Dolby Conference Phone
Administrator's guide
Contents

1 Introduction 7
  1.1 About this guide 7
  1.2 New in this version 7
  1.3 Related documentation 9
  1.4 Deployment guides 10
  1.5 Problem reports 10

2 Solution architecture 12
  2.1 Dolby Conference Phone software application 12
  2.2 Network configurations 12
  2.3 Operational modes of the Dolby Conference Phone 13
    2.3.1 Integrating with your conferencing service provider 14
    2.3.2 Supported IP PBX call control platforms 14
  2.4 Ways to set up the phone 15

3 Preparation and requirements 17
  3.1 Installation and setup process 17
  3.2 Conference room requirements 17
  3.3 Power requirements 18
  3.4 Network requirements 18
  3.5 Supported DHCP parameters 19
  3.6 Network ports used 20
  3.7 Bandwidth planning and codec selection 20
  3.8 Primary and secondary VLANs 21

4 Plug-and-Play Setup 25
  4.1 How Plug-and-Play Setup works 25
  4.2 Server addresses 25

5 Automatic Local Setup 27
  5.1 Automatic Local Setup preparation 27
  5.2 Out-of-the-box discovery of the provisioning server 28
  5.3 Rediscovering the provisioning server 28

6 Configuring the phone with Dolby Conferencing Console 30
  6.1 Reasons for using Dolby Conferencing Console 30
    6.1.1 The purpose of a provisioning server 30
    6.1.2 What is Dolby Conferencing Console? 31
    6.1.3 How the phone connects to Dolby Conferencing Console 31
  6.2 Supported provisioning protocols with Dolby Conferencing Console 32
  6.3 Updating software using Dolby Conferencing Console 32

7 Configuring phone features 33
  7.1 Configurable phone features 33
    7.1.1 Configuration parameters 33
    7.1.2 Deprecated configuration parameters 35
  7.2 Configuring certificates 35
    7.2.1 Adding certificate authority certificates 36
7.2.2 Viewing certificate authority certificates 36
7.2.3 Device certificate 37
7.3 Configuring phone preferences 37
7.3.1 Using the recent calls list 38
7.3.2 Enabling user feedback 38
7.3.3 Using call forwarding 38
7.3.4 Enabling automatic answer 39
7.3.5 Enabling do not disturb 39
7.3.6 Setting the language 40
7.3.7 Setting the time and date display 41
7.4 Options for provisioning 41
7.4.1 Scheduling a software update 41
7.4.2 Setting recurring provisioning 42
7.4.3 Disabling the reboot prompt 42
7.5 Phone access control 43
7.5.1 Changing the administrative password 43
7.6 Directory options 43
7.6.1 Using a corporate directory 43
7.6.2 Adding the corporate directory configuration 44
7.6.3 Using the contact directory 45
7.6.4 Creating a local contact directory by using the provisioning server 45
7.7 Configuring IP PBX for the phone 46
7.7.1 Configuring PBX server redundancy 47
7.7.2 Configuring the Voice Activation Detection (VAD) parameter for the phone 48
7.8 Disabling Bluetooth advertisement 49

8 Deploying the phone 50
8.1 First-time use of the phone 50
8.1.1 Setting up the phone using Plug-and-Play Setup 51
8.1.2 Setting up the phone using Automatic Local Setup 54
8.1.3 Connecting the phone to the network using Manual Setup 55
8.1.4 Connecting the phone to Dolby Conferencing Console or the provisioning server using Manual Setup 57
8.2 Deploying in a secure network 59
8.2.1 Deploying with 802.1X authentication 59
8.2.2 HTTPS provisioning 61
8.3 Changing network configuration after out-of-the-box setup 62
8.3.1 Configuration and rediscovery of the provisioning server 62
8.3.2 Network configuration 62
8.3.3 Configuring IP Network options 63
8.3.4 Configuring LLDP 63
8.3.5 Configuring the secondary VLAN 64
8.3.6 Configuring the time server 65
8.3.7 Configuring 802.1X after out-of-the-box setup 66
8.3.8 IEEE 802.1p/Q 67
8.3.9 Configuring proxy autoconfiguration (PAC) and web proxy autodiscovery (WPAD) protocol 67
8.3.10 Proxy authentication 68

9 Administering the phone 69
9.1 Error messages 69
9.2 Viewing the Status menu 73
9.3 Log files 75
9.3.1 Parameters for changing the log level 76
9.3.2 Log levels 76
9.3.3 About syslog logging 76
9.3.4 Audio logging 77
9.4 Accessing the Dolby Conference Phone web interface 78
9.5 Exporting the Dolby Conference Phone configuration 80
9.6 Rebooting the Dolby Conference Phone 81
9.7 Call and media statistics 82
9.8 Viewing diagnostics 83
9.9 Diagnostic shell 83
9.10 Bluetooth LE initialization and advertisement 84
9.10.1 Confirming Bluetooth LE initialization 84
9.10.2 Confirming Bluetooth LE advertisement 85
9.11 Collection of usage data 86
9.11.1 Enabling Privacy block 86
9.12 Phone memory resources 87
9.13 Resetting to factory defaults 88
9.14 LLDP and supported type-length values 88
9.14.1 Supported type-length values 89
9.15 Trusted certificates and issuers 91
9.15.1 TLS cipher suites 93

10 Configuring the Dolby Conference Phone provisioning server 96
10.1 Reasons for using a provisioning server 96
10.2 Building the provisioning server 96
10.2.1 Requirements for provisioning servers 97
10.2.2 Supported provisioning protocols with provisioning servers 97
10.3 Security for provisioning servers 97
10.4 Setting up an FTP server 97
10.5 HTTPS server setup 98
10.6 Master configuration file 98
10.6.1 Setting up the CA certificate files for the phone to download 100
10.7 Template files 100
10.8 Configuration file (JSON) 101
10.9 Recommended file and directory layout 101
10.10 Redundant provisioning servers 102
10.11 Log directory 102
10.12 Updating preinstalled software using a provisioning server 102
10.12.1 Available software packages 103
10.12.2 Upgrading and downgrading phone software 103
10.12.3 Upgrading phones to the latest Dolby Conference Phone software 104
10.12.4 Downgrading phones to an earlier version of Dolby Conference Phone software 104
10.13 Sample configurations 105
10.13.1 Directory structure 105
10.13.2 Master configuration file 105
10.13.3 Simple IP PBX–only configuration 105

11 Troubleshooting 108
11.1 Phone issues and solutions 108
11.1.1 Power and start-up issues 108
11.1.2 Hardware issues 108
11.1.3 Network access issues 109
11.1.4 Provisioning issues 111
1 Introduction

The Dolby Conference Phone offers an intuitive touch-screen interface that lets you easily join and manage meetings. The phone is a dual-mode device that can be used for Dolby Voice meetings and for traditional telephony.

- About this guide
- New in this version
- Related documentation
- Deployment guides
- Problem reports

1.1 About this guide

IT administrators can use this documentation as a guide for setting up and provisioning the Dolby Conference Phone.

We assume that users of this guide are IT administrators or equivalent and are familiar with:

- Basics of computer networking and Linux administration
- IP private branch exchange (PBX) call controls used by your organization
- Conferencing service provider functionality used by your organization

This guide provides information about:

- Configuring the phone with Dolby Conferencing Console
- Using Dolby Conferencing Console to manage the phone or groups of phones
- Configuring the phone with a provisioning server
- Using the phone user interface (UI) and phone web interface
- Configuration parameters and configuring phone features
- Troubleshooting common issues with the phone

1.2 New in this version

This release of the Dolby Conference Phone includes several new and updated features, including:

- Dynamic Host Configuration Protocol (DHCP) options 66 and 132 autodiscovery mechanisms are no longer supported. References to DHCP virtual LAN discovery were removed.
- Firmware improvements.
- New Plug-and-Play Setup method that makes phone setup extremely easy.
- New privacy block feature.
- Updated workflows and screens in the setup wizard.
- Automatic Setup is now called Automatic Local Setup.
Manual Setup has additional phone screens for proxy and virtual LAN information.

New configuration parameter called \texttt{Sip.Vad.SignalAnnexB} to override the default behavior of G.729AB for phones at sites that require G.729 Annex A for VAD (Voice Activity Detection). This parameter allows you to control the phone to signal to its peer that it supports G.729A (by turning Annex B off).

Link Layer Discovery Protocol is disabled by default during out-of-the-box setup and can be manually reenabled after completing out-of-the-box setup.

Various improvements to accuracy and clarity.

**New topics**

These topics are new:

- Problem reports on page 10
- Ways to set up the phone on page 15
- Plug-and-Play Setup on page 25
- How Plug-and-Play Setup works on page 25
- Server addresses on page 25
- Configuring IP PBX for the phone on page 46
- Configuring the Voice Activation Detection (VAD) parameter for the phone on page 48
- Disabling Bluetooth advertisement on page 49
- Setting up the phone using Plug-and-Play Setup on page 51
- Bluetooth LE initialization and advertisement on page 84
- Confirming Bluetooth LE advertisement on page 85
- Collection of usage data on page 86
- Plug-and-Play Setup issues and solutions on page 120
- Dolby Voice Console issues on page 120
- Provisioning service issues on page 121
- Setup app issues on page 123

**Updated topics**

These topics have been updated:

- Network requirements on page 18
- Supported parameters on page 19
- Server addresses on page 25
- Primary and secondary VLANs on page 21
- Automatic Local Setup on page 27
- Automatic Local Setup preparation on page 27
- Out-of-the-box discovery of the provisioning server on page 28
- Configuring the phone with Dolby Conferencing Console on page 30
- Configurable phone features on page 33
- Configuration parameters on page 33
1.3 Related documentation

Review all of the Dolby Conference Phone documents to ensure that the phone is set up correctly and that you have the best conferencing experience possible.

These documents are available:

- **Dolby Conference Phone quick start guide**
  
  This guide describes the contents of the phone package, how to assemble the phone, and how to connect the phone to the network. The quick start guide is included in the phone package. It is also available from the Dolby Conference Phone support pages.

- **Dolby Conference Phone user's guide**
  
  This guide describes how to use the basic and advanced phone features, and how to customize the phone.

- **Dolby Conference Phone open source software guide**
  
  This guide describes the open source software used in the Dolby Conference Phone software.

- **Dolby Satellite Microphones quick start guide**
  
  This guide describes the contents of the microphone package and how to connect them to the Dolby Conference Phone. The quick start guide is included in the microphone package. It is also available from the Dolby Conference Phone support pages.

- **Dolby Voice compatibility guide**
  
  This guide describes the compatibility relationships between the various Dolby Voice products.
1.4 Deployment guides

For information about integrating the Dolby Conference Phone with your conferencing service provider and a supported IP PBX, see the deployment guide for your call control platform.

The following deployment guides are available:

- Configuring the Dolby Conference Phone for BT MeetMe with Dolby Voice
- Configuring the Dolby Conference Phone with Cisco Unified Communications Manager
- Configuring the Dolby Conference Phone with Avaya Aura Platform 6
- Configuring the Dolby Conference Phone with Unify OpenScape
- Configuring the Dolby Conference Phone for iMeet
- Configuring the Dolby Conference Phone for West conferencing

1.5 Problem reports

Before you report problems to your conferencing service provider, please be prepared to provide basic information about the phone, configuration files and logs, and a full description of the issue.

- Basic information about the phone:
  - Phone serial number
  - Version of software currently on the phone

- Configuration files and logs:
  - Phone configuration: If Dolby Conferencing Console is not being used as the provisioning server, provide the relevant configuration files from the provisioning server for the phone, or export your entire configuration from the phone.
  - Any relevant log files showing the problem occurring. If you have not enabled logging, you should enable it for the phone experiencing the issue, reproduce the issue, and provide those logs.
  - Have you been able to reproduce the problem? If so, please detail how.
  - Is there anything that you think might be relevant in the log? Did anything unusual occur? Did the system generate any high-severity log messages? If so, please attach an extract.

- Description of the issue:
  - When did the problem occur? How often does it occur? Is there any pattern or trend to the occurrence?
  - What was the scope of the problem? How many users did it affect? Was there any pattern or trend to the affected users?
  - Any symptoms observed.
  - Any error messages displayed on the phone UI or web interface.
  - Any obvious triggers. (What was the user doing before the error message displayed?)
  - If the issue was reproducible. (Does it happen regularly or after certain tasks are performed?)
• How widespread the issue appears to be. (Does it affect a single user only or the whole organization?)
• Any other information you have that might assist in understanding the issue.
• What operating system and version are being used by the client? What browser and version are being used by the client?
• What kind of Internet connection is the client using (ADSL/cable/wireless/mobile)?
• What other observations have you made? Is there anything else you think might assist us in identifying the root cause of the problem?

Related information
First-time use of the phone on page 50
Master configuration file on page 105
Exporting the Dolby Conference Phone configuration on page 80
Log files on page 75
2 Solution architecture

The Dolby Conference Phone supports advanced functionality, including local conferencing, multiple call appearances, Hypertext Transfer Protocol Secure (HTTPS) secure provisioning, and deployment in conference service provider and IP PBX environments.

- Dolby Conference Phone software application
- Network configurations
- Operational modes of the Dolby Conference Phone
- Ways to set up the phone

2.1 Dolby Conference Phone software application

The Dolby Conference Phone software consists of two basic components: the application that loads the phone software when the phone is first powered on and implements the phone functions and features, and the configuration files that contain the phone settings.

The phone software application manages the protocol stack, the DSP, the UI, and the network interaction. This application implements these functions and features:

- VoIP signaling for a range of voice telephony functions using Session Initiation Protocol (SIP) signaling for call setup and control
- Industry-standard security techniques for ensuring that all provisioning, signaling, and media transactions are authenticated and encrypted
- Advanced audio signal processing for communications using a group of audio codecs
- Flexible provisioning methods to support various deployment scenarios

The phone software application also performs these tasks once you power up or reboot the phone:

- Enables you to set various network and provisioning options
- Formats the file system, and removes any application and configuration files if new updates are downloaded
- Determines what files on the provisioning server are required by the phone
- Downloads the application and configuration files
- Installs the application, and uploads an event log file from the boot cycle to the provisioning server

The phone software application is a binary file image and contains a digital signature that prevents tampering or the loading of rogue phone software images. There is a new image file in each new release of phone software.

2.2 Network configurations

From an administrator’s perspective, the Dolby Conference Phone is a SIP endpoint in a network that interoperates with other compatible hardware, such as application servers, media servers, gateways, switches, voice bridges, and other endpoints.

For the Dolby Conference Phone to successfully operate as a SIP endpoint in the network, you will require:
• A working IP network
• Network routers and switches configured for VoIP
• VoIP gateways configured for SIP
• Adequate firewall security
• The latest Dolby Conference Phone software image (or a compatible version)
• An active, configured call server to receive and send SIP messages
• Dolby Conferencing Console or provisioning server on the IP network

There are many ways to set up a phone network using the Dolby Conference Phone. This figure is just one example of a network setup.

*Figure 1: Dolby Conference Phone in a network*

2.3 Operational modes of the Dolby Conference Phone

The operational modes of the Dolby Conference Phone can integrate with the conferencing service provider as a conference endpoint, register to an IP PBX call control platform as a SIP endpoint, or do both simultaneously.

The mode the phone operates in determines what features are supported. For example, if the operational mode is set to **Conferencing Only Mode**, then the phone cannot be configured to connect to an IP PBX, and features such as forwarding and transferring will be unavailable. Similarly, if the operational mode is set to **IP PBX Only Mode**, then the phone cannot be configured to connect to a Dolby Voice enabled conferencing service provider.
For more information, see the deployment guide for your call control platform. This table lists the parameter you can configure for this feature.

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selects the operational mode</td>
<td>Features.OperationMode</td>
</tr>
</tbody>
</table>

**Web interface**

To set the operational mode from the web interface, go to **Settings > Features** and select the appropriate option.

**Related information**

Deployment guides on page 10

### 2.3.1 Integrating with your conferencing service provider

You can integrate the Dolby Conference Phone with your conferencing service provider. For information, see the deployment guide for your conferencing service provider.

**Related information**

Deployment guides on page 10

### 2.3.2 Supported IP PBX call control platforms

An IP PBX provides audio communications through a Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack for endpoints on internal networks and interconnects with a public switched telephone network (PSTN) for telephony connections for external endpoints.

The Dolby Conference Phone supports these IP PBX call control platforms:

**Cisco Unified Communications Manager**

Cisco Unified Communications Manager is an IP-based communications system integrating voice, video, data, and mobility products and applications.

Supported versions: The Dolby Conference Phone interoperates with Cisco Unified Communications Manager 7.1, 8.5/8.6, 9.1, 10.5, and 11.

**Avaya Aura Platform**

Avaya Aura Platform is an IP-based communications system integrating voice and video endpoints.

Supported versions: The Dolby Conference Phone interoperates with Avaya Aura Platform 6.1, 6.2, and 6.3.

**Unify OpenScape Enterprise Express**

Supported versions: The Dolby Conference Phone interoperates with Unify OpenScape Enterprise Express 8.0.x.

**Standard SIP call control platform**

The Dolby Conference Phone is a SIP compliant endpoint and interoperates with any call control platform designed to comply with RFC 3261. For Transport Layer Security (TLS)
transport, the phone is limited by the existing security configuration, and this information should be noted:

- If the phone transport is configured as AUTO, TLS transport will be attempted only if the phone fails to connect to TCP and User Datagram Protocol (UDP) transports.
- The CA certificate of the Session Initiation Protocol server must be downloaded to the phone through provisioning.
- TLS 1.0, 1.1, and 1.2 are supported. TLS 1.2 is the preferred protocol, but version 1.0 or 1.1 may be used depending on the peer’s support.
- As the phone acts as a client, it is up to the server to decide whether or not mutual authentication is required. (Normally, SIP servers are configured with client authentication only.)
- The use of certificate revocation lists (CRLs) is not supported.
- Simple Certificate Enrollment Protocol (SCEP) and Online Certificate Status Protocol (OCSP) are not supported.
- The phone device certificate cannot be replaced at this time.
- If you try to setup IP PBX with explicit TLS transport instead of taking advantage of the Auto transport feature, you must set the transport port explicitly. If you change your configuration from TLS to Auto then you need to set the port back to the correct default port.

The best practice is to use Auto transport, which is the system default.

When TLS is operational on the phone, Secure Real-time Transport Protocol (SRTP) is enabled; when TLS is not operational on the phone, SRTP is disabled. By default, if TLS is enabled, SRTP is set to Mandatory. The Dolby Conference Phone offers a predefined list of cipher suites.

**Related information**

[ TLS cipher suites on page 93 ]

### 2.4 Ways to set up the phone

There are several ways to set up the Dolby Conference Phone. They are listed in order of easiest and fastest first:

- Plug-and-Play Setup
  
  This is the easiest and fastest method to use if your phone can connect to the Dolby Voice Console. Your service provider can preconfigure your Dolby Conference Phone serial number in the Dolby Voice Console to provide the optimized Plug-and-Play Setup experience. Even if your device is not preconfigured, during the setup process you can select your conferencing service provider and still use the Plug-and-Play Setup method.

- Automatic Local Setup
  
  This is the next easiest method if you want an on-premise, bulk-setup method using the Dolby Conferencing Console. However, it requires that you do some advance planning and setup.

- Manual Setup
Use this method if the phone did not discover a provisioning server by any of the other methods or you just want manual control. Manual Setup is started when you skip selection of a service provider during the phone setup.

**Related information**

- Plug-and-Play Setup on page 25
- Automatic Local Setup on page 27
- Connecting the phone to the network using Manual Setup on page 55
- Connecting the phone to Dolby Conferencing Console or the provisioning server using Manual Setup on page 57
3 Preparation and requirements

Before you use the Dolby Conference Phone, review the requirements for room size, power, and network connectivity.

- Installation and setup process
- Conference room requirements
- Power requirements
- Network requirements
- Supported DHCP parameters
- Network ports used
- Bandwidth planning and codec selection
- Primary and secondary VLANs

3.1 Installation and setup process

Once you have received a Dolby Conference Phone, you can set it up in a conference room or an executive’s office.

Before you begin, read the Dolby Conference Phone quick start guide first. This printed guide is shipped in the phone package.

The Dolby Conference Phone is a class 3 PoE device, which consumes a maximum of 12.95 W. The phone reports this through LLDP type length value (TLV) as 13 W.

Make note of the media access control (MAC) address of each phone that you want to deploy. The MAC address is the 12-digit hexadecimal number on a label on the underside of the phone and on the outside of the shipping box.

Note: Depending on how you want each phone to behave (that is, which features are enabled), you may need the MAC address of each phone that you want to deploy. If you want different features on some phones, you will need a list of all MAC addresses.

If you plan to support one or two Dolby Satellite Microphones with the phone, read the Dolby Satellite Microphone quick start guide first. The phone must be running Dolby Conference Phone 2.1 or later software.

Related information
Power requirements on page 18

3.2 Conference room requirements

Before you install the Dolby Conference Phone, make sure that the room does not exceed the maximum recommended room size. If the room is large, you may need satellite microphones in addition to the conference phone.

We recommend that you place the phone on a solid table in the center of the room.

Small, medium, and large conference rooms
The maximum room size is 20 × 30 feet (6 × 9 m). Only one Dolby Conference Phone is required.
Large conference rooms and boardrooms
The maximum room size is 20 × 40 feet (6 × 12 m).
Installing the Dolby Conference Phone with two Dolby Satellite Microphones is ideal.

Choosing a Dolby Conference Phone solution based on the size of the room is important because it ensures natural and effective conversational flow for the usual seating positions in the room. Participant behavioral factors and environmental factors influence the overall voice quality in the room and impact your experience. For example:

• Participant seating position
• Participant voice volume
• Ambient noise level
• Reverb level
• Floor, wall, and ceiling materials
• Ceiling fans
• Projector placement

When the Dolby Conference Phone is deployed in acoustically challenging rooms, we recommend testing the setup to determine whether the actual results meet your requirements.

3.3 Power requirements
The Dolby Conference Phone requires PoE, which can be obtained by a network port supporting PoE, or a PoE adapter from a wall socket.

Follow the instructions in the Dolby Conference Phone quick start guide to connect the phone to the network using a PoE source.

If a PoE source is not available, connect the phone to an AC power source. To connect the phone to an AC power source, you will need an AC power kit that includes a power adapter, a regional power cord, and an IEEE 802.3af–compliant power injector cable (for example, the Phihong Single Port 15.4 W PoE Adapter PSA16U IEEE 802.3af compliant). Follow the power injector cable instructions carefully.

Note: AC power and PoE adapters are not included in the phone package. If you require one, contact your phone reseller.

3.4 Network requirements
The Dolby Conference Phone is a VoIP device. It connects physically through a Cat5 cable to a standard office twisted-pair (IEEE 802.3) 10/100/1,000 Mbps Ethernet LAN, and it sends and receives all data using the same packet-based technology.

IP network requirements differ according to the partner application to be used.

You should have a DHCP server and Domain Name System (DNS) server already set up within your organization.

Network connectivity should be available to all locations where you intend to deploy the Dolby Conference Phone.

Connecting the Dolby Conference Phone to the LAN will initiate this sequence of events:
1. The phone establishes network connectivity.

2. DHCP negotiations occur between the network and Internet Protocol (IP) address, network addressing options, default network gateway address, and time server.

   Note: If the phone reboots, the Dolby Conference Phone attempts to use the same IP address in the DHCP discovery request that was already assigned in the DHCP discovery before the reboot.

3. Appropriate security and Quality of Service (QoS) settings are applied.

4. The connection to the provisioning server is attempted.

5. The phone provisioning process starts.

The Dolby Conference Phone will not function until this link is established.

The phone is configured to automatically negotiate the Ethernet speed and duplex mode so that no special configuration is required. Although you have the option to change the line speed and duplex configuration on the switch network port, we recommend that you keep the autonegotiation settings. If you do change the settings, you should do so before deploying the phones.

If your organization uses an HTTP or HTTPS proxy server to manage Internet traffic, see the requirements for proxy authentication.

If your organization separates voice and data traffic by the use of VLANs, see the requirements for primary and secondary VLANs.

Related information
Deployment guides on page 10
Primary and secondary VLANs on page 21
Configuration parameters on page 33
Proxy authentication on page 68

### 3.5 Supported DHCP parameters

When the Dolby Conference Phone has established network connectivity, it needs to acquire several IP network settings to be fully functional. These settings are typically obtained from a DHCP server.

If some DHCP parameters are unavailable, you have the option to set these DHCP parameters manually from the phone UI or in the phone web interface.

This table details the settings that are configurable through the DHCP protocol for the phone and where they are used.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>DHCP option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet mask</td>
<td>1</td>
</tr>
<tr>
<td>IP gateway</td>
<td>3</td>
</tr>
<tr>
<td>DNS server IP address</td>
<td>6</td>
</tr>
<tr>
<td>DNS domain</td>
<td>15</td>
</tr>
<tr>
<td>NTP servers</td>
<td>42</td>
</tr>
<tr>
<td>Proxy autoconfiguration</td>
<td>252</td>
</tr>
</tbody>
</table>
**3.6 Network ports used**

The network port used by the Dolby Conference Phone depends on protocol, data type, and whether it is sent by UDP or TCP.

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Data</th>
<th>UDP or TCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>SSH</td>
<td>Diagnostics</td>
<td>TCP</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>Not applicable</td>
<td>TCP</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>Not applicable</td>
<td>TCP</td>
</tr>
<tr>
<td>5,060</td>
<td>SIP</td>
<td>SIP signaling</td>
<td>UDP or TCP</td>
</tr>
<tr>
<td>5,061</td>
<td>SIP over TLS</td>
<td>Secure signaling</td>
<td>TCP</td>
</tr>
<tr>
<td>16,400–16,431†</td>
<td>RTP/RTCP</td>
<td>Media, audio</td>
<td>UDP</td>
</tr>
</tbody>
</table>

* Port 80 is always redirected to port 443.
† Real-time Transport Protocol (RTP) ports are always even numbers; RTP Control Protocol (RTCP) ports are always the odd numbers. The numbers always start from 16,400/16,401 and move on to 16,402/16,403 and so forth until they reach the end of the range. At this point, they revert back to 16,400/16,401 and start over again.

**3.7 Bandwidth planning and codec selection**

Bandwidth planning depends on the audio codecs used.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Raw bit rate</th>
<th>IP bit rate</th>
<th>Sampling rate</th>
<th>Supported payload size</th>
<th>Effective audio bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711μ-law RFC 1890</td>
<td>64 kilobits per second (kbps)</td>
<td>80 kbps</td>
<td>8 kHz</td>
<td>10 ms (default)†</td>
<td>4 kHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 ms</td>
<td>30 ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4 kHz</td>
<td>4 kHz</td>
</tr>
</tbody>
</table>

| G.711a-law RFC 1890 | 64 kbps | 80 kbps | 8 kHz | 10 ms (default)† | 4 kHz |
|                     | 20 ms | 30 ms | 40 ms | 50 ms | 60 ms | 80 ms | 4 kHz |

† Real-time Transport Protocol (RTP) ports are always even numbers; RTP Control Protocol (RTCP) ports are always the odd numbers. The numbers always start from 16,400/16,401 and move on to 16,402/16,403 and so forth until they reach the end of the range. At this point, they revert back to 16,400/16,401 and start over again.
<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Raw bit rate</th>
<th>IP bit rate</th>
<th>Sampling rate</th>
<th>Supported payload size</th>
<th>Effective audio bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722 RFC 3551</td>
<td>48, 56, 64 kbps</td>
<td>64, 70, 80 kbps</td>
<td>16 kHz</td>
<td>10 ms/20 ms (default) †</td>
<td>8 kHz</td>
</tr>
<tr>
<td>G.729ab</td>
<td>8 kbps</td>
<td>26.8 kbps</td>
<td>8 kHz</td>
<td>10 ms/20 ms (default) †</td>
<td>4 kHz</td>
</tr>
<tr>
<td>Internet low bit-rate codec (iLBC) RFC 3952</td>
<td>15.2 kbps</td>
<td>24 kbps</td>
<td>8 kHz</td>
<td>20 ms (default) †</td>
<td>4 kHz</td>
</tr>
<tr>
<td>DVC-2 in 2.0 and later (proprietary)</td>
<td>48 kbps</td>
<td>179 kbps (peak) 64 kbps (average)</td>
<td>16 kHz</td>
<td>20 ms (default) †</td>
<td>8 kHz</td>
</tr>
</tbody>
</table>

* The IP bit rate depends primarily on the tunnel type used.
† The Dolby Conference Phone always sends 20 ms payloads to the peer.

Note: During a call, the LED halo glows blue if the DVC-2 codec is being used, and glows green if a different codec is being used.

### 3.8 Primary and secondary VLANs

The Dolby Conference Phone requires Internet access to connect to the conferencing service. In some environments, voice and data traffic are handled by different VLANs.

If the voice VLAN lacks Internet connectivity, modify firewall policies to allow the phone to connect to your conferencing service. Alternatively, you can set up the phone on the data VLAN. If neither of these solutions works for you, then you need a dual VLAN setup. Once you enable dual VLANs, communicate over the Internet with servers for your conferencing service provider passes through the secondary VLAN. With separate VLANs, the phone will have two IP addresses, one on each VLAN. (Also see Configuring the secondary VLAN.)

When the secondary VLAN is enabled, the primary VLAN is designated as the voice VLAN, and the secondary VLAN is designated as the data VLAN. When the secondary VLAN is disabled, the phone can be placed on either data VLAN or voice VLAN. If your organization has a strict policy on segregating voice and data VLANs, and you want to configure the phone for both IP PBX and conferencing service, enable the secondary VLAN.

The secondary VLAN has these limitations:
- Only DHCP is supported on the secondary VLAN for device IP assignment.
- The secondary VLAN shares all QoS settings with the primary VLAN. QoS automatic discovery is not available on the secondary VLAN.
There are two status fields that you can check to verify the status for the primary and secondary VLAN:

**DNS Server Status**
Displays status of DNS for the primary VLAN.

*Note:* If the same DNS server is configured on both the primary VLAN and secondary VLAN, all DNS queries go through the primary VLAN.

**Default Gateway Status**
If the secondary VLAN is configured, and DNS is not shared between primary and secondary VLAN, use this field to check DNS status of the secondary VLAN.

The **Status** screen with the VLAN settings is shown in this figure.

*Figure 2: Status screen displaying VLAN settings*

Network traffic is allocated onto different VLANs based on the traffic type, as listed in this table.
Table 4: Traffic-type-to-network-interface mapping

<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Network interface</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Primary and secondary</td>
<td>Works independently on both</td>
</tr>
<tr>
<td>Web Proxy Automatic Discovery (WPAD)</td>
<td>Primary and secondary</td>
<td>Works independently on both</td>
</tr>
<tr>
<td>Proxy automatic configuration (PAC)</td>
<td>Primary and secondary</td>
<td>Works independently on both</td>
</tr>
<tr>
<td>DNS †</td>
<td>Primary and secondary</td>
<td>DNS queries made on the network interface where the DNS requestor application runs</td>
</tr>
<tr>
<td>Conferencing services</td>
<td>Secondary</td>
<td></td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol (LDAP)</td>
<td>Secondary</td>
<td></td>
</tr>
<tr>
<td>Web server</td>
<td>Primary and secondary</td>
<td></td>
</tr>
<tr>
<td>SSH server</td>
<td>Primary and secondary</td>
<td></td>
</tr>
<tr>
<td>Syslog</td>
<td>Primary</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Primary</td>
<td></td>
</tr>
<tr>
<td>Provisioning</td>
<td>Primary and secondary</td>
<td></td>
</tr>
<tr>
<td>SIP call</td>
<td>Primary</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>* PAC on primary VLAN works for proxy determination of FTP/HTTP-based provisioning. PAC on secondary VLAN works for proxy determination of some conferencing service providers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>† If the primary virtual LAN shares the same DNS settings, then DNS traffic will run on primary virtual LAN only.</td>
</tr>
</tbody>
</table>

Check the items in the following sections to determine whether your network is ready for dual VLAN deployment.

**Voice VLAN checklist**

Set up the Dolby Conference Phone on the tagged voice VLAN with proper IP PBX configuration, and confirm that IP PBX calls can be successfully made:

- The Dolby Conference Phone can discover voice VLAN through LLDP.
- For IP PBX configuration instructions, see Deployment guides on page 10.

**Data VLAN checklist**

Keep the Dolby Conference Phone on the same Ethernet switch port, then set up the Dolby Conference Phone on the data VLAN (usually, the untagged VLAN):

- If the Dolby Conference Phone discovers the Voice VLAN using LLDP, you can disable LLDP under Administrative settings > Network configuration > Ethernet > LLDP enabled.

Once the device is successfully set on the data VLAN, configure the necessary settings for connecting to your conference service provider.

**If both checklist tests work**

If both tests work, you have the correct setup to proceed with the dual VLAN configuration.
**Note:** When the dual VLAN feature is used in conjunction with a Cisco switch port with 802.1X authentication enabled, it works only if the Ethernet port on the switch is configured to Single-Host or Multiple-Hosts mode. If the port is set to Multidomain Authentication or Multiauthentication mode, dual VLAN will not work on the phone.

**Related information**
- Deployment guides on page 10
- Troubleshooting on page 108
- Configuring the secondary VLAN on page 64
4 Plug-and-Play Setup

The Plug-and-Play Setup is a fast and easy way to set up phones using your conferencing service provider’s provisioning service. It makes trials and small-scale deployments of Dolby Conference Phones easier for administrators.

• How Plug-and-Play Setup works
• Server addresses

4.1 How Plug-and-Play Setup works

When you perform Plug-and-Play Setup, you are provisioning the Dolby Conference Phone using your conferencing service provider’s provisioning service.

If you use this method, you do not need to set up and use an on-premise instance of Dolby Conferencing Console or an on-premise provisioning server.

These actions occur when the phone boots up:

Note: If you completed the preparation work for Automatic Local Setup, the screens and prompts in the setup wizard are different than described here. Instead, you are prompted to connect to your on-premise instance of Dolby Conferencing Console or your on-premise provisioning server.

1. If the phone has Internet access as described in Server addresses on page 25, the phone connects to the Dolby Voice Console.

   The Dolby Voice Console is a provisioning discovery service that recognizes and redirects phones to provisioning services.

2. One of these things happens:

   a. If the phone is recognized by the Dolby Voice Console, the phone is redirected and connects to your conferencing service provider’s provisioning service.
   b. If the phone is not recognized by the Dolby Voice Console, you can select your conferencing service provider. The phone is then redirected and connects to your conferencing service provider’s provisioning service.

You also have the option to skip Plug-and-Play Setup and go through manual setup if needed.

Related information

Automatic Local Setup on page 27
Setting up the phone using Plug-and-Play Setup on page 51

4.2 Server addresses

With Plug-and-Play Setup, the Dolby Conference Phone is provisioned automatically by your conferencing service provider's provisioning service.

Plug-and-Play Setup requires that the phone have Internet access to both of these servers using HTTPS protocol (port 443):
The Dolby Voice Console at https://console.dolbyvoice.com/

Your conferencing service provider’s provisioning server (see the deployment guide for your conferencing service provider)

Your conferencing service provider’s setup app (see the deployment guide for your conferencing service provider)

As part of Plug-and-Play Setup, the phone must be able to connect to your conferencing service provider’s setup app through the Internet. Once the phone connects to the setup app, screens and workflows that are specific to your conferencing service provider display on the phone. After out-of-the-box setup is complete, the phone then uses your conferencing service provider’s conferencing application, which is a separate application from the setup app.

The phone can utilize your HTTP proxy server to connect to the aforementioned servers. During Plug-and-Play Setup, the phone will automatically discover the proxy server on your network.

The phone supports 802.1x as the authentication server. You can enter the authentication server credentials during the out-of-the-box setup. For more information, see Deploying with 802.1X authentication on page 59.

If your network does not implement proxy autodiscovery using WPAD, you can configure a PAC URL from the setup wizard. The phone supports NTLMv2, Digest, and Basic for proxy authentication methods.
5 Automatic Local Setup

Unless Plug-and-Play Setup is used, we recommend using Automatic Local Setup. This setup method simplifies deployment and minimizes configuration errors (compared to Manual Setup). In order to use this method, you must plan ahead and complete the preparation work described in this chapter.

- Automatic Local Setup preparation
- Out-of-the-box discovery of the provisioning server
- Rediscovering the provisioning server

Before you attempt to deploy the phone using Automatic Local Setup, make sure you have completed the preparation described in this chapter.

5.1 Automatic Local Setup preparation

If Automatic Local Setup is used, the setup wizard can discover the Dolby Conferencing Console or the provisioning server on your network. This makes setup easier for multiple-site deployment scenarios. You must prepare for Automatic Local Setup before you attempt to set up the phone with the out-of-the-box setup wizard.

To use Automatic Local Setup, you must have administrative access to the DNS server on your network. Once the DNS server is enabled, the setup wizard can discover your FTP, HTTP, or HTTPS provisioning server using a Domain Name System service record (DNS SRV).

Syntax example using Ubuntu BIND9 service

For example, if the DNS server is using Ubuntu BIND9 service, open the forward zone file on the DNS server and then add the DNS SRV record to the file. The record is an entry in the zone file. Make sure that you know the host name and domain name of the provisioning server.

Add the HTTPS SRV record using this syntax example:

\[
\text{service}_\text{protocolName} \text{ IN SRV priority weight portNO subdns.domain.com}
\]

\[
\text{service}_\text{protocolName}
\]

For HTTPS provisioning servers, the phone queries the HTTPS server using the service name \_dccs\_tcp to retrieve the DNS SRV record.

For HTTP provisioning servers, the phone queries the HTTPS server using the service name \_dcc\_tcp to retrieve the DNS SRV record.

priority

Numeric. Lower gets first priority.

weight

Numeric. Higher gets used more often.

portNO

The numeric value relevant to the service name listed.
443: The typical port used by the HTTPS provisioning server.
80: The typical port used by the HTTP provisioning server.

*subdns.domain.com*

The fully qualified domain name (FQDN) of the provisioning server, which consists of both the host name and the domain name.

**Examples**

DNS SRV record for HTTPS provisioning servers:

```
_dccs._tcp  SRV  1  1  443  hostname.domain.org.
```

DNS SRV record for HTTP provisioning servers:

```
_dcc._tcp  SRV  1  2  80  hostname.domain.org.
```

**Related information**

*Setting up the phone using Automatic Local Setup* on page 54

---

### 5.2 Out-of-the-box discovery of the provisioning server

If you complete the necessary network preparation for Automatic Local Setup, the first time you plug in the Dolby Conference Phone, the setup wizard detects the provisioning server and completes setup.

The setup wizard displays on the phone UI. You can use the setup wizard to find and connect the phone to Dolby Conferencing Console or any provisioning servers that you have set up on the network.

Note this information about provisioning phones using Automatic Local Setup:

- The phone uses the DNS SRV record to discover Dolby Conferencing Console and any provisioning servers that you have set up on the network.
- If your network requires IEEE 802.1X authentication, you can rediscover the provisioning server after you configure IEEE 802.1X settings and connect the phone to the network (see *Deploying with 802.1X authentication* on page 59).

When you use Automatic Local Setup, the setup wizard discovers either the Dolby Conferencing Console or a provisioning server and the phone automatically connects to the provisioning server. If you have not completed the preparation work properly, the phone will not be able to discover the on-premises Dolby Conferencing Console or provisioning server and you will need to manually configure the phone with the provisioning server.

There are some differences in the use of the setup wizard and provisioning procedures when you use Dolby Conferencing Console. For more information, see *Dolby Conferencing Console operations and management guide*.

---

### 5.3 Rediscovering the provisioning server

If needed, you can rediscover Dolby Conferencing Console or the provisioning server from the phone UI or phone web interface. You do not need to reset the phone to factory defaults.
Procedure

1. To rediscover the provisioning server from the phone UI:
   a) Tap this sequence:
      ![Sequence]
   b) When prompted, enter the administrative password (1739 by default).
   c) Update provisioning settings as needed, and then tap the confirm button.

2. To rediscover the provisioning server from the phone web interface:
   a) From the Settings tab, navigate to Provisioning > Server.
   b) Turn off manual provisioning by clicking the On button next to Manual Server Configuration.
   c) If the provisioning server is detected, confirm that you want to connect to it.
6 Configuring the phone with Dolby Conferencing Console

An easy way to set up multiple Dolby Conference Phones is to use Dolby Conferencing Console as the provisioning server. We recommend using Dolby Conferencing Console if you have more than five Dolby Conference Phones to manage.

- Reasons for using Dolby Conferencing Console
- Supported provisioning protocols with Dolby Conferencing Console
- Updating software using Dolby Conferencing Console

6.1 Reasons for using Dolby Conferencing Console

A provisioning server allows for flexibility in installing, upgrading, maintaining, and configuring the phone. You must have a provisioning server in order to bulk set up and upgrade Dolby Conference Phones.

You have these choices for provisioning phones:

- Use your conferencing service provider’s provisioning service.
  
  For more information, see Plug-and-Play Setup on page 25.
- Set up and use Dolby Conferencing Console as your provisioning server.
- Set up and use an FTP, HTTP, or HTTPS server as your provisioning server.
  
  For more information, see Configuring the Dolby Conference Phone provisioning server on page 96.

You can use Dolby Conferencing Console to provision devices, group them into device pools for ease of management, obtain analytic information about them, and monitor device status on both an individual and group level.

We recommend using Dolby Conferencing Console for provisioning if:

- You have a large number of phones (more than five).
- You want full control over how your phones are managed.
  
  For example, with Plug-and-Play Setup, your phones are managed by someone else.
- You want to allow calls to and from a conferencing service and from regular (IP PBX) phone calls.

6.1.1 The purpose of a provisioning server

A provisioning server contains configuration files, which contain configuration parameters. It may also contain logs from phones if the phones have been configured to upload logs to the provisioning server. When a phone reboots, configuration parameters from the provisioning server are downloaded to the phone.

This server allows the administrator to centrally manage phones from one location. For example, without a provisioning server, the administrator must configure settings on one phone at a time.
6.1.2 What is Dolby Conferencing Console?

Dolby Conferencing Console is device-management software for Dolby Conference Phones. We recommend using it because it provides additional features to simplify the administrator’s work.

Dolby Conferencing Console accelerates Dolby Conference Phone deployment by enabling bulk provisioning, and removes management complexity with monitoring, support, and remote control capabilities. Key capabilities and benefits include:

Phone provisioning and updates
Simple provisioning and updating of large numbers of Dolby Conference Phones, utilizing device pools and profiles, saves time and improves IT productivity.

Device management
Allows for real-time tracking of assets using various attributes to improve planning and reduce costs.

Monitoring, diagnostics, and remote control
View Dolby Conference Phone status in real time, troubleshoot problems, and control devices remotely, speeding issue resolution.

Usage statistics and analytics
Get statistical intelligence about phone usage with detailed device and network analytics and reports to optimize your resource decisions.

System dashboard
Get a quick view into the overall system status to make informed decisions.

Web portal with popular browser support
Access anywhere, anytime, enabling participants to connect from their desks or remotely via PCs and mobile devices.

Data exportability
Highly extensible platform with RESTful application programming interface (API) and Simple Network Management Protocol (SNMP) version 2 (SNMPv2) support lets you easily export data and integrate with management and business intelligence solutions.

6.1.3 How the phone connects to Dolby Conferencing Console

You can connect the Dolby Conference Phone to Dolby Conferencing Console automatically or manually. Automatic Local Setup requires some preparation of the DNS server on the network.

If you complete the preparation for Automatic Local Setup, the first time you plug in the phone, the setup wizard automatically detects Dolby Conferencing Console and any provisioning servers that you have on the network.

For instructions about how to connect the phone to Dolby Conferencing Console, see the sources listed in the table.

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up Dolby Conferencing Console</td>
<td>Dolby Conferencing Console operations and management guide</td>
</tr>
<tr>
<td>Completing preparations that allow the phone to discover Dolby Conferencing Console</td>
<td>Automatic Local Setup on page 27</td>
</tr>
</tbody>
</table>
Task | For more information
--- | ---
Connecting the phone to Dolby Conferencing Console automatically | Setting up the phone using Automatic Local Setup on page 54
Connecting the phone to Dolby Conferencing Console manually | Connecting the phone to Dolby Conferencing Console or the provisioning server using Manual Setup on page 57

### 6.2 Supported provisioning protocols with Dolby Conferencing Console

HTTP and HTTPS provisioning protocols are supported with Dolby Conferencing Console.

If you connect the Dolby Conference Phone to Dolby Conferencing Console, the recommended protocol is HTTPS. If you connect the phone to Dolby Conferencing Console over an HTTP proxy, you must use the HTTPS protocol.

Both Digest and Basic authentication schemes are supported when using HTTP or HTTPS. Custom certificates, including those from certificate authorities, can be added to the phone for Transport Layer Security server authentication on HTTPS provisioning servers.

### 6.3 Updating software using Dolby Conferencing Console

Dolby Conferencing Console supports the use of multiple firmware releases, so you have the option of uploading new firmware releases and pushing these new releases out, as needed, to groups of phones (device pools).

Make sure that you reference the correct documentation when attempting to update software on phones. This varies depending on whether you use Dolby Conferencing Console or a provisioning server to provision phones.

Task | For more information
--- | ---
Using Dolby Conferencing Console to update software on phones | Dolby Conferencing Console operations and management guide
Using the provisioning server to update software on phones | Updating preinstalled software using a provisioning server on page 102
7 Configuring phone features

As the administrator, you can configure common features that are intended for end users of the Dolby Conference Phone (for example, call forwarding, automatic answer, and do not disturb). You can also set passwords and connect the phone to your corporate directory.

- Configurable phone features
- Configuring certificates
- Configuring phone preferences
- Options for provisioning
- Phone access control
- Directory options
- Configuring IP PBX for the phone
- Disabling Bluetooth advertisement

7.1 Configurable phone features

As the administrator, you can configure features for a group of Dolby Conference Phones, and can configure features one phone at a time using the phone web interface.

Note: If you use Plug-and-Play Setup, you cannot configure features for a group of phones because your phones are provisioned by your conferencing service provider. You can still configure features one phone at a time using the phone web interface (for example, if you want to configure IP PBX settings, which are not provisioned by your conferencing service provider’s provisioning service).

Configuration parameters affect features on the phone. The phone receives and stores configuration parameters from Dolby Conferencing Console or the provisioning server. For example:

- With Dolby Conferencing Console, you can create profiles, which are used to group configuration parameters. Then you apply each profile to a group of phones. (See the Dolby Conferencing Console operations and management guide.)
- The provisioning server hosts the master configuration file, which links to individual configuration files containing configuration parameters that you want to distribute to a group of phones.

You can change some configuration parameters from the phone web interface, and you can change some from the phone UI.

However, configuration parameters coming from Dolby Conferencing Console or the provisioning server are unavailable (appear dimmed). The phone does not allow you to change the configuration parameters at all, from the phone UI or web interface.

Related information
Plug-and-Play Setup on page 25

7.1.1 Configuration parameters

Configuration parameters dictate the behavior of the Dolby Conference Phone once it is running the executable specified in the master configuration file.
Configuration parameters are used to configure all phone features and functions. A detailed description of all configuration parameters, along with the default or permitted values for those parameters, is provided with each software build, in the file dvcp-rel-x.y.z.buildIDcfg-help.html, where x.y.z.build represents the build name. To configure a specific feature, find the feature in Configuring phone features on page 33.

Finding the phone software version

Knowing the version number of software on the phone is useful when troubleshooting problems or submitting a support request, or when determining whether you are using the latest software available, but it is also an important part of understanding what configuration parameters exist on the phone. Configuration parameters change from release to release, so phones with different software versions have differences in configuration parameters. To find out what configuration parameters are on a specific phone, you must know its software version.

You can view the phone software version number from the phone UI:

Tap ☰ > ⋯ > About > General.

Locked configuration parameters

Configuration parameters that come from Dolby Conferencing Console are locked (grayed out) and cannot be changed from the phone UI or web interface.

Default values

If a configuration parameter has not been configured in the master configuration file in Dolby Conferencing Console or the provisioning server, or from any other location (such as the phone UI or web interface), the default value will be used.

When configuration parameters change

When certain configuration parameters are changed, the phone might reboot if applying that particular parameter requires a reboot.

If the phone requires a reboot, a reboot prompt displays on the phone screen and phone web interface. It is enabled by default, prompting you to accept firmware upgrades or reboot due to configuration changes. If you take no action (for example, if you do not cancel the reboot) for 20 seconds the phone reboots automatically. Active calls are not interrupted; the reboot is delayed until those calls have ended. You can turn off the reboot prompt if desired (see Disabling the reboot prompt on page 42).

The configuration parameter changes are prioritized in these ways:

- Current values in the configuration files from Dolby Conferencing Console or the provisioning server override all other changes.
- User changes made from the phone UI or web interface override prior changes made by the user.

Additional information about configuration parameters when using a provisioning server

If you are using a provisioning server, this information about configuration parameters applies:

Note: If you are using Dolby Conferencing Console, this information does not apply. Skip this list.
• For Boolean configuration parameters, the values allowed in the configuration templates are case sensitive; only the values false and true are acceptable.

• If a parameter value is invalid, the value is ignored. Invalid parameter values can occur when enumerated-type parameters do not match a predefined value, when numeric parameters are set to nonnumeric values or outside of their valid range, when string parameters are either too long or too short, or when using null strings in numeric fields. All such situations are logged in the phone log files.

• Null should be interpreted as the empty string (that is, attributeName="" when the file is viewed in a JavaScript Object Notation (JSON) editor).

• If you accidentally set a configuration parameter two or more times in the same configuration file or in different configuration files, the parameter will take the last value being parsed by the program.

• Passwords are stored as encrypted strings on the phone.

Related information
Accessing the Dolby Conference Phone web interface on page 78

7.1.2 Deprecated configuration parameters

Dolby may occasionally deprecate old configuration parameters in new releases of Dolby Conference Phone software.

Currently, there is only one deprecated configuration parameter:
Dvms.Server.UseSystemCertStore

When using a provisioning server

If a configuration parameter is deprecated, we recommend that you remove the parameter from your provisioning server. Upgrading your phones to the latest version of Dolby Conference Phone does not remove deprecated configuration parameters from the provisioning server. You must search the configuration files on your provisioning server for the parameter and then manually delete it.

If you choose not to do this, the Dolby Conference Phone and other components (such as Dolby Conferencing Console) will continue to work as expected. Deprecated parameters have no negative impact on functionality. However, they may cause confusion in the future about what parameters are on the phone and are being used, which is why we recommend removing them.

When using Dolby Conferencing Console

If you use Dolby Conferencing Console to manage your phones, no action is needed. Deprecated parameters are removed from the phone when you upgrade the phone and will not appear in Dolby Conferencing Console.

7.2 Configuring certificates

The collection of certificate authority and device certificates installed on the Dolby Conference Phone are security features and are used for authentication with features such as HTTPS provisioning, LDAP TLS connection, 802.1X, and Conferencing Service enabled with Dolby Voice.

The phone can trust certificates issued by widely recognized certificate authorities when trying to establish a connection to a provisioning server for phone provisioning. To establish
new trust relationships, you can add new certificates to the phone through Dolby
Conferencing Console or the provisioning server.

Related information
Trusted certificates and issuers on page 91

7.2.1 Adding certificate authority certificates
A certificate that is issued by a certificate authority (CA) establishes a point of trust between
two entities (for example, the phone and the LDAP directory or the provisioning server).

About this task
If you want the phone to trust any CAs, you must add their certificates to the phone in a CA
certificate directory. This file must be in Privacy-enhanced Electronic Mail (PEM) encoded
format.

You can add CA certificates in these ways:
• Use the Dolby Conferencing Console.
  For more information, see the Dolby Conferencing Console operations and management
guide.
• Use the provisioning server.
• Use the phone web interface.

  From the Tools tab, navigate to Certificates and then click Import CA certificates. A
standard file selection dialog box displays. Select file you want to use, and click Open.

7.2.2 Viewing certificate authority certificates
You can view the basics of CA certificates stored on the Dolby Conference Phone.

About this task
All certificates are validated every time the certificate store changes, as well as every 24
hours if scheduled provisioning is enabled. If a certificate is set to expire within seven days,
the Expiring soon count increases on the CA certificates status screen.

You must replace the certificate before expiry, or certain features will stop working on the
phone. If a certificate expires, the Expired count increases on the CA certificates status page.
Warnings and error messages are available from the phone web interface.
Procedure

1. To view CA certificates from the phone UI:
   a) Tap this sequence:
      ![Sequence Image]

2. To view CA certificates from the phone web interface:
   a) From the Status tab, click Device.
   b) Next to CA Certificate Details, click the Click for more details link.

Related information
Accessing the Dolby Conference Phone web interface on page 78

7.2.3 Device certificate

A device certificate is installed on all Dolby Conference Phones at the manufacturing facility. The device certificate is an X.509 digital certificate signed by the Dolby root certificate authority. It can be used to authenticate the phone when initiating TLS communications, such as those used for HTTPS provisioning and TLS SIP signaling encryption. The X.509 digital certificate is set to expire 256 years from now.

The digital certificate and associated private key are stored on the phone in its nonvolatile memory as part of the manufacturing process. For more information on digital certificates, see www.ietf.org/html.charters/pkix-charter.html and IETF RFC 2459.

Note: At this time, the user is not able to change the device certificate.

7.3 Configuring phone preferences

You can set up these preferences for your users, or you can allow users to set them themselves.
7.3.1 Using the recent calls list

The Dolby Conference Phone can hold a list of the 100 most recently missed, placed, and received calls if it is configured as an IP conference phone.

About this task

This list contains call information such as remote party identification, time and date of the call, and call duration. The recent calls list is enabled by default. The list is downloaded from the phone to the provisioning server after each call is complete. A count of the missed calls is displayed adjacent to the recent calls list icon. If the list is disabled, the count is not displayed.

The list can be used to redial previous outgoing calls, return missed calls, and save contact information to the contact directory. The list can be cleared manually by individual phone users. The list is retained when the phone reboots or when the phone software is upgraded.

There are several ways to configure the recent calls list.

• Set the configuration parameter to enable or disable the recent calls list:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable the recent calls list.</td>
<td>Features.RecentCallsEnabled</td>
</tr>
</tbody>
</table>

• Use the web interface to enable or disable the recent calls list:

Go to Settings > Features, and select the recent calls list Off/On option.

• Use the phone interface to clear the recent calls list:

a) Tap this sequence:

> Preferences > Clear User Data > Clear Recent Calls

b) Tap Yes to confirm.

7.3.2 Enabling user feedback

You can set up the Dolby Conference Phone to solicit feedback from users about their experience with the phone, from a simple thumbs-up to requesting a call to provide more detailed feedback. By default, this feature is enabled.

Procedure

Set these configuration parameters to enable user feedback.

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable user feedback.</td>
<td>Features.UserFeedback.Enabled</td>
</tr>
<tr>
<td>Call user feedback hotline.</td>
<td>Features.UserFeedback.Hotline</td>
</tr>
</tbody>
</table>

7.3.3 Using call forwarding

The phone automatically provides a flexible call forwarding feature that enables you to forward incoming calls to another party.

About this task

There are three ways to apply call forwarding:
To all calls
• When the phone is busy
• When the phone is not answered after 40 seconds

There are several ways to configure call forwarding.

• Set these configuration parameters:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the number where all calls are forwarded.</td>
<td>Preferences.ForwardAllNumber</td>
</tr>
<tr>
<td>Enter the number where the call is forwarded if the user is busy.</td>
<td>Preferences.ForwardBusyNumber</td>
</tr>
<tr>
<td>Enter the number where the call is forwarded if the user does not answer.</td>
<td>Preferences.ForwardNoAnswerNumber</td>
</tr>
</tbody>
</table>

• Use the web interface:
  Go to Settings > Preferences, and enter the phone number in the appropriate forwarding options.

• Use the phone interface:
  Tap ☎ > Call Forward. Enter the phone number in the appropriate forwarding option.

### 7.3.4 Enabling automatic answer

In certain circumstances, you may be unable to physically answer an incoming call. This feature allows you to set up the phone so that incoming calls are answered automatically. The phone rings once. The call is answered with the microphone muted.

**About this task**

There are several ways to configure automatic answer.

• Set the configuration parameter:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable automatic answer.</td>
<td>Preferences.AutoAnswerEnabled</td>
</tr>
</tbody>
</table>

• Use the web interface:
  Go to Settings > User Preferences, and select the automatic answer Off/On option.

• Use the phone interface:
  Tap ☎ and tap automatic answer Off/On.

### 7.3.5 Enabling do not disturb

You can use the do not disturb feature to temporarily stop incoming calls. You can also turn off audio alerts and receive visual call alerts only, or you can make your phone appear busy to incoming callers.

**About this task**

Incoming calls received while do not disturb is turned on are logged as missed.

There are several ways to configure the do not disturb feature.
• Set the configuration parameter:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable do not disturb behavior.</td>
<td>Preferences.DndEnabled</td>
</tr>
</tbody>
</table>

• Use the web interface:

  Go to Settings > User Preferences, and select the do not disturb Off/On option.

• Use the phone interface:

  Tap 📞 and tap do not disturb Off/On.

### 7.3.6 Setting the language

You can change the language displayed on the phone UI. For certain languages, the available date formats also change. By default, English is shown.

**About this task**

There are several ways to set the language.

• Set the configuration parameter:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the language. Possible values include:</td>
<td>Preferences.Localization.Language</td>
</tr>
<tr>
<td>• English</td>
<td></td>
</tr>
<tr>
<td>• French</td>
<td></td>
</tr>
<tr>
<td>• German</td>
<td></td>
</tr>
<tr>
<td>• Italian</td>
<td></td>
</tr>
<tr>
<td>• Spanish</td>
<td></td>
</tr>
<tr>
<td>• Portugal Portuguese</td>
<td></td>
</tr>
<tr>
<td>• Brazilian Portuguese</td>
<td></td>
</tr>
<tr>
<td>• Simplified Chinese</td>
<td></td>
</tr>
<tr>
<td>• Traditional Chinese</td>
<td></td>
</tr>
<tr>
<td>• Japanese</td>
<td></td>
</tr>
<tr>
<td>• Korean</td>
<td></td>
</tr>
<tr>
<td>• Hebrew</td>
<td></td>
</tr>
<tr>
<td>• Arabic</td>
<td></td>
</tr>
</tbody>
</table>

• Use the web interface:

  Go to Settings > User Preferences > Localization > Language.

• Use the phone interface:

  Tap 📞 > Preferences > Language, and select the desired language from the list.

**Results**

If you change the language displayed on a user’s phone remotely, no Please wait message is displayed.
7.3.7 Setting the time and date display

A clock and calendar are enabled by default. You can display the time and date for your time zone in several formats. The phone will synchronize with the local time server. The user may be able to set the time zone through the phone UI.

About this task

The available date formats may change depending on the language selection.

There are several ways to set the time and date display.

• Set the configuration parameters:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the time zone.</td>
<td>Preferences.Localization.Timezone</td>
</tr>
<tr>
<td>Set the time format.</td>
<td>Preferences.Localization.TimeFormat</td>
</tr>
<tr>
<td>Set the date format.</td>
<td>Preferences.Localization.DateFormat</td>
</tr>
</tbody>
</table>

• Use the web interface:

Go to Settings > User Preferences > Localization, and select the Time parameters.

• Use the phone interface:

To change the time zone, tap Preferences > Time zone and select the desired time zone from the list.

To change the time format, tap Preferences > Time Format and select the desired format from the list.

To change the date format, tap Preferences > Date Format and select the desired format from the list.

7.4 Options for provisioning

You can select different provisioning options when preparing the phone for use.

7.4.1 Scheduling a software update

A phone software update initiates whenever there is new phone software on the provisioning server. This triggers a reprovisioning of your phone software. You can also trigger a reprovisioning of the Dolby Conference Phone manually.

About this task

Use any of these methods to trigger a reprovisioning:

• Use Dolby Conferencing Console to push a configuration to multiple devices.
  Select the devices and then click the Push Configuration button.

• Set a recurring provisioning time through the configuration files or web interface.

• Power off and on the phone.

• Use the phone user interface by tapping Reboot Phone.
• Use the web interface by selecting **Tools** and then selecting the reboot or reprovisioning link.

• Use the diagnostic shell command **system provision**.

### 7.4.2 Setting recurring provisioning

You can set a recurring time for the phone to perform a provisioning check. For example, if you set `Provisioning.Scheduled.StartTime` to 5 and `Provisioning.Scheduled.Duration` to 30, then a provisioning check will randomly occur every day between 5:00 a.m. and 5:30 p.m. By default, there is no scheduled check.

**About this task**

You can use configuration parameters or the web interface to schedule provisioning. You cannot schedule provisioning from the phone user interface.

• Set the configuration parameters:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables or disables scheduled provisioning</td>
<td>Provisioning.Scheduled.Enabled</td>
</tr>
<tr>
<td>Sets the provisioning request start time</td>
<td>Provisioning.Scheduled.StartTime</td>
</tr>
<tr>
<td>Sets the provisioning delay</td>
<td>Provisioning.Scheduled.Duration</td>
</tr>
</tbody>
</table>

• Use the web interface:

  Tap **Settings > Provisioning > Scheduled** and set the appropriate parameters.

### 7.4.3 Disabling the reboot prompt

The reboot prompt is enabled by default, prompting you to accept firmware upgrades or reboot due to configuration changes. If you take no action in 20 seconds—for example, cancel the reboot—the phone reboots automatically.

**About this task**

This procedure disables both the reboot prompt and the software update prompt.

For more information, see **Configuration parameters** on page 33 > *When configuration parameters change*.

You can use either configuration parameters or the web interface to disable the reboot prompt. You cannot disable the reboot prompt from the phone user interface.

• Set the configuration parameter:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables/disables the reboot and software update prompt</td>
<td>Provisioning.CfgChange.UserAcknowledgement Enabled</td>
</tr>
</tbody>
</table>

• Use the web interface:

  a) Go to **Settings > Provisioning > On Configuration Change**.

  b) Set **User acknowledgment enabled** to **Off**.
7.5 Phone access control

The administrative settings can be changed to suit the needs of your organization. You can control access to the phone from the command-line interface (CLI) shell and the web interface, as well as the phone itself.

7.5.1 Changing the administrative password

The phone Administrative Settings menu is protected with an administrative password. The phone displays a password prompt before it grants access to the subsequent menu options.

About this task

The default administrative password is 1739. Change the administrative password from the default value as soon as possible. If you leave the administrative password unchanged or use weak passwords, the phone is vulnerable to various network attacks.

The Dolby Conference Phone web interface is also protected by the administrative password.

Use one of these methods to change the administrative password.

Note: We recommend that you do not enter passwords in configuration files, as it poses a security risk.

- Use the configuration parameter.
  
  Authentication.Local.Admin sets the local administrative password for the phone.

- Use the web interface.
  
  Go to Settings > Authentication > Local Account and enter a new administrative password.

- Use the phone user interface.
  
  a) Tap this sequence:

    🔄 > ⚙️ > Administrative Settings

  b) Enter the current password, and then tap Change password.

  c) Enter the new password, and then confirm the new password.

7.6 Directory options

You can select different directory options. For example, you can allow users access to your organization’s corporate directory.

7.6.1 Using a corporate directory

You can connect your phone to a directory server that supports the LDAP version 3.

About this task

The corporate directory is a flexible feature. You can configure the LDAP directory parameters listed below. Certain parameters are set by default (for example, search filter, scope, time-out, limit, and attributes). Once it is set up on the phones, users can search the corporate directory. Users can also call numbers and save entries retrieved from the LDAP server to the local contact directory on the phone.
Note: For saved entries to work, you must format them in a manner that is consistent with your call control platform. For example, you may need to include the number 9 or a plus sign (+) at the beginning of the entry.

If you are required to access the LDAP server in a secure manner, you must download the appropriate CA certificate to the phone (see Adding certificate authority certificates).

Only Microsoft Active Directory 2003 SP2 and later is supported at this time. Microsoft Active Directory supports server-side sorting.

Tip: Consult your LDAP administrator when changing any corporate directory configuration information. For more information on LDAP attributes, see IETF RFC 4510.

There are several ways to configure a LDAP directory:

- Set the Directory.Ldap configuration parameter:
  - Specify:
    - LDAP server location
    - Log-in name and password
    - Base domain name
    - LDAP attributes and other settings

- Use the web interface:
  Tap Settings > Corporate Directory, and set the appropriate parameters.

- Use the phone interface:
  Review the LDAP server status by tapping ☰ > ⋯ > About > Status > Directory Service, and then set the appropriate parameters.
  To search the corporate directory, tap the Phone icon, and then tap the Directory icon. Enter the search criteria.

### 7.6.2 Adding the corporate directory configuration

If the Cisco Unified Communications Manager is connected to an LDAP directory, you can connect to the same LDAP directory.

**About this task**

You need this information to connect the phone to the LDAP directory:

- The IP address or host name of the LDAP server
- The log-in name and password for the LDAP server
- The base domain name for the search of the LDAP server

To change the configuration file:

**Procedure**

1. Edit or add the following parameters:
   a) Set Directory.Ldap.URIList to the LDAP server URI.
      Use a comma-separated list to add more than one server. For example:
      ldap://10.101.21.5,ldap://10.120.21.6
   b) Set Directory.Ldap.LoginName to the log-in name.
c) Set directory.ldap.Password to the log-in password.

d) Set Directory.ldap.BaseDN to the base domain name for the search.

e) Set Directory.ldap.SecureConnection to true or false, depending on the security settings on the LDAP server.

2. Reboot the phone.

3. Make sure that the configuration process completed correctly by tapping this sequence on the phone:

```
  > > About > Status > Directory Service
```

4. Confirm that the Cisco Unified Communications Manager IP primary and secondary server addresses and the configuration files downloaded to the phone.

Results

Once the reboot is complete, users can search for contacts in the LDAP server from the phone.

Related information

Template files on page 100

7.6.3 Using the contact directory

If the Dolby Conference Phone is configured as an IP conference phone, users can save contacts manually or save recent calls and corporate directory search results locally. The phones can support up to 1,000 contacts. All saved contacts can be manually cleared by individual phone users.

About this task

You can also provide a local contact directory for users. When the phone reboots, this directory is downloaded from the provisioning server to the user’s phone.

To clear the contact directory:

Procedure

1. Tap the Settings button on the home screen.

2. Select Preferences > Clear personal data > Clear local contacts.

3. Tap Yes to confirm.

Related information

Master configuration file on page 98

Adding the corporate directory configuration on page 44

7.6.4 Creating a local contact directory by using the provisioning server

On the provisioning server, you can create a local contact directory for users.

About this task

You can save recent calls and corporate directory search results locally.
To create a local directory:

**Procedure**

Using a JSON editor, create a file that includes the contacts you want users to view (for example, directory.json).

This example shows a sample local contact directory.

```json
{
  "entries": [{
    "firstName": "Gerolomo",
    "lastName": "Grande",
    "number": "2222"
  },
  {
    "firstName": "Tatsuaki",
    "lastName": "Tanaka",
    "number": "2224"
  }]
}
```

Note: Dolby Conferencing Console version 1.2 and later allows you to provision a directory.

### 7.7 Configuring IP PBX for the phone

If you want to use the Dolby Conference Phone as an IP PBX (regular telephone) as well as a conferencing phone, you must first configure IP PBX settings.

**About this task**

Use the phone web interface to specify the account settings for your IP PBX and register the phone. This involves modifying the settings for **Account**, **Server** and **Credential** settings within the **IP PBX** section.

**Procedure**

1. Set the operation mode for the phone. From the phone web interface, from the **Settings** tab, navigate to **Features** and choose **Dual mode** or **IP PBX** for the **Operation Mode**.

2. From the **Settings** tab, navigate to **IP PBX Settings > Account** to configure the account and extension information.
   
   a) In the **Display Name** field, enter the device name.
   
   b) In the **Extension number/Address field** enter the extension or Session Initiation Protocol address for the phone.
3. From the **Settings** tab, navigate to **IP PBX Settings > Server** and then enter the settings for the primary server and any secondary (failover) server.

   For specific instructions, see the *configuration guide* for your conferencing service provider or call control platform.

   ![IP PBX Settings interface](image)

4. Expand the **Credential** section, and then enter the user credential name, user credential password, and server realm.

   These settings are mandatory for digest authentication.

   For specific instructions, see the *configuration guide* for your call control platform.

   **Results**

   After you finish setting up the phone for IP PBX, the phone icon on the phone home screen no longer appears dimmed next to the conferencing icon.

### 7.7.1 Configuring PBX server redundancy

Server redundancy is often required in IP PBX deployments to ensure continuity of phone service.

**About this task**

You must plan for times when the call server needs to be taken offline for maintenance, the server fails, or the connection between the phone and the server fails. For the Dolby Conference Phone, having a second call server of equivalent capability that takes over from the offline or failed server preserves the full phone system functionality.

There are several ways to configure redundancy:

- Set the configuration parameters:
### Configuration parameter description

<table>
<thead>
<tr>
<th>Configuration parameter name</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the secondary call server address or outbound proxy address</td>
<td>Sip.Pbx.OutboundProxy2</td>
</tr>
<tr>
<td>Specifies the secondary call server or outbound proxy address port</td>
<td>Sip.Pbx.OutboundProxy2Port</td>
</tr>
</tbody>
</table>

- Use the web interface:
  Tap **Settings > IP PBX Settings > Server**, and set the appropriate parameters.
- Use the phone interface to review the call server status:
  Tap **Menu > About > Status > Call server**.

### 7.7.2 Configuring the Voice Activation Detection (VAD) parameter for the phone

The Dolby Conference Phone by default signals G.729AB (G.729A with Annex B) to its peer. If your IP PBX configuration requires the phone to signal G.729A, you can set the `Sip.Vad.SignalAnnexB` configuration parameter to false to override the default behavior.

**About this task**

The Dolby Conference Phone supports the G.729AB codec and also allows Annex B in its Session Description Protocol (SDP) to be turned off.

You can perform this procedure from the phone web interface or from Dolby Conferencing Console.

**Procedure**

1. From the phone web interface:
   a) From the **Settings** tab, expand the **IP PBX Settings** section, and then expand the **VAD** section.
   b) Turn off **Signal G729 Annex B**.
      This option controls the `Sip.Vad.SignalAnnexB` parameter.

2. Alternatively, from Dolby Conferencing Console:
   a) From the home screen, select the device pool than contains the device for which you want to edit parameters.
   b) Select the device you want to edit.
   c) In the left navigation bar, click the edit button.
      The Device configuration screen displays.
   d) Navigate to **IP PBX Settings > > VAD**
   e) Drag **Signal G729 Annex B** to the device configuration in the upper right-hand side of the screen.
      The `Sip.Vad.SignalAnnexB` parameter appears in the device configuration.

3. Turn the `SIP.Vad.SignalAnnexB` parameter off.

**Results**

The phone now signals peers using G.279A.
7.8 Disabling Bluetooth advertisement

By default, the Dolby Conference Phone is configured to allow the phone to advertise a Bluetooth LE signal that can be detected by other Bluetooth-enabled devices. When used in conjunction with other Bluetooth-enabled devices, such as mobile phones, this feature can allow the phone to be controlled remotely. You can turn it off for security reasons, if needed.

About this task
You can perform this procedure from the phone web interface or from Dolby Conferencing Console.

Procedure
1. From the phone web interface:
   a) From the Status tab, expand the Device section.
   b) Turn Bluetooth Module Initialization off.
      This option controls the Dvms.Service.EnableBluetoothAdvertisement parameter.

2. Alternatively, from Dolby Conferencing Console:
   a) From the home screen, select the device pool than contains the device for which you want to edit parameters.
   b) Select the device you want to edit.
   c) In the left navigation bar, click the edit button.
      The Device configuration screen displays.
   d) Navigate to Dolby Voice Conferencing Service > Service.
   e) Drag the Allow bluetooth advertisement to the device configuration.
      The Dvms.Service.EnableBluetoothAdvertisement parameter appears in the device configuration.
   f) Turn the parameter off.

Related information
Bluetooth LE initialization and advertisement on page 84
Confirming Bluetooth LE advertisement on page 85
8 Deploying the phone

The deployment process varies depending on whether you perform Plug-and-Play Setup, Automatic Local Setup, or Manual Setup. The setup wizard screens vary depending on the setup methods available and the choices you make. The wizard guides you through network setup, if needed, and connecting to a provisioning service.

- First-time use of the phone
- Deploying in a secure network
- Changing network configuration after out-of-the-box setup

8.1 First-time use of the phone

Deploying the phone starts with unboxing the Dolby Conference Phone and physically connecting it to a PoE Ethernet port on the network using an Ethernet cable. When you do this, the setup wizard displays on the phone user interface.

The setup wizard begins differently depending on:

- If you use Plug-and-Play Setup and your phone is recognized by the Dolby Voice Console
- If you use Plug-and-Play Setup and your phone is not recognized by the Dolby Voice Console
- If you prepared your network for Automatic Local Setup
- If you perform Manual Setup

For non-Plug-and-Play Setup deployments, the network setup is an important part of the process and the first half of the setup wizard covers network setup. You must connect the phone to the network before you can connect it to Dolby Conferencing Console or the provisioning server.
8.1.1 Setting up the phone using Plug-and-Play Setup

Use Plug-and-Play Setup if you want to provision the Dolby Conference Phone using your conferencing service provider's provisioning service instead of setting up and using an on-premise instance of Dolby Conferencing Console or an on-premise provisioning server.

About this task

Be aware that if you completed the preparation work for Automatic Local Setup, the screens and prompts in the setup wizard are different than described here. Instead, you are
prompted to connect to your on-premise instance of Dolby Conferencing Console or your on-premise provisioning server as described in Setting up the phone using Automatic Local Setup on page 54.

**Procedure**

1. Make sure that the Ethernet port that you plan to use has Internet access to the server addresses as described in Server addresses on page 25.

2. Connect the phone to a PoE Ethernet port on the network using an Ethernet cable.
   
   The setup wizard displays on the phone user interface.

3. Wait for the phone to connect to the network.

   ![Dolby Conference Phone](image)

   If the phone connects to the Dolby Voice Console and is recognized, the phone connects to your conferencing service provider’s provisioning service.

   If the phone connects to the Dolby Voice Console and is not recognized, the Select your Dolby Voice service provider screen displays.

   If the phone fails to connect to the Dolby Voice Console, you must choose Manual setup. After that, you are prompted to choose a language and time zone. Next, an error screen displays letting you know that there was a problem with Plug-and-Play Setup (see Plug-and-Play Setup issues and solutions on page 120).

   ![Dolby Conference Phone](image)

4. If the phone connected to the Dolby Voice Console and you still want to perform Plug-and-Play Setup, choose your conferencing service provider from the list and then complete these steps:
   
   a) From the Welcome screen, enter a name for the phone and then tap Next.

   b) From the Allow Dolby to collect usage data screen, tap Yes or No.
For more information, see Collection of usage data on page 86.

c) From the **Setup phone service**, choose **Yes** if you want to allow regular telephone (IP PBX) calls to and from the phone.

Write down the URL provided on this screen. From your computer, go to this location ([http://bit.ly/2nLsBNM](http://bit.ly/2nLsBNM)) for more information and instructions.

d) Tap **Finish**.

e) Wait while the phone automatically reboots.

If the phone fails to provision using your conferencing service provider’s provisioning service, instead you must either:

- Change the network configuration to allow Plug-and-Play Setup.
• Set up the phone using Automatic Local Setup or Manual Setup.

Results

Your setup is now complete and you can instruct users to start making calls.

If you chose to allow regular phone calls to and from the phone, the phone icon appears next to the conferencing icon, but appears dimmed until you configure the IP PBX settings.

Note: After Plug-and-Play Setup successfully completes, if you need to place the phone on a specific virtual LAN (such as a voice virtual LAN), you must enable Link Layer Discovery Protocol in the Settings menu or manually set up the VLAN.

What to do next

If desired, go to the URL provided earlier (http://bit.ly/2nLsBNM) about how to allow regular (IP PBX) calls to and from the phone. Follow the instructions provided to complete IP PBX setup.

Related information

How Plug-and-Play Setup works on page 25
Collection of usage data on page 86

8.1.2 Setting up the phone using Automatic Local Setup

The first part of out-of-the-box setup involves network setup. You can use the setup wizard to connect the Dolby Conference Phone to the network, discover the Dolby Conferencing Console or the provisioning server, and complete the phone setup.

About this task

This procedure assumes that you have completed the preparation described in Automatic Local Setup on page 27. If you have not, go back and complete the preparation.

Procedure

1. Connect the phone to a PoE Ethernet port on the network using an Ethernet cable.

   The setup wizard displays on the phone user interface.

2. Wait for the phone to connect to the network.

3. Once the phone successfully discovers a provisioning server, tap Yes on the Setup Provisioning screen for the phone to connect to the discovered provisioning server.
The setup wizard connects the phone to the provisioning server.

4. If prompted, enter a user name and password for the provisioning server.
   This depends on your specific environment and network setup. You may not be prompted for this information at all.

5. If you are connecting to an HTTPS provisioning server, when prompted, confirm that you accept the provisioning server certificate.
   If you are connecting to a different provisioning server, such as FTP or HTTP, this step is skipped.

6. Wait for the phone to connect to the provisioning server, and then reboot.

7. Confirm that the Dolby Voice software and the configuration files on the provisioning server are now on the phone.
   From the phone user interface, tap > > > About > Status > Provisioning server. Scroll down to Configuration files.

8. Monitor the log files uploaded to the provisioning server.
   Log files are uploaded to the folder specified in Provisioning.Server.UploadDir.

Results
You can now instruct users to start making calls.

Related information
Automatic Local Setup preparation on page 27

8.1.3 Connecting the phone to the network using Manual Setup

The first part of out-of-the-box setup involves network setup. You can use the setup wizard to connect the phone to the network manually, if desired. After you complete this portion and have connected to the network, the next step is connecting to the provisioning server.

Procedure

1. Connect the phone to a PoE Ethernet port on the network using an Ethernet cable.
   The setup wizard displays on the phone user interface.

2. If the phone did not discover a provisioning server, then this screen displays on the phone user interface. Tap Manual setup.
If the phone is not recognized by the Dolby Voice Console, the **Select your Dolby Voice service provider** screen displays.

3. From the Select language screen, choose a language. If needed, scroll up or down to find the language.

4. From the Select time zone screen, choose a time zone. If needed, scroll up or down to find the time zone.

5. Optional: From the Network setup screen, you can change your VLAN settings, if needed.
By default, Link Layer Discovery Protocol is disabled.

6. From the Network setup screen, you can change your proxy settings, if needed.

7. If challenged for 802.1X authentication, tap Confirm certificate, and then follow the instructions in Deploying with 802.1X authentication on page 59.

8. Wait for the phone to connect to the network.

What to do next
After you have connected to the network, continue through the setup wizard to connect the phone to the provisioning server.

To reenable Link Layer Discovery Protocol, you must do it manually in Settings either on the phone user interface or with the Dolby Conferencing Console.

Related information
Ways to set up the phone on page 15
First-time use of the phone on page 50

8.1.4 Connecting the phone to Dolby Conferencing Console or the provisioning server using Manual Setup

We recommend that you connect to Dolby Conferencing Console or the provisioning server using Automatic Local Setup, but you can connect using Manual Setup, if desired.
Procedure

1. Connect the phone to the Dolby Conferencing Console or the provisioning server using one of these procedures:
   • Setting up the phone using Automatic Local Setup on page 54
   • Connecting the phone to the network using Manual Setup on page 55

2. From the Setup Provisioning screen, choose Manual setup.

   ![Setup Provisioning](image)

   **Note:** If your network is not configured to support Automatic Local Setup, you will only see one option listed here: Manual setup.

3. From the Setup Provisioning screen, tap Protocol, choose FTP, HTTP, or HTTPS, and then go back to the previous screen.

   ![Select protocol](image)

4. From the Setup Provisioning screen, tap Server address and enter an IP address or host name, and then tap Save.
5. If prompted, enter a user name and password for the provisioning server. This depends on your specific environment and network setup. You may not be prompted for this information at all.

6. Wait for the phone to connect to the provisioning server, and then reboot.

7. If you are connecting to an HTTPS provisioning server, when prompted, confirm that you accept the provisioning server certificate. If you are connecting to a different provisioning server, such as FTP or HTTP, this step is skipped automatically.

8. Confirm that the Dolby Voice software and the configuration files on the provisioning server are now on the phone.

   From the phone user interface, tap > > > > About > General.

9. Monitor the log files uploaded to the provisioning server.

   Log files are uploaded to the folder specified in Provisioning.Server.UploadDir.

**Results**

You can now instruct users to start making calls.

**What to do next**

To reenable Link Layer Discovery Protocol, you must do it manually in **Settings** on the phone user interface.

**Related information**

- [Ways to set up the phone](#) on page 15
- [First-time use of the phone](#) on page 50

### 8.2 Deploying in a secure network

During out-of-the-box setup, you may be prompted to confirm the certificate for the 802.1X authentication server, and later to confirm the certificate for the provisioning server. 802.1X authentication prevents unknown devices from connecting to the network. For example, if a guest were visiting the office and plugged their computer into a network port without permission, 802.1X authentication prevents them from being able to connect.

#### 8.2.1 Deploying with 802.1X authentication

If your network requires 802.1X (commonly known as Port Guard in Cisco networking environments) during the network setup portion of the setup wizard, you are required to complete 802.1X setup. Depending on the 802.1X configuration, you may need to accept the
authentication server certificate in the setup wizard. The setup wizard guides you through the process.

About this task
Depending on the authentication server configuration, you may be prompted to enter authentication credentials before you accept the server certificate.

Procedure
1. If a PKI-based authentication method is selected by the authentication server, you are prompted to review the server certificate information. From the Network setup screen, tap Confirm certificate.

2. From the Confirm server identity? screen, review the certificate information. If it is correct, tap Yes.

The phone connects to the 802.1X authentication server.
3. From the 802.1X authentication screen, enter the identity and password of the 802.1X authentication server. Tap the confirm button.

4. Tap Next.

What to do next
After you complete these steps, return to the provisioning task that you were working on before you were prompted to confirm this certificate.

Related information
First-time use of the phone on page 50

8.2.2 HTTPS provisioning

If you are using an HTTPS provisioning server, you are prompted to confirm the certificate of the provisioning server. This happens during the provisioning setup portion of the out-of-the-box setup wizard.

HTTPS encrypts communication and provides a secure connection between the phone and the HTTPS provisioning server. Using an HTTPS provisioning server prevents impostor devices from connecting to the network. This is accomplished by using certificates.

For example, by default, the phone does not trust any provisioning servers. When you perform out-of-the-box setup, you are prompted to accept the provisioning server certificate.

After you tap Save, this screen displays. Tap Yes to accept the server identity.
8.3 Changing network configuration after out-of-the-box setup

After you complete out-of-the-box setup, you may need to change the phone network configuration parameters. You can change network configuration parameters from the phone user interface, web interface, or the configuration files on Dolby Conferencing Console or the provisioning server.

You can change provisioning server parameters only from the phone user interface.

**Note:** Certain parameters are dependent on other settings. For example, if DHCP is enabled, the Phone IP Address and Subnet Mask parameters are not editable, because the DHCP server automatically supplies the values.

8.3.1 Configuration and rediscovery of the provisioning server

You can modify these configuration parameters from the **Provisioning server** menu on the phone user interface:

- **Type**
  - If the provisioning type is set to **Manual**, you must set the provisioning server address.
  - If the provisioning type is set to **Automatic**, you can rediscover the provisioning server from the menu.
- **Server**
- **Protocol**
- **User name**
- **Password**

For the user name and password, if you are connecting to a Dolby Conferencing Console server, contact your system administrator for device pool access control credentials. If you are using an FTP provisioning server, see the values you set in Setting up an FTP server on page 97.

For more information about these parameters, and about which parameters are dependent on others, see **Configuration parameters** on page 33.

**Note:** Changing the provisioning server IP address, type, user, and password will not cause the phone to reboot; the phone will be reprovisioned.

8.3.2 Network configuration

When configuring the network parameters on the Dolby Conference Phone, you must change certain parameters based on your particular network settings, whereas others can be left at their default values. Your organization’s IT administrator will be able to assist you.
8.3.3 Configuring IP Network options

From the IP Network menu, you can modify certain network configuration parameters.

About this task

You can modify these configuration parameters:

- DHCP flag: If DHCP is enabled, the DHCP server will provide the IP address and subnet mask of the phone. Otherwise, you must enter those values.
- IPv4 address: If DHCP is disabled, you must enter the IP address for the phone.
- Subnet mask: If DHCP is disabled, you must enter the subnet mask for the phone.
- Gateway.
- DNS server 1: If DHCP is disabled, you must enter the organization’s primary DNS server IP address.
- DNS server 2: If DHCP is disabled, you must enter the organization’s secondary DNS server IP address.
- DHCP VLAN option.

There are several ways to configure these options:

- Set the configuration parameters:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whether or not to enable DHCP (default true)</td>
<td>Network.DHCP</td>
</tr>
<tr>
<td>IP address of the phone</td>
<td>Network.IpAddress</td>
</tr>
<tr>
<td>Subnet mask of the network interface (available only if Network.DHCP is false)</td>
<td>Network.Subnet</td>
</tr>
<tr>
<td>Default gateway</td>
<td>Network.DefaultGateway</td>
</tr>
<tr>
<td>Primary DNS server IP address (available only if Network.DHCP is false)</td>
<td>Network.DNS1</td>
</tr>
<tr>
<td>Secondary DNS server IP address (available only if Network.DHCP is false)</td>
<td>Network.DNS2</td>
</tr>
<tr>
<td>User-configured VLAN ID</td>
<td>Network.Vlan.ManualVlanId</td>
</tr>
</tbody>
</table>

- Use the web interface:

  Go to Settings > Network and edit the desired parameters.

- Use the phone interface:

  Tap 📱 > ⏯️ > Administrative Settings > Network Configuration > IP network and edit the desired parameters.

8.3.4 Configuring LLDP

From the Ethernet menu, you can modify the VLAN ID configuration parameter.

About this task

A VLAN can be used to separate and assign higher priority to a voice VLAN as a way of minimizing latency.
The phone will tag all outbound Ethernet packets, except the LLDP advertisement, with an 802.1Q VLAN header when:

- A valid VLAN ID is obtained from LLDP voice VLAN network policy type-length values; see LLDP and supported type-length values on page 88.
- A valid VLAN ID is specified in the phone network configuration.

There are several methods by which the phone can be configured to work on a particular VLAN:

- LLDP is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network. LLDP-MED capabilities are also supported.
- Static: The VLAN ID can be manually set from the phone UI or from a configuration file.

If the phone receives a VLAN setting from multiple of the above methods, the priority is as follows (from highest to lowest):

- LLDP (and LLDP-MED)
- Static VLAN ID

There are several ways to enable or disable LLDP discovery:

- Set the configuration parameter:
<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables or disables LLDP discovery</td>
<td>Network.Services.LLDPEnabled</td>
</tr>
</tbody>
</table>

- Use the web interface:
  Go to **Settings > Network > Services > Enable LLDP** and select On or Off.

- Use the phone interface:
  Tap ![icon] > ![icon] > **Administrative Settings > Network Configuration > Ethernet > LLDP enabled**.

### 8.3.5 Configuring the secondary VLAN

Some organizations use a secondary VLAN to isolate voice and data traffic.

**About this task**

If you need information about setting up a secondary VLAN, continue reading, but also make sure that you review Primary and secondary VLANs on page 21.

If you need to isolate voice and data traffic by using different VLANs, you can enable the secondary VLAN. The secondary VLAN does not support static IP configuration and must be configured using DHCP.

Once the secondary VLAN is enabled, the Dolby Conference Phone will create a secondary virtual network interface that is on the secondary VLAN ID. Then the phone would have two IP addresses, one on the primary (or default) VLAN and the other on the secondary VLAN.

**Note:** WPAD and PAC work independently on the primary and secondary VLANs.

There are several ways to enable and configure the secondary VLAN:

- Set the configuration parameters:
Configuration parameter description | Configuration parameter name
--- | ---
Whether or not to enable the secondary VLAN | Network2.Enabled
Enables WPAD | Network2.Proxy.AutoDiscover
Specifies the PAC configuration URL | Network2.Proxy.PacUrl
Specifies the proxy server log-in name | Network2.Proxy.UserName
Specifies the proxy server log-in password | Network2.Proxy.Password

- Use the web interface:
  a) Go to Settings > Network > Secondary VLAN and select On.
  b) To set the user-configured VLAN ID, go to Settings > Network > Secondary VLAN > Virtual LAN and enter a valid VLAN ID.

- Use the phone interface:
  Tap > > Administrative Settings > Network Configuration > Secondary VLAN and change the On/Off option to On.

8.3.6 Configuring the time server

The Dolby Conference Phone uses a time server to synchronize the clocks on all of the phones on the network. If your network has a local NTP server, we highly recommend that you configure it.

About this task
By default, the phone uses DHCP option 42 to configure the time server. If the phone cannot configure the time server using DHCP option 42, then the time server is set to time.nist.gov as the primary NTP server and pool.ntp.org as the secondary NTP server. If the connection fails and the phone is connected to an IP PBX, the IP PBX supplies the time, and that is shown on the Dolby Conference Phone user interface and web interface.

Note: The network must have a DNS server in order for the phone to resolve the host name and connect to the default NTP servers.

There are several ways to set and check the time server parameters:

- Set the configuration parameters:

  | Configuration parameter description | Configuration parameter name |
  --- | ---
  Sets the primary NTP server IP address | Network.Ntp.Server1 |
  Sets the secondary NTP server IP address | Network.Ntp.Server2 |

- Use the web interface:
  To set the NTP server IP addresses, go to Settings > Network > NTP and enter the parameters.

- Use the phone interface:
  To review the time server status, go to > > About > Status > Network time synchronization.
8.3.7 Configuring 802.1X after out-of-the-box setup

IEEE 802.1X is a port-based Network Access Control (PNAC). It provides an authentication mechanism to devices trying to attach to a LAN.

About this task

802.1X authentication is disabled on the Dolby Conference Phone until challenged by the network switch. The authentication method is based on the network requirements.

In the 802.1X menu, you can enter these configuration parameters:

- EAPOL Identity: The identity (or user name) required for 802.1X authentication
- EAPOL Password: The password required for 802.1X authentication

The phone supports these authentication methods:

- EAP-PEAP: Requires the device to validate the CA certificate, and the user to enter a user name and/or password for network authentication.
- EAP-MD5: Requires the phone to create an MD5 hash of a random value from the network and a user’s password to authenticate.
- EAP-TTLS: The only supported secondary authentication method is MSCHAPv2.
- EAP-FAST with automatic PAC provisioning: The phone supports anonymous or authenticated in-band PAC provisioning. Manual PAC provisioning and the “do not use PAC” provisioning modes are not supported.

Note: Your first attempt on 802.1X authentication using EAP-FAST with automatic PAC provisioning will fail due to initial PAC file provisioning. Authentication will be successful on the second attempt and thereafter. As a result, there will be a delay up to 60 seconds on device boot up.

There are several ways to specify the 802.1X credentials:

- Set the configuration parameters:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the IEEE 802.1X user identity</td>
<td>Network.Eapol.Identity</td>
</tr>
<tr>
<td>Sets the IEEE 802.1X password</td>
<td>Network.Eapol.Password</td>
</tr>
</tbody>
</table>

- Use the web interface:

  Go to Settings > Network > IEEE 802.1X and enter the parameters.

- Use the phone interface:
a) Review the call server status.

   Go to > Administrative settings from the phone home screen.

b) Enter the current password, and then tap Network configuration > 802.1X.

c) Enter the IEEE 802.1X user identity and password, and tap ✔.

8.3.8 IEEE 802.1p/Q

The Dolby Conference Phone supports two types of configuration for Quality of Service (QoS) and differentiated services tagging, in priority order: provisioning configuration and LLDP.

The phone will use the values in the configuration file. However, if provisioning configuration is unavailable, LLDP configures QoS settings.

For each voice/signaling packet, layer 2 and layer 3 priorities (Differentiated Services Code Point (DSCP) and link layer class of service) are set from LLDP.

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the priority and link-layer priority of voice and signaling channels</td>
<td>Network.QoS.*</td>
</tr>
</tbody>
</table>

8.3.9 Configuring proxy autoconfiguration (PAC) and web proxy autodiscovery (WPAD) protocol

Proxy auto configuration allows network administrators to automatically configure complex proxy settings across the network.

About this task

- PAC: Specify the URL of a JavaScript file that contains a function to be used to determine the appropriate proxy for each outgoing HTTP and HTTPS connection. The PAC functions are used for conferencing and provisioning connections. The maximum size of a proxy PAC file is 64 KB. The phone supports ECMA-262 specification and does not support proprietary extensions.
- WPAD protocol: Let the system autodiscover the URL of the PAC file through a DHCP option and DNS A record lookup.

Note: If Dvms.Proxy is configured, Network.Proxy.* is ignored when connecting the phone to the conferencing service. If Dvms.Proxy is configured and the secondary VLAN is enabled, Network2.Proxy.* is also ignored. This allows existing configurations to remain valid after a Dolby Conference Phone software upgrade to 2.1 or later.

There are two ways to set up automatic proxy configuration:

- Set the configuration parameters:

<table>
<thead>
<tr>
<th>Configuration parameter description</th>
<th>Configuration parameter name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables WPAD</td>
<td>Network.Proxy.AutoDiscover</td>
</tr>
<tr>
<td>Specifies the PAC configuration URL</td>
<td>Network.Proxy.PacUrl</td>
</tr>
<tr>
<td>Specifies the proxy server log-in name</td>
<td>Network.Proxy.UserName</td>
</tr>
<tr>
<td>Specifies the proxy server log-in password</td>
<td>Network.Proxy.Password</td>
</tr>
</tbody>
</table>

- Use the web interface:
• To set the PAC/WPAD parameters, go to **Settings > Network > Proxy** and enter the parameters.

• To check the PAC/WPAD status, go to **Status > Network**.

### 8.3.10 Proxy authentication

The Dolby Conference Phone can utilize the HTTP proxy server in a customer’s network to connect to services on the Internet.

These methods are supported for proxy server authentication:

- No authentication
- Digest
- Basic
- NTLMv2

**Related information**

*Network requirements* on page 18
9 Administering the phone

You can view status information, diagnostic information, and error messages from the Dolby Conference Phone. You can perform administrative tasks, such as exporting a phone configuration or downloading logs, from the phone web interface.

- Error messages
- Viewing the Status menu
- Log files
- Accessing the Dolby Conference Phone web interface
- Exporting the Dolby Conference Phone configuration
- Rebooting the Dolby Conference Phone
- Call and media statistics
- Viewing diagnostics
- Diagnostic shell
- Bluetooth LE initialization and advertisement
- Collection of usage data
- Phone memory resources
- Resetting to factory defaults
- LLDP and supported type-length values
- Trusted certificates and issuers

9.1 Error messages

The warning notification feature provides users a visual indication that one or more error conditions exist.

When an error occurs, users will see:

- A warning icon on the phone home screen
- An informative message when the warning is first detected

Most of the errors listed in this table will be logged to the phone log file. However, if you are having trouble connecting to the provisioning server, the phone may not be able to upload every error.

This table lists important error messages, causes, and possible solutions.

<table>
<thead>
<tr>
<th>Error message</th>
<th>What the administrator should do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter does not exist.</td>
<td>You have added a configuration parameter that is not supported by the phone in the configuration file. Remove it, and try again.</td>
</tr>
<tr>
<td>Invalid value.</td>
<td>Enter a valid value.</td>
</tr>
<tr>
<td>Invalid value range.</td>
<td>Enter a value within the valid range.</td>
</tr>
<tr>
<td>Invalid value type.</td>
<td>You entered a value of a different type (for example, using an integer instead of a Boolean value). Enter a value of the correct type.</td>
</tr>
</tbody>
</table>
### Table 5: Error messages that display on the Dolby Conference Phone (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>What the administrator should do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid value length.</td>
<td>You entered a string that is too short or long. Enter a valid string.</td>
</tr>
<tr>
<td>Write access denied.</td>
<td>You are trying to set a configuration parameter in the configuration file that cannot be changed in that way. For information on parameters, see Configuration parameters on page 33.</td>
</tr>
<tr>
<td>Invalid numeric value.</td>
<td>You entered a numeric value that does not match the parameter range rule. (For example, it is larger than the maximum value or smaller than the minimum value.) Enter a valid numeric value.</td>
</tr>
<tr>
<td>Invalid alphabetic value.</td>
<td>You entered a value that contains invalid characters for an alphabetical parameter. Enter a valid alphabetical value.</td>
</tr>
<tr>
<td>Invalid alphanumeric value.</td>
<td>You entered a value that contains invalid characters for an alphanumeric parameter. Enter a valid alphanumeric value.</td>
</tr>
<tr>
<td>IPPBX service is not available. Try again later.</td>
<td>The IP PBX is not available, or the phone is not registered to the IP PBX. Contact the IP PBX administrator.</td>
</tr>
<tr>
<td>Invalid input.</td>
<td>You entered an invalid value. Verify and try again.</td>
</tr>
<tr>
<td>Invalid server address. Try again.</td>
<td>You entered an invalid provisioning server address. Verify and try again.</td>
</tr>
<tr>
<td>Reboot is required to apply new configuration, would you like to reboot now? Phone will reboot automatically in x seconds.</td>
<td>A change in the phone configuration parameter required the phone to reboot. If you want to delay rebooting the phone, tap No immediately.</td>
</tr>
<tr>
<td>The services application has stopped responding, press Debug to stop rebooting.</td>
<td>See Fatal error issues on page 119.</td>
</tr>
<tr>
<td>Unable to download software image file.</td>
<td>See Software update issues on page 118.</td>
</tr>
<tr>
<td>Invalid signature on software image file.</td>
<td>See Software update issues on page 118.</td>
</tr>
<tr>
<td>Unable to download meta file.</td>
<td>See Software update issues on page 118.</td>
</tr>
<tr>
<td>Invalid software image file.</td>
<td>See Software update issues on page 118.</td>
</tr>
<tr>
<td>Invalid meta file.</td>
<td>See Software update issues on page 118.</td>
</tr>
<tr>
<td>Software update failed. Contact system administrator.</td>
<td>See Software update issues on page 118.</td>
</tr>
<tr>
<td>Invalid IP.</td>
<td>You entered an IP address that does not conform to the IP address format requirement. Enter a valid IP address.</td>
</tr>
<tr>
<td>Invalid IP address. Try again.</td>
<td>You entered an invalid IP address. Verify the address, and enter a valid IP address.</td>
</tr>
<tr>
<td>Invalid domain value.</td>
<td>You entered a domain name that does not conform to the domain name format requirement. Enter a valid domain name.</td>
</tr>
<tr>
<td>Error message</td>
<td>What the administrator should do</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Invalid URL value.</td>
<td>You entered a URL that does not conform to the URL format requirement. Enter a valid URL.</td>
</tr>
<tr>
<td>Failed to connect to server.</td>
<td>The phone cannot connect to the provisioning server. Check network connections.</td>
</tr>
<tr>
<td>Failed to connect to the server due to SSL error.</td>
<td>The phone cannot connect to the HTTPS provisioning server. Check network connections, verify that the provisioning server CA certificate was downloaded to the phone, and confirm that the phone time is current.</td>
</tr>
<tr>
<td>Invalid credentials. Try again.</td>
<td>The phone cannot connect to provisioning server. HTTPS provisioning server. Verify that CA certificate was downloaded to the phone from the HTTPS provisioning server. Check provisioning server credentials. Check that Dolby Conference Phone credentials match the device pool credentials setup on Dolby Conferencing Console.</td>
</tr>
<tr>
<td>Could not find master configurations.</td>
<td>The master configuration files are not on the provisioning server.</td>
</tr>
<tr>
<td>Invalid configurations. Press the &quot;More Options&quot; button for more information.</td>
<td>See Provisioning issues on page 111.</td>
</tr>
<tr>
<td>Provisioning failed. Try again.</td>
<td>There was an error during the first-time provisioning of the phone.</td>
</tr>
<tr>
<td>Server address is required for static provisioning.</td>
<td>If you want to use static provisioning, you must enter a provisioning server IP address.</td>
</tr>
<tr>
<td>Write access not allowed for provisioning.</td>
<td>A .json file on the provisioning server contains a configuration parameter that is not writable to the current .json file on the phone. The parameter is not allowed to be configured from the provisioning server. See Provisioning issues on page 111.</td>
</tr>
<tr>
<td>Failed to get or set configuration.</td>
<td>The configuration files or certificates listed in the master configuration file are not on the provisioning server.</td>
</tr>
<tr>
<td>Not allowed to update provisioned configuration.</td>
<td>There was an attempt to update a configuration parameter that is presently in the configuration file on the provisioning server. Remove these parameters from the configuration files on the provisioning server, and try again.</td>
</tr>
<tr>
<td>Write not allowed for provisioning.</td>
<td>You specified a parameter in the configuration file on the provisioning server that cannot be modified by provisioned interface. Remove the parameter from the configuration file, and try again.</td>
</tr>
<tr>
<td>IEEE 802.1X is unconfigured but challenged.</td>
<td>You have to configure the IEEE 802.1X user identity and password to be able to use the phone on the current network.</td>
</tr>
</tbody>
</table>
### Table 5: Error messages that display on the Dolby Conference Phone (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>What the administrator should do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsupported IEEE 802.1X authentication method required by RADIUS server.</td>
<td>The current network requires an authentication method that is not supported by the phone. To use the phone, you must move it to another network or get the network administrator to change the current authentication method to one that the phone supports. For a list of supported authentication methods, see <a href="#">Configuring 802.1X after out-of-the-box setup</a> on page 66.</td>
</tr>
<tr>
<td>IEEE 802.1X authentication failed due to wrong credentials.</td>
<td>Verify that the correct credential has been provided for 802.1X authentication.</td>
</tr>
<tr>
<td>IEEE 802.1X authentication failed due to certificate validation.</td>
<td>Verify that the correct CA certificate is installed on the phone prior to 802.1X authentication if you are using EAP-PEAP authentication. Verify the installed certificate on the phone through the Dolby Conference Phone web interface. Select <strong>Status &gt; Network &gt; Device</strong> and scroll down to <strong>CA certificates</strong>. If the certificate is successfully installed, you should see the CA certificate for the 802.1X TLS authentication. If the certificate is not present, you must set up the configuration file for the phone to download the CA certificate. See <a href="#">Adding certificate authority certificates</a> on page 36.</td>
</tr>
<tr>
<td>ERROR: Certificate &lt;certificate fingerprint&gt; is expired: ddd mmm dd hh:mm:ss yyyy&gt;</td>
<td>This message displays on the CA certificate status screen only. This certificate has expired and needs to be replaced on the phone. Contact the issuer (for example, Dolby or your conferencing service provider) for a new certificate.</td>
</tr>
<tr>
<td>WARNING: Certificate &lt;certificate fingerprint&gt; will expire soon: ddd mmmdd hh:mm:ss yyyy&gt;</td>
<td>This message displays on the CA certificate status screen only. This certificate will expire within the next seven days. Contact the issuer (for example, Dolby or your conferencing service provider) for a new certificate.</td>
</tr>
<tr>
<td>Unsupported authentication method.</td>
<td>An unsupported 802.1X authentication method was used in the configuration files. Change it to a supported method, and reboot the phone.</td>
</tr>
<tr>
<td>Failed to download PAC file.</td>
<td>The PAC file did not download. The administrator needs to check and, if necessary, correct the URL for downloading the PAC file; confirm that the phone can reach that URL; and then download the PAC file.</td>
</tr>
<tr>
<td>Invalid PAC file.</td>
<td>The downloaded PAC file is invalid.</td>
</tr>
<tr>
<td>PAC syntax error.</td>
<td>The PAC file has syntax errors and cannot be processed. Correct the errors and try again.</td>
</tr>
<tr>
<td>PAC file too large.</td>
<td>The PAC file size is greater than 64 kB. This is the maximum supported size.</td>
</tr>
<tr>
<td>Unresolvable hostname error</td>
<td>The proxy server host name is not resolvable. Verify the server name in the PAC file.</td>
</tr>
<tr>
<td>Unreachable error</td>
<td>The proxy server is unreachable. Verify the server name in the PAC file. Verify that the proxy server is online.</td>
</tr>
</tbody>
</table>
Table 5: Error messages that display on the Dolby Conference Phone (continued)

<table>
<thead>
<tr>
<th>Error message</th>
<th>What the administrator should do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication error</td>
<td>Proxy authentication failed. Verify the user name and/or password for the proxy server.</td>
</tr>
<tr>
<td>Passcode is not supported by the service.</td>
<td>The user entered an invalid passcode. Verify the passcode, and ask them to try again.</td>
</tr>
<tr>
<td>Higher logging level is enabled. Performance might be impacted due to excessive logging. Contact administrator to reset.</td>
<td>Reset logging level. See Parameters for changing the log level on page 76.</td>
</tr>
<tr>
<td>DHCP lease is not obtained on secondary VLAN.</td>
<td>Check whether the secondary VLAN ID is configured properly. If so, check whether the DHCP server is online on the secondary VLAN.</td>
</tr>
<tr>
<td>IP address conflict is detected on secondary VLAN.</td>
<td>As only DHCP is supported on secondary VLAN, this is unlikely to happen. When it does happen, check the DHCP server logs to find out where the source of the conflict is.</td>
</tr>
<tr>
<td>Secondary VLAN failed.</td>
<td>General error.</td>
</tr>
<tr>
<td>Secondary VLAN is shadowed by primary.</td>
<td>Even though the secondary VLAN is enabled, it is the same as the primary VLAN. Informational error only.</td>
</tr>
<tr>
<td>Default gateway is unreachable on secondary VLAN.</td>
<td>As only DHCP is supported on the secondary VLAN, this is unlikely to happen. When it does happen, check if the assigned default gateway is online.</td>
</tr>
<tr>
<td>Not allowed to update provisioned configuration.</td>
<td>You attempted to make a local configuration change to a parameter that is provisioned, where local means either on the web user interface or through a shell command. The phone user interface disables entry of the provisioned parameters, so you can view the value but not make a change.</td>
</tr>
<tr>
<td>Invalid PBX codec list.</td>
<td>You entered an invalid IP PBX codec list as the last entry in the table.</td>
</tr>
<tr>
<td>Invalid domain.</td>
<td>You entered an invalid SIP domain name.</td>
</tr>
<tr>
<td>Invalid URL.</td>
<td>You entered an invalid URL.</td>
</tr>
<tr>
<td>Duplicate parameter.</td>
<td>The provisioned configuration file contains multiple instances of the same parameter. Remove the duplication, and try again.</td>
</tr>
</tbody>
</table>

9.2 Viewing the Status menu

Debugging of a single phone may be possible by examining the phone status menu.

Procedure

1. Tap the settings button on the home screen.

2. Tap the advanced settings button and then choose About > Status to view the Status menu:
3. Scroll to one of the **Status** menu items, and tap the desired item.

If 📱 is displayed on the home screen and you tap it, you’re taken directly to the **Status** menu.

**Results**

In the **Status** menu, you can view your phone communication status with external systems.

Status icons ✅ and ⚪️ display for following:

- DHCP server
- Provisioning server
- Call server
- Directory server
- Conferencing registration
- Network time synchronization
- IP network
- Secondary VLAN
- CA certificates
- Log file upload
- Logging impact
- Reboot required
- Dolby Satellite Microphones
- Bluetooth Module
- Phone software update (if an error occurred when downloading the image or the user ignored the request)

This figure shows good communications with all external systems.

If any communications have failed, they are marked as ⚪️ and a message directing the user to contact the system administrator appears at the top of the Status list screen (shown in the previous figure).
9.3 Log files

The Dolby Conference Phone will log various events to files stored in the flash file system and will periodically upload these log files to the provisioning server.

The files are stored on the phone. The maximum log file size is 2 MB. You can also configure a phone to send log messages to a syslog server. Using a syslog server allows for better centralized management.

There can be up to two log files for the Dolby Voice software.

You can download the logs from the phone by using the Dolby Conference Phone web interface. From the web interface home page, select Tools > Utilities from the Navigation menu and click the log file link.

If you want the log files written to the provisioning server, you need to enable logging, Logging.Upload.Enable, and provide a location for the log files, Provisioning.Server.UploadDir. The provisioning server directory for the log files to be uploaded to must exist.

You can provide a location as follows:

- `/logs`: The log files will be uploaded to the provisioning server logs directory. If the provisioning server is set to `ftp://10.12.122.124`, the upload path will be `ftp://10.12.122.124/logs`.
- `/logs/[MAC]` or `/logs/[SN]`: The log files will be uploaded to the provisioning server logs/[MAC] or logs/[SN] directory. Each phone will upload its logs to a separate folder. For example, a phone with serial number D0230030 will upload its logs to `../logs/d0230030`.

When a phone uploads its log files, they are saved on the provisioning server with the serial number of the phone prepended to the file name. By default, log files are uploaded every five minutes, but you can change the interval through Logging.Upload.Interval. For example, D0025436-messages and D0025436-messages.0 are uploaded to the provisioning server every five minutes. Log messages are written to the files in a cyclic manner: messages, then rename messages to messages.0, and then back to messages.

The amount of logging that the phone performs can be tuned for the application to provide more or less detail on specific components of the phone software. For example, if you are troubleshooting a SIP signaling issue, you are not likely interested in DSP events. Logging levels are adjusted in the configuration files or through the Dolby Conference Phone web interface. You should not modify the default logging levels unless directed to by Dolby Customer Support. Inappropriate logging levels can cause performance issues on the phone.
For more information on logging parameters, see Parameters for changing the log level on page 76.

Check the Status menu to see whether or not the log file upload to the provisioning server was successful (see Viewing the Status menu on page 73).

Related information
Accessing the Dolby Conference Phone web interface on page 78

9.3.1 Parameters for changing the log level
Each of the components of the Dolby Voice software is capable of logging events of different severity. This allows you to capture low-severity events in one part of the application, and high-severity events for other components.

A full description of all log-level parameters can be found in the file dvcp-rel-x.y.z.buildID.cfg-help.html. They are Logging.Level.module_name, where module_name can be ACME, Api, Auth, BLE, CallLog, Ccapi, Cdsp, Cfg, DCC, DCS, Dev, DVTSC, Evs, Ldp, Net, Pvs, Security, Shl, Sip, UI, Upd, or Web.

The range of log levels, in order of detail and verbosity from lowest to highest, includes NONE, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFO, DEBUG, and DEBUG1. (DEBUG1 contains maximum verbose trace information.) By default, all Logging.Level.module_name parameters are set to INFO.

Note: When testing or troubleshooting is complete, remember to return the log configuration parameter to its default value in the configuration file.

9.3.2 Log levels
The priority level of the log files is referred to as log levels.

In the log files, messages can be one of these (in order of highest to lowest verbosity):

- **debug**: Indicates verbose traces generated only when log level is set to DEBUG
- **info**: Indicates normal phone behavior
- **notice**: Indicates minor issues or failures, but could be normal behavior
- **warn**: Indicates that an error may occur if action is not taken
- **err**: Indicates that a failure or loss of functionality occurred
- **crit**: Indicates that an unrecoverable failure of a semi-important component occurred
- **alert**: Indicates that an unrecoverable failure of an important component occurred
- **emerg**: Indicates that a complete unrecoverable system failure occurred

The warn, err, crit, alert, and emerg messages indicate problems of increasing severity.

9.3.3 About syslog logging
syslog is a standard for forwarding log messages in an IP network.

The term syslog is often used both for the actual syslog protocol and for the application or library sending syslog messages. The syslog messages contain much of the same information as the Dolby Conference Phone logs, with the exception of the events during the
early stage of the phone initialization (as the device is not yet configured to send syslog messages).

The syslog protocol is simple: the syslog sender sends a small textual message (less than 1,024 bytes) to the syslog receiver. The receiver is commonly called syslogd, syslog daemon, or syslog server. Syslog messages can be sent through UDP, TCP, or TLS. The data is sent in clear text.

Because syslog is supported by a wide variety of devices and receivers, syslog can be used to integrate log data from many different types of systems into a central repository.

By default, syslog is disabled. (Logging.RemoteSysLog.Enable is false.) To use syslog, you must set the syslog server address (Logging.RemoteSysLog.Address). Messages relating to developer logs and intermodule communication are sent to the DEBUG level. Messages pertaining to user action (if logged) and module initialization (if any) are available in the INFO level. Error and warning messages are logged in ERROR and WARNING, respectively.

For more information on the syslog protocol, see RFC 3164.

Related information

Configuration parameters on page 33

9.3.4 Audio logging

For the audio module of the Dolby Conference Phone software, you can enable logging through configuration files or the Dolby Conference Phone web interface.

You can log these audio characteristics:

- Echo reference input
- Echo reference output
- Jitter buffer input
- Jitter buffer output

A full description of all audio logging configuration parameters can be found in the file dvcp-rel-x.y.z.buildID.cfg-help.html.

By default, all audio logging is disabled. If you want the audio log files written to the provisioning server, you need to set the audio logging mode, Logging.Audio.Mode. The supported modes are Disabled, Statistics, and Diagnostics.

If the audio logging mode is set to Statistics or Diagnostics:

- A call statistics log containing per-second statistical information (including jitter buffer and packet loss) is uploaded to the provisioning server. For example, the file D0025454-call_stats_b502bb32-2bddd-49da-8ae7-0d89ff295a01.json is uploaded from the device numbered D0025454.
- An audio dump of preprocessing statistics that contains metadata about the preprocessing algorithm is uploaded to the provisioning server. For example, the file D0025454-vsV_stats_20140529163458.bin is uploaded from the device numbered D0025454.

If the audio logging mode is set to Diagnostics, the recorded diagnostic data is uploaded to the provisioning server. For example, the file D0025454-audiolog_20140529141935.gz is uploaded from the device numbered D0025454. In this audio logging mode, a diagnostics icon displays during calls in the top-right corner of the screen. If users have any issues in any call, they should tap the icon and select an issue from the displayed list.
Note: The Statistics audio logging mode may impact the end of a call (when data is uploaded to the provisioning server). The Diagnostics audio logging mode impacts the entire call, adding approximately 10–15% overhead.

9.4 Accessing the Dolby Conference Phone web interface

The Dolby Conference Phone settings can be changed using the web interface in addition to using the provisioning server and phone user interface. Any configuration changes made to individual phones using the web interface will override configuration settings made with the provisioning server, and changes made manually using a phone user interface will override changes made using the web interface.

About this task

You can access the Dolby Conference Phone web interface using any of these web browsers:

- Microsoft Internet Explorer 10.0.x or later on Windows-based computers (backward compatibility not supported)
- Mozilla Firefox 26.0.x or later
- Google Chrome 31.0.x or later
- Apple Safari 7.0.2.x or later on Apple-based computers

Note: The Dolby Conference Phone web interface has been optimized for modern browsers, and the best experience will be obtained using one of the supported browsers. Versions 8 and 9 of Internet Explorer will work in a degraded fashion; support for these browsers is deprecated and will be removed in a future release.

By default, access to the web interface is enabled. You can disable access only through the configuration files by changing `Network.Services.WebServerMode`.

You can view the configuration parameter descriptions (`dvcp-rel-x.y.z.buildID/cli-help.html`) and the diagnostic shell command descriptions (`dvcp-rel-x.y.z.buildID/cfg-help.html`) through the web interface. Go to Tools > Help.

You can access the web interface by entering the phone Internet Protocol address into the address bar of an Internet browser. Then you will be prompted to enter the administrative user name and password. The administrative user name is `admin` and the default administrative password is 1739.

Note: We recommend that you change the default administrative password.

Procedure

1. Open one of the supported web browsers.
2. Get the phone IP address.
   From the home screen, tap 🎉 > ⬤ > About > General and scroll down until you see the IP address.
3. Enter `https://your phone IP address` in the browser address bar (as shown in this figure).
Figure 4: Phone Internet Protocol in the address bar of an Internet browser

A web page similar to the one shown in this figure displays.

Figure 5: Dolby Conference Phone log-in page

4. Log in as the administrator. (Default values are admin and 1739.)

A web page similar to the one shown in this figure displays.

Figure 6: Dolby Conference Phone web interface main page

This page provides you with specific information about the phone you logged into.

Contextual help on other pages of the web interface provides you with instructions on how to navigate the menus and detailed explanations of the current configuration of the phone.

You can change the phone settings from the Settings tab. You can view the phone status from the Status tab, where you will see these icons:

- Functioning normally
- Requires attention
Not applicable

The warning icon displays on the web interface as shown in this figure.

You can perform other tasks—such as exporting the configuration files, rebooting the phone, and viewing the log and help files—from the Tools tab.

You can view the details of CA certificates stored on the phone through the Dolby Conference Phone web interface. Select Status > Network > Device, and scroll down to CA Certificates.

Related information
Changing the administrative password on page 43
Configuration parameters on page 33

9.5 Exporting the Dolby Conference Phone configuration

You can export the files that represent the Dolby Conference Phone configuration by using the Dolby Conference Phone web interface.

About this task
This is primarily a tool to help you create multiple configuration files.

To export the current phone configuration:

Procedure

1. From the web interface home page, select Tools > Export from the navigation menu.

   A web page similar to the one shown in this figure displays.
• (Optional) Enter the fully qualified phone software image URL. For example, dvcp-dev-2.2.0.123.tar.gz or http://10.203.131.56/something/dvcp-dev-2.2.0.38.tar.gz.

• (Optional) Enter the certificate URLs separated by commas. For example, cert.pem, ldap.pem.

2. Click Generate JSON files.
   The three configuration files are displayed and validated (as JSON).

3. Click Download for each file.
   The files are downloaded to the default download directory on your computer.
   (Depending on your browser settings, you may be prompted to keep the first file.)

4. Copy these files to the appropriate location on your provisioning server, and modify them with a JSON editor.

Related information
Accessing the Dolby Conference Phone web interface on page 78

### 9.6 Rebooting the Dolby Conference Phone

You can reboot the Dolby Conference Phone by using either the Dolby Conference Phone web interface or the phone user interface.

About this task
Rebooting with the web interface is useful if the phone is in a different office or at a remote location.

To reboot the phone from the Dolby Conference Phone user interface:

Procedure
1. Tap this sequence:
Reboot Phone

2. Tap the confirmation button.

9.7 Call and media statistics

Through the Dolby Conference Phone web interface, you can view call statistics for active calls and recently active calls.

To view call statistics: From the web interface home page, select **Status > Call Statistics** from the navigation menu on the left-hand side of the web page.

The call statistics web page shows:

- Call information
- Calling party first and last name
- Calling party address (phone extension)
- Call duration in minutes and seconds
- Type of call (IP PBX or conferencing service provider)
- Call status (active or on hold)
- Audio codec type
- Network statistics
  - Packet count
  - Average jitter
  - Packet loss rate
  - Packet loss burstiness (rate of audio packet losses occurring in a burst)
  - Concealed packet count
  - Jitter histogram
- Audio diagnostics
  - Average automatic gain control gain
  - Voice capture level
  - Voice rendering level
  - Signal-to-noise level
  - Signal-to-echo level
  - Average round-trip time (RTT)
  - Signal-to-noise level too low
  - Signal-to-echo level too low
  - Low input power detected
  - Microphone input clipping
9.8 Viewing diagnostics

You can view diagnostic information from the Diagnostics menu on your phone.

Procedure

1. Tap this sequence:

   ![Sequence Image]

   > Diagnostics > Test Hardware

2. Select one of these menu items to perform a hardware diagnostic test:

   - **LED diagnostics**: Test the LED halo on the phone.
   - **Key diagnostics**: Press the three keys, one by one.
   - **Touch screen diagnostics**: Test the touch screen response area.
   - **Microphone diagnostics**: Test the phone microphones. If satellite microphones are connected, they are also testable.
   - **Speaker diagnostics**: Test the speakers.

What to do next

As part of the diagnostics tools on the phone, pinging can be used to troubleshoot network connectivity issues. You can run pings through the diagnostic shell.

9.9 Diagnostic shell

The diagnostic shell provides a command-line interface for you to query the phone state, run diagnostics, and configure selected parameters. The shell service has a client component and a server component.

The shell service is accessed via SSH. Only one instance of the shell service is supported at any given time. Once a connection to the shell service is established, subsequent requests will be denied until the current session is terminated. The session will time out after 30 minutes of inactivity. The service starts when the phone boots up, but it is accessible only if the configuration parameter—Network.Services.SSHEnabled—is enabled, which is the default. You must enter the administrative user name and password to use the diagnostic shell. Shell service commands are automatically generated for each phone software release. They can include localized command help, function calls, and diagnostic tests.

A list of commands is provided with each phone software build, in the file dvcp-rel-x.y.z.buildID.cli-help.html.
Figure 7: Diagnostic shell command sample

Note: Use the <Tab> key on the command line to prompt for additional command information. For example, if you enter system and then press <Tab>, the possible system commands are listed and the command is repeated on the command line for you to finish command entry. If you enter system traceroute, and press <Tab>, the format of the parameter IP address of the host displays, and the command is repeated on the command line for you to enter the IP address. Do not use <Tab> to complete the shell or quit commands.

9.10 Bluetooth LE initialization and advertisement

The Bluetooth LE module is a hardware component attached to the motherboard of the phone. If this component is faulty or does not initialize, then phone cannot transmit a Bluetooth LE advertisement.

Related information
Disabling Bluetooth advertisement on page 49

9.10.1 Confirming Bluetooth LE initialization

You can confirm that the Bluetooth LE hardware is initialized from the phone user interface.

About this task

If the Bluetooth LE module fails to initialize, a red status alarm ![exclamation mark] displays from the phone user interface and phone web interface.

When the phone boots, it attempts to initialize the Bluetooth LE module (up to ten times). If initialization fails, each attempt is recorded in the syslog with this warning:

**Bluetooth module initialization failed. Retrying...**
If all initialization attempts fail, the phone records this warning in the syslog and quits Bluetooth LE module initialization:

**Unable to initialize module. Quit application.**

**Procedure**

1. From the phone user interface, tap this sequence:
   
   ![Image](image1)

2. Scroll down, and then tap **Bluetooth**.
   
   A green ![Green](image2) or red ![Red](image3) status icon indicates the status of this feature.

### 9.10.2 Confirming Bluetooth LE advertisement

You can confirm whether the phone is advertising a Bluetooth LE signal. However, be aware that the phone only advertises Bluetooth LE under certain circumstances. Lack of Bluetooth LE advertisement is only a problem if your conferencing application allows the phone to advertise Bluetooth LE and it is not.

**About this task**

In order for the phone to advertise a Bluetooth LE signal, these criteria must be met:

- The Bluetooth LE hardware module on the phone is working and initialized.
- You have configured the Bluetooth LE advertisement as described in **Disabling Bluetooth advertisement** on page 49.
- The conferencing application on the phone allows and has turned on Bluetooth LE advertisement.
  
  If allowed by your conferencing service provider, the conferencing application allows the phone to advertise Bluetooth LE.

The `Dvms.Service.EnableBluetoothAdvertisement` parameter described in **Disabling Bluetooth advertisement** on page 49 controls whether the phone can advertise Bluetooth LE. However, the conferencing application controls whether the phone does or does not advertise Bluetooth LE.

**Procedure**

1. From the phone user interface, tap this sequence:
   
   ![Image](image4)

2. Scroll down to **Bluetooth**, and confirm that the status is green.
   
   a) If the status is green, tap **Bluetooth** and check the status of **Bluetooth advertisement**.
      
      ![Green](image5)

      If the phone is advertising, the status is **Active**. If it is not, it is **Inactive**.

   b) If the status is red, Bluetooth LE module initialization failed (see **Confirming initialization** on page 84) and advertisement does not work.

   ![Red](image6)

**Related information**

**Disabling Bluetooth advertisement** on page 49
9.11 Collection of usage data

The Dolby Conference Phone can collect and report a variety of data to your conferencing service provider’s provisioning service or your on-premise instance of the Dolby Conferencing Console. If you are using your conferencing service provider’s provisioning service, you may wish to protect yourself by blocking the collection of usage data.

If you perform Plug-and-Play Setup, this screen appears in the setup wizard.

If you choose No, Privacy block is enabled. The phone cannot share data with your conferencing service provider’s provisioning service.

If you choose Yes, the phone shares data with your conferencing service provider’s provisioning service. This includes diagnostics reports, core dump records, call detail records, log files, and screenshots of the phone user interface.

Related information

Setting up the phone using Plug-and-Play Setup on page 51

9.11.1 Enabling Privacy block

If you change your mind about using Privacy block, you can enable or disable it at any time from the phone user interface, phone web interface, or command-line interface. The name of the configuration parameter that controls this feature is Provisioning.Server.PrivacyBlock.

About this task

Privacy block is not a provisionable feature. You must enable or disabled it one phone at a time.

Procedure

1. From the phone web interface:
   a) From the Settings tab, expand the Provisioning section.
   b) Expand the Server section.
   c) Turn on Disable Privacy-related Uploads.
      The Provisioning.Server.PrivacyBlock configuration parameter is now true. The phone cannot share data with your conferencing service provider’s provisioning service.

2. Alternatively, from the phone user interface:
   a) Tap this sequence:
b) Enter the administrator password.
   The default administrator password is 1739.

c) Tap **Network configuration > Provisioning Server**.

d) Scroll down to **Privacy block**.

![Privacy block]

The **Provisioning.Server.PrivacyBlock** configuration parameter is now true. The phone cannot share data with your conferencing service provider’s provisioning service.

### 9.12 Phone memory resources

The Dolby Conference Phone is designed to operate in a variety of office environments and deployments.

New phone software releases may add new features that require varying amounts of phone memory resources. To ensure that the phone and its configured features operate easily, you will need to check that the phone has adequate available memory from time to time.

When the phone resources start to run low, you may notice that the phone reboots or freezes.

You can check the available memory on the phone by running the command `show memory` through the diagnostic shell, by viewing the log file, or by accessing the Dolby Conference Phone web interface. Typically, you want the phone to be using less than 95% of its available memory.

If you find that it is using more than 95%, you can reduce this amount by following these steps:

- Check how the corporate directory (LDAP) is set up, and make possible configuration parameter changes.
- Return the log configuration parameters to the default values when you are finished testing or troubleshooting issues.

The phone logs the current memory usage every hour as part of the syslog files, which can be accessed via Dolby Conferencing Console or the Dolby Conference Phone web interface. If the overall memory usage is 75 MB or higher, the logging level will change from info to warning. The logging level can be accessed on the web interface under **Settings > Logging > Level**, or on Dolby Conferencing Console.

The Boolean configuration variable **Logging.ReportFreeMemory** can be set to True through the Dolby shell so that the log will include free memory on every log entry.

**Related information**

- [Accessing the Dolby Conference Phone web interface](#) on page 78
- [Diagnostic shell](#) on page 83
- [Using a corporate directory](#) on page 43
- [Log files](#) on page 75
### 9.13 Resetting to factory defaults

Resetting the phone to factory defaults clears the user data—such as the recent calls list and contact directory—and removes log files and cached data.

**Procedure**

1. You can perform the reset in several ways:

<table>
<thead>
<tr>
<th>Method</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Through the phone user interface</td>
<td>From the home screen, tap ☰️ &gt; ⭕️, and then <strong>Administrative Settings &gt; Factory reset</strong>. Enter the administrative password—by default, it is 1739—when prompted.</td>
</tr>
<tr>
<td>Through the diagnostic shell command</td>
<td>Enter the factory reset command, <code>system factoryReset</code>.</td>
</tr>
<tr>
<td>Through the Dolby Conference Phone web interface</td>
<td>Go to <strong>Tools &gt; Utilities</strong> and click the factory reset link.</td>
</tr>
<tr>
<td>Through the multiple key combination when the home screen displays</td>
<td>Press the mute and volume-down buttons simultaneously for 10 seconds.</td>
</tr>
<tr>
<td>Through the multiple key combination when the phone reboots</td>
<td>Press the mute and volume-down keys simultaneously for five seconds. The LED turns green, and then turns yellow to show the phone is reset to factory default.</td>
</tr>
</tbody>
</table>

2. You will be asked to confirm the reset in all cases.

**Results**

If you confirm the option, the phone reboots to complete the reset process even if a call is active.

### 9.14 LLDP and supported type-length values

The LLDP is a vendor-neutral Layer 2 protocol that allows a network device to advertise its identity and capabilities on the local network.

The protocol was updated by [IEEE standard 802.1AB](https://standards.ieee.org) in September 2009.

The LLDP feature supports VLAN and QoS discovery, and LLDP power management, but not power negotiation. LLDP has a higher priority than DHCP VLAN discovery.

These mandatory type-length values are supported:

- **Chassis ID**: Must be first type-length value
- **Port ID**: Must be second type-length value
- **Time to live**: Must be third type-length value, set to 120 seconds
- **System capabilities**: Set as telephone capability
- **MAC/PHY configuration status**: Detects duplex mismatch
- **LLDP-MED capabilities**: 1
- **LLDP-MED network policy**: VLAN, L2 QoS, L3 QoS
• LLDP-MED extended power via MDI type-length value: Power type, power source, power priority, power value

• End of LLDP DU: Must be last type-length value

The following optional type-length values are supported:

• Port description

• System name: Administrator-assigned name

• System description: Includes device type, phone number, hardware version, and Dolby Conference Phone software version

• Management address: Used for network discovery

An LLDP frame must contain all mandatory type-length values. The frame will be recognized as LLDP only if it contains mandatory type-length values. The Dolby Conference Phone supports LLDP frames with both mandatory and optional type-length values.

All outbound LLDP packets are sent to multicast MAC address 01:80:c2:00:00:0e.

Related information

Supported type-length values on page 89

9.14.1 Supported type-length values

The Dolby Conference Phone uses an LLDP frame and type-length values to determine the phone identity, its capabilities, and organizations to which the phone belongs.

The basic type-length value format is as follows:

• Type-length value type (7 bits) [06]

• Type-length value length (9 bits) [7–15]

• Type-length value information (0–511 bytes)

Each type-length value appears only once, except for the network policy type-length value, which may appear twice. The order of the four type-length values (chassis ID, port ID, time to live, and end of LLDP DU) are fixed; the others may appear in any order.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type (7 bits)</th>
<th>Length (9 bits)</th>
<th>Org. code (3 bytes)</th>
<th>Sub type</th>
<th>Value (sample)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID</td>
<td>1</td>
<td>7</td>
<td>-</td>
<td>4: MAC address</td>
<td>(00:d0:46:00:01:9f)</td>
</tr>
<tr>
<td>Port ID</td>
<td>2</td>
<td>7</td>
<td>-</td>
<td>3: MAC address</td>
<td>(00:d0:46:00:01:9f)</td>
</tr>
<tr>
<td>Time to live</td>
<td>3</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>120 seconds *</td>
</tr>
<tr>
<td>Port description</td>
<td>4</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>eth0</td>
</tr>
<tr>
<td>System name</td>
<td>5</td>
<td>0 to 255</td>
<td>-</td>
<td>-</td>
<td>(DVCP-D0020473)</td>
</tr>
<tr>
<td>System description</td>
<td>6</td>
<td>0 to 255</td>
<td>-</td>
<td>-</td>
<td>(SN:D00XXXXXX/R evX/SW:X.X.X.X)</td>
</tr>
<tr>
<td>Name</td>
<td>Type (7 bits)</td>
<td>Length (9 bits)</td>
<td>Org. code (3 bytes)</td>
<td>Sub type</td>
<td>Value (sample)</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>---------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System capabilities</td>
<td>7</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>• Other: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Repeater: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Bridge: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• WLAN access point: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Router: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Telephone: Capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• DOCSIS cable device: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Station only: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• C_VLAN component of a VLAN bridge: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• S_VLAN component of a VLAN bridge: Not capable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Two-port MAC relay: Not capable</td>
</tr>
<tr>
<td>Management address</td>
<td>8</td>
<td>12</td>
<td>-</td>
<td>-</td>
<td>• Address string length: 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Address subtype: IPv4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Management address: (example) 10.203.188.92</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Interface subtype: ifIndex</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Interface number: X</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• OID string length: 0</td>
</tr>
<tr>
<td>Organizationally specific</td>
<td>127</td>
<td>9</td>
<td>0x00120fc v: IEEE 802.3</td>
<td>1: MAC/PHY configuration status</td>
<td>• Auto negotiation support: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Auto negotiation status: 0 or 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Auto negotiation advertised capability: Asymmetric and symmetric PAUSE: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Symmetric PAUSE: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Asymmetric PAUSE: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• PAUSE: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 100Base-TX full duplex: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 100Base-TX half duplex: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 10BASE-T full duplex: 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 10BASE-T half duplex: 1</td>
</tr>
<tr>
<td>Name</td>
<td>Type (7 bits)</td>
<td>Length (9 bits)</td>
<td>Org. code (3 bytes)</td>
<td>Sub type</td>
<td>Value (sample)</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>--------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Organizationally specific | 127          | 7              | 0x00120 bb: TR-41  | 1: Media capabilities | • LLDP-MED capabilities: 1  
• Network policy: 1  
• Location identification: 0  
• Extended power via MDI-PSE: 0  
• Extended power via MDI-PD: 1  
• Inventory: 0 |
| Organizationally specific | 127          | 8              | 0x00120 bb: TR-41  | 2: Network policy | • Application type: Voice or voice signaling  
• Unknown policy flag: 0 or 1  
• Tagged flag: 0 or 1  
• VLAN ID: 0 to 4094  
• Link layer priority: 0 to 7  
• DSCP: 0 to 63 |
| Organizationally specific | 127          | 7              | 0x00120 bb: TR-41  | 4: Extended power via MDI | • Power type: PD device  
• Power source: PSE  
• Power priority: Unknown  
• Power value: 13 watts† |

End of LLDP DU 0 0 - - -

* Time to live value is 0 seconds when the phone is powered on.
† The Dolby Conference Phone is a class 3 device that has a maximum power consumption of 12.95 watts.

### 9.15 Trusted certificates and issuers

The Dolby Conference Phone trusts the certificates listed here.

<table>
<thead>
<tr>
<th>Certificate name</th>
<th>Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.lobby.pp.icong.net</td>
<td>Entrust Certification Authority - L1K</td>
</tr>
<tr>
<td>AddTrust External CA Root</td>
<td>AddTrust External CA Root</td>
</tr>
<tr>
<td>Amazon</td>
<td>Amazon Root CA 1</td>
</tr>
<tr>
<td>Amazon Root CA 1</td>
<td>Starfield Services Root Certificate Authority - G2</td>
</tr>
<tr>
<td>Baltimore CyberTrust Root</td>
<td>Baltimore CyberTrust Root</td>
</tr>
<tr>
<td>Baltimore CyberTrust Root</td>
<td>Baltimore CyberTrust Root</td>
</tr>
<tr>
<td>C=US/O=Digital Signature Trust Co./OU=DST (ANX Network) CA</td>
<td>Digital Signature Trust Company</td>
</tr>
<tr>
<td>C=US/O=Digital Signature Trust Co./OU=DSTCA E1</td>
<td>Digital Signature Trust Company</td>
</tr>
<tr>
<td>C=US/O=Digital Signature Trust Co./OU=DSTCA E2</td>
<td>Digital Signature Trust Company</td>
</tr>
<tr>
<td>Certificate name</td>
<td>Issuer</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>C=US/O=Digital Signature Trust Co./OU=DST-Entrust GTI CA</td>
<td>Digital Signature Trust Company</td>
</tr>
<tr>
<td>C=US/O=Equifax/O=Equifax Secure Certificate Authority</td>
<td>Equifax Secure Certificate Authority</td>
</tr>
<tr>
<td>C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority</td>
<td>ValiCert</td>
</tr>
<tr>
<td>C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority</td>
<td>The Go Daddy Group, Inc.</td>
</tr>
<tr>
<td>C=US/O=VeriSign, Inc./OU=Class 2 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network</td>
<td>VeriSign, Inc.</td>
</tr>
<tr>
<td>C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network</td>
<td>VeriSign, Inc.</td>
</tr>
<tr>
<td>Class 2 Primary CA</td>
<td>Class 2 Primary CA</td>
</tr>
<tr>
<td>Cybertrust Public SureServer SV CA</td>
<td>Baltimore CyberTrust Root</td>
</tr>
<tr>
<td>Deutsche Telekom Root CA 2</td>
<td>Deutsche Telekom Root CA 2</td>
</tr>
<tr>
<td>DigiCert Assured ID Root CA</td>
<td>DigiCert Assured ID Root CA</td>
</tr>
<tr>
<td>DigiCert Assured ID Root G2</td>
<td>DigiCert Assured ID Root G2</td>
</tr>
<tr>
<td>DigiCert Assured ID Root G3</td>
<td>DigiCert Assured ID Root G3</td>
</tr>
<tr>
<td>DigiCert Global Root CA</td>
<td>DigiCert Global Root CA</td>
</tr>
<tr>
<td>DigiCert Global Root G2</td>
<td>DigiCert Global Root G2</td>
</tr>
<tr>
<td>DigiCert Global Root G3</td>
<td>DigiCert Global Root G3</td>
</tr>
<tr>
<td>DigiCert High Assurance EV Root CA</td>
<td>DigiCert High Assurance EV Root CA</td>
</tr>
<tr>
<td>DigiCert Trusted Root G4</td>
<td>DigiCert Trusted Root G4</td>
</tr>
<tr>
<td>Entrust.net Certification Authority (2048)</td>
<td>Entrust.net Certification Authority (2048)</td>
</tr>
<tr>
<td>Entrust.net Certification Authority (2048)</td>
<td>Entrust.net Certification Authority (2048)</td>
</tr>
<tr>
<td>Entrust Root Certification Authority</td>
<td>Entrust Root Certification Authority</td>
</tr>
<tr>
<td>Entrust Root Certification Authority - G2</td>
<td>Entrust Root Certification Authority - G2</td>
</tr>
<tr>
<td>GeoTrust Global CA</td>
<td>GeoTrust Global CA</td>
</tr>
<tr>
<td>GeoTrust Global CA 2</td>
<td>GeoTrust Global CA 2</td>
</tr>
<tr>
<td>GeoTrust Primary Certification Authority</td>
<td>GeoTrust Primary Certification Authority</td>
</tr>
<tr>
<td>GeoTrust Primary Certification Authority - G3</td>
<td>GeoTrust Primary Certification Authority - G3</td>
</tr>
<tr>
<td>GeoTrust Universal CA</td>
<td>GeoTrust Universal CA</td>
</tr>
<tr>
<td>GeoTrust Universal CA 2</td>
<td>GeoTrust Universal CA 2</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>GlobalSign</td>
</tr>
<tr>
<td>GlobalSign Root CA</td>
<td>GlobalSign Root CA</td>
</tr>
<tr>
<td>Go Daddy Root Certificate Authority - G2</td>
<td>Go Daddy Root Certificate Authority - G2</td>
</tr>
<tr>
<td>Go Daddy Root Certificate Authority - G2</td>
<td>Go Daddy Root Certificate Authority - G2</td>
</tr>
<tr>
<td><a href="http://www.valicert.com/">http://www.valicert.com/</a> emailAddress=<a href="mailto:info@valicert.com">info@valicert.com</a></td>
<td><a href="http://www.valicert.com/">http://www.valicert.com/</a> emailAddress=<a href="mailto:info@valicert.com">info@valicert.com</a></td>
</tr>
<tr>
<td>lync-DOLBYVOICE2-CA</td>
<td>lync-DOLBYVOICE2-CA</td>
</tr>
</tbody>
</table>
## 9.15.1 TLS cipher suites

The Dolby Conference Phone offers a predefined list of cipher suites. This list cannot be changed at this time.

**Note:** The current SRTP implementation supports the **AES_CM_128_HMAC_SHA1_80** and **AES_CM_128_HMAC_SHA1_32** cipher suites. It does not support the **F8_128_HMAC_SHA1_8** cipher suite.

### Table 6: TLS cipher suites

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Cipher suites</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x000a</td>
<td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0x000d</td>
<td>TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0x0010</td>
<td>TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0x0016</td>
<td>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0x002f</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0x0030</td>
<td>TLS_DH_DSS_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0x0031</td>
<td>TLS_DH_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0x0033</td>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0x0035</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0x0036</td>
<td>TLS_DH_DSS_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0x0037</td>
<td>TLS_DH_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0x0039</td>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0x003c</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>Cipher</td>
<td>Cipher suites</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>0x003d</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA256</td>
</tr>
<tr>
<td>0x003e</td>
<td>TLS_DH_DSS_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>0x003f</td>
<td>TLS_DH_RSA_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>0x0041</td>
<td>TLS_RSA_WITH_CAMELLIA_128_CBC_SHA</td>
</tr>
<tr>
<td>0x0042</td>
<td>TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA</td>
</tr>
<tr>
<td>0x0043</td>
<td>TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA</td>
</tr>
<tr>
<td>0x0045</td>
<td>TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA</td>
</tr>
<tr>
<td>0x0067</td>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>0x0068</td>
<td>TLS_DH_DSS_WITH_AES_256_CBC_SHA256</td>
</tr>
<tr>
<td>0x0069</td>
<td>TLS_DH_RSA_WITH_AES_256_CBC_SHA256</td>
</tr>
<tr>
<td>0x006b</td>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</td>
</tr>
<tr>
<td>0x0084</td>
<td>TLS_RSA_WITH_CAMELLIA_256_CBC_SHA</td>
</tr>
<tr>
<td>0x0085</td>
<td>TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA</td>
</tr>
<tr>
<td>0x0086</td>
<td>TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA</td>
</tr>
<tr>
<td>0x0088</td>
<td>TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA</td>
</tr>
<tr>
<td>0x009c</td>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0x009d</td>
<td>TLS_RSA_WITH_AES_256_GCM_SHA256</td>
</tr>
<tr>
<td>0x009e</td>
<td>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0x009f</td>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA256</td>
</tr>
<tr>
<td>0x00a0</td>
<td>TLS_DH_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0x00a1</td>
<td>TLS_DH_RSA_WITH_AES_256_GCM_SHA256</td>
</tr>
<tr>
<td>0x00a4</td>
<td>TLS_DH_DSS_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0x00a5</td>
<td>TLS_DH_DSS_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0xc003</td>
<td>TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0xc004</td>
<td>TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0xc005</td>
<td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0xc008</td>
<td>TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0xc009</td>
<td>TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0xc00a</td>
<td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0xc00d</td>
<td>TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0xc00e</td>
<td>TLS_ECDH_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0xc00f</td>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0xc012</td>
<td>TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0xc013</td>
<td>TLS_ECDH_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0xc014</td>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0xc017</td>
<td>TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA</td>
</tr>
<tr>
<td>0xc018</td>
<td>TLS_ECDH_anon_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>0xc019</td>
<td>TLS_ECDH_anon_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0xc023</td>
<td>TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>Cipher</td>
<td>Cipher suites</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>0xc024</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384</td>
</tr>
<tr>
<td>0xc025</td>
<td>TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>0xc026</td>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>0xc027</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>0xc028</td>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</td>
</tr>
<tr>
<td>0xc029</td>
<td>TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256</td>
</tr>
<tr>
<td>0xc02a</td>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384</td>
</tr>
<tr>
<td>0xc02b</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0xc02c</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>0xc02d</td>
<td>TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0xc02e</td>
<td>TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>0xc02f</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0xc030</td>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>0xc031</td>
<td>TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>0xc032</td>
<td>TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
</tbody>
</table>
10 Configuring the Dolby Conference Phone provisioning server

If you do not have Dolby Conferencing Console, you can connect the phone to a provisioning server instead.

- Reasons for using a provisioning server
- Building the provisioning server
- Security for provisioning servers
- Setting up an FTP server
- HTTPS server setup
- Master configuration file
- Template files
- Configuration file (JSON)
- Recommended file and directory layout
- Redundant provisioning servers
- Log directory
- Updating preinstalled software using a provisioning server
- Sample configurations

10.1 Reasons for using a provisioning server

The provisioning server allows for flexibility in installing, upgrading, maintaining, and configuring the Dolby Conference Phone.

Note: If you are already using a provisioning server in your organization, you can continue to use these procedures to provision your phones. However, if you are using Dolby Conferencing Console for provisioning the phones, you can skip this chapter.

The provisioning server can be set up on the local LAN or anywhere on the Internet. Configuration, log, and directory files are normally located on the provisioning server.

If you allow the phone write access to your provisioning server, the phone can use the provisioning server to upload files (such as logs) and store the user’s files. If it cannot locate a provisioning server when it boots up, the phone is designed to operate with internally saved parameters.

10.2 Building the provisioning server

Before you attempt to plug in the phone, review the provisioning server requirements, and decide what type of provisioning server to use (FTP, HTTP, or HTTPS). Make sure that the provisioning server is set up and ready for use.

Review these topics:

- Requirements for provisioning servers on page 97
- Security for provisioning servers on page 97
10.2.1 Requirements for provisioning servers
You can use either a Windows- or Linux-based server as your provisioning server. The FTP, HTTP, or HTTPS servers can reside on the same server. However, this should be a separate server from the server running your call control platform.

10.2.2 Supported provisioning protocols with provisioning servers
File Transfer Protocol (FTP), HTTP, and HTTPS provisioning protocols are supported with a provisioning server.

Both digest and basic authentication schemes are supported when using HTTP or HTTPS. Custom certificates, including those from certificate authorities, can be added to the phone for Transport Layer Security server authentication on HTTPS provisioning servers.

10.3 Security for provisioning servers
File permissions should give the minimum access required, and the account used should have no other rights on the server.

Note: For organization purposes, we recommend configuring a separate log file directory, though this is not required. The different directories can have different access permissions. For example, you can allow log files to have write access.

Log files provide backup copies of changes users make to the phone configuration. Centralization logging management is performed through syslog.

You can also download the log from the Dolby Conference Phone web interface. These log files greatly assist in the ability to provide customer support for diagnosing issues that may occur with the phone operation.

The phone needs to be able to write to the upload file directory and the provisioning directory. All other files that the phone needs to read, such as the application executable and the standard configuration files, should be made read-only through file server file permissions.

Each phone may open multiple connections to the server.

Related information
About syslog logging on page 76

10.4 Setting up an FTP server
A simple provisioning operation uses File Transfer Protocol (FTP). Although most FTP servers are free, they require installation and use log-ins and passwords.

About this task
A free and popular server, FileZilla Server, is available for Windows at filezilla-project.org. For Unix, we suggest Red Hat Enterprise Linux FTP. This section provides instructions for setting up FileZilla.
To set up an FTP server using FileZilla Server:

Procedure

1. Download and install the latest version of FileZilla Server.

2. After installation, a Connect to Server pop-up displays on your computer. Select OK to open the administrative user interface.

3. To configure a user, select Edit > Users in the status bar.

4. Select Add. Enter the user name for the phone (for example, bill123), and select OK. Select the Password check box, and enter a password (for example, 1234). The phone will use this password to log in.

5. Select Page > Shared folders to specify the server-side directory where the provisioning files will be located (and the log files uploaded).

6. Select Add, and pick the directory.

7. To allow the phone to upload logs onto the provisioning server, select Shared Folders > Files, select the Write and Delete check boxes, and then select OK.

8. Determine the IP address of the FTP server by entering cmd in the Run dialog on your Start menu, and ipconfig in the command prompt. The IP address of the FTP server is shown.

10.5 HTTPS server setup

You can provision the Dolby Conference Phone with an HTTPS provisioning server.

You must ensure that the CA certificate of the HTTPS provisioning server certificate is installed on the phone before it attempts to communicate with your HTTPS server.

Related information

First-time use of the phone on page 50

10.6 Master configuration file

The master configuration files can be used to configure the Dolby Conference Phone individually or to configure all phones at once.

Single phone master configuration file

If customization is required separately for each phone, the files should be named dvcp-<MACaddress>.cfg, where MACaddress is the MAC address (or serial number) of the phone. For a–f hexadecimal digits, use lower case only, for example, dvcp-0004f200106c.cfg. The MAC address can be viewed through the > General menu. It is also printed on a label on the back of the phone. If this file cannot be downloaded, the phone will search for the default master configuration file (described below).

Default master configuration file

For systems in which the configuration is identical for all phones (that is, there are no unique dvcp-<MACaddress>.cfg files), the default master configuration file may be used to configure all phones. The file named dvcp-default.cfg is the default master configuration file, and we recommend that you store this file on the provisioning server. If a phone does not find its own dvcp-<MACaddress>.cfg file, it will use this one, and establish a baseline configuration. This file is part of the standard distribution of configuration files. It should be used as the template for the dvcp-<MACaddress>.cfg files.
The default master configuration file, `dvcp-default.cfg`, is shown below.

```json
{
    "img_file" : "dvcp-1.0.0.<buildID>.tar.gz",
    "cfg_files" : [
        ""
    ]
}
```

Master configuration files must contain these JSON attributes:

- **img_file**
  The path name of the application executable. It can have a maximum length of 255 characters. This can be a URL with its own protocol, user name and password. For example, `dvcp-rel-2.20.212.tar.gz`.

- **cfg_files**
  A comma-separated list of configuration files. Each file name has a maximum length of 255 characters, and the list of file names has a maximum length of 2,047 characters, including commas and white space. Each configuration file can be specified as a URL with its own protocol, user name, and password. For example, `http://admin:password@prov.example.com/phone2034.cfg`. Note that the order of the configuration files listed in `cfg_files` is significant:
  - The files are processed in the order listed (left to right).
  - If the same parameter is included in more than one file or more than once in the same file, the last (right) parameter read will be used.

Master configuration files may also contain these JSON attributes:

- **certificates**
  A comma-separated list of certificate files. Each file name has a maximum length of 255 characters, and the list of file names has a maximum length of 2,047 characters, including commas and white space.

- **directory_file**
  A local directory (or phone book) that will be loaded into the phone. The file name has a maximum length of 255 characters. A sample master configuration file is shown below. The configuration parameters are split between two configuration files in this sample, namely `common.json` and `office.json`.

Here is an example file:

```json
{
    "img_file" : "dvcp-1.0.0.1234.tar.gz",
    "cfg_files" : [
        "common.json",
        "office.json"
    ],
    "certificates: [ 
        "ca_pem.pem"
    ],
    "directory_file: [ 
        "vandirectory.json"
    ]
}
```

If you have a requirement for different behaviors on different phones on the same provisioning server, you can create a variable, `[MAC]`, in the master configuration file that is
replaced by the MAC address of each phone when it reboots. You can also create a variable, [SN], that is replaced by the serial number of each phone. The sample master configuration file shown below allows for different phones to use a different set of configuration parameters and a different directory. All MAC address-specific files must reside on the provisioning server.

```json
{
   "img_file" : "dvcp-1.0.0.1234.tar.gz",
   "cfg_files" : [
      "common.json",
      "[MAC].office.json"
   ],
   "directory_file": [
      "[MAC].directory.json"
   ]
}
```

### 10.6.1 Setting up the CA certificate files for the phone to download

Update the master configuration file to specify the location of the CA certificate file, so that it may be downloaded to the phones.

**About this task**

**Procedure**

1. Download the PEM file to the provisioning server where the configuration files reside.
2. Add the file name to the master configuration file.

```json
{
   "img_file" : "dvcp-1.0.0.1234.tar.gz",
   "cfg_files" : [
      "dvcp-config1.json"
   ],
   "certificates": [
      "ca_certs.pem"
   ]
}
```

3. Reboot the phone.

### 10.7 Template files

Use these template files to create a filename.json file for the configuration parameters that you need to change to configure the desired phone features.

- **dvcpcfg-core.json**: Parameters that must be set for a phone to make and receive calls
- **dvcpcfg-user.json**: User-related parameters
- **dvcpcfg-common.json**: Site-specific parameters
Use `dvcpcfg-all.json` only as a reference, as all parameters are not required. A sample user-specific configuration file is shown in this figure.

```json
{
    "Sip.Account.DisplayName": "Sarah Chu",
    "Sip.Account.UserName": "3105",
    "Sip.Credential.Name": "3105",
    "Sip.Credential.Password": "1234",
    "Sip.Credential.Realm": "*",
    "Preferences.AutoAnswerEnabled": true
}
```

### 10.8 Configuration file (JSON)

Administrators can use configuration parameters to dictate the behavior of the Dolby Conference Phone once it is running the executable specified in the master configuration file.

To verify JSON files to be used for provisioning the phone, go to [http://www.jsonlint.com](http://www.jsonlint.com) and follow the directions.

**Related information**

*Accessing the Dolby Conference Phone web interface* on page 78

### 10.9 Recommended file and directory layout

You must create at least two configuration files for the Dolby Conference Phone to boot up, and certain parameters will need to be changed for the phone to be usable within your organization. The Dolby Conference Phone software package comes with sample configuration files for you to use.

*Figure 8: Sample grouping of configuration files for provisioning*

For additional information related to recommended file and directory layout:
Related information

<table>
<thead>
<tr>
<th>Related information</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>The use of multiple configuration files for the configuration parameters.</td>
<td>Master configuration file on page 98</td>
</tr>
<tr>
<td>A description of the template files you can use to create the common and user-specific configuration files.</td>
<td>Template files on page 100</td>
</tr>
<tr>
<td>Which parameters apply to each phone feature.</td>
<td>Configuring phone features on page 33</td>
</tr>
<tr>
<td>Information about having different features on some phones. You will need to create a number of configuration files, one for each phone that you want to deploy. You will also need the list of MAC addresses you created.</td>
<td>Conference room requirements on page 17</td>
</tr>
</tbody>
</table>

**Note:** The configuration on the provisioning server overrides any existing configuration of the phone. For example, if there are no certificates on the provisioning server, but there are existing certificates on the phone, those certificates will be removed during the provisioning process.

### 10.10 Redundant provisioning servers

With large-scale deployments (for example, 10,000 devices or more), consider setting up multiple (redundant) provisioning servers (an active and a backup version). This ensures that the user does not experience service disruptions or performance problems.

If you have Dolby Conferencing Console, you can use it to set up redundant provisioning servers (see *Dolby Conferencing Console operations and management guide*).

If you do not have Dolby Conferencing Console, you can configure multiple (redundant) provisioning servers—one logical server with multiple addresses—by mapping the provisioning server DNS name to multiple IP addresses. The default number of provisioning servers is one, and the maximum number is two.

If you set up multiple provisioning servers, you must be able to reach all of the provisioning servers with the same protocol, and the contents on the provisioning servers must be identical.

### 10.11 Log directory

The Dolby Conference Phone is typically configured to upload log files to the provisioning server.

We recommend creating a subdirectory for uploading log files, so they are not confused with configuration and phone software files. The phone must be configured to upload log files to the new directory; see *Log files* on page 75.

### 10.12 Updating preinstalled software using a provisioning server

The Dolby Conference Phone software is available for download from the provider of your phone. Updates are issued periodically.
Make sure that you reference the correct documentation when attempting to update software on phones. This varies depending on whether you use Dolby Conferencing Console or a provisioning server to provision phones.

If your organization uses Dolby Conferencing Console, skip this section and see the following documentation instead:
- [Updating software using Dolby Conferencing Console](#) on page 32
- [Dolby Conferencing Console operations and management guide](#)

### 10.12.1 Available software packages

If your organization uses a provisioning server, download the software packages described here and then refer back to the instructions in [Configuring the Dolby Conference Phone provisioning server](#) on page 96. The Dolby Conference Phone software packages must be uncompressed on the provisioning server for the phone (or a temporary location if you have not set up your provisioning server yet).

The software package, `dvcp-rel-<x.y.z.buildID>.zip`, contains these files:
- `dvcp-rel-<x.y.z.buildID>.tar.gz`
  - Dolby Voice application image file
- `dvcp-rel-<x.y.z.buildID>.meta`
  - Dolby Voice application `.meta` file (checksums and digital signature)

  **Note:** The prefixes of the `.tar.gz` and `.meta` files must match, or the phone software will not download to the phone correctly.

- `dvcp-default.cfg`
  - Master phone configuration file
- Three configuration parameter template files
  - `dvcp-rel-<x.y.z.buildID>.cli-help.html`
    - Diagnostic shell command descriptions
  - `dvcp-rel-<x.y.z.buildID>.cfg-help.html`
    - Configuration parameter descriptions
  - `internalConf-rel-<x.y.z.buildID>.xml`
    - Configuration parameter definitions
  - `internalConfEnum-rel-<x.y.z.buildID>.xml`
    - Configuration parameter enumerations

When you download the phone software, a notice will display asking you to accept the download. Read the notice, click the button indicating that you have read the notice, and then click the **Submit** button to continue the phone software package `.zip` download.

See the latest release notes for a detailed description of each file in the distribution, issues that are fixed in this release, and issues that still remain (with possible workarounds).

### 10.12.2 Upgrading and downgrading phone software

You can upgrade the phone software that is running on all Dolby Conference Phones in your organization. Or you can upgrade the phones one at a time.

You may be prompted to confirm the upgrade operation. Tap **Update** or **Skip**. If you do not respond within 20 seconds, the upgrade will automatically proceed.

If you tap **Skip**, this icon displays:
Note: While the phone software update is in progress, the progress displays at the top of the Dolby Conference Phone web interface page.

Related information
Viewing the Status menu on page 73

10.12.3 Upgrading phones to the latest Dolby Conference Phone software

The Dolby Conference Phone software and configuration can be updated together using the centralized provisioning model.

Procedure

1. Back up your existing application (and configuration files).
2. Create new configuration files.
   Configuration file changes and enhancements are explained in the release notes that accompany the phone software.
3. Save the new configuration files and phone software images on your provisioning server.
4. Reboot the phone.
   From the phone user interface, tap > > Reboot phone, or, from the phone web interface, select Tools and click the reboot link.
5. Ensure that the configuration process completed correctly.
   From the phone user interface, tap > > About > General.
   Confirm the Dolby Voice software version and the configuration files downloaded to the phone.
6. Monitor the log files uploaded to the provisioning server.

10.12.4 Downgrading phones to an earlier version of Dolby Conference Phone software

The Dolby Conference Phone software and configuration can be reverted to earlier versions if the software and configurations have been backed up.

Procedure

1. Back up your existing application (and configuration files).
2. Create new configuration files.
   Configuration file changes and enhancements are explained in the release notes that accompany the phone software.
3. Save the new configuration files and phone software images on your provisioning server.
4. Reboot the phone.
   The phone file system may be reformatted.
5. Ensure that the configuration process completed correctly.
   From the phone user interface, tap > > About > General.
Confirm the Dolby Voice software version and the configuration files downloaded to the phone.

6. Monitor the log files uploaded to the provisioning server.

10.13 Sample configurations

Use the sample configuration files provided with the Dolby Conference Phone software package to create your own configuration file.

The best configuration reference is available in the phone software package:

- Configuration directives: dvcp-rel-\textit{x}.\textit{y}.\textit{z}.\textit{build}.cfg-help.html
- Shell commands: dvcp-rel-\textit{x}.\textit{y}.\textit{z}.\textit{build}.cli-help.html and in the web interface of the phone: Tools > Help.

10.13.1 Directory structure

The following examples each assume the same directory structure on the provisioning server. They assume a top-level directory that contains all of the configuration and phone software files, and a subdirectory called /\textit{logs} to contain the uploaded log files.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>Location of phone software and all configuration files</td>
</tr>
<tr>
<td>/\textit{logs}</td>
<td>Destination for uploading files</td>
</tr>
</tbody>
</table>

10.13.2 Master configuration file

The master configuration file is common to all phones and specifies the phone software version that the phones should load, and the names of the configuration files and certifications that the phones should load.

```json
{
    "img_file" : "dvcp-rel-2.0.1.116.tar.gz",
    "cfg_files" : [ "common.json", "[MAC].office.json" ],
    "certificates": [ "rootCA.cer", "otherRootCA.cer" ]
}
```

In this example:

- \textit{dvcp-rel-2.0.1.116.tar.gz} is the name of the phone software image the phones should run.
- rootCA.cer and otherRootCA.cer are the names of certificate files the phones should load, for example, Secure Sockets Layer (SSL) certificate authority root certificates.

10.13.3 Simple IP PBX–only configuration

This is a basic configuration that enables the Dolby Conference Phone to register with and use an IP PBX for telephone calls.
In the common configuration file, you would place any of the common parameters, such as the proxy server details. In the device-specific configuration file, place the device-specific parameters, such as the SIP registration details to be used and the local time zone of the phone.

Figure 9: Simple IP PBX-only configuration

File: common.json

In this configuration it is important to configure the operation mode correctly and configure the SIP proxies as they will be shared, and we recommend you configure common logging options.

```
{
  "Features.OperationMode": "IPPBXONLYMODE",
  "Sip.Pbx.OutboundProxy1": "a.b.c.d",
  "Sip.Pbx.OutboundProxy2": "e.f.g.h",
  "Logging.Upload.Enable": true,
  "Provisioning.Server.UploadDir": "logs"
}
```

In this example:

- `a.b.c.d` and `e.f.g.h` are the IP addresses of one or two call servers or outbound proxy servers that the phone should use.
- `logs` is the name of the subdirectory on the provisioning server where log files will be stored.

File: [MAC].office.json

This file will contain any configuration items specific to the device you are configuring. Within a configuration file value, the string `[MAC]` is replaced by the MAC address of the specific phone you are configuring.
To create a configuration file specific to the phone with MAC address 1a:2b:3c:4d:5e:6f you would create a file called: 1a2b3c4d5e6f.user.json.

A simple user configuration file would include:

```json
{
  "Preferences.Localization.Timezone": "tzspec",
  "Sip.Account.DisplayName": "displayname",
  "Sip.Account.UserName": "username",
  "Sip.Credential.Name": "credname",
  "Sip.Credential.Password": "credpass"
}
```

In this example:

- `tzspec` is the name of the time zone in which the user resides. For example, Australia/Sydney.
- `displayname` is the name that should be displayed for the user.
- `username` is the extension number or address of the user.
- `credname` is the name used when authenticating the user.
- `credpass` is the password used when authenticating the user.
11 Troubleshooting

If you encounter an issue with the Dolby Conference Phone, we recommend that you attempt basic troubleshooting before you contact Support. The information in this chapter describes likely causes of phone issues and corrective actions you can take to resolve them. Follow the available troubleshooting procedures to review logs and error messages, run diagnostics, and possibly upgrade the phone software.

- Phone issues and solutions
- Plug-and-Play Setup issues and solutions
- Decommissioning and disposing of the phone

11.1 Phone issues and solutions

Use this information for likely causes and corrective actions for your phone.

11.1.1 Power and start-up issues

For power and start-up issues, see these possible solutions.

**Issue**
The phone has power issues or the phone has no power.

**Solution**
Determine whether the problem is caused by the phone, the AC outlet, or the PoE switch. Do one of the following:

- If using PoE, ensure that the port is a PoE port and not just a regular Ethernet port.
- If using a power injector, ensure that the injector is plugged into a functional AC outlet.
- Verify that no lights appear on the unit when it is powered up.
- Check for faulty cable. Replace cable and try again.

11.1.2 Hardware issues

These are possible solutions to hardware issues.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Buttons do not work. For example, when the phone is idle, pressing the volume button does not bring up the ringer widget, and you cannot hear the ringer tone. | Tap the phone icon on the home screen. Tap the keypad digits on the dialer screen.  
- If you can hear the dual-tone multifrequency (DTMF) tone, then there might be a problem with the hardware. To confirm whether the keys are working, tap >  > Diagnostics > Test > Hardware > Keys and follow the instructions.  
- If you cannot hear the DTMF tone, wait until the fatal error screen displays (see Fatal error issues on page 119) and the phone reboots. Log files from the error are uploaded to the provisioning server and will assist you in finding the problem. |
| Touch screen is not accurate. For example, when you touch the screen, the coordinates in the phone software do not compare to where you touched the screen. | It is possible that the touch screen is not accurately calibrated.  
Go to >  > Diagnostics > Test > Hardware > Touch Screen and follow the instructions.  
Once it is confirmed that the phone touch screen is not accurately calibrated, go to the diagnostics shell and enter `system removetouchscreencalibrationdata`, then reboot the phone by entering `system reboot`. This forces the phone to go to a calibration screen to recalibrate. |
| One or more speakers are not working. | To verify, go to >  > Diagnostics > Test > Hardware > Speakers and follow the instructions. |
| One or more microphones are not working. | To verify, go to >  > Diagnostics > Test > Hardware > Microphones and follow the instructions. This test allows testing one microphone at a time. |

**Related information**  
[Fatal error issues](#) on page 119

### 11.1.3 Network access issues

Here are possible solutions to network access issues.
On the Dolby Conference Phone web interface Status page, the network device system status appears as a red circle. Position your mouse pointer over the red circle to view the network status code.

If one of these status codes appears, check whether the switch is correctly set up and if the Ethernet cable is acceptable:

- **Link is dormant**—Network is pending authentication.
- **Link is down**.
- **Unknown link error**—There is an unknown network error.

If one of these status codes appears, check whether there is an unmanaged switch connecting the LLDP switch and the phone:

- **LLDP Ethernet speed/duplex mismatch**—Ethernet speed/duplex mismatch reported by LLDP.
- **Two or more LLDP neighbors detected**—Device is connected to an unmanaged switch.
- **LLDP neighbor end device detected**. Device is connected to an unmanaged switch—An LLDP end device neighbor is detected. The phone is connected to an unmanaged switch.

If this status code appears, check the LLDP VLAN settings on switch:

- **LLDP Voice and Voice Signaling VLANID mismatch detected**—LLDP Voice VLAN and Voice Signaling VLAN ID conflict detected.

If this status code appears, check the network status:

- **FAIL_DHCP**—DHCP failed.

If this status code appears, check whether another phone on the network is using the same IPv4 address:

- **String of Mac address**: Another phone on the network is using the same IPv4 address.

If one of these status codes appears, check whether the default gateway is up:

- **Default gateway is unreachable**.
- **Default gateway is unconfigured**.

If one of these status codes display, check if the DNS servers are up:

- **DNS servers are unreachable**.
- **DNS servers are unconfigured**.
- **Only secondary DNS server is reachable**—Primary DNS server is unreachable while secondary DNS server is reachable.

If one of these status codes displays, check that the Dynamic DNS (DDNS) is correctly configured on the DNS servers and DHCP server.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DNS hostname unresolvable—Host name DVCP-Dxxxxxxx is not resolvable.</td>
<td>If this status code appears, check whether the NTP server is correctly configured and accessible: • NTP is manually disabled. You can also check the network status codes through the diagnostic shell by using the command show configuration all.</td>
</tr>
<tr>
<td>• DNS servers are unconfigured.</td>
<td></td>
</tr>
<tr>
<td>The phone does not obtain an IP address on the secondary VLAN.</td>
<td>The secondary VLAN was configured incorrectly. For example, the wrong VLAN ID was specified. Verify the VLAN ID and try to provision the phone again.</td>
</tr>
<tr>
<td>The phone obtains an IP address on only one VLAN when the dual VLAN feature is enabled in conjunction with the Cisco switch port with 802.1X authentication enabled.</td>
<td>Set the authentication host mode of the Cisco switch port to either single-host or multiple-host mode. For more information on Cisco 802.1X host modes, see <a href="http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/50sg/configuration/guide/Wrapper-46SG/dot1x.html#wp1240475">http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/50sg/configuration/guide/Wrapper-46SG/dot1x.html#wp1240475</a>.</td>
</tr>
<tr>
<td>The phone does not obtain an IP address on the secondary (data) VLAN when the dual VLAN feature is enabled and port security is enabled on the Cisco switch port.</td>
<td>Run a command similar to the following example on the Cisco switch: switchport port-securitymac-address 00:d0:46:0a:00:29 vlan access The 00:d0:46:0a:00:29 is the MAC address of the selected phone. This command allows the phone with the specified MAC address to be on both the voice and data VLANs at the same time. For more information on Cisco switch port security, see <a href="http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html">http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html</a> .</td>
</tr>
<tr>
<td>You see a Failed to load message from your conferencing service provider, or a service unavailable message from the conferencing service.</td>
<td>Your organization uses a dual VLAN, and the phone was unable to connect to your conferencing service provider over the Internet. See Primary and secondary VLANs on page 21 and Configuring the secondary VLAN on page 64</td>
</tr>
</tbody>
</table>

11.1.4 Provisioning issues

Here are some possible solutions for first-time provisioning issues.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The phone does not obtain an IP address.</td>
<td>The phone usually takes about 50 to 60 seconds to boot up. If it takes much longer than that (for example, more than 90 seconds), the phone may not be obtaining its IP address. The phone waits up to 90 seconds at start-up for the DHCP response, and if it does not get the IP address, it uses a self-allocated link-local IP address (see RFC 3927) and continues with the boot. Make sure the phone has proper network connectivity and is connected to a port that allows the device to get DHCP IP configuration. There may also be a VLAN configuration issue, and in the case that the phone cannot obtain an IP address from the default VLAN, wait until the phone boots up, then modify the VLAN manually by going to <strong>Administrator Settings &gt; Network configuration &gt; Ethernet</strong>.</td>
</tr>
</tbody>
</table>
| The phone cannot connect to the provisioning server.      | Once you enter the provisioning server IP and access credentials, the phone attempts to connect to the provisioning server. If the access fails, the phone displays a message that the connection to the provisioning server has failed. The following error conditions display on the UI:  
  - Network error  
  - Authentication failure  
  - SSL error  
Make sure to provide the correct:  
  - IP address  
  - Credentials  
**Note:** During the first-time provisioning, changing these settings does not require the device to go through a reboot cycle.  
You can tap and go back to the start screen to correct the input. |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
</table>
| There are errors in the configuration files on the provisioning server. | If there is an error in the configuration file, the phone displays error messages similar to the following:  
• Invalid configuration files or parameters. Press the “More” button for more information.  
• A list of the parameters in error  
Correct the configuration files on the provisioning server based on the information provided on the phone screen. Possible errors are:  
• Write access not allowed for provisioning — The parameter is not allowed to be configured from the provisioning server.  
• Data validation error — The value supplied is not valid and has failed validation on the phone.  
• Invalid parameter — The parameter specified in the configuration file is not recognized by the phone.  
Configuration errors are also displayed in the Dolby Conference Phone web interface when you position the mouse pointer over the red circle in the Provision Successful field. |
| The phone is unable to connect to an HTTPS provisioning server.       | If you want to use an HTTPS provisioning server, the phone may not be able to connect to the provisioning server due to security settings issues if not configured properly. The phone must first be initially provisioned in a nonsecure environment, in an FTP or HTTP protocol, to download the server CA certificate to the phone. Then it needs to be switched over to the HTTPS provisioning server. See Configuring the Dolby Conference Phone provisioning server on page 96. |
### Issue 11.1.5 Authentication issues

Here are possible solutions to authentication issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You cannot remember the administrative password. (The default administrative password is 1739.)</td>
<td>Do the following:</td>
</tr>
<tr>
<td></td>
<td>• Back up the configuration files.</td>
</tr>
<tr>
<td></td>
<td>• Perform a factory reset on the phone. See Resetting to factory defaults on page 88.</td>
</tr>
<tr>
<td></td>
<td>• Restore the configuration files.</td>
</tr>
</tbody>
</table>

**Related information**

- [Resetting to factory defaults](#) on page 88
- [Adding certificate authority certificates](#) on page 36
### 11.1.6 IP PBX calling issues

Here are possible solutions for IP PBX calling issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
</table>
| The user cannot make a call because the phone button is grayed out, and Settings shows a red circle on the home screen. | Tap ![Image] to validate whether there is a red circle adjacent to CallServer. If there is, then the phone is not registered to the call server. Through the Dolby Conference Phone web interface, go to Status > System > Device, find SIP Registered, and position the mouse pointer over the red circle to obtain the failure details. The reason could be one of the following:  
  - The phone cannot connect to the call server due to network errors.  
  - The phone cannot connect to the call server due to authentication failures (incorrect credentials).  
  - The phone cannot connect to the call server due to other configuration errors. You can review all configuration parameters under Sip. |
| The user always gets the busy tone after dialing a number.            | The possible reasons for the failure are:  
  - The dial plan on the server side is set incorrectly.  
  - The phone the user is calling is no longer registered to the server.  
  - The phone is using an incompatible codec configuration. Through the Dolby Conference Phone web interface, tap ![Image] > IP PBX Settings > Server > PBX > Codec List. It is possible that the phone that the user is trying to call does not support the same codec. See Bandwidth planning and codec selection on page 20. |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user cannot receive a call.</td>
<td>The possible reasons for the failure are:</td>
</tr>
<tr>
<td></td>
<td>• The do not disturb feature is enabled. To disable, tap <img src="image" alt="Do Not Disturb" /> &gt; Off / On option to Off. If do not disturb is enabled, a scrolling message displays on the home screen.</td>
</tr>
<tr>
<td></td>
<td>• The call forwarding feature is enabled. To disable, tap <img src="image" alt="Call Forwarding" /> &gt; Call Forwarding, then delete the appropriate forwarded number. If call forwarding is enabled, a scrolling message displays on the home screen.</td>
</tr>
<tr>
<td></td>
<td>• The phone is using an incompatible codec configuration. To see a list of supported codecs, tap <img src="image" alt="IP PBX Settings" /> &gt; Server &gt; PBX &gt; Codec List. It is possible that the phone the user is trying to call does not support the same codec. See Bandwidth planning and codec selection on page 20.</td>
</tr>
<tr>
<td>During a call, the user cannot hear or be heard by the other end of the call, but the call timer shows an increasing call length.</td>
<td>The possible reasons for the failure are:</td>
</tr>
<tr>
<td></td>
<td>• Network connectivity is lost between the phone and the other end of the call.</td>
</tr>
<tr>
<td></td>
<td>• The phone encountered a serious error. Go to Fatal error issues on page 119.</td>
</tr>
<tr>
<td></td>
<td>• The signal processing on the phone does not get packets from the network or send packets to the network.</td>
</tr>
<tr>
<td></td>
<td>Through the Dolby Conference Phone web interface, go to Status &gt; Call Statistics to view the run-time call statistics as shown below. If the receiver (Rx) or transmitter (Tx) counts grow, this indicates that the signal processing is sending or receiving packets to or from the network. Check whether the audio gateway is working correctly by sending a silence packet and ignoring the packets sent by another phone. If the receiver counts do not grow, this indicates that the phone is not receiving any packets from the other end.</td>
</tr>
</tbody>
</table>
11.1.7 Audio quality issues

If users experience audio quality issues, they can use the audio diagnostic feature to collect more information about the problem.

**Issue**

Users have commented that there are audio or echo issues during calls.

**Solutions**

Ask users to provide information by tapping during a call and selecting a possible issue from the list provided on the phone. Possible issues are:

- Others can’t hear me
- Others hear me sound robotic
- Others hear echo from my phone
- I hear echo
- I hear choppy/robotic audio
- I can’t hear anyone
- I hear noises when I talk
- Other problems

**Related information**

Audio logging on page 77
11.1.8 Software update issues

Here are solutions for Dolby Conference Phone software update issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The message Unable to download image file appears on the phone.</td>
<td>After uncompressing the dvcp-rel-.y.z.buildIDzip release package, place both dvcp-rel-.y.z.buildIDtar.gz and dvcp-rel-x.y.z.buildIDmeta on the provisioning server. The file names must match the master configuration file, so make sure that the dvcp-rel-x.y.z.buildIDtar.gz file is specified in the master configuration file. Tap &gt; Software update to retry the download process.</td>
</tr>
<tr>
<td>The message Invalid signature on software image file appears on the phone.</td>
<td>For security reasons, you must obtain phone software from Dolby to upgrade the Dolby Conference Phone. The image is signed by Dolby and the phone performs a validation at phone software upgrade. If you see this message, you are using an unauthorized image. Contact Dolby Customer Support if you received the image from Dolby.</td>
</tr>
<tr>
<td>The message Invalid software image file appears on the phone.</td>
<td>After downloading the image, the phone performs a checksum validation. This message appears if the validation failed. Reasons for this include transmission errors or that the image file is corrupt. If the image file came from Dolby, contact Dolby Customer Support. If the issue persists, check with your organization's IT department to investigate any network transmission errors.</td>
</tr>
<tr>
<td>The message Failed to complete software update for an unknown reason appears on the phone.</td>
<td>During the phone software upgrade, a possible flash error was detected. Retry the phone software update. If the message appears again, contact Dolby Customer Support.</td>
</tr>
</tbody>
</table>

11.1.9 Corporate directory issues

Here are solutions for corporate directory issues.

**Issue**

The user cannot connect to the LDAP directory.

The home screen shows ☢. The system status shows there is a directory error.

**Solution**

The possible reasons for the failure are:

- An incorrect LDAP server IP address
- Incorrect LDAP server access credentials
- An incorrect or missing LDAP server root CA certificate (necessary when accessing LDAP server using SSL)

Through the Dolby Conference Phone web interface, go to **Status > System > Device**. Find LDAP connected. A red circle indicates an LDAP error. Position your mouse pointer over the red circle to see the specific error that occurred.
11.1.10 Fatal error issues

Here are possible solutions to fatal error issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
</table>
| The main application encountered a fatal error.  
The message The services application has stopped responding. Press Debug to stop rebooting. appears on the screen after one to two minutes. | You can choose to debug the problem. This stops the phone from performing the automatic reboot. If you do not tap Debug, the phone automatically reboots after five seconds.  
If the phone is configured to upload log files, the phone uploads the core dump (if there is any) to the provisioning server during the next reboot. The core dump file name is `SW-timestamp-core.appname`. For example, D0025416-1402090840-core.services_app is a core dump generated from the services_app application on the device numbered D0025416.  
Attach the uploaded log files as well as the core dump file, and create a bug report for Dolby Customer Support to perform further analysis.  
**Note:** Uploading a core dump during boot time prolongs boot time. |
| The phone user interface continues to display the Dolby logo and does not display the home screen, even after 90 seconds. | A combination of configuration and phone software issues have left the phone in a state from which it cannot recover.  
Reboot the phone. As the Dolby logo appears, perform a factory reset (see Resetting to factory defaults on page 88). The LED halo flashes yellow when the factory reset is complete. The home screen should display.  
If the phone user interface still shows the Dolby logo and the phone software was recently upgraded, reboot the phone again while pressing and holding the Mute and Volume Up keys until the LED halo shows blue, about 10 seconds. Then reboot the phone again. This downgrades the phone software.  
If the phone user interface still shows the Dolby logo, return it to Dolby for return merchandise authorization. |

**Related information**

Hardware issues on page 108
IP PBX calling issues on page 115
Resetting to factory defaults on page 88

11.1.11 Dolby Satellite Microphone issues

Here are possible solutions for Dolby Satellite Microphone issues.

**Issue**

The user plugs in one or both Dolby Satellite Microphones, but no tone plays.

**Solution**

Verify that the phone software is Version 2.1 or later.

- If it is not, update the phone software.
- If it is, check the microphones in another phone.
# 11.2 Plug-and-Play Setup issues and solutions

Use this information for likely causes and corrective actions if you are using Plug-and-Play Setup to deploy your phone. These messages appear on the Dolby Conference Phone screen.

## 11.2.1 Dolby Voice Console issues

These are possible solutions to Dolby Voice Console issues when deploying the phone with Plug-and-Play Setup.

These messages appear on the Dolby Conference Phone screen.

<table>
<thead>
<tr>
<th>Issue code</th>
<th>Message displayed</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>101</td>
<td>Dolby Voice Console is unreachable from this network because it requires 802.1x authentication. Tap Next to configure 802.1x or contact your IT help desk for assistance.</td>
<td>Your network requires 802.1X network authentication. Depending on the specific authentication method, you may need to accept a certificate, and/or enter authentication credentials. Tap the Next button to move to the next screen and complete the 802.1X configuration.</td>
</tr>
<tr>
<td>102</td>
<td>Dolby Voice Console is unreachable from this network due to a DHCP failure. Contact your IT help desk for assistance.</td>
<td>The phone was unable to obtain a valid IP address for communicating with the Dolby Voice Console. Tap the Next button to review the network configuration. You need to plug the phone into a different port on the wall, modify VLAN settings on the phone, or work with your IT help desk for assistance.</td>
</tr>
<tr>
<td>103</td>
<td>Dolby Voice Console is unreachable from this network due to an unconfigured DNS. Contact your IT help desk for assistance.</td>
<td>The phone was unable to obtain a DNS server address for communicating with the Dolby Voice Console. Tap the Next button to review the network configuration. You can manually configure the DNS server address on the next screen, if needed.</td>
</tr>
<tr>
<td>104</td>
<td>Dolby Voice Console is unreachable because the phone cannot complete proxy auto detection. Contact your IT help desk for assistance.</td>
<td>The phone was unable to communicate with the Dolby Voice Console because it was unable to download the PAC file to complete PAC. Tap the Next button to move to the next screen and review the PAC setting. Work with your IT help desk to make sure the PAC file is reachable from the phone. Alternatively, you can manually configure a valid PAC URL, or turn off PAC completely from the network setup screen.</td>
</tr>
<tr>
<td>105</td>
<td>Dolby Voice Console is unreachable from this network due to a proxy authentication error. Tap Next to provide the credentials for proxy authentication or contact your IT help desk for assistance.</td>
<td>The phone was unable to connect to Dolby Voice Console because the proxy requires authentication. Tap the Next button and move to the next screen to supply proxy authentication credentials and try again.</td>
</tr>
<tr>
<td>106</td>
<td>Dolby Voice Console is unreachable from this network due to an unknown proxy error. Contact your IT help desk for assistance.</td>
<td>The phone was unable to connect to the proxy server. Work with your IT help desk to make sure the proxy server is up and running.</td>
</tr>
<tr>
<td>Issue code</td>
<td>Message displayed</td>
<td>Solution</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>107</td>
<td><strong>Dolby Voice Console is unreachable from this network due to an unresolvable hostname problem. Contact your IT help desk for assistance.</strong></td>
<td>The phone was unable to communicate with the Dolby Voice Console because the DNS server was not able to resolve the Dolby Voice Console host name. Tap the <strong>Next</strong> button to review the network configuration. You can manually configure the DNS server address on the next screen if needed.</td>
</tr>
<tr>
<td>108</td>
<td><strong>Dolby Voice Console is unreachable from this network. Contact your IT help desk for assistance.</strong></td>
<td>The phone was unable to connect to the Dolby Voice Console. This could mean that the Dolby Voice Console is temporarily out of service or that your network prohibited the phone from connecting to the Dolby Voice Console. For more information, see <strong>Server addresses</strong> on page 25.</td>
</tr>
<tr>
<td>109</td>
<td><strong>Dolby Voice Console is unreachable from this network due to an unknown SSL issue. Contact your IT help desk for assistance.</strong></td>
<td>The phone was unable to connect to the Dolby Voice Console due to an SSL issue. This is very unlikely to happen, but if it does, contact your conferencing service provider who will contact the Dolby support team for assistance.</td>
</tr>
<tr>
<td>110</td>
<td><strong>Dolby Voice Console provided an unknown response to the phone. Contact your IT help desk for assistance.</strong></td>
<td>The phone received an unrecognizable response from the Dolby Voice Console. This is very unlikely to happen, but if it does, contact your conferencing service provider who will contact the Dolby support team for assistance.</td>
</tr>
<tr>
<td>111</td>
<td><strong>The phone encountered an unknown error with the Dolby Voice Console. Contact your IT help desk for assistance.</strong></td>
<td>The phone encountered an unknown error from the Dolby Voice Console. This is very unlikely to happen, but if it does, contact your conferencing service provider who will contact the Dolby support team for assistance.</td>
</tr>
</tbody>
</table>

### 11.2.2 Provisioning service issues

These are possible solutions to provisioning service issues when deploying the phone with Plug-and-Play Setup.

These messages appear on the Dolby Conference Phone screen.
<table>
<thead>
<tr>
<th>Issue code</th>
<th>Message displayed</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Provisioning failed because the phone could not communicate with the provisioning server. Contact your IT help desk for assistance. Communication with the provisioning server could not be established.</td>
<td>The phone was unable to connect to the provisioning server that was provided by the Dolby Voice Console. The screen lists specific server errors such as those related to IP network configuration, DNS failure, and so on. Review the errors listed, and move to the next screen to adjust the network configuration. It could also mean that the firewall has blocked access to the conferencing service provider’s provisioning service. To determine which servers need access to your network, see the deployment guide for your conferencing service provider or call control platform.</td>
</tr>
<tr>
<td>202</td>
<td>Failed to connect to the server due to an SSL error. Contact your IT help desk for assistance.</td>
<td>Due to an SSL error, the phone was unable to connect to the provisioning server that was provided by the Dolby Voice Console. This is very unlikely to happen, but if it does, contact your conferencing service provider who will contact the Dolby support team for assistance.</td>
</tr>
<tr>
<td>203</td>
<td>Provisioning failed because invalid credentials were provided to the provisioning server. Contact your IT help desk for assistance.</td>
<td>The phone was unable to connect to the provisioning server that was provided by the Dolby Voice Console due to an authentication failure. This is very unlikely to happen, but if it does, contact your conferencing service provider who will contact the Dolby support team for assistance.</td>
</tr>
<tr>
<td>204</td>
<td>Could not find the master configurations. Contact your IT help desk for assistance.</td>
<td>The phone was unable to connect to the provisioning server that was provided by the Dolby Voice Console due to a missing configuration. This is very unlikely to happen, but if it does, contact your conferencing service provider who will contact the Dolby support team for assistance.</td>
</tr>
<tr>
<td>205</td>
<td>Could not find the configuration file. Contact your IT help desk for assistance.</td>
<td>The phone was unable to connect to the provisioning server that was provided by the Dolby Voice Console due to a missing configuration. This is very unlikely to happen, but if it does, contact your conferencing service provider who will contact the Dolby support team for assistance.</td>
</tr>
<tr>
<td>206</td>
<td>Invalid master configurations. Contact your IT help desk for assistance.</td>
<td>The phone was unable to connect to the provisioning server that was provided by the Dolby Voice Console due to an invalid configuration. This is very unlikely to happen, but if it does, contact your conferencing service provider who will contact the Dolby support team for assistance.</td>
</tr>
<tr>
<td>207</td>
<td>Failed to download the meta file. Contact your IT help desk for assistance.</td>
<td>The phone was unable to connect to the provisioning server that was provided by the Dolby Voice Console due to an invalid configuration.</td>
</tr>
</tbody>
</table>
### 11.2.3 Setup app issues

These are possible solutions to setup app issues when deploying the phone with Plug-and-Play Setup.

As part of Plug-and-Play Setup, the phone must be able to connect to your conferencing service provider’s setup app through the Internet. Once the phone connects to the setup app, screens and workflows that are specific to your conferencing service provider display on the phone. After out-of-the-box setup is complete, the phone then uses your conferencing service provider’s conferencing application, which is a separate application from the setup app.

<table>
<thead>
<tr>
<th>Issue code</th>
<th>Message displayed</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>301</td>
<td>The setup app encountered a program failure. Contact your IT help desk for assistance.</td>
<td>The setup app that the phone was trying to load has a program error. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
<tr>
<td>302</td>
<td>The phone failed to download the setup app because some files are missing. Contact your IT help desk for assistance.</td>
<td>The setup app is a missing file that the phone was trying to load. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
<tr>
<td>303</td>
<td>The phone failed to download the setup app due to a network error. Contact your IT help desk for assistance.</td>
<td>The phone was unable to download the setup app due to a network failure. This could mean that your firewall blocked access to the conferencing service provider's provisioning service. To determine which servers need access to your network, see the deployment guide for your conferencing service provider or call control platform. The screen displays specific server errors, such as <strong>There was a problem with the DNS server</strong> and so on. Contact your IT help desk for assistance.</td>
</tr>
<tr>
<td>304</td>
<td>The server has refused the setup app download request. Contact your IT help desk for assistance.</td>
<td>The server that hosts the conferencing application has refused the download request from the phone. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
<tr>
<td>Issue code</td>
<td>Message displayed</td>
<td>Solution</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>305</td>
<td>The phone failed to download the setup app due to a network error.</td>
<td>The phone was unable to download the setup app due to a network failure. This could mean that your firewall blocked access to the conferencing service provider's provisioning service. To determine which servers need access to your network, see the deployment guide for your conferencing service provider or call control platform.</td>
</tr>
<tr>
<td>306</td>
<td>The phone failed to download the setup app due to a DNS error. Contact your IT help desk for assistance.</td>
<td>The phone was unable to download the setup app because of a DNS server error. Contact your IT help desk to adjust network settings and manually configure the DNS server if needed.</td>
</tr>
<tr>
<td>307</td>
<td>The phone failed to download the setup app due to a network timeout. Contact your IT help desk for assistance.</td>
<td>The phone was unable to download the setup app due to a network timeout error. It could mean that the server where the setup app resides is temporarily out of service. Contact your conferencing service provider for help.</td>
</tr>
<tr>
<td>308</td>
<td>The phone failed to download the setup app due to a proxy error. Contact your IT help desk for assistance.</td>
<td>The phone was unable to download the setup app due to a proxy error. Contact your IT help desk to review the proxy setup and make sure the conferencing application download request is correctly handled by the proxy server. You can view the proxy settings by moving to the next screen.</td>
</tr>
<tr>
<td>309</td>
<td>The phone failed to download the setup app due to an SSL error. Contact your IT help desk for assistance.</td>
<td>The phone was unable to download the setup app due to an SSL error. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
<tr>
<td>310</td>
<td>The phone failed to download the setup app because the server has rejected the request. Contact your IT help desk for assistance.</td>
<td>The server that hosts the setup app has rejected the download request from the phone. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
<tr>
<td>311</td>
<td>The phone failed to download the setup app due to an authentication failure. Contact your IT help desk for assistance.</td>
<td>The phone was unable to download the setup app due to authentication failure. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
<tr>
<td>312-313</td>
<td>The setup app encountered a program failure. Contact your IT help desk for assistance.</td>
<td>The setup app that the phone was trying to load contains a program error. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance. Provide them with the exact code of the error you encountered.</td>
</tr>
<tr>
<td>314</td>
<td>The setup app contains an invalid certificate. Contact your IT help desk for assistance.</td>
<td>There is a certificate error with the setup app. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
<tr>
<td>315</td>
<td>The setup app contains an invalid signature. Contact your IT help desk for assistance.</td>
<td>The signature of the setup app is invalid. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
</tbody>
</table>
### Issue code

<table>
<thead>
<tr>
<th>Message displayed</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>316</strong> The setup app contains an invalid checksum. Contact your IT help desk for assistance.</td>
<td>The signature of the setup app is invalid. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
<tr>
<td><strong>317</strong> The setup app has failed its name validation. Contact your IT help desk for assistance.</td>
<td>The name validation of the setup app has failed. This is very unlikely to happen, but if it does, contact your conferencing service provider for assistance.</td>
</tr>
</tbody>
</table>

### 11.3 Decommissioning and disposing of the phone

Ensure that faulty devices are disposed of in an appropriate way, according to local regulations.

**About this task**
The Dolby Conference Phone Support website includes a disposal guide about how to properly decommission and dispose of the phone.

**Procedure**

2. Click the **Support** tab.
3. Scroll down to **Decommissioning and Disposal Process** and then click the disposal guide.
Glossary

API
Application programming interface. A set of functions that can be used to access the functions of an operating system or other type of software.

Bluetooth LE
Bluetooth low energy. A chip technology that produces radio waves to connect a device to other Bluetooth devices. The low-energy version uses less power than standard Bluetooth, but maintains a similar communication range.

CLI
Command-line interface.

DHCP
Dynamic Host Configuration Protocol.

DNS
Domain Name System. An Internet service that translates Internet domain and host names to IP addresses and conversely. DNS automatically converts between the name entered in a web browser and the IP addresses of the web server hosting the site whose URL is entered in the web browser.

DNS SRV
Domain Name System service record. A service record (SRV record) defines the location (the host name and port number) of a server in a Domain Name System (DNS).

DoS
Denial of service. Events that render systems on a computer network temporarily unusable. DoS can happen accidentally as the result of actions taken by network users, but is often malicious.

DSCP
Differentiated Services Code Point. An IP header field that allows a router to provide different levels of service to different types of network traffic.

DSP
Digital signal processor. A specialized microprocessor optimized for digital signal processing.

DTMF
Dual-tone multifrequency. A system that is used by touch-tone telephones to assign a specific frequency (consisting of two separate tones) to each key so that it can easily be identified by a microprocessor.

FTP

HTTP
HTTPS
Hypertext Transfer Protocol Secure. An application protocol for secure communication over a network and the Internet that provides authentication of websites and keeps user information private.

IEEE
Institute of Electrical and Electronics Engineers.

iLBC
Internet low bit-rate codec. An open-source royalty-free narrowband speech audio coding format codec and reference implementation.

IP
Internet Protocol.

IP address
Internet Protocol address. A numerical identifier assigned to a device that is a member of a network that uses the Internet Protocol for communication.

JSON
JavaScript Object Notation. A lightweight data-interchange format that is easy for humans to read and write, and for machines to parse and generate.

kbps
Kilobits per second.

LAN
Local area network.

LDAP
Lightweight Directory Access Protocol. An application protocol for querying or modifying items in corporate directories that allows sharing of information about users, devices, and applications on a network.

LLDP
Link Layer Discovery Protocol. A vendor-neutral link layer protocol for Ethernet network devices such as switches, routers, and wireless LAN access points to announce information about themselves to other nodes on the network and store the information they discover, as defined in IEEE 802.1AB.

MAC address
Media access control address. A unique identifier assigned to a network interface for communications on a network. Media access control (MAC) addresses are typically assigned by the network interface manufacturer.

MPEG
Moving Picture Experts Group. An ISO/IEC working group that develops video and audio encoding standards. Also the name of a family of digital video and audio coding standards.

NAT
Network Address Translation. An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.
NTLMv2
A Microsoft security protocol that provides authentication, integrity, and confidentiality to users. NTLMv2 is part of Windows NT LAN Manager, which is a suite of security protocols.

NTP

PAC
Proxy automatic configuration. A file that defines how web browsers and other user agents can automatically choose the appropriate proxy server (access method) for fetching a given URL.

PBX
Private branch exchange. A phone system that is delivered as a hosted service.

PEM
Privacy-enhanced Electronic Mail. A file format for security certificates in email communication.

PoE
Power over Ethernet. A solution in which an electrical current is run to networking hardware over Ethernet category 5 or higher data cabling.

PSTN
Public switched telephone network. A circuit-switched telephone network operated by national, regional, or local operators.

RTCP

RTP

SBC
Session border controller. A piece of network equipment or a collection of functions that controls real-time session traffic at the signaling, call control, and packet layers as they cross a notional packet-to-packet network border between networks, or between network segments.

SIP
Session Initiation Protocol. An application-layer communications protocol used for signaling and controlling communications sessions.

SNMP

SRTP
Secure Real-time Transport Protocol. An RTP (Real-time Transport Protocol) profile that provides encryption, message authentication, and integrity, and replay protection to the RTP data in both unicast and multicast applications.
SSH
Secure Shell protocol. An encrypted network protocol for secure data communication, remote command-line log-in, remote command execution, and other secure network services between two networked computers.

SSL
Secure Sockets Layer. A security protocol that works at a socket level.

TCP/IP
Transmission Control Protocol/Internet Protocol. Communications protocols that specify how data should be formatted, addressed, transmitted, routed, and received at the destination. Part of the Internet protocols communications suite.

TLS
Transport Layer Security. A cryptographic protocol designed to provide communications security over a computer network.

TLV
Type length value. Within data communication protocols, a format for encoding optional information.

UDP
User Datagram Protocol. A communications protocol that uses no handshaking dialogues to establish a connection with the remote host. The User Datagram Protocol is a member of the Internet protocol suite.

UI
User interface.

URI
Uniform Resource Identifier. A group of characters identifying a resource on a network (typically, the Internet).

VLAN
Virtual LAN. Any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

VoIP
Voice over Internet Protocol. A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks.

WPAD
Web Proxy Automatic Discovery. An Internet protocol that enables a web browser to automatically connect to a cache server (or proxy server) location in a network to retrieve stored web pages more quickly by than leaving the network to request the web page from the site of the originating web server.