI	Authentication User Name and Password	XSI User Name and Password	Mailbox Name and Number
-	- -			
-	- -			
-	- -			
-	- -			
-	- -			
-	- -			

