Dolby Conference Phone Version 4.5

Configuration Guide for iMeet

29 January 2020

Notices

Copyright

Trademarks

Patents

Contents

Introduction

Deploying the Dolby Conference Phone with iMeet is a multi-step process that involves preparing your network, Dolby Conferencing Console, or your provisioning server, and configuring the iMeet conferencing app.

- About this guide
- New in this version
- Related documentation
- Documentation feedback
- Solution architecture

1.1 About this guide

This document provides instructions for configuring the Dolby Conference Phone to work with iMeet. Use this document to guide you through the deployment process and ensure a successful and timely deployment at your site.

Before you begin deployment, make sure that you have copies of the related documentation. You may need to refer to other documents for more information and specific instructions.

1.2 New in this version

Dolby Conference Phone software (version 4.5) does not include any updates to this document.

1.3 Related documentation

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

These documents are available:

- *Dolby Conference Phone Administrator's Guide*

  This guide explains how to set up and provision the Dolby Conference Phone.
- *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 for iMeet*

  This guide describes how to use the basic and advanced phone features, and how to customize the phone.
- *Dolby Conference Phone Third-Party Software Guide*

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

1.4 Documentation feedback

If you have comments or feedback about this documentation, send us an email at dolbyvoicedocs@dolby.com.

1.5 Solution architecture

Before you begin the deployment process, make sure that you understand what is involved and how you can make the process go more smoothly.

Components

A deployment of the Dolby Conference Phone for iMeet utilizes a number of components. Understanding what they are and how they interact with each other can make the deployment processes easier, and may help you with troubleshooting later.

The key components required for deployment are listed in this table.

Component	Description
App deployment server	PGi hosts an app deployment server in its service infrastructure. The app deployment server contains the conferencing app. The Dolby Conference Phone downloads the conferencing app from the app deployment server through Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) when it boots up for the first time. The phone also periodically checks for and automatically downloads new versions. If an HTTP proxy is required for connecting the phone to the app deployment server, the phone can utilize the HTTP proxy to download the conferencing app. PGi deploys new versions of the conferencing app when they are available.
iMeet conferencing app	The conferencing app is hosted on the app deployment server.
Dolby Conference Phone	Dolby Conference Phones are deployed at your site. Based on its configuration, the phone downloads the conferencing app from the app deployment server. ⚠️ **Important:** The iMeet conferencing app version 1.0 is compatible with Dolby Conference Phone software version 3.1 or later. If the phone does not use software version 3.1 or later, you must upgrade the phone. For instructions, see the *Dolby Conference Phone Administrator's Guide*.
Service back end enabled for Dolby Voice	The service back end enabled for Dolby Voice is the service infrastructure created and maintained by PGi. The conferencing app uses HTTP, WebSocket, Session Initiation Protocol (SIP), and Real-time Transport Protocol (RTP) to communicate with the service back end.
Dolby Conferencing Console or other provisioning server	The provisioning server allows for flexibility in installing, upgrading, maintaining, and configuring the Dolby Conference Phone at scale. The provisioning server is typically located at your site and is managed by your IT group. The Dolby Conference Phone supports File Transfer Protocol (FTP), HTTP, and HTTPS for provisioning; it also supports automatic provisioning server discovery through a Domain Name System (DNS) SRV record.
Proxy server	In certain customer environments, an HTTP proxy server may be required to allow network clients to connect to an Internet server. The Dolby Conference Phone supports the HTTP proxy server, which can be either statically configured or dynamically configured through a proxy automatic configuration (PAC) file.

Figure 1: On-premise deployment
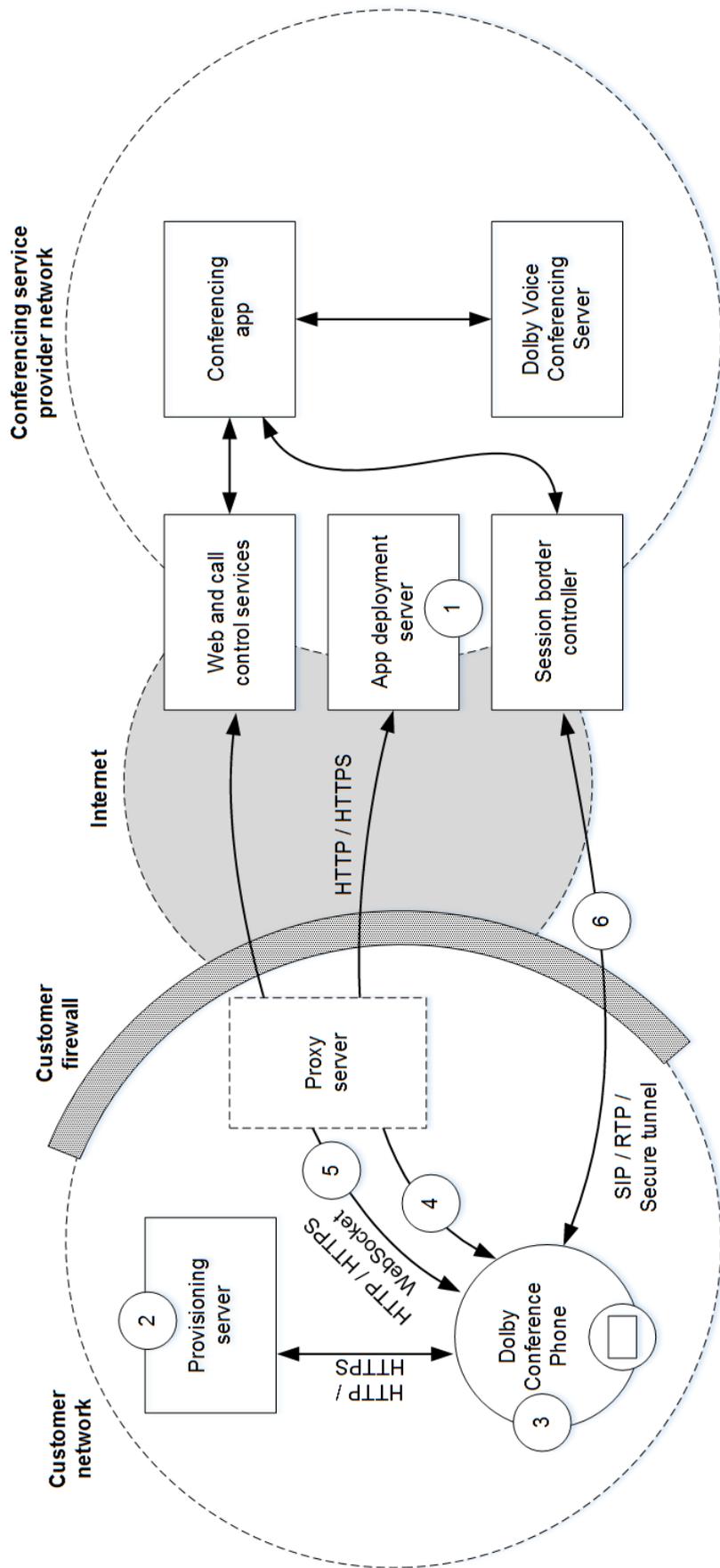
1. PGi deploys the conferencing app on the app deployment server.

2. Configuration profiles on Dolby Conferencing Console or your provisioning server enable the phone to connect to the PGi infrastructure.

3. The phone connects to the provisioning server to retrieve configuration files.

4. The phone accesses the app deployment server and downloads the conferencing app. Once the download is complete, the phone loads the conferencing app.

5. The conferencing app uses HTTP and WebSocket to interact with the PGi web and call-control services.

6. The responding instructions from the PGi web and call-control services connect the phone to the infrastructure to join an audio conference.

1.5.1 Provisioning phones

An easy way to set up and use the Dolby Conference Phone 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.

Using a provisioning server to configure phones

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 two choices:

- Use Dolby Conferencing Console as the provisioning server for phones.
- Set up an FTP, HTTP, or HTTPS server as the provisioning server for phones.

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

What is Dolby Conferencing Console?

Dolby offers Dolby Conferencing Console, a web-based dashboard and management portal powered by a highly secure and scalable back-end server.

The Dolby Conferencing Console replaces manual, time-consuming configuration and provisioning tasks with a streamlined and automated bulk-provisioning process. It also provides real-time operational awareness via detailed device and network analytics and reports, enabling IT to track assets, proactively monitor systems, and remotely diagnose and resolve issues.

Because the Dolby Conferencing Console acts as a provisioning server, you can avoid the complex task of setting up your own provisioning server. In addition, a RESTful application programming interface (API) and SNMPv2 protocol simplify integration into PGi enterprise network management platforms.

For more information about setting up and using Dolby Conferencing Console or a provisioning server to configure phones, see the *Dolby Conferencing Console Operations and Management Guide* and the *Dolby Conference Phone Administrator's Guide*.

Supported provisioning protocols

The Dolby Conference Phone supports FTP, HTTP, and HTTPS for provisioning. HTTPS is the recommended protocol, because it provides the best performance and security.

For more information, see the *Dolby Conferencing Console Operations and Management Guide* and the *Dolby Conference Phone Administrator's Guide*.

Configuration parameters

You must set certain configuration parameters to connect the phone to the app deployment server and download the conferencing app.

For more information, see Setting iMeet configuration parameters on page 23.

Automatic Local Setup

The Dolby Conference Phone can automatically discover Dolby Conferencing Console or the provisioning server on the network using a DNS SRV record. This simplifies the deployment of the phone and minimizes configuration errors. To take advantage of this feature, you must plan ahead.

For more information, see the *Dolby Conference Phone Administrator's Guide*.

1.5.2 TLS configuration

The Dolby Conference Phone supports Transport Layer Security (TLS).

The phone uses HTTPS to download configuration parameters and firmware from Dolby Conferencing Console or your provisioning server. It also uses HTTPS to download the conferencing app from the app deployment server.

The conferencing app communicates with PGi web and call-control services using HTTPS or Secure WebSocket.

In all these scenarios, the phone must be installed with adequate CA certificates to allow for successful TLS negotiation. The software on the phone already includes the CA certificates needed for the iMeet conferencing app. The phone can load additional CA certificates. Dolby Conferencing Console also supports easy-to-use mechanisms for deployment.

1.5.3 iMeet conferencing app

The iMeet conferencing app provides a customized interface for iMeet.

Configuring the conferencing app is the final step of the deployment process. Once finished, you and your end users are ready to host and join iMeet meetings from the phone.

Related information

2

Configuration procedures

After you configure the Dolby Conference Phone network settings and options, you can activate the phone with iMeet.

- Plugging in and setting up the phone automatically
- Configuring 802.1X
- Opening the phone web interface
- Configuring the operational mode
- Configuring Network Time Protocol (NTP)
- Proxy configuration
- Voice VLAN settings
- Configuring the firewall
- Setting the phone display name
- Setting phones to personal mode
- Reserved configuration parameters

## 2.1 Plugging in and setting up the phone automatically

Each Dolby Conference Phone requires a wired network connection, preferably supporting Power over Ethernet (PoE). Once your phone is plugged in, many settings may be automatically detected.

Procedure

1. Plug in the phone.

   If the customer network is already set up with either Dynamic Host Configuration Protocol (DHCP) option 66 or DNS SRV record, the phone automatically detects the presence of Dolby Conferencing Console or a provisioning server, which saves you having to manually enter data.

   If the customer network is not set up, you see this screen:
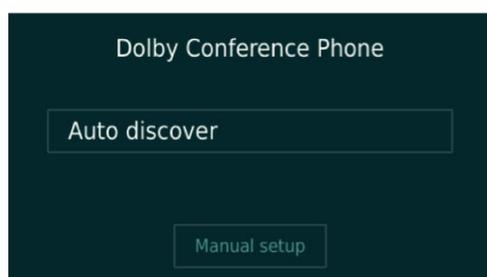
2. Select **Manual setup**, and follow the screen prompts if automatic discovery is not available on the customer network.

2.2 Configuring 802.1X

If your network requires 802.1X during the network setup portion of the setup wizard, you must complete 802.1X setup.

About this task

Depending on the 802.1X configuration, you may need to accept the authentication server certificate. The setup wizard guides you through the process and detects many of the settings for you, including your virtual LAN (VLAN) and IP network settings. In this figure, the Dolby Conference Phone has detected those settings on initial setup.
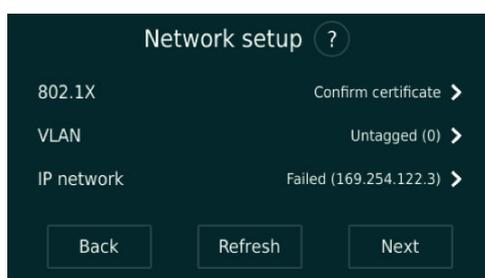
If you see this screen, you can configure some 802.1X options directly in the wizard.

You can also upload certificates to the Dolby Conference Phone using the phone web interface.

> 📑 **Note:** If you use a self-signed authentication certificate, or a certificate authority that is not in the default Dolby Conference Phone trusted certificate authority list, we recommend that you use local setup with the Dolby Conferencing Console for 802.1X. The Dolby Conferencing Console makes it easier to distribute the certificate. For more information, see 802.1X deployment with Dolby Conferencing Console.

Procedure

1. If a public key infrastructure-based authentication method is selected by the authentication server, you are prompted to review the server certificate information.
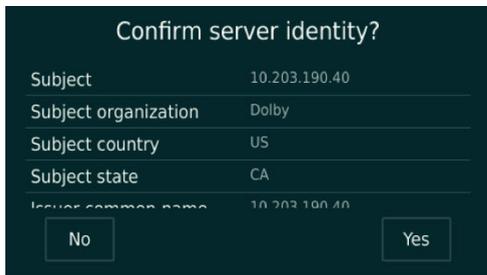
2. Enter the user name and password when the server requires credentials for authentication. Depending on the authentication server configuration, you may be prompted to enter authentication credentials before you accept the server certificate.

2.3 Opening the phone web interface

Enter the phone IP address in your web browser to open the phone web interface.

Prerequisites

You must have a network-connected desktop or laptop computer with a web browser supporting HTML5 installed. (Modern versions of Internet Explorer, Firefox, Chrome, and Safari are supported.)
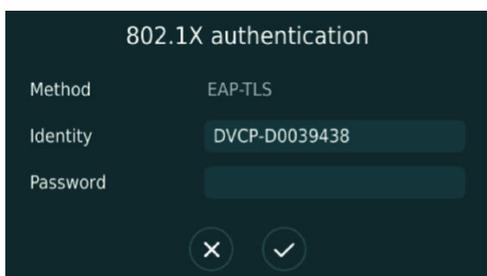
The web browser will be used to configure the phone, so it must have IP network connectivity to the Dolby Conference Phone.

Procedure

1. From the phone home screen, tap this sequence:

     > > **About** > **General**

2. Scroll down until you see the IP address.

3. Enter this URL in the browser address bar.

    If a security warning displays, accept the warning and proceed.

```
https://your-phone-IP-address
```

4. Log in to the Dolby Conference Phone using the default credentials:

   - **Username** = *admin*
   - **Password** = *1739*
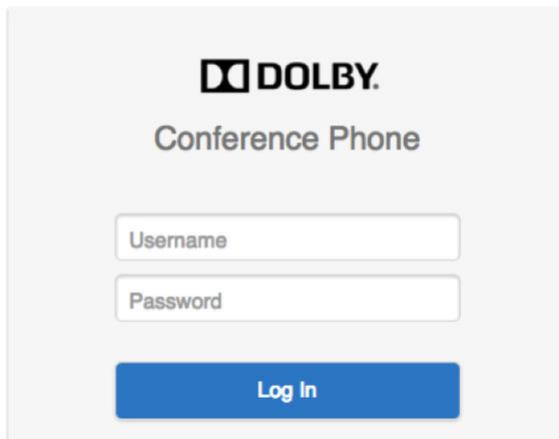
2.4 Configuring the operational mode

You can configure the Dolby Conference Phone for either Conferencing mode or Dual mode.

About this task

Conferencing mode

Use if you plan on using your phone with the iMeet only.

Dual mode

Use if you want to integrate IP private branch exchange (PBX) with the iMeet.

Configuration parameter description	Configuration parameter name
Selects the operational mode	`Features.OperationMode`

Procedure

1. Go to **Settings** > **Features** in the phone web interface.

2. Choose a value for **Operation Mode**.

   In Dual mode, the home screen appears as shown in this figure.
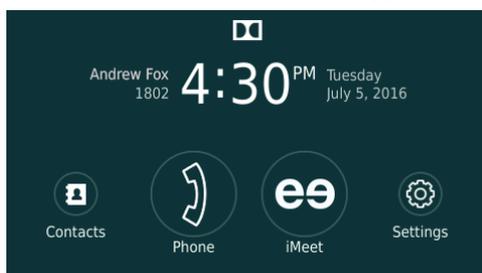
2.5 Configuring Network Time Protocol (NTP)

The Dolby Conference Phone uses a time server to synchronize the clock. You must specify Network Time Protocol (NTP) servers in the network settings so that you can use features like the calendar and other functionality dependent on accurate time and date.

About this task

We recommend that the Dolby Conference Phone and the Intel Next Unit of Computing (NUC) reference the same NTP server. Default NTP servers are available. However, if your network blocks access to NTP servers on the Internet, you must configure a local NTP server.

Procedure

1. Click the **+** to open the network settings parameters.
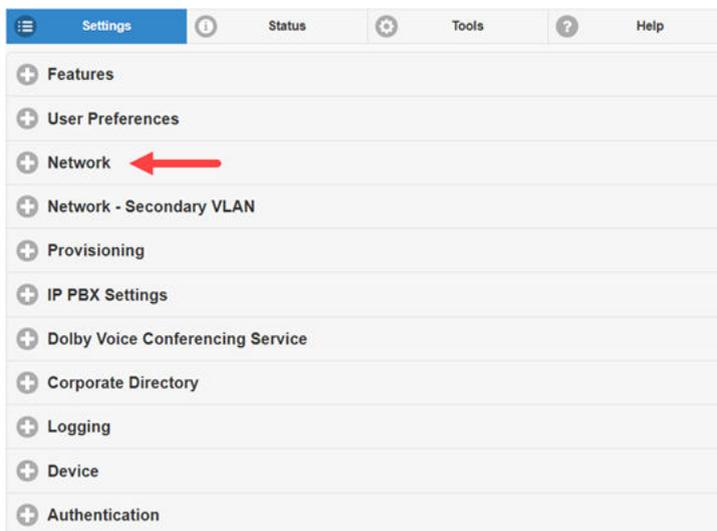
2. Click the **+** to open the **NTP** section.

3. Enter the server addresses provided by your local system administrator.

What to do next

For more information about configuring NTP, see the *Dolby Conference Phone Administrator's Guide*.

2.6 Proxy configuration

Some network configurations and phone software require that you specify a proxy server.

📄 **Note:** Depending on your network settings and phone software version, this procedure may not be necessary. For a complete description of this functionality, see the *Dolby Conference Phone Administrator's Guide*.

The information listed in this table is required.

Attributes	Description
Proxy server address	IP address.
Proxy server credentials: User name and password	If the proxy server requires devices to authenticate before being allowed access, then a user name and password are required.

In many cases, networks require clients to go through a proxy server to communicate with Internet services. The phone supports the HTTP proxy in these scenarios:

- The phone downloads its configuration and firmware from the provisioning server or the Dolby Conferencing Console.
- The phone downloads the conferencing app from the app deployment server.
- The conferencing app communicates with the BlueJeans web and call-control services using HTTPS and secure WebSocket.

The Dolby Conference Phone supports PAC and Web Proxy Automatic Discovery (WPAD) for automatic proxy configuration.

You can configure the proxy server in two ways:

For more information about PAC and WPAD, see the *Dolby Conference Phone Administrator's Guide*.

2.6.1 Specifying a proxy configuration with a PAC URL

Configure a PAC URL that instructs the Dolby Conference Phone to automatically discover the proxy settings based on the target URL.

About this task

Dolby Conference Phone supports the WPAD method for locating the PAC URL. Enable this to trigger automatic proxy discovery in the network. This is the recommended mechanism, because it allows for more flexibility in dynamically allocating proxy resources in your network.

Additionally, you can use one of these methods to specify the proxy configuration:

Procedure

- Use the Dolby Conference Phone web interface:
    a) Navigate to **Settings** > **Network** > **Proxy**.
    b) Switch **Enable WPAD** to **On**, and then complete these steps:
        - In the **Proxy Server Login Name** field, type a proxy authentication user name.
        - In the **Proxy Server Login Password** field, type a proxy authentication password.

        If your network does not implement WPAD, leave this parameter off and manually set the PAC URL by using the **PAC Configuration URL** field as described in the next step.
    c) If your network does not implement PAC, leave **Enable WPAD** off (described in the previous step) and complete these steps:
        - In the **PAC Configuration URL** field, enter the PAC URL.
        - Optional: In the **Proxy Server Login Name** field, type a proxy authentication user name.
        - Optional: In the **Proxy Server Login Password** field, type a proxy authentication password.
- Use the Dolby Conferencing Console:
    a) From the Dolby Conferencing Console, select a device, and then click the **Edit device configuration** button.

    b) If your network supports WPAD, from **Network** > **Proxy**, drag **Enable WPAD** to the device configuration. Switch `Network.Proxy.AutoDiscover` to **ON**, and then complete these steps:
        - Drag **Proxy Server Login Name** to the device configuration. In the `Network.Proxy.UserName` field, type a proxy authentication user name.
        - Drag **Proxy Server Login Password** to the device configuration. In the `Network.Proxy.Password` field, type a proxy authentication password.

        If your network does not implement WPAD, leave this parameter off and manually set the PAC URL by using `Network.Proxy.PacUrl` as described in the next step.
    c) If your network does not support WPAD, navigate to **Network** > **Proxy** and then complete these steps:

- Drag **PAC Configuration URL** to the device configuration. In the `Network.Proxy.PacURL` field, type the PAC URL.

  The phone uses the `Network.Proxy.PacUrl` parameter to determine which proxy server to communicate with in the BlueJeans infrastructure.
- Optional: Drag **Proxy Server Login Name** to the device configuration. In the `Network.Proxy.UserName` field, type a proxy authentication user name.
- Optional: Drag **Proxy Server Login Password** to the device configuration. In the `Network.Proxy.Password` field, type a proxy authentication password.

2.6.2 Specifying a conferencing app-specific proxy server

Configure a conferencing app-specific proxy server using `Dvms.Proxy.x` configuration parameters.

About this task

If your network does not implement a PAC file, configure a conferencing app-specific proxy server. If both proxy configuration methods are implemented, the `Dvms.Proxy.x` parameters for conferencing app network communications are used; the PAC file is not utilized.

For more information on proxy setup, see the *Dolby Conference Phone Administrator's Guide*.

Use one of these methods to configure a conferencing app-specific proxy server.

Procedure

- Use the phone web interface:
  a) Navigate to **Settings** > **Dolby Voice Conferencing Service** > **Proxy**.
  b) In the **Proxy Address** field, type the proxy address.
  c) Set the **Proxy Port** by typing in the value or using the slider to set the value.
  d) In the **Proxy User** field, type the proxy authentication user name.
  e) In the **Proxy Password** field, type the proxy password.
- Use Dolby Conferencing Console:
  a) From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button.
  b) From **Dolby Voice Conferencing Service** > **Proxy**, drag **Proxy Address** to the device configuration.

  This parameter specifies a statically configured proxy server address, dedicated to the conferencing app. After configured, the phone goes through the specified proxy server to download the conferencing app. All network communications initiated from the conferencing app go through this proxy server.
  c) In the `Dvms.Proxy.Address` field, type the proxy address.
  d) Drag **Proxy Port** to the device configuration.

  By default, this parameter is set to 8080. It specifies the network port for the proxy server.
  e) Set `Dvms.Proxy.Port` by typing in a value or using the slider to set a value.
  f) Drag **Proxy User** to the device configuration.
  g) In the `Dvms.Proxy.User` field, type the proxy authentication user name.
  h) Drag **Proxy Password** to the device configuration.
  i) In the `Dvms.Proxy.Password` field, type the proxy authentication password.

2.7 Voice VLAN settings

If the VLAN and LAN settings are not configured automatically, enter the LAN or VLAN information in the network settings. The phone can be configured on single or dual-VLAN networks.

Prerequisites

You will need information about the voice and data VLAN settings for your organization. See this table for the information that is required.

Attributes	Description
Voice and data VLAN.	Determine whether there are separate voice and data VLANs.
Do the LAN switches have Link Layer Discovery Protocol (LLDP) enabled?	If your network is configured this way, the phone is placed on the voice VLAN automatically through LLDP discovery. If you do not want to place your phone on the voice VLAN, you must disable LLDP.
Does the Voice VLAN have access to the Internet via these proxies?	If no, the phone cannot be placed in the voice VLAN and must be placed in the data VLAN. 📰 **Note:** You may have to disable LLDP to achieve this.

About this task

The Dolby Conference Phone supports LLDP VLAN autodiscovery. By default, the phone uses LLDP to detect voice VLAN. If VLAN is available, the phone places itself on the voice VLAN.

Depending on your network settings and phone software version, this procedure may not be necessary. Note that:

- If your network does not implement voice VLAN and data VLAN segregation, then ignore this topic and move on.
- If your network implements voice VLAN, but does not restrict Internet access from the voice VLAN, then ignore this topic and move on.
- If you are using **Conferencing Only Mode** and your voice VLAN restricts Internet access, we recommend using the data VLAN by disabling LLDP VLAN autodiscovery.
- If you are using **Dual Mode**, you must use the voice VLAN and allow Internet access from the voice VLAN.

For a complete description of this functionality, including additional VLAN options, see the *Dolby Conference Phone Administrator's Guide*.

Procedure

Use one of these procedures to configure VLAN and LAN settings:

- Use the Dolby Conferencing Console software:

    a) From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button.

- Use the phone web interface:

What to do next

If your VLAN settings are configured to be discoverable, use the phone web interface to enable LLDP.

📰 **Note:** This parameter cannot be set from Dolby Conferencing Console.

Navigate to **Network** > **Services** and switch **Enable LLDP** to **On** .

2.8 Configuring the firewall

All Dolby Voice clients, including the Dolby Conference Phone, must connect to the Dolby Voice-enabled back end server through either a direct SIP connection or a SIP connection over a secure tunnel.

To ensure that real-time packet traffic can be initiated with the backend server enabled for Dolby Voice, see the *iMeet deployment guide* (created and provided by PGi) for information about which firewall ports and outbound destination address (ranges) need to be opened.

2.9 Setting the phone display name

The display name on the phone will appear in the conference roster when the phone joins conference calls, so this should be configured to a meaningful name.

Procedure

Use one of these procedures to set the display name of the phone:

- From the Dolby Conferencing Console software:

  a) From Dolby Conferencing Console, select a device, and then click the **Edit device configuration** button.

  b) From **IP IPBX** > **Account**, drag **Display name** to the device configuration.

  c) In the `Sip.Account.DisplayName` field, type a device name.

- From the phone web interface:

  a) Click the **+** to open the **IP PBX Settings** > **Account** section.

  b) In the **Display Name** field, enter the device name.

2.10 Setting phones to personal mode

End users can host iMeet meetings from the Dolby Conference Phone in conference rooms that are shared by many different people, or from a personal office.

About this task

As the administrator, you choose the mode of phones. Set the mode for the phone based on where the phone is physically located and who will use it.

Personal mode

Use this mode for personal phones that are in executive or private offices.

By default, personal mode is disabled.

Public mode

Use this mode for phones that are in conference rooms and are shared by many different people.

By default, the phone functions in public mode.

No setup by a host or participants is required.

When personal mode is enabled, hosts can save their access number and chairperson passcode on the Dolby Conference Phone. They can avoid reentering information each time they host a meeting.

You can switch the phone from public mode to personal mode from either Dolby Conferencing Console or the phone web interface:

Procedure

- Use the Dolby Conferencing Console software:
  a) Select a device, and then click the **Edit device configuration** button.

  b) From **Features** > **Personal Mode**, drag **Set phone for personal use** to the device configuration.
  c) Switch **Features.PersonalMode.Enabled** to **ON**.
- Use the phone web interface:
  a) Navigate to **Features** > **Personal Mode**.
  b) Switch **Set phone for personal use** to **On**.

2.11 Reserved configuration parameters

Certain configuration parameters are utilized by the iMeet app and should not be included in any provisioning server configuration.

Do not use these configuration parameters:

- `Dvms.Custom.Parameter1`
- `Dvms.Custom.Parameter2`
- `Dvms.Custom.SecureParameter1`

For more information, see

3

Configuring iMeet

After the phone is connected to the network and either Dolby Conferencing Console or your provisioning server, you are ready to configure iMeet.

- Setting iMeet configuration parameters
- Known issue with v3.0.0 and 3.0.1 firmware
- Utility functions

3.1 Setting iMeet configuration parameters

The phone does not connect to iMeet by default. You must configure the phone to automatically connect to iMeet.

About this task

We recommend that you use Dolby Conferencing Console to manage your devices, but the information in this topic applies when using a provisioning server or the phone web interface.

Procedure

Add these configuration parameters to the device configuration with these settings:

Table 1: Configuration parameters required for iMeet

Parameter name	Setting	Task
`Dvms.Server.Address`	Enter the address or domain of the Dolby Voice web server with your iMeet conferencing application files. The phone will download the files from this location (for example, https://dcp-download.pgibob.com/imeet-app/).	From Dolby Conferencing Console: 1. From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button. 2. From **Dolby Voice Conferencing Service** > **Server**, drag **Dolby Voice Conferencing Server Address** to the device configuration. 3. In the **Dvms.Server.Address** field, type the URL. From the phone web interface: 1. Navigate to **Settings** > **Dolby Voice Conferencing Service** > **Server**. 2. In the **Dolby Voice Conferencing Server Address** field, type the URL.
`Dvms.Service.Logo`	Set this parameter to **Disabled**.	From Dolby Conferencing Console: 1. From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button. 2. From **Dolby Voice Conferencing Service** > **Service**, drag **Logo** to the device configuration. 3. In the **Dvms.Service.Logo** drop-down list, select **Disabled**. From the phone web interface: 1. Navigate to **Settings** > **Dolby Voice Conferencing Service** > **Service**. 2. In the **Logo** drop-down list, select **Disabled**.

Table 1: Configuration parameters required for iMeet (continued)

Parameter name	Setting	Task
`Dvms.Service.Name`	Set the Dolby Voice conferencing service name that will appear on the home screen of the device. Set this parameter to *iMeet*.	From Dolby Conferencing Console: 1. From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button. 2. From **Dolby Voice Conferencing Service** > **Service**, drag **Name** to the device configuration. 3. In the **Dvms.Service.Name** field, type *iMeet*. From the phone web interface: 1. Navigate to **Settings** > **Dolby Voice Conferencing Service** > **Service**. 2. In the **Name** field, type *iMeet*.
`Dvms.Service.Provider`	Select a service provider from the list. Set this parameter to **Custom**.	From Dolby Conferencing Console: 1. From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button. 2. From **Dolby Voice Conferencing Service** > **Service**, drag **Service provider** to the device configuration. 3. In the **Dvms.Service.Provider** drop-down list, select **Custom**. From the phone web interface: 1. Navigate to **Settings** > **Dolby Voice Conferencing Service** > **Service**. 2. In the **Service provider** drop-down list, select **Custom**.

Table 1: Configuration parameters required for iMeet (continued)

Parameter name	Setting	Task
Dvms.Service.Type	Select the conferencing service provider application type. Set this parameter to **App**.	From Dolby Conferencing Console: 1. From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button. 2. From **Dolby Voice Conferencing Service** > **Service**, drag **Application type** to the device configuration. 3. In the **Dvms.Service.Type** field, select **App**. From the phone web interface: 1. Navigate to **Settings** > **Dolby Voice Conferencing Service** > **Service**. 2. In the **Application type** field, select **App**.
Features.Operation Mode	Set this parameter to **Conferencing Only Mode** or **Dual Mode**. For more information about the differences in these operations modes, see Configuring the operational mode on page 14.	From Dolby Conferencing Console: 1. From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button. 2. From **Features**, drag **Operation Mode** to the device configuration. 3. In the **Features.OperationMode** field, select **Conferencing Only Mode** or **Dual Mode**. From the phone web interface: 1. Navigate to **Settings** > **Features**. 2. In the **Operation Mode** drop-down list, select **Conferencing Only Mode** or **Dual Mode**.

Results

You are ready to start hosting and joining iMeet meetings from the phone. For more information, see *Dolby Conference Phone User's Guide for iMeet*.

Note: If you are using version 3.0.0 or 3.0.1 firmware, see Known issue with v3.0.0 and 3.0.1 firmware on page 25. Some additional steps are still required.

3.2 Known issue with v3.0.0 and 3.0.1 firmware

There is a known firmware issue in version 3.0.0 and 3.0.1 of the Dolby Conference Phone that causes iMeet meetings to fail to start.

In this situation, after the phone reboots, the first iMeet calls fails. A **Connecting to User's meeting** message displays, the LED halo turns blue, and then a time-out error displays saying the call cannot be completed. After three calls, all subsequent calls work normally.

To workaround this issue, change the configuration parameters as listed in this table.

Table 2: Configuration parameters required for workaround

Parameter name	Setting	Task
`Sip.Pbx.OnlyAcceptCallServerEvents`	Set this parameter to **off** (or **false**).	From Dolby Conferencing Console: 1. From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button. 2. From **IP PBX Settings** > **Server**, drag **Only accept call server SIP events** to the device configuration. 3. Switch **Sip.Pbx.OnlyAcceptCallServerEvents** to **OFF**. From the phone web interface: 1. Navigate to **Settings** > **IP PBX Settings** > **Server**. 2. Switch **Only accept call server SIP events** to **Off**.
`Sip.Pbx.Domain`	If the phone is set to **Conferencing Only Mode**, then you must enter a value, but it can be anything.	From Dolby Conferencing Console: 1. From Dolby Conferencing Console, select a device and then click the **Edit device configuration** button. 2. From **IP PBX Settings** > **Server**, drag **SIP Domain Name** to the device configuration. 3. In the **SIP Domain Name** field, enter any domain name. From the phone web interface: 1. Navigate to **Settings** > **IP PBX Settings** > **Server**. 2. In the **SIP Domain Name** field, enter any domain name.

3.3 Utility functions

The iMeet app uses certain configuration parameters for local storage on the Dolby Conference Phone.

As explained in Reserved configuration parameters on page 21, you should never provision these configuration parameters. However, you can use them to perform certain utility functions by manually clearing them from the phone web interface.

`Dvms.Custom.Parameter1`
   Clears the recent calls list

`Dvms.Custom.Parameter2`
   Clears all iMeet app internal storage

`Dvms.Custom.SecureParameter1`
   Resets the iMeet app to its initial state

4

Troubleshooting

If you encounter an issue with the Dolby Conference Phone, we recommend that you attempt basic troubleshooting before you contact Support.

- Error messages
- Viewing information about the iMeet conferencing app
- Support contacts
- Manually overriding DHCP assigned DNS settings

4.1 Error messages

Error messages describe the causes and possible solutions to problems.

Table 3: Issue types

Issue type	Action
Network issue	Check your network configuration, and confirm that the phone can connect the PGi infrastructure.
Invalid input issue	Check meeting details (URL, dial in host passcode, access number) in the PGi desktop application.

Table 4: Error messages

Error message	More information	Issue type
`Meeting not found`		
`The meeting could not be found. Verify that the contact has the correct meeting URL.`	The user provided a meeting URL that does not have a meeting associated with it.	Invalid input
`The meeting could not be found. Verify that the access number and host dial in passcode are still valid.`	The user provided an invalid access number and chairperson dial-in passcode combination.	Invalid input
`Incorrect host dial in passcode`		
`The host dial in passcode is incorrect. Verify the meeting information.`	The user provided an incorrect chairperson dial-in passcode.	Invalid input
`Cannot start meeting`		
`The meeting could not be started. Contact your IT administrator regarding this issue.`	There was a problem establishing a connection with the conference service.	Invalid input
`Unable to connect to the meeting. The connection to conference service timed out.`	While looking up the meeting information, the connection to the conference service timed out. Try again. If the problem persists, there is likely a problem with the networking setup or conditions.	Network
`Cannot join meeting`		
`Unable to connect to the meeting. The connection to conference service timed out.`	While looking up the meeting information, the connection to the conference service timed out. Try again. If the problem persists, there is likely a problem with the networking setup or conditions.	Network
`Leaving meeting issue`		

Table 4: Error messages (continued)

Error message	More information	Issue type
`There was an issue leaving the meeting. Contact your IT administrator regarding this issue.`	There was a problem closing the connection with the conference service. This usually has no ill effect, but if the problem persists, it can indicate an incorrect networking setup or conditions.	Network
`Meeting connection issue`		
`There was an issue muting your phone. Try again. Contact your IT administrator if this issue persists.`	There was an issue reporting the phone mute status to the conference service. Trying again will probably correct the issue. If the problem persists, it can indicate a problem with the networking setup or conditions.	Network
`The meeting connection was lost. Try joining again. Contact your IT administrator regarding this issue.`	There was an unrecoverable issue with the connection to the conference service. Issue should be reported to the PGi support team.	Network
`There was an issue connecting to the meeting. Contact your IT administrator if this issue persists.`	There was an issue communicating meeting changes to the conference service. Trying again will probably correct the issue. If the problem persists, it can indicate a problem with the networking setup or conditions.	Network
`Connection timeout`		
`There was an issue with the meeting connection. The meeting information may not be updated. Contact your IT administrator if this issue persists.`	The phone is only partially connected to the conference service, so the meeting information may not be updated. Restarting the call should address the connectivity issue. If the problem persists, there is likely a problem with the networking setup or conditions.	Network
`There was an issue muting all participants. Try again. Contact your IT administrator if this issue persists.`	There was an issue requesting that all participants be muted by the conference service. Trying again will probably correct the issue. If the problem persists, it can indicate a problem with the networking setup or conditions.	Network

4.2 Viewing information about the iMeet conferencing app

You can view information about the iMeet conferencing app, such as the version number of the conferencing app or the loading status.

Procedure

1. From the phone user interface (UI), tap this sequence:

    > > **About** > **Status**

2. Scroll down, and then tap **Conferencing app**.

4.3 Support contacts

If you have a problem, we recommend that you review this document and the related documentation. If you cannot troubleshoot the problem on your own, contact PGi for support.

For additional information and support:

- Visit the iMeet Community (if included with your account).
- View video tutorials.
- Get the latest User Guides and Release Notes.

You can also send an email directly to iMeet Care:

North America: care@imeet.com
EMEA: emeacare@imeet.com
Asia Pacific: apcare@imeet.com
Japan: jpcare@imeet.com

4.4 Manually overriding DHCP assigned DNS settings

If you want to use another set of DNS settings, or if you do not have a valid DNS configuration, you can manually override the DHCP-assigned DNS settings.

About this task

You can manually assign the domain name, the DNS server address, and the alternative DNS server address.

📧 Note:

> When dual VLAN configuration is enabled, manual override is available only on the primary VLAN.

For more information, see the *Dolby Conference Phone Administrator's Guide*.

Procedure

1. From the phone home screen, tap this sequence:

     > > **Administrative Settings**

2. Enter the administrator password, and tap **Enter**.

3. Select **Network configuration** > **IP network**.

4. Enable **Manual DNS**.

5. Modify the **Domain name**, the **DNS server 1**, and the **DNS server 2**, as required, and tap ✔.

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.

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.

FTP
File Transfer Protocol. A network-based protocol designed for transferring data using a client-server architecture.

HTTP
Hypertext Transfer Protocol. An application protocol for hypermedia information systems, and the foundation for data communication for the World Wide Web.

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.

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 IP for communication.

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 local area network (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.

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
Network Time Protocol. A network protocol for clock synchronization on computers.

NUC
Next Unit of Computing. A small-form-factor personal computer designed by Intel.

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.

PKI

Public key infrastructure. A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

PoE

Power over Ethernet. A solution in which an electrical current is run to networking hardware over Ethernet category 5 or higher data cabling.

RTP

Real-time Transport Protocol. An IP network audio and video protocol.

SIP

Session Initiation Protocol. An application-layer communications protocol used for signaling and controlling communications sessions.

TCP

Transmission Control Protocol. A communications protocol that specifies 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.

UDP

User Datagram Protocol. A communications protocol that uses no handshaking dialogues to establish a connection with the remote host. UDP is a member of the IP suite.

VLAN

Virtual LAN. Any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

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.