DOLBY
VOICE

# Dolby Conferencing Console

## Operations and Management Guide

Version 2.1
29 October 2018

# Copyright



**Dolby Laboratories, Inc.**
1275 Market Street
San Francisco, CA 94103-1410 USA
Telephone 415-558-0200
Fax 415-645-4000
http://www.dolby.com

# Trademarks

Dolby and the double-D symbol are registered trademarks of Dolby Laboratories

The following are trademarks of Dolby Laboratories:

Dialogue Intelligence™
Dolby®
Dolby Advanced Audio™
Dolby Atmos®
Dolby Audio™
Dolby Cinema™
Dolby Digital Plus™
Dolby Digital Plus Advanced Audio™
Dolby Digital Plus Home Theater™
Dolby Home Theater®
Dolby Theatre®
Dolby Vision™
Dolby Voice®
Feel Every Dimension™
Feel Every Dimension in Dolby™
Feel Every Dimension in Dolby Atmos™
MLP Lossless™
Pro Logic®
Surround EX™

All other trademarks remain the property of their respective owners.

# Patents

This product is protected by one or more patents in the United States and elsewhere. For more information, including a specific list of patents protecting this product, please visit http://www.dolby.com/patents.

# End User Licensing Agreement

END-USER LICENSE AGREEMENT FOR DOLBY SOFTWARE

The following is Dolby's current version of the End User License Agreement ("EULA"). Dolby may modify this End User License Agreement: (A) immediately in any way which does not reduce or degrade Reseller's rights or benefits pursuant to the policy or (B) in all other instances, on forty five (45) days written notice; provided, however, that the End User License Agreement in effect at the time of the sale of any Product unit shall continue to govern such Product unit.

This EULA is a legal agreement between you (as an individual hereinafter referred to as "you" or "Customer") and Dolby Laboratories, Inc., a California Corporation, and Dolby International AB, a Swedish company residing in The Netherlands (collectively "Dolby") for the Dolby® software that accompanies this EULA, which includes computer software and may include associated media,

printed materials, "online" and electronic documentation (collectively, the "Software"). Dolby may be providing you with the Software pursuant to a separate agreement between you (or a third party such as your employer) and one of Dolby's licensees (a "Parent Agreement"). In the case of a conflict this EULA takes priority over the Parent Agreement and governs your use of the Software. YOU HEREBY AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT BY ACCEPTING THIS AGREEMENT, OR BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT DO NOT INSTALL, COPY, OR USE THE SOFTWARE.

1. LICENSE GRANT. Dolby grants you only those rights expressly granted to you in this EULA provided that you comply with all terms and conditions of this EULA.

   1.1 Software License Grant. Dolby grants you a nonexclusive, revocable, limited, non-transferable license to (a) install and run the Software solely for the purpose of using the Dolby Conference Phone or if applicable, accessing the conferencing service solutions provided under the Parent Agreement and (b) make one copy of the Software solely for backup or archival purposes.

   1.2 Documentation. You may make and use an unlimited number of copies of the documentation, if any, provided that such copies shall be used solely for your own use in association with the Software and are not to be republished nor distributed (in hard copy, electronic or any other form) beyond your premises or to any third party.

   1.3 Beta Materials. The following apply to any Software provided as “pre-release” or “beta:” (a) You shall identify errors, potential improvements, and provide other feedback to Dolby about the pre-release or beta Software as reasonably requested by Dolby, and (b) Dolby reserves the right not to commercially release pre-release or beta Software or, if it does so, to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, and other characteristics of the commercial release.

2. RESERVATION OF RIGHTS AND OWNERSHIP. Dolby reserves all rights not expressly granted to you in this EULA. The Software is protected by copyright, patent and/or other intellectual property laws and treaties and contains trade secrets of Dolby and its suppliers. Dolby and its suppliers own the title, copyright, and other intellectual property rights in the Software. Notwithstanding any statements to the contrary contained in any terms of sale for the Software, the Software is licensed, not sold and Dolby retains ownership of all copies of the Software.

3. LIMITATIONS ON LICENSE. You are expressly prohibited from using the Software in any manner not specifically authorized by Dolby in this EULA. You may not make any copies of the Software except and to the extent necessary for backup and archival purposes. You may not modify, create derivative works, reverse engineer, decompile, or disassemble the Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not rent, lease, lend or provide commercial hosting services with the Software. You may not delete, fail to reproduce or modify any patent, copyright, trademark or other proprietary rights notices which appear on or in the Software or documentation. No license, right, or interest in any Dolby trademark, trade name or service mark is granted to you pursuant to this EULA.

4. TERMINATION. Without prejudice to any other rights, Dolby may immediately terminate this EULA if you are in material breach of any of the terms or conditions of Sections 1-3 of this EULA which has not been remedied within 14 days of written notice from Dolby to you. In such event, you must immediately cease using the Software and destroy all copies of the Software and all of its component parts.

5. REPRESENTATIONS AND WARRANTIES.

   5.1 You represent, warrant, and covenant that your use of the Software will at all times comply with the terms of this EULA, applicable laws and regulations and that you will not install, use, access, or run the Software for purposes other than using the Dolby

Conferencing Console or if applicable, accessing the conferencing services provided under the Parent Agreement.

5.2 Dolby represents and warrants that (a) it owns or has the right to license the Software and (b) that the Software is complete, correct, effective, and capable of meeting the specifications included in the documentation, if any, provided under the Parent Agreement. Your sole remedy for breach of the foregoing representation in Section 5.2(b) shall be Dolby's commercially reasonable efforts to redeliver the affected Software.

6. DISCLAIMER OF WARRANTIES. EXCEPT AS OTHERWISE SET FORTH ABOVE, DOLBY MAKES NO WARRANTIES REGARDING THE SOFTWARE. FURTHER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, DOLBY AND ITS SUPPLIERS PROVIDE THE SOFTWARE AS IS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT, AND ANY WARRANTIES ARISING OUT OF COURSE OF DEALING, USAGE OR TRADE. THERE IS NO WARRANTY THAT THE SOFTWARE WILL OPERATE IN THE COMBINATIONS THAT YOU MAY SELECT FOR USE, THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR-FREE OR UNINTERRUPTED OR THAT ALL SOFTWARE ERRORS WILL BE CORRECTED. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED FROM DOLBY OR ELSEWHERE WILL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT. THE ENTIRE RISK AS TO THE QUALITY, OR ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.
7. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. IN NO EVENT WILL DOLBY BE LIABLE TO YOU FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) OR FOR THE COST OF PROCURING SUBSTITUTE PRODUCTS OR SERVICES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR THE USE OR PERFORMANCE OF THE SOFTWARE, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND WHETHER OR NOT DOLBY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. YOU AGREE THAT THESE LIMITATIONS WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.
8. LIMITATION OF LIABILITY AND REMEDIES. NOTWITHSTANDING ANY DAMAGES THAT YOU MIGHT INCUR FOR ANY REASON WHATSOEVER (INCLUDING, WITHOUT LIMITATION, ALL DAMAGES REFERENCED HEREIN AND ALL DIRECT OR GENERAL DAMAGES IN CONTRACT OR ANYTHING ELSE), THE ENTIRE LIABILITY OF DOLBY AND ANY OF ITS SUPPLIERS UNDER ANY PROVISION OF THIS EULA AND YOUR EXCLUSIVE REMEDY HEREUNDER (OTHER THAN THE LIMITED REMEDY DESCRIBED IN SECTION 5.2 ABOVE) SHALL BE LIMITED TO THE AMOUNT OF USD$10.00 (TEN US DOLLARS). THE FOREGOING LIMITATIONS, EXCLUSIONS AND DISCLAIMERS (INCLUDING SECTIONS 6,7 AND 8) SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EVEN IF ANY REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.
9. GOVERNING LAW: The validity, interpretation and performance of this Agreement shall be governed by and construed in accordance with the laws, without respect to conflict of laws provisions, and you agree to submit to the jurisdiction of the court, set forth below based on the applicable region where you are located:

| Region | Governing law | Court jurisdiction |
| --- | --- | --- |
| Countries in the European Economic Area | England | English Courts |
| All other countries | State of California, USA | State or Federal Courts located in San Francisco, CA |
| People’s Republic of China | State of California, USA | Arbitration at the Hong Kong International Arbitration Centre in accordance with the UNCITRAL Arbitration Rules ("UNCITRAL Rules"). The arbitration tribunal shall consist of one arbitrator to be appointed according to the UNCITRAL Rules. The language of the arbitration shall be English. |

Notwithstanding the foregoing, nothing in this Section 9 shall prevent Dolby from seeking any injunctive or equitable relief by a court of competent jurisdiction that is necessary to protect Dolby's rights or property until such dispute is resolved. This Agreement will be interpreted and construed in accordance with the English language. The parties agree that the provisions of the Uniform Computer Information Transactions Act ("UCITA") and the U.N. Convention on Contracts for the International Sale of Goods will have no force or effect on these terms and conditions.

10. THIRD PARTY SOFTWARE AND / OR OPEN SOURCE. The Software contains open source components and other third party components, subject to the applicable licensing terms and conditions. From time to time, Dolby may include additional third party software and components subject to third party terms and conditions of use. For more information about these software components, see the following:

    - www.dolby.com/us/en/about/warranty-and-maintenance-policies.html
    - *Dolby Conferencing Console open source software guide*

# Contents

# 1 Introduction to this guide

The Dolby Conferencing Console software provides an interface for IT administrators to use in managing Dolby Voice devices.



As an administrator, you can use the Dolby Conferencing Console software 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.

## 1.1 About this documentation

IT administrators can use this documentation as a guide for setting up and provisioning the Dolby Conferencing Console software.

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 details on:

- Installing the Dolby Conferencing Console software either on Linux (natively) or as a virtual appliance
- Using the Dolby Conferencing Console software to manage individual devices or groups of devices

## 1.2 New in this version

This version of the documentation has been updated to include information about new and updated features. It has also been reorganized and rewritten, where needed. Missing or incorrect information has been addressed.

- New topic for *Enabling Device Restriction*
- Updates to *Importing Device Configurations*
- Updates to *Enabling SNMP on RPM-based installations*
- Updates to *Using Webmin*
- Updates to *Monitoring Devices*

## 1.3 Related documentation

The documentation for the Dolby Voice product family consists of software documentation, release notes, and guides. Several of these guides are especially useful for users of the Dolby Conferencing Console software.

The *Dolby Conference Phone Administrator's Guide* describes how to install and administer the Dolby Conference Phone.

The *Dolby Conference Phone User's Guide* describes how to use the basic and advanced phone features, and how to customize the phone.

The *Dolby Conferencing Console Open Source Software Guide* describes third-party open-source software that is incorporated into the Dolby Conferencing Console software.

The *Dolby Voice Room Quick Start Guide* describes the contents of the Dolby Voice Room package, how to assemble the Dolby Conference Phone, the Dolby Voice Camera, Dolby Voice Hub, and how to connect Dolby Voice Room to the network. The quick start guide is included in the Dolby Voice Room package. It is also available from the Dolby Voice Room support pages.

The *Dolby Voice Room Administrator's Guide* describes how to install and administer the Dolby Voice Room system.

The *Dolby Voice Room Open Source Software Guide* describes the open source software used in the Dolby Voice Room software.

The *Dolby Voice Product Compatibility Guide* describes the compatibility relationships between the various Dolby Voice devices.

## 1.4 Accessing API documentation

You can access application programming interface (API) documentation for the Dolby Conferencing Console software from the user interface.

**Procedure**

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.
   
2. Click the **References** tab.
3. Click the **Web API reference** link to download the document.

## 1.5 Problem reports

When escalating issues to Dolby, please provide answers to these questions.

- Which version of the product is affected?
- 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?
- 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.
- What operating system and version are being used by the user? What browser and version are being used by the client?
- What other observations have you made? Is there anything else you think might assist us in identifying the root cause of the problem?

## 1.6 Documentation feedback

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

# 2 Architectural overview

This chapter describes the Dolby Conferencing Console product architecture.



## 2.1 Dolby Conferencing Console

The Dolby Conferencing Console software allows IT administrators to provision, configure, and administer devices.

Using the Dolby Conferencing Console software, you can:

- Bulk provision and configure devices
- Establish secure network communications between devices and the Dolby Conferencing Console software
- Remotely access device status information, make changes, and restart devices
- Obtain statistical status usage information for devices
- Manage inventory

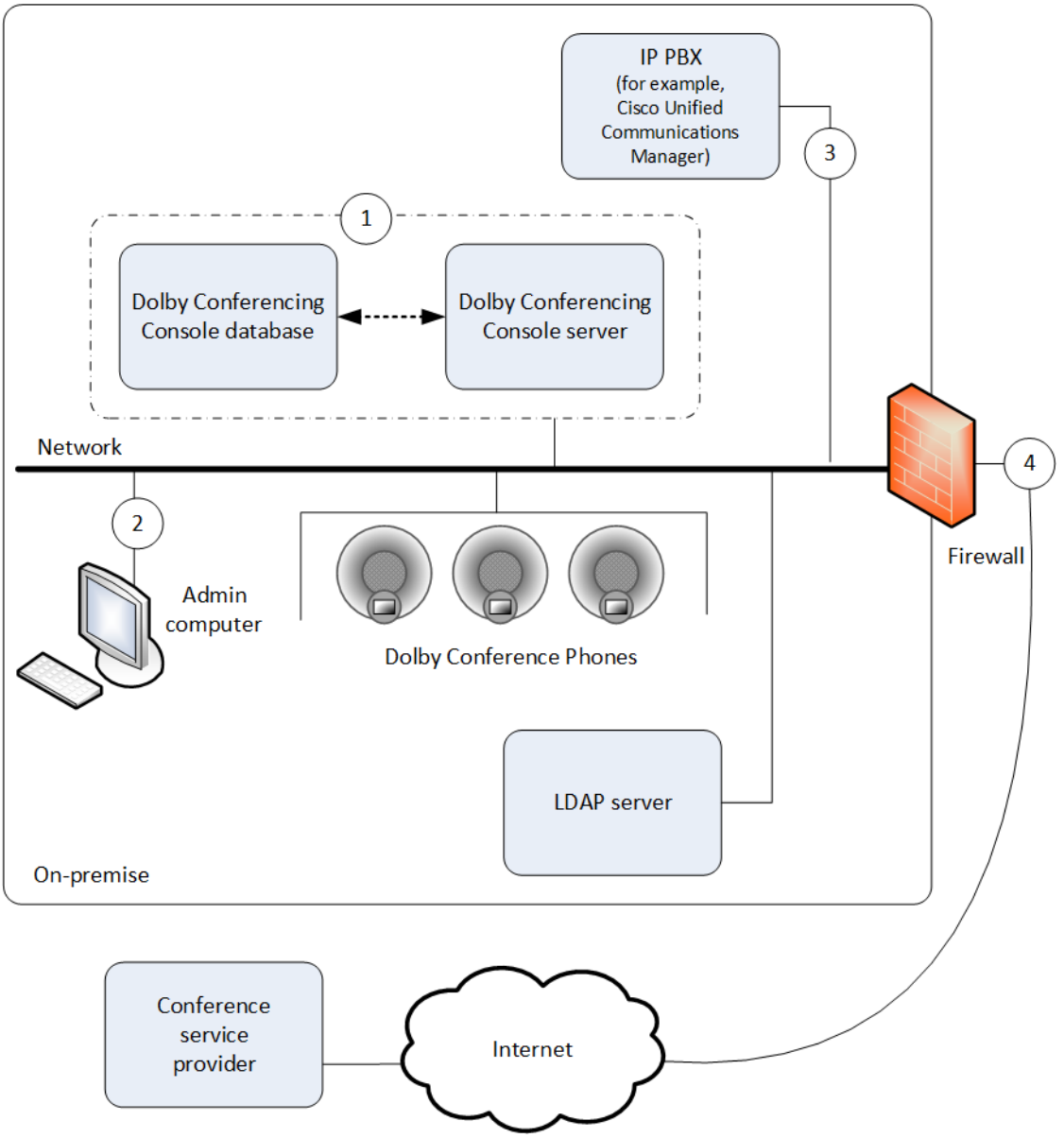
## 2.2 Architecture

This section provides a high-level overview of how the Dolby Conferencing Console software works with the rest of your network.

The exact architecture of your Dolby Conferencing Console software solution depends on whether you use the open virtual appliance (OVA) file or RPM Package Manager (RPM) method of installation. This high-level diagram shows an open virtual appliance file deployment of the Dolby Conferencing Console software. For information and diagrams of other deployments, see:


- Single-server deployment requirements on page 19
- Multiple-server deployment requirements on page 20

*Figure 1: Open virtual appliance deployment of the Dolby Conferencing Console software*




Key:

1. The Dolby Conferencing Console software stores data about devices and their usage to a database for administration. When you perform an open virtual appliance file deployment, the database is automatically created on the same physical or virtual hardware as the Dolby Conferencing Console server (as represented by the dashed line). You do not need create the database separately yourself. However, if you decide to perform an RPM deployment instead, then you will need to create and configure the database yourself.
2. Administrators can manage profiles, pools, and devices from a convenient interface on their computer.
3. The Dolby Conference Phone uses a Session Initiation Protocol (SIP) IP connection to your PBX. Cisco Unified Communications Manager is supported. For information about what other IP PBXs are supported, see the *Dolby Conference Phone administrator's guide* .
4. Secure communication through firewall to the conferencing service.

**Related information**

Single-server RPM deployment requirements on page 19

Multiple-server RPM deployment requirements on page 20

## 2.3 Security features

The Dolby Conferencing Console software allows you to secure all components, communications, and devices.

**User authentication with Lightweight Directory Access Protocol (LDAP)**
You can use LDAP for user authentication. Once configured, LDAP users can log in with their corporate user name and password.

**Retrieve passwords with Simple Mail Transfer Protocol (SMTP)**
You can use SMTP to allow non-LDAP users to retrieve passwords on their own.

**Device access**

You can choose to use Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) from the Dolby Conferencing Console software.

You can use the utility provided in the Dolby Conferencing Console software to generate a self-signed certificate, or you can provide a certificate authority (CA) certificate.

**Access password encryption**
All Dolby Conferencing Console account passwords are encrypted when stored on the server.

**Rogue device access prevention**
You can specify device access restrictions for each device pool to help protect against botnets and other threats.

**Password fields**
Passwords are obfuscated upon entry so that the password values cannot be hijacked.

**Network ports**
Upon install, the default port 80 allows initial access for the web user interface (UI). Root user access through port 22 (SSH) is disabled.

# 3 Requirements

This chapter describes the Dolby Conferencing Console supported hardware, software, and installation requirements.



## 3.1 Supported installation types

Before you install the Dolby Conferencing Console software, review the two types of available installations. Choose the installation that makes the most sense based on your environment and goals.

| Open virtual appliance (OVA) installation | RPM installation |
|---|---|
| The Dolby Conferencing Console software can be installed as a virtual appliance. The Dolby Conferencing Console software is available in the .ova file format. | The Dolby Conferencing Console software can be installed as a stand-alone application with RPM, which is a command-line utility. The Dolby Conferencing Console software is available in the .rpm file format. |
| Install the .ova file on one of these popular virtual machine (VM) environments:<br>• VMware Workstation Player 5.0 or later<br>• VMware vSphere 5.0 or later<br>• Oracle VM VirtualBox 5.0.10 or later | Install the RPM package on a Linux-based computer or Linux-based virtual machine running one of these operating systems:<br>• CentOS 6.0 and 7.0<br>• RedHat Enterprise Linux 6 and 7<br>• Amazon Linux (for Amazon Web Services (AWS)) |

### Which installation to use

For trials and small- to medium-scale deployments (less than 500 Dolby Voice devices), we recommend that you install the Dolby Conferencing Console software on virtual machines by using the .ova installation file. This is the simplest installation process and requires 30 minutes or less.

For other deployments, especially those involving more than 500 Dolby Voice devices and where scalability is important, we recommend that you install the Dolby Conferencing Console software on Linux-based computers by using the RPM package.

## 3.2 Minimum hardware specifications

The Dolby Conferencing Console software requires a minimum hardware specification on both physical and virtual servers.

The minimum physical or virtual hardware specification for a single-server deployment is:

- Quad-core 64-bit Intel-compatible , 2.2 GHz or greater
- 8 GB RAM
- 250 GB hard disk
- 1 Gbps Ethernet interface

For multi-server deployment hardware requirements, see Multiple-server deployment requirements on page 20.

For AWS installations, a `t2.xlarge` EC2 instance meets the minimum specification.

A minimum of 50GB of space is required for installation and minimal log storage. You need to allocate additional space based on how many log files you want to keep.

Dolby Voice device log files average approximately 2MB - 4MB per hour in a call.

For example, if you have 100 Dolby Voice devices provisioned and your devices average four hours of calls per day, you need to allocate approximately 50GB of space to save 30 day's worth of call logs (100*4MB*4*30 = 48GB).

If you add it to the base DCC disk space requirement of 50GB, you need to allocate a total of 100GB.

**Note:** The Dolby Conferencing Console software should be installed on a separate server from the ones being used to run the conferencing service provider and/or the IP PBX call control platform.

## 3.3 Supported operating systems

The Dolby Conferencing Console software is supported on specific versions of Linux.

You can install the Dolby Conferencing Console software on these operating systems:

- CentOS 6.0 and 7.0
- Red Hat Enterprise Linux 6 and 7
- Amazon Linux

## 3.4 Supported browsers

Accessing the Dolby Conferencing Console web interface requires a supported web browser.

You can access the Dolby Conferencing Console web interface by using any of these web browsers:

- Apple Safari 11
- Google Chrome 65
- Microsoft Internet Explorer 11
- Mozilla Firefox 59

## 3.5 Supported devices and device numbers

The Dolby Conferencing Console software supports Dolby Voice devices.

If you install with open virtual appliance file, up to 500 devices per customer site are supported per each instance of the Dolby Conferencing Console software.

If you install with the RPM package, up to 10,000 devices per customer site are supported when multiple Dolby Conferencing Console nodes are installed.

# 3.6 Network requirements

The Dolby Conferencing Console software has specific requirements for network services, connectivity, ports, and security.

The minimum network requirements include:

- A Domain Name System (DNS) server
- A Dynamic Host Configuration Protocol (DHCP) server
- HTTP or HTTPS connectivity between the locations where you will deploy the devices

## 3.6.1 Network ports

Certain network ports allow the Dolby Conferencing Console software to interact with and manage Dolby Voice devices. They also allow you to remotely access the Dolby Conferencing Console software from administrator computers.

- 22: SSH

  **Note:** For AWS deployments, opening this port is optional, and may be convenient for system administration tasks such as installing software updates.

- 80: HTTP, default network access port for web UI and provisioning
- 443: HTTPS
- 10000: Webmin

Check your network and firewall configurations to make sure that these ports are open.

When you install using the open virtual appliance file, these ports are open on the Dolby Conferencing Console software by default. However, when you install with RPM, the ports are closed by default and the administrator must open them. If the ports remain closed, you will not be able to use the Dolby Conferencing Console software to manage your Dolby Voice devices.

## 3.6.2 Network security

We recommend certain network security measures.

**Firewalls**

Ensure that the standard ports for HTTP (80) and HTTPS (443) are open for incoming connections on the server that hosts the Dolby Conferencing Console software. Run one of these commands as root to enable the required connectivity on the server:

For Redhat 6 and CentOS 6.0

```
iptables -I INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -I INPUT -p tcp -m tcp --dport 443 -j ACCEPT
iptables -I INPUT -p tcp -m tcp --dport 10000 -j ACCEPT
service iptables save
```

For Redhat 7 and CentOS 7.0

```
firewall-cmd --zone=public --add-service http --permanent
firewall-cmd --zone=public --add-service https --permanent
firewall-cmd --zone=public --add-port=10000/tcp --permanent
firewall-cmd --reload
```

#### Certificates

The Dolby Conferencing Console software includes a default certificate that is available for use upon startup. It is a good idea to set up secure access by creating and using your own certificates.

#### TLS

Transport Layer Security (TLS) version 1.2 is required if any of the Dolby Voice devices in your environment are running firmware version 3.1 or later.

To limit Dolby Conferencing Console to TLS version 1.2, add this line to /etc/dcc/web.ini:

```
ssl_protocols TLSv1.2;
```

## 3.7 Additional requirements and considerations for RPM deployments

Use the RPM package for medium and large-scale deployments that include up to 10,000 devices.

Before you install the Dolby Conferencing Console software using the RPM package, make sure you can answer some basic questions about the needs of your company and about your environment.

You can use the RPM package in different ways, including single-server and multiple-server deployments, which are described in this document.

You can also take multiple-server deployments one step further by adding redundancy. For information about setting up redundancy, see RPM deployments with redundancy on page 37.

Review all of the information about deployment in this document and then consider your answers to these important questions:

- How many devices will you have (for example, 500 Dolby Voice devices or less, or up to 10,000 Dolby Voice devices)?
- Will you perform a single-server deployment or multiple-server deployment?
- On what physical or virtual hardware will you install the Dolby Conferencing Console software?
- For multiple-server deployments, how many external device access service nodes do you need to handle device traffic? What physical or virtual hardware will use for those servers?
- For multiple-server deployments, which server will be the master node? Which servers will be device access service nodes?
- For multiple-server deployments, do you want redundancy?
- Where will your database server be?
- Where will your file storage server be?

To learn more about terms such as master node and device access service, review the Related information.

**Related information**

Setting up secure access on page 45
Multiple-server RPM deployment requirements on page 20
RPM deployments with redundancy on page 37
Device access service node requirements on page 23

## 3.7.1 Single-server RPM deployment requirements

There are specific requirements for deploying Dolby Conferencing Console with the RPM package when using a single virtual or physical server running Dolby Conferencing Console software and its supporting server software packages.

A single-server deployment can support up to 500 devices. You will need:

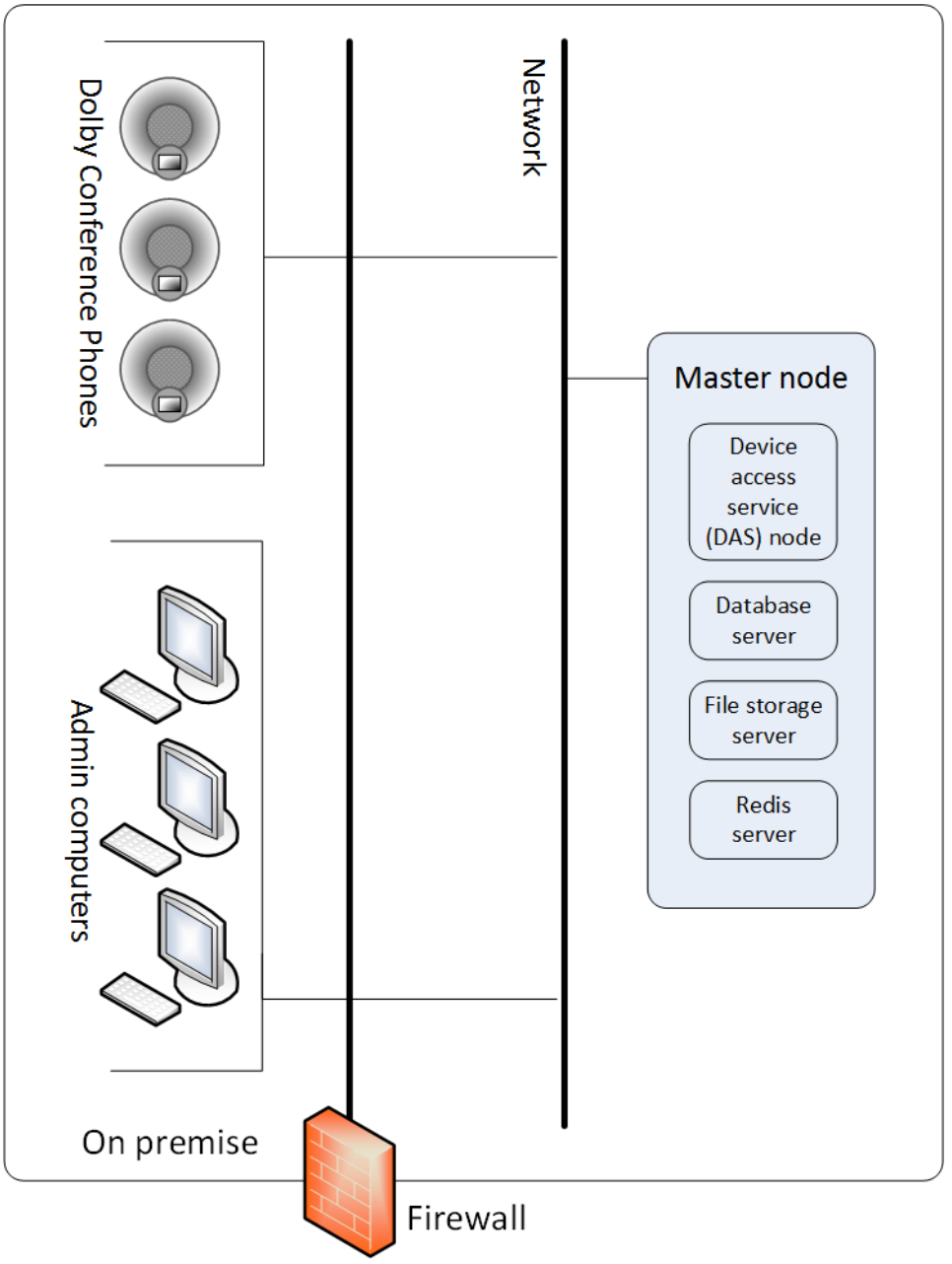
- At least one administrator computer
- At least one instance of physical or virtual hardware running the Dolby Conferencing Console software. This may be referred to as the Dolby Conferencing Console server or the master node.
- Three supporting software servers:
  - A database server
  - A file storage server
  - A Redis server

  These supporting software servers are typically installed on the same physical or virtual hardware as the Dolby Conferencing Console software. However, they may optionally be installed on separate physical or virtual hardware on the local network.

For more information about different types of nodes, see:

- Master node requirements on page 23
- Device access service node requirements on page 23

*Figure 2: RPM deployment with a single Dolby Conferencing Console server*




**Related information**

Architecture on page 12
Master node requirements on page 23
Device access service node requirements on page 23

## 3.7.2 Multiple-server RPM deployment requirements

There are specific requirements for deploying the Dolby Conferencing Console software with the RPM package to support 500–10,000 devices when using multiple servers running Dolby Conferencing Console software.

You will need:

- At least one administrator computer.
- One master node: This is an instance of physical or virtual hardware running the Dolby Conferencing Console software with `mode` set to `master`.

  The master node server (and its backup node, if present) must have a dual-core 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 4 GB of RAM.
- At least one device access service node, separate from the master node: These are instances of physical or virtual hardware running the Dolby Conferencing Console software with `mode` set to `das`.

  The device access service node servers must have a 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 2 GB of RAM.
- One or more database servers: These are completely separate from all instances of physical or virtual hardware running the Dolby Conferencing Console software.

  The database servers must have a quad-core 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 8 GB of RAM.
- One Redis server: this component serves as a memory cache and as a point of communication between the solution components.

  The Redis server must have a quad-core 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 8 GB of RAM.
- One file-storage server: This must be accessible to all Dolby Conferencing Console nodes (the master node and device access service nodes).

  The file storage server must have a 64-bit Intel-compatible CPU, 2.2 GHz or greater, and at least 2 GB of RAM.

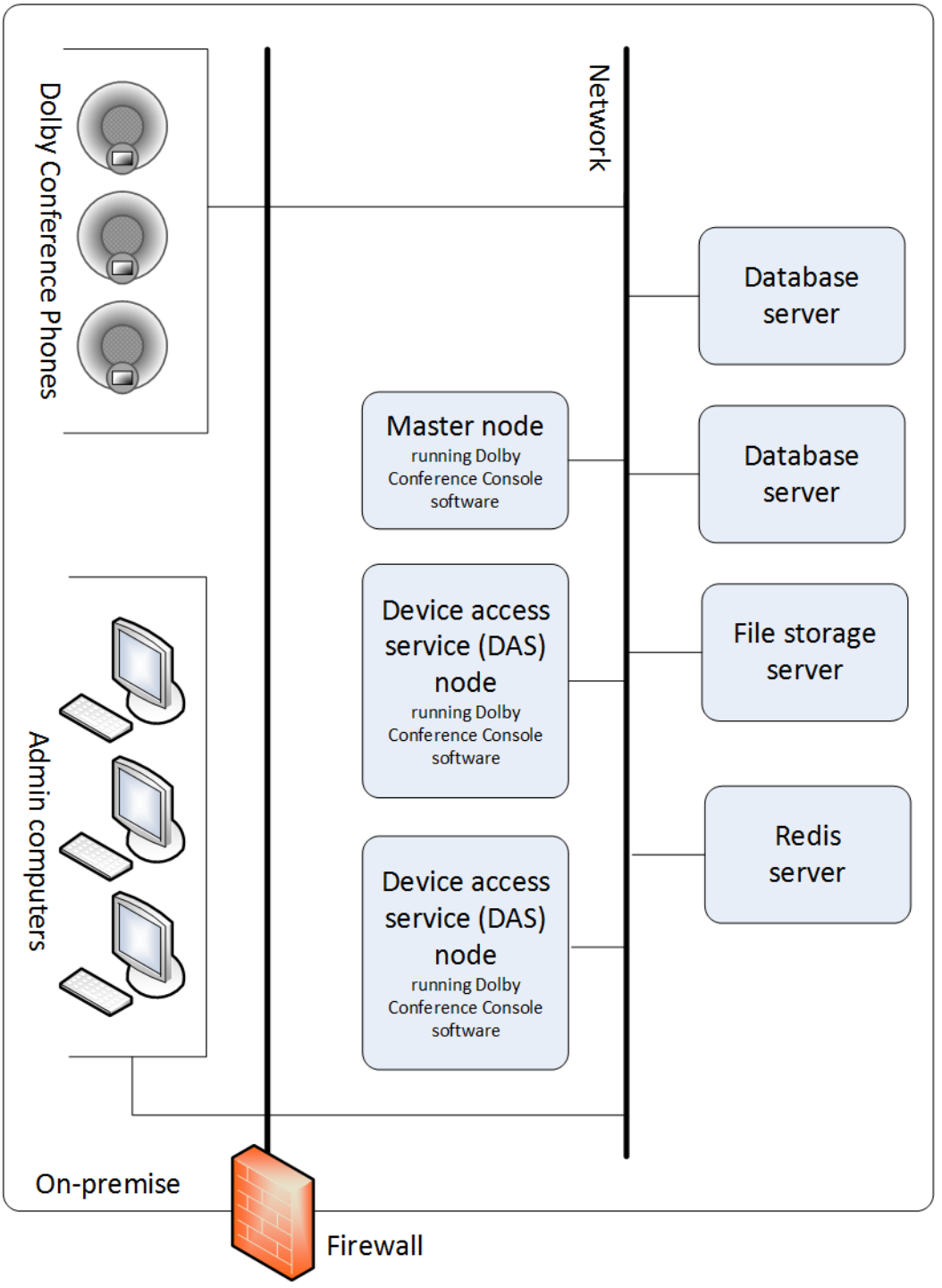
All of the physical and virtual servers must meet these hardware requirements, in addition to the requirements stated above:

- 250 GB hard disk
- 1 Gbps Ethernet interface

For more information about different types of nodes, see:

- Master node requirements on page 23
- Device access service node requirements on page 23

*Figure 3: RPM deployment with multiple Dolby Conferencing Console servers*




**Related information**

Architecture on page 12
Additional requirements and considerations for RPM deployments on page 18
Master node requirements on page 23
Device access service node requirements on page 23

## 3.7.3 Redis server requirements

The Dolby Conferencing Console requires a Redis server to serve as a memory cache and a point of communication between multiple components.

Before you set up a Redis server for Dolby Conferencing Console, determine which version of Redis you require based on the number of devices at your site.

CentOS version 6.0 includes Redis version 2.4 in the Extra Packages for Enterprise Linux (EPEL) repository by default. This version of Redis can support up to 6,000 devices. However, if you have more than 6,000 devices, Redis version 3.0 is required because it can support up to 10,000 devices.

If you have more than 6,000 devices, you have these options:

- Use CentOS version 6.0 and then upgrade to Redis version 3.0.
- Use CentOS version 7.0, which comes with Redis version 3.0.

The Redis server can use CentOS, Ubuntu, RedHat, or Debian as its operating system.

## 3.7.4 Master node requirements

The master node manages communications between the Dolby Conferencing Console server (master node), device access service nodes, database servers, and file-storage server.

- Only one active master node is required per deployment. This applies to both single-server and multiple-server deployments.
- The master node is an instance of physical or virtual hardware running the Dolby Conferencing Console software with `mode` set to `master`. When you install the Dolby Conferencing Console software with the RPM package, the hardware is set this way by default.

**Related information**

Single-server RPM deployment requirements on page 19
Multiple-server RPM deployment requirements on page 20

## 3.7.5 Device access service node requirements

Device access service nodes serve a different purpose than the master node. They manage device traffic.

How many device access service nodes you have and where they are on your network depend on these factors:

- For every 3,000 devices, you need one device access service node to handle device traffic. For example, if you have 10,000 devices, you need one master node and four separate, external device access service nodes.
- By default, master nodes have an internal device access service node and will handle all device traffic. However, once you add external device access service nodes for multiple-server deployment, the master node handles very little of the device traffic and the external device access service nodes start handling the traffic instead.
- Because a master node includes an internal device access service node by default, single-server deployments do not require external device access service nodes. In this case, the master node can handle all of the device traffic on its own.
- Multiple-server deployments involve more devices, so additional device access service nodes are required to handle device traffic.
- For multiple-server installations, you install the Dolby Conferencing Console software on multiple hardware instances, but you change `mode` to `das` on all device access service nodes

except for the master node. This changes those servers from master nodes to device access service nodes.

**Related information**

Additional requirements and considerations for RPM deployments on page 18
Single-server RPM deployment requirements on page 19
Multiple-server RPM deployment requirements on page 20

## 3.7.6 Database server requirements

Both single-server and multiple-server installations require a database server. For high availability, you may need multiple database servers.

The procedures for setting up the database are slightly different, depending on the type of installation you choose:

- For single-server installations, the database server can be on the same physical or virtual hardware as the Dolby Conferencing Console server. However, this is not a requirement. You can choose to use a separate database server that is somewhere else on the network.
- For multiple-server installations, the database server must be completely separate from the Dolby Conferencing Console server.
- For multiple-server installations where the database server is not colocated in the same master node and any device access service nodes, confirm that the connection between the Dolby Conferencing Console server and the database is functioning. If you use a database on another host, add the `DB_HOST` variable to /etc/dcc/settings.ini and confirm that port 5432 is reachable on `DB_HOST`.
- For single-server installations, the database server does not have to be separate from the file-storage server.

## 3.7.7 File Storage Server

Both single-server and multiple-server installations require a file-storage server. Only one file-storage server is required per deployment.

**About this task**

For single-server installations, the file-storage server can be on the same physical or virtual hardware as the Dolby Conferencing Console server. However, this is not a requirement. You can choose to use a separate file-storage server that is somewhere else on the network.

For multiple-server installations, you must use a file-storage server that is accessible to all Dolby Conferencing Console nodes (the master node and any device access service nodes).

### Procedure

1. (Optional for single-server installations) Set the file-storage client on the Dolby Conferencing Console server to access the remote file-storage server.
2. Configure the file-storage client (in this case, it is the Dolby Conferencing Console master node or device access service node) with this command:

```
yum install nfs-utils nfs-utils-lib
```

3. Mount /var/lib/dcc/files with this command. Assume that /home is the directory you need to access on the file-storage server.

```
mount nfs.company.com:/home /var/lib/dcc/files
```

4. Confirm that the mount is configured with the **df -h** command:

   Sample output:

```
[root@dcc ~]# df -h
Filesystem     Size Used Avail Use%
Mounted on /dev/mapper/vg_dsvddmspf1-lv_root

18G 2.1G 15G 13% / tmpfs
939M 76K 939M 1% /dev/shm /dev/sda1
477M 33M 419M 8% /boot
nfs.company.com:/home 45G 1.9G 41G 5% /var/lib/dcc/files
```

5. Modify the /etc/fstab to have a persistent shared mount drive after the server reboots with the command:

```
nfs.company.com:/home /var/lib/dcc/files nfs defaults 0 0
```

   Sample configuration:

```
/etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Oct 29 12:51:12 2015
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#

/dev/mapper/vg_dsvddmspf2-lv_root /                       ext4    defaults        1 1
UUID=83c2a6d9-85e6-40bf-acf2-2e64da6c23f2 /boot                   ext4    defaults
   1 2
/dev/mapper/vg_dsvddmspf2-lv_swap swap                    swap    defaults        0 0
tmpfs                   /dev/shm                tmpfs   defaults        0 0
devpts                  /dev/pts                devpts  gid=5,mode=620  0 0
sysfs                   /sys                    sysfs   defaults        0 0
```

```
proc                    /proc                   proc    defaults        0 0
nfs.company.com:/home    /var/lib/dcc/files     nfs     defaults        0 0
```

6. Change owner of /var/lib/ddms/files to dcc instead of root with the **chown** command:

```
[root@dsv-ddmspf-1 ~]# chown -R dcc:dcc /var/lib/dcc/files

[root@dcc ~]# ls -lat /var/lib/dcc/files
total 16
drwxr-xr-x. 2 nobody nobody 4096 Jan 7 17:02 uploads
drwxr-xr-x. 4 nobody nobody 4096 Jan 7 16:31 .
drwxr-xr-x. 2 nobody nobody 4096 Jan 7 16:19
fw drwxrwxr-x. 3 dcc dcc 4096 Jan 7 15:26 ..
[root@dcc ~]#
```

# 4 Installation

You have several options for installing the Dolby Conferencing Console software and setting up the system. Read through this chapter, and choose the options that best suit your needs.



## 4.1 Available software packages

Dolby Conferencing Console software packages are available for download from your Dolby Voice device provider.

These software packages are available:

- dcc-2.1.0.ova (for open virtual appliance file installations)
- dcc-2.1.0-1.el6.x86_64.rpm (for Linux RPM installations on RedHat/CentOS 6)
- dcc-2.1.0-1.el7.x86_64.rpm (for Linux RPM installations on RedHat/CentOS 7)
- dcc-2.1.0-1.amzn.x86_64.rpm (for AWS installations)

After installation, we recommend that you periodically check with your provider for updates.

## 4.2 Open virtual appliance deployments

For trials and small-scale deployments (less than 500 Dolby Voice devices), we recommend that you install the Dolby Conferencing Console software on virtual machines using the open virtual appliance file. This is the simplest installation process and requires 30 minutes or less.

Keep in mind:

- The open virtual appliance file is used to create a new virtual machine on your computer, and contains a complete installation of the Dolby Conferencing Console software.
- The new virtual machine (the guest system) for the Dolby Conferencing Console software is based on a Linux operating system (the guest operating system).

**Note:** The default Linux password for the `root` account on the virtual machine is `dolby`. The default account for the Dolby Conferencing Console software is `admin`, with the password `admin`.

We recommend that you change these passwords after installing the virtual machine. If you are working with an already-installed virtual machine, keep in mind that a colleague may have already changed one or both passwords.

### 4.2.1 Installing with the open virtual appliance

Before you begin, make sure you know which virtual machine application you want to use.

### About this task

**Note:** This topic assumes that you know how to use third-party virtual machine applications such as VMware Workstation Player 5.0 or later, VMware vSphere 5.0 or later, and Oracle VM VirtualBox 5.0.10 or later. These are applications that install and run virtual machines. Specific directions about how to use these applications is beyond the scope of this document.

### Procedure

1. If needed, install a virtual machine application on your computer.
2. Click the .ova file (dcc-2.1.0.ova) to open it with your virtual machine application.

   The .ova file is a virtual appliance or appliance. The virtual machine application imports it.

   For example, if you use Oracle VM VirtualBox:

   - When you open the file, the **Appliance settings** screen appears.
   - You can see that **Virtual System I** is named **DCC-2.1.0**.
3. Follow the onscreen prompts to import the Dolby Conferencing Console software.

   For example, if you use Oracle VM VirtualBox, after you click the **Import** button, there is a new virtual machine named **DCC-2.1.0** on your computer.
4. Start the Dolby Conferencing Console virtual machine.
5. On the virtual machine, from the command line, log in to the Dolby Conferencing Console software with the default user name (`root`) and password (`dolby`).

   **Note:** User names and passwords are case sensitive. We recommend that you change the password from the default as soon as possible for security reasons.
6. Use the `ifconfig` command to obtain the IP address of the Dolby Conferencing Console server.

   For example:

   ```
   dcc login: root
   Password: dolby
   [root@dcc ~]# ifconfig
   eth0    Link encap:Ethernet HWaddr 08:00:27:02:85:00 HW Address HWaddr
   08:00:27:02:85:00
           inet addr: 10.112.100.167  Bcast 10.112.101.255  Mask: 255.255.254.0
   ```
7. From an Internet browser, perform these steps to open the Dolby Conferencing Console user interface:

   a) Enter the IP address of the Dolby Conferencing Console software (from the previous step).

   b) Log in with the default user name (`admin`) and password (`admin`).

   **Note:** User names and passwords are case sensitive. We recommend that you change the password from the default as soon as possible for security reasons.

### Related information

Changing passwords on page 81

# 4.3 RPM deployments

Single- and multiple-server RPM deployments require installing the RPM on one or more servers, installing a database, and setting up file storage.

Before you begin, read Additional requirements and considerations for RPM deployments on page 18 and determine which type of deployment is appropriate for you. That section includes specific information and diagrams about how these types of deployments will be configured on your network.

You will need the Linux root or "superuser" password to perform the procedures in this section. For RPM deployments, Dolby software never sets your root password; consult the other system administrators in your organization to learn the password.

## 4.3.1 Installing a database

Before you install the Dolby Conferencing Console software with the RPM package, install a database to handle the data.

**About this task**
Steps 3-7 are optional for single-server deployments, but mandatory for multiple-server deployments.

**Procedure**

1. Open a command line, and use **yum** to install the database:

```
# yum install postgresql-server
# service postgresql initdb
# service postgresql start
```

2. Create the database with full access granted to the Dolby Conferencing Console software:

```
# su postgres -c psql
postgres=# CREATE DATABASE dcc;
postgres=# CREATE USER dcc WITH PASSWORD 'secret';
postgres=# GRANT ALL PRIVILEGES ON DATABASE dcc to dcc;
postgres=# \q
```

   **Note:** Secret is only a placeholder until you create the password. The password can be anything you choose.

3. (Mandatory for multiple-server deployments) Open port 5432 to allow the Dolby Conferencing Console server to communicate with the database, and then check the status of the firewall by entering these commands:
   For Redhat 6:

```
iptables -I INPUT -p tcp -m tcp --dport 5432 -j ACCEPT
service iptables save
service iptables status
```

For Redhat 7:

```
firewall-cmd --zone=public --add-port=5432/tcp --permanent
firewall-cmd --reload
```

4. Allow the database to listen to any remote servers (such as the Dolby Conferencing Console server) instead of the default `localhost`.
   a) Modify the /var/lib/pgsql/data/postgresql.conf file.
   b) Uncomment `listen_addresses`
   c) Change`localhost` to `"*" listen_addresses = 'localhost' change to listen_addresses = '*'`.
5. Modify /var/lib/pgsql/data/pg_hba.conf to allow remote servers (such as the Dolby Conferencing Console server) to access the `dcc` user and `dcc` database created in step 2. Use authentication method `md5`. For example, if you want to allow access to the address range `10.0.0.0/8` :

```
# IPv4 local connections:
host     all     all     127.0.0.1/32    ident
host     dcc     dcc     10.0.0.0/8      md5
```

   **Note:** In this example, PostgreSQL is not installed on the master node.

6. Increase the maximum number of database threads allowed:
   a) Go to the /var/lib/pgsql/data/postgresql.conf file.
   b) Change `max_connections` from 100 to 300. For example:

```
max_connections = 300
```

7. If you made any changes to the PostgreSQL configuration in steps 4, 5, or 6, restart the database service with this command:

```
service postgresql restart
```

8. Configure postgresql to start automatically when the system reboots.
   For example on CentOS

```
chkconfig postgresql on
```

**Related information**

Installing with the RPM package on a server on page 33

## 4.3.2 Installing and configuring a Redis server

Single-server and multiple-server RPM deployments require a Redis server. Install and configure the Redis server before you install Dolby Conferencing Console software on any servers.

**Prerequisites**

Review Redis server requirements on page 22 and determine which version of Redis you require based on the number of devices at your site. Redis version 3.0, which is included with CentOS 7.0 and later, is required if you have more than 6,000 devices.

### Procedure

1. From the computer or virtual machine with CentOS that you will use as your Redis server, enter these commands to install Redis:
   For Redhat 6:

   ```
   yum install -y epel-release
   yum install -y redis
   ```

   **Note:** If you encounter difficulties installing the epel-release package, see this page for suggestions:

   http://www.tecmint.com/how-to-enable-epel-repository-for-rhel-centos-6-5/

   For Redhat 7:

   ```
   yum install https://download.fedoraproject.org/pub/epel/epel-release-
   latest-7.noarch.rpm
   yum install -y redis
   ```

2. Perform one of these steps:
   - For Redhat 6, edit the `/etc/sysctl.conf` file.
   - For Redhat 7, create and edit the `/etc/sysctl.d/99-dcc.conf` file.
3. Append these `sysctl` parameters to tune the node for high network load.

   ```
   fs.file-max=188146
   net.core.somaxconn=8192
   net.netfilter.nf_conntrack_max=131072
   ```

4. After you edit the **`sysctl`** parameters, enter this command to apply the changes:
   For Redhat 6:

   ```
   sysctl -p
   ```

   For Redhat 7:

   ```
   sysctl --system
   ```

   You may encounter the following error:

   ```
   error: "net.netfilter.nf_conntrack_max" is an unknown key
   ```

   This error means that your system administrator has not installed the `nf_conntrack` module on this host. You can ignore this error if you do not anticipate high network load. Otherwise, contact your system administrator to install the `nf_conntrack` module. You can still proceed with next step of installation.

   The Dolby .ova image does not have the `nf_conntrack` module installed.
5. Edit the /etc/redis.conf file, and add the following line:

   ```
   maxclients 20000
   ```

6. Edit the /etc/redis.conf file, and make one of the following changes:
   - For a single node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the /etc/redis.conf file.
   - For a multiple node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the /etc/redis.conf file and modify it to `bind` *`IP_address`*, where *`IP_address`*

is the IP address associated with the interface (for example, `eth0`, `bond 0`, and so on) that is used for communication between the nodes of the Dolby Conferencing Console cluster.

**Note:** For a multiple node Dolby Conferencing Console deployment, if you specify `bind 0.0.0.0`, it will open the Redis server to all interfaces and introduce a security risk if the Redis host is reachable via the Internet. See the bind description in the redis.conf file for more details.

7. Edit and set the Redis server limits configuration.

   **Note:** If the Redis server limits configuration file is not present, create the file.

   For example, on Community Enterprise Operating System 6.x., edit the /etc/security/limits.d/95-redis.conf file, and set the limit.

   ```
   redis soft nofile 32000
   redis hard nofile 32000
   ```

   For example, on Community Enterprise Operating System 7.x., edit the /etc/systemd/system/redis.service.d/limit.conf file, and set the limit.

   ```
   LimitNOFILE=32000
   ```

8. Enter one of these commands to open the Redis server port on your firewall and check the status of the firewall:
   For Redhat 6:

   ```
   iptables -I INPUT -p tcp --dport 6379 -i eth0 -j ACCEPT
   service iptables save
   service iptables status
   ```

   For Redhat 7:

   ```
   firewall-cmd --zone=public --add-port=6379/tcp --permanent
       firewall-cmd --reload
       firewall-cmd --list-all
   ```

9. Configure postgresql to start automatically when the system reboots.
   For example on CentOS

   ```
   chkconfig postgresql on
   ```

10. Start the Redis server:

    ```
    service redis start
    ```

11. For Redis versions 2.6 and later, verify that the `maxclients` value is set to `20000`:

    ```
    redis-cli -h redis-ipaddress config get maxclients
    ```

    If you do not receive a `maxclient` output perform these steps:

    - Check the Redis server limits configuration
    - Reduce the `maxclients` value
    - Restart the Redis server
    - Re-check the `maxclients` value

12. Configure Dolby Conferencing Console to start automatically when the system reboots:

For example, on CentOS:

```
chkconfig dcc on
```

13. Verify that Redis is configured to start automatically:

```
chkconfig --list redis
```

```
redis           0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

### 4.3.3 Installing with the RPM package on a server

You can install the Dolby Conferencing Console software with the RPM package on Linux-based computers or Linux-based virtual machines.

**Prerequisites**

Do not proceed unless you have already installed a database (see Installing a database on page 29) and set up a Redis server (see Installing and configuring a Redis server on page 30).

**Procedure**

1. From a Linux-based computer or Linux-based virtual machine, use the **su** command to log in as superuser. Enter this command:

```
$ su
```

2. Set up Network Time Protocol (NTP) on the server, and sync it with your company NTP server or any public NTP server:

   a) Enter `yum install ntpdate`.

   b) Enter `ntpdate` *company_NTP_server* or `ntpdate time.nist.gov`.

3. Download the RPM package file to the server.

4. Use the **yum** command to install the Dolby Conferencing Console software. Enter this command:

```
yum install dcc-version-arch.rpm
```

   This list explains what values to enter based on this example:

   *version*
   The version of the Dolby Conferencing Console software.

   *arch*
   This is either `1.el6.x86_64` for Redhat 6 or `1.el7.x86_64` for Redhat 7.

   **Note:** Both the Dolby Conferencing Console software and postgresql-libs (a dependency) install.

5. (Optional) In the Dolby Conferencing Console web server, create and sign an Secure Sockets Layer (SSL) certificate and store the results in /etc/dcc/web-cert.key and /etc/dcc/web-cert.pem.

You perform this step only when replacing the default certificate with a CA certificate as described in Replacing the default server certificate with a CA certificate on page 47.

6. (Required for single-server installations) Ensure that connections between the Dolby Conferencing Console server and the database are functioning by checking the listed entries in these files, and ensuring that your firewall allows for these port connections:

```
/etc/dcc/settings.ini
DB_HOST

/etc/dcc/web.ini
HTTP port: 80; HTTPS port: 443 HW Address HWaddr 08:00:27:02:85:00
```

**Note:** To check connectivity, the PostgreSQL client is required.

If you need to install the PostgreSQL client, use this command:

```
yum install -y postgresql
```

After the PostgreSQL client is installed, you can then use this command to check connectivity:

```
psql -U dcc -h database.company.com -p 5432
```

**Note:** Confirm that both HTTP port 80 and HTTPS port 443 are open; otherwise, you will not be able to log in from a web browser. For more information, see Network security on page 17.

7. From the Dolby Conferencing Console server, edit `etc/dcc/settings.ini` file and enter these directives to define the connection between the Dolby Conferencing Console server and the Redis server. For multiple-server deployments, you must repeat this step on each device access service and master node.

Sample configuration:

```
/etc/dcc/settings.ini
[database]
DB_USER=dcc
DB_NAME=dcc
DB_PASSWORD=secret
DB_HOST=database.company.com
```

**Note:** This is the password you created during the database installation.

```
[redis]
HOST=10.2.0.1
DB=5
PASSWORD=password
PORT=6379
```

This list explains what values to enter based on this example:

*HOST*
The host name of the Redis server. The default value, and the required value for single-server installations, is `localhost`.

*PORT*
The Redis server port number (default: 6379).

*DB*
The Redis database number: This directive is required for multiple-server installations if there are other Redis consumers not using Dolby Conferencing Console. This directive is not required for single-server installations. The value must be a number equal or greater than zero and that does not include decimals.

*PASSWORD*
Required only if the Redis server is password protected. If you have a single-server installation or you use the AWS platform, the Redis server is not accessible to the outside world unless you explicitly grant access. If the Redis server is on a separate physical or virtual server and you do not use the AWS platform, we recommend that you configure a Redis server password.

8. Use the **service** command to start the Dolby Conferencing Console software. For example, enter this command:

```
service dcc start
```

9. Enter one of these commands to obtain the IP address of the Dolby Conferencing Console:
   - For Redhat 6 the command is**ifconfig**:

```
dcc login: root
[root@dcc ~]# ifconfig
eth0    Link encap:Ethernet  HWaddr 08:00:27:02:85:00
        inet addr: 10.112.100.167  Bcast 10.112.101.255  Mask: 255.255.254.0
```

   - For Redhat 7 the command is **ip addr**:

```
dcc login: root
[root@dcc ~]# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen
1000
    link/ether 08:00:27:87:f0:d2 brd ff:ff:ff:ff:ff:ff
    inet 10.120.100.173/23 brd 10.120.101.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe87:f0d2/64 scope link
       valid_lft forever preferred_lft forever
```

10. From an Internet browser, enter the IP address and then perform these steps from the Dolby Conferencing Console user interface:
    a) Log in with the default user name (`admin`) and password (`admin`).
    b) If desired, change your password (recommended).
11. For Redhat 7 only: Configure the firewall to allow HTTPS connections.

```
firewall-cmd --zone=public --add-service https
    firewall-cmd --reload
```

**Related information**

Replacing the default certificate with a new self-signed certificate on page 46
Changing passwords on page 81
Installing a database on page 29

### 4.3.4 Installing with the RPM package on multiple servers

Installing the Dolby Conferencing Console software with the RPM package on multiple servers is the same as installing it on one server, but with some additional steps.

**Procedure**

1. Install the Dolby Conferencing Console software on multiple servers.

   For more information, see Installing with the RPM package on a server on page 33.

2. Decide which server will be your master node and which will be device access service nodes.

   For more information, see Master node requirements on page 23 and Device access service node requirements on page 23.

3. On each server that you want to use as a device access service node, perform these steps:

   a) Go to the /etc/sysconfig/dcc file, and set the `MODE` variable to das.

   b) Restart the server using this command:

   ```
   service dcc restart
   ```

4. On the remaining server that you are using as the master node, edit /etc/dcc/das-nodes.ini as described here. You must list all of your device access service nodes so that they are available to the master node.

   **Note:** If you want redundancy, perform this step for the backup master node as well. The active master and backup master nodes must have the same configuration for redundancy to work.

   Sample configuration:

   ```
   /etc/dcc/das-nodes.ini
   ```

   ```
                       # the upstream for DAS nodes
   upstream das {
       # List of all DAS nodes in nginx "upstream" compatible format
       server 10.0.0.101:8001 weight=10;
       server 10.0.0.102:8001 weight=10;
       server 10.0.0.103:8001 weight=10;
       # !!! DO NOT DELETE THIS LINE !!!
       server unix:/var/run/dcc/das.sock;
   }
   ```

### 4.3.5 Setting up file storage for multiple servers

A file-storage server is required for all RPM installations (both single-server and multiple-server installations).

**Prerequisites**

Before you begin, review requirements for file-storage servers at File-storage server requirements.

**Procedure**

1. Install file-storage programs on the server with this command:

```
yum install nfs-utils nfs-utils-lib
```

2. Run these scripts:

```
chkconfig nfs on
service rpcbind start
service nfs start
```

3. Export the desired share directory.
   For example, to share the /home directory on the file-storage server, append these lines to /etc/exports . Assume that 10.203.131.179 is the active node and that 10.203.131.180 is the redundancy node.

```
/home 10.203.131.179(rw,async,no_root_squash,no_subtree_check)
/home 10.203.131.180(rw,async,no_root_squash,no_subtree_check)
```

4. Run this command to export:

```
exportfs -a
```

5. Open the firewall (**iptables**) for the file-storage server port 2049 with this command:
   Example for Redhat 6 and CentOS 6.0:

```
iptables -I INPUT -p tcp -m tcp --dport 2049 -j ACCEPT
```

   Save iptables, and check the status of the firewall with these commands:

```
service iptables save
service iptables status
```

   Example for Redhat 7 and CentOS 7.0:

```
firewall-cmd --zone=public --add-port=2049/tcp --permanent
firewall-cmd --reload
firewall-cmd --list-all
```

# 4.4 RPM deployments with redundancy

With large-scale deployments (1,000 devices or more), redundancy ensures that users do not experience service disruptions or performance problems.

Set up the Dolby Conferencing Console software with these components: master nodes, device access service nodes, and database nodes. For each type of node, create both an active and a backup version. These are identical (or redundant), but if a master fails, the backup becomes the new active node.

**Related information**

Additional requirements and considerations for RPM deployments on page 18

## 4.4.1 Setting up master node redundancy

You can set up redundant nodes by using failover software (**keepalived**).

### Prerequisites

Do not proceed unless you have already completed these prerequisite tasks:

- Set up the Dolby Conferencing Console software with the following components: master node, database node, and network file storage mounted to `/var/lib/dcc/files` on the master node.
- Create a backup master node with the same configuration as the active master node.

### About this task

The information here is for example only; the actual IP addresses you use will be different:

- The IP address of the active master node is 10.112.100.230.
- The IP address of the backup node is 10.112.100.231.
- The IP address (virtual IP address) of the Dolby Conferencing Console server (dcc.ourcompany.com) is 10.112.100.233.

### Procedure

1. On both the active and backup master nodes, install **keepalived**.

   ```
   yum install keepalived
   ```

2. On both the active and backup master nodes, edit `/etc/sysconfig/dcc` and uncomment these lines:

   ```
   DCC_DAS_WORKERS = 16
   DCC_TASKQUEUE_WORKERS = 8
        (Two workers are recommended for every 3,000 devices.)
   DCC_WEBSOCKETS_WORKERS = 4
        (One worker is required for every 3,000 devices.)
   ```

3. Perform one of these steps:
   - For Redhat 6, edit the `/etc/sysctl.conf` file.
   - For Redhat 7, create and edit the `/etc/sysctl.d/99-dcc.conf` file.
4. Append these `sysctl` parameters to tune the node for high network load.

   ```
   fs.file-max=188146
   net.core.somaxconn=8192
   net.netfilter.nf_conntrack_max=131072
   ```

5. If needed, configure your firewall so that Virtual Router Redundancy Protocol (VRRP) is allowed through, and confirm the change.
   Example for Redhat 6 and CentOS 6.0:

   ```
   iptables -I INPUT -p 112 -i eth0 -j ACCEPT
   service iptables save
   service iptables status
   ```

   Example for Redhat 7 and CentOS 7.0:

   ```
   firewall-cmd --add-rich-rule='rule protocol value="vrrp" accept' --permanent
   firewall-cmd --reload
   firewall-cmd --list-all
   ```

6. On the active master node, back up the default keepalived.conf configuration file and configure a new file. Then enable and start `keepalived`.

The command for backing up keepalived.conf is `mv /etc/keepalived/keepalived.conf /etc/keepalived/keepalived.conf_default`.

```
cat > /etc/keepalived/keepalived.conf <<__EOF__
! Configuration File for keepalived
global_defs {
    router_id DCC_ASP
}
vrrp_instance DCC {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 101
    advert_int 1
    notify /usr/bin/dcc-keepalived-notify.sh
    authentication {
        auth_type PASS
        auth_pass longandwindingroad
    }
    virtual_ipaddress {
    10.112.100.233
    }
}
__EOF__
service keepalived start
chkconfig keepalived on
```

7. Repeat the previous step on the backup node, but make sure that the backup priority value is less than the active master priority value.
   For example, if the active master has a priority value of 101, then the backup master node must have a priority value of 100 or less.

```
cat > /etc/keepalived/keepalived.conf <<__EOF__
! Configuration File for keepalived
global_defs {
   router_id DCC_ASP
}
vrrp_instance DCC {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 100
    advert_int 1
    notify /usr/bin/dcc-keepalived-notify.sh
    authentication {
        auth_type PASS
        auth_pass longandwindingroad
    }
    virtual_ipaddress {
        10.112.100.233
    }
}
__EOF__
```

```
service keepalived start
chkconfig keepalived on
```

8. Confirm that the device access service nodes listed in the /etc/dcc/das-nodes.ini file on both the active and backup master nodes match.

   **Note:** For redundancy to work, the active and backup master nodes need have the same configuration. For more information, including a sample configuration of the /etc/dcc/das-nodes.ini file, see step 4 in Installing with the RPM package on multiple servers on page 36.

9. Confirm that the Dolby Conferencing Console server is available at the `virtual_ipaddress` configured in these steps (for example, 10.112.100.233).

10. Test your failover by shutting down the active master node. Confirm that the Dolby Conferencing Console server is available on the same IP address (you may need to log in again).

11. Review the `logrotate` settings in /etc/logrotate.d/dcc and update them, if needed. By default, the logs are rotated on a daily basis.

    For example, if a rotated log file gets too large when rotated on a daily basis, add the size trigger for those logs.

```
/var/log/dcc/nginx-*.log {
        size 750M
        missingok
        rotate 10
        notifempty
        sharedscripts
        nodateext
        postrotate
            /etc/init.d/dcc logrotate
        endscript
}
```

## 4.4.2 Installing and configuring a Redis server

Single-server and multiple-server RPM deployments require a Redis server. Install and configure the Redis server before you install Dolby Conferencing Console software on any servers.

### Prerequisites

Review Redis server requirements on page 22 and determine which version of Redis you require based on the number of devices at your site. Redis version 3.0, which is included with CentOS 7.0 and later, is required if you have more than 6,000 devices.

### Procedure

1. From the computer or virtual machine with CentOS that you will use as your Redis server, enter these commands to install Redis:
   For Redhat 6:

```
yum install -y epel-release
yum install -y redis
```

   **Note:** If you encounter difficulties installing the epel-release package, see this page for suggestions:

   http://www.tecmint.com/how-to-enable-epel-repository-for-rhel-centos-6-5/

For Redhat 7:

```
yum install https://download.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
yum install -y redis
```

2. Perform one of these steps:
   - For Redhat 6, edit the `/etc/sysctl.conf` file.
   - For Redhat 7, create and edit the `/etc/sysctl.d/99-dcc.conf` file.
3. Append these `sysctl` parameters to tune the node for high network load.

```
fs.file-max=188146
net.core.somaxconn=8192
net.netfilter.nf_conntrack_max=131072
```

4. After you edit the **`sysctl`** parameters, enter this command to apply the changes:
   For Redhat 6:

```
sysctl -p
```

   For Redhat 7:

```
sysctl --system
```

   You may encounter the following error:

```
error: "net.netfilter.nf_conntrack_max" is an unknown key
```

   This error means that your system administrator has not installed the `nf_conntrack` module on this host. You can ignore this error if you do not anticipate high network load. Otherwise, contact your system administrator to install the `nf_conntrack` module. You can still proceed with next step of installation.

   The Dolby .ova image does not have the `nf_conntrack` module installed.
5. Edit the /etc/redis.conf file, and add the following line:

```
maxclients 20000
```

6. Edit the /etc/redis.conf file, and make one of the following changes:
   - For a single node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the /etc/redis.conf file.
   - For a multiple node Dolby Conferencing Console deployment, uncomment the `bind 127.0.0.1` line in the /etc/redis.conf file and modify it to `bind` *`IP_address`*, where *`IP_address`* is the IP address associated with the interface (for example, `eth0`, `bond 0`, and so on) that is used for communication between the nodes of the Dolby Conferencing Console cluster.

   **Note:** For a multiple node Dolby Conferencing Console deployment, if you specify `bind 0.0.0.0`, it will open the Redis server to all interfaces and introduce a security risk if the Redis host is reachable via the Internet. See the bind description in the redis.conf file for more details.
7. Edit and set the Redis server limits configuration.

   **Note:** If the Redis server limits configuration file is not present, create the file.

For example, on Community Enterprise Operating System 6.x., edit the /etc/security/limits.d/95-redis.conf file, and set the limit.

```
redis soft nofile 32000
redis hard nofile 32000
```

For example, on Community Enterprise Operating System 7.x., edit the /etc/systemd/system/redis.service.d/limit.conf file, and set the limit.

```
LimitNOFILE=32000
```

8. Enter one of these commands to open the Redis server port on your firewall and check the status of the firewall:
   For Redhat 6:

   ```
   iptables -I INPUT -p tcp --dport 6379 -i eth0 -j ACCEPT
   service iptables save
   service iptables status
   ```

   For Redhat 7:

   ```
   firewall-cmd --zone=public --add-port=6379/tcp --permanent
       firewall-cmd --reload
       firewall-cmd --list-all
   ```

9. Configure postgresql to start automatically when the system reboots.
   For example on CentOS

   ```
   chkconfig postgresql on
   ```

10. Start the Redis server:

    ```
    service redis start
    ```

11. For Redis versions 2.6 and later, verify that the `maxclients` value is set to `20000`:

    ```
    redis-cli -h redis-ipaddress config get maxclients
    ```

    If you do not receive a `maxclient` output perform these steps:

    - Check the Redis server limits configuration
    - Reduce the `maxclients` value
    - Restart the Redis server
    - Re-check the `maxclients` value

12. Configure Dolby Conferencing Console to start automatically when the system reboots:

For example, on CentOS:

```
chkconfig dcc on
```

13. Verify that Redis is configured to start automatically:

```
chkconfig --list redis
```

```
redis           0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

## 4.4.3 Setting up device access service node redundancy

device access service redundancy is achieved simply by having more device access service nodes than are required to handle traffic.

### About this task

When a device access service node goes down, nginx on the active master node detects this condition and stops sending traffic to it, and then periodically checks the device access service node state. Once the node is back up, nginx starts sending requests to it again.

Sample configuration:

```
/etc/dcc/das-nodes.ini
# the upstream for DAS nodes
upstream das {
    # List of all DAS nodes in nginx "upstream" compatible format
    server 10.0.0.101:8001 weight=10;
    server 10.0.0.102:8001 weight=10;
    server 10.0.0.103:8001 weight=10;
    # !!! DO NOT DELETE THIS LINE !!!
    server unix:/var/run/dcc/das.sock;
}
```

### Procedure

1. To run the Dolby Conferencing Console software as a device access service node, edit /etc/sysconfig/dcc and set `MODE = das` and `DCC_DAS_WORKERS = 32`.
2. On each device access service node, confirm that port 8001 is open so that the active and backup master nodes can access them with these commands:
   Example for Redhat 6 and CentOS 6.0

```
iptables -I INPUT -p tcp -m tcp --dport 8001 -j ACCEPT
service iptables save
service iptables status
```

   Example for Redhat 7 and CentOS 7.0

```
firewall-cmd --zone=public --add-port=8001/tcp --permanent
firewall-cmd --reload
firewall-cmd --list-all
```

3. Perform one of these steps:
   - For Redhat 6, edit the `/etc/sysctl.conf` file.

- For Redhat 7, create and edit the `/etc/sysctl.d/99-dcc.conf` file.

4. Append these `sysctl` parameters to tune the node for high network load.

```
fs.file-max=188146
net.core.somaxconn=8192
net.netfilter.nf_conntrack_max=131072
```

### 4.4.4 Setting up database redundancy

You can use any solution for high-availability PostgreSQL setup.

For example, you can use a combination of the **pgpool** and **repmgr** tools described in Set up a redundant PostgreSQL database with repmgr and pgpool. In this case, all nodes should point to the **pgpool** machine as a database server. In case of active master node failure, **pgpool** will detect this condition and switch all database traffic to standby mode.

## 4.5 AWS deployments

Single- and multiple-server AWS deployments require installing the Dolby Conferencing Console AWS-specific RPM package on one or more servers, installing a database, and setting up file storage.

### 4.5.1 Installing a single Dolby Conferencing Console instance on AWS

You can install all of the components of a Dolby Conferencing Console installation on a single Amazon Linux `t2.xlarge` EC2 instance. This type of installation supports up to 1,000 devices.

**Procedure**

1. Spawn an Amazon Linux EC2 instance with ports 22, 80, 443 open for inbound connections.
2. Use **ssh** to log in to the instance.
3. Install the PostgreSQL database on the instance.

   For instructions, see Installing a database on page 29.
4. Enable epel.

```
yum-config-manager --enable epel
```

5. Install the Redis server on the local instance.

   For instructions, see Installing and configuring a Redis server on page 30.
6. Download the Dolby Conferencing Console RPM for AWS from Dolby.

   You can use **curl** or **wget** to download the RPM package. You can also upload the package to the Amazon Web Services host. The release email from Dolby contains the URL for downloading the RPM package.

```
wget url_from_release_email
curl -O url_from_release_email
```

7. Download these two prerequisite packages to the same folder as the Dolby Conferencing Console RPM package on the instance.

These required packages are not included in Amazon Linux:

- http://s3.amazonaws.com/dcc-s3-rpm-repo/3p/xmlsec1-1.2.20-1.x86_64.rpm
- http://s3.amazonaws.com/dcc-s3-rpm-repo/3p/xmlsec1-openssl-1.2.20-1.x86_64.rpm

8. Install the three packages, working from the directory into which they have been downloaded:

```
sudo yum install xmlsec1-openssl-1.2.20-1.x86_64.rpm xmlsec1-1.2.20-1.x86_64.rpm
    dcc-2.1.0-1.amzn.x86_64.rpm
```

9. Edit /etc/dcc/settings.ini to specify the PostgreSQL account information.

```
[database]
DB_USER=dcc_aws
DB_NAME=dcc_aws
DB_PASSWORD=sekretvord
```

10. Start the Dolby Conferencing Console server.

```
sudo service dcc start
```

### 4.5.2 Installing Dolby Conferencing Console on multiple AWS servers

You can install the Dolby Conferencing Console software and its supporting servers on multiple Amazon instances. This configuration can support up to 10,000 devices (optionally with redundancy to prevent service disruptions or performance problems).

**About this task**

Follow the instructions in these sections, making any necessary changes for the AWS platform:

- RPM deployments on page 29
- RPM deployments with redundancy on page 37

## 4.6 Setting up secure access

The Dolby Conferencing Console software uses HTTPS for secure web UI access and secure provisioning. This is an overview of the procedures involved in setting up secure access for your system.

**Assign a server host name**
This allows devices and the IT administrators to connect to the Dolby Conferencing Console software using a host name as opposed to an IP address. See Changing the host name on page 46.

**Replace the default certificate**
The Dolby Conferencing Console software package contains a default self-signed certificate using the common name dcc. For a higher level of security, you should replace this with either a self-signed certificate or a certificate authority (CA) certificate. See Replacing the default certificate with a new self-signed certificate on page 46 and Replacing the default server certificate with a CA certificate on page 47.

**Connect a device to the Dolby Conferencing Console software using HTTPS**
You can connect a Dolby Voice device to your Dolby Conferencing Console securely. See Connecting a device over HTTPS on page 48.

**Note:** You can accept the server certificate at the device during the first-time provisioning stage, or later through a user-interface menu.

Once you have configured secure access, you can use HTTPS to connect to the Dolby Conferencing Console web interface. Enter https://*hostname* in the browser to connect securely.

**Note:** When a self-signed certificate is in use, most browsers display a warning, You can simply ignore this warning and log in to Dolby Conferencing Console.

**Related information**

Additional requirements and considerations for RPM deployments on page 18

## 4.6.1 Changing the host name

You can change the server host name for the Dolby Conferencing Console server. This allows devices and IT administrators to access the Dolby Conferencing Console software by using a convenient and easy-to-remember name instead of an IP address.

**About this task**

To change the server host name, set up the Dolby Conferencing Console host name and populate the DNS records.

**Procedure**

1. Log in to the Dolby Conferencing Console software as the root user.
2. Perform one of these steps:
   - For Redhat 6 and CentOS 6.0:

     Edit the /etc/sysconfig/network file, and change the value of the `HOSTNAME` field from the default, `dcc`, to the desired name.
   - For Redhat 7 and CentOS 7.0:

     Use the hostnamectl command to change the host name:

     ```
     hostnamectl set-hostname my_dcc
     ```

     Where `my_dcc` is your server host name.
3. Edit the /etc/sysconfig/network-scripts/ifcfg-eth0 file, and add the line `DHCP_HOSTNAME="`*`my_dcc`*`"`, where *my_dcc* is your server host name.
4. Restart the network service by using this command:

   ```
   service network restart
   ```

## 4.6.2 Replacing the default certificate with a new self-signed certificate

Use this procedure to replace the default certificate with a self-signed certificate.

**Procedure**

1. On the server that hosts your Dolby Conferencing Console software, log in as the root user.
2. Open a console, and enter this command to open the certificate utility:

   ```
   /usr/bin/dcc-generate-self-signed-cert
   ```

The certificate utility sends certificate parameter requests to the console.

3. Respond to these console requests.

| Option | Description |
|---|---|
| Pass phrase for **web-cert.key** | Any string |
| Pass phrase for **web-cert.key** | Must match previous entry |
| Country name (two-letter code) | Two-letter code for country |
| State or province name (full name) | State or province name for your organization |
| Locality name (city) | City name for your organization |
| Organization name | Name of your company |
| Organization unit name | Name of your team or division within the company |
| Common name | The fully qualified domain name (FQDN) for your server (for example, dcc.*your-company*.net)<br>**Important:** This name must match the host name used when you connect a device over HTTPS. See Connecting a device over HTTPS on page 48. |
| Email address | An administrator email address (your valid email address) |
| Challenge password | Optional extra password |

### Results

After you have entered the desired information, the utility generates a certificate. The certificate is then ready for use.

### Related information

Replacing the default server certificate with a CA certificate on page 47

## 4.6.3 Replacing the default server certificate with a CA certificate

Some organizations prefer to use CA signed certificates for their SSL web servers. The Dolby Conferencing Console software supports CA signed certificates.

### About this task

On the server that hosts your Dolby Conferencing Console software, log in as the root user.

### Procedure

1. Generate the certificate key, using the preferred data encryption standard (DES) for your organization. For example:

```
openssl genrsa -des3 -out /tmp/web-cert.key 2048
```

2. Generate a certificate signing request (CSR):

```
openssl req -new -key /tmp/web-cert.key -out /tmp/web-cert.csr -sha256
```

openssl sends certificate parameter requests to the console.

3. Respond to these console requests:

| Option | Description |
|---|---|
| Pass phrase for **web-cert.key** | Any string |

| Option | Description |
|---|---|
| Pass phrase for **web-cert.key** | Must match previous entry |
| Country name (two-letter code) | Two-letter code for country |
| State or province name (full name) | State or province name for your organization |
| Locality name (city) | City name for your organization |
| Organization name | Name of your company |
| Organization unit name | Name of your team or division within the company |
| Common name | The fully qualified domain name for your server (for example, dcc.your-company.net)<br>**Important:** This name must match the host name used when you connect a device over HTTPS. See Connecting a device over HTTPS on page 48. |
| Email address | An administrator email address (your valid email address) |
| Challenge password | Optional extra password |

Once you have finished the entries, openssl generates a certificate.

4. Retrieve the CSR file at /tmp/web-cert.csr.
5. Use **scp** to copy the file to a remote Linux server at this server address:

```
scp /tmp/web-cert.csr user@server.address:remoteDirectory
```

6. Submit the file ending in .csr to a commercial SSL provider for signing.
7. After you receive the signed certificate, upload it to Dolby Conferencing Console.

```
scp user@server.address:/remoteDirectory/web-cert.pem /tmp/
```

8. Replace the server certificate located at /etc/dcc-web-cert.pem.

```
mv /tmp/web-cert.pem /etc/dcc/web-cert.pem
mv /tmp/web-cert.key /etc/dcc/web-cert.key
```

9. Fix the owner/group for the file:

```
chown dcc:dcc /etc/dcc/web-cert.*
```

10. Restart the server:

```
service dcc restart
```

**Related information**

Replacing the default certificate with a new self-signed certificate on page 46

## 4.6.4 Connecting a device over HTTPS

You can connect a Dolby Voice device to your Dolby Conferencing Console securely over HTTPS.

### About this task

When you plug in a device and it powers up for the first time, it launches an out-of-box wizard. This wizard requests some basic information for its network connection, along with information about a provisioning server.

When you use the Dolby Conferencing Console software as a provisioning server, you are prompted to accept the server identity (server certificate). Verify the server certificate information, and then accept it.

**Note:** Without an accepted server identity, a Dolby Voice device is not able to connect to the Dolby Conferencing Console server, and it displays a warning on the home screen.

### Procedure

1. Plug in the device.
   A configuration screen begins a setup wizard. Follow the wizard until you get to the **Provisioning Configuration** screen.
2. For provisioning type, select **static**.
3. For protocol type, select **https**.
4. For host name, enter the fully qualified host name (for example, *dcc.your-company*.net).

   **Important:** This server host name must match the common name used when you replace the default certificate with a CA certificate or a new self-signed certificate.
5. If the Dolby Conferencing Console software is configured to restrict access to the server, enter the user name and password as requested.

### What to do next

If the Dolby Conference Phone is not able to connect to the Dolby Conferencing Console software over HTTPS, the device displays a red warning icon on the Dolby Conference Phone home screen. Change the device provisioning server settings under the administrative settings menu.

1. Log in to the device using the default Dolby Conference Phone administrator password 1739.
2. Tap the **Settings** menu, then tap **Provisioning Server** and **Accept server identity**.
3. When server certificate information displays, confirm all of the data by scrolling to the bottom and then tapping **Confirm**.

   The device reboots and picks up the changes. It then reconnects to the Dolby Conferencing Console software over HTTPS.

Steps 1–3 describe the manual setup process. Alternatively, you can set the Dolby Conference Phone so that it detects the Dolby Conferencing Console address, and then you can avoid entering the address manually.

For example, in the DHCP server, use **option 66** for the Dolby Conference Phone to automatically connect to the Dolby Conferencing Console software. In option 66, enter https://*dcc.yourcompany*.net , where *dcc* is your Dolby Conferencing Console host name.

**Note:** If you performed steps 1–3, you do not need to enter the company name in option 66. For more information, see the *Dolby Conference Phone Administrator's Guide*.

### Related information

Replacing the default certificate with a new self-signed certificate on page 46
Replacing the default server certificate with a CA certificate on page 47

## 4.6.5 Configuring HTTP and HTTPS access

You can increase security by disabling HTTP access on port 80. You can optionally allow HTTPS access.

### Procedure

1. Disable HTTP port 80.

   The HTTP port (80) can be disabled completely to increase security for Dolby Conferencing Console.

   a) Make the /etc/dcc/web.ini file writable:

   ```
   chmod +w /etc/dcc/web.ini
   ```

   b) Delete the first line from that file where it enables port 80.

   c) Restart the Dolby Conferencing Console software:

   ```
   service dcc restart
   ```

   d) Make the /etc/dcc/web.ini file read only again:

   ```
   chmod -w /etc/dcc/web.ini
   ```

2. (Optional) Enable HTTPS access through the server firewall.

   In some cases, it is possible that the firewall has disabled port 443 access. To open port 443 for HTTPS access and check the status of the firewall, use these commands:

   Example for Redhat 6 and CentOS 6.0:

   ```
   iptables -I INPUT -p tcp -m tcp --dport 443 -j ACCEPT
   service iptables save
   service iptables status
   ```

   Example for Redhat 7 and CentOS 7.0:

   ```
   firewall-cmd --zone=public --add-service https --permanent
   firewall-cmd --reload
   firewall-cmd --list-all
   ```

## 4.6.6 Enabling SSH access on open virtual appliance file installations

SSH access is disabled by default on open virtual appliance file installations. You can optionally enable SSH access.

### About this task

On open virtual appliance file installations, perform these steps to enable root user access through port 22 (SSH) by editing the **sshd_config** file:

### Procedure

1. Enter this command:

```
vi /etc/ssh/sshd_config
```

2. Change `PermitRootLogin no` to `PermitRootLogin yes`.
3. Save the file.
4. Restart **sshd** with this command:

```
service sshd restart
```

## 4.7 Setting the time zone

Use the Linux command line on the Dolby Conferencing Console server to update the symbolic link for /etc/localtime to match your local time.

### Prerequisites

To set the time zone, you need to know the Linux `root` password for the server. For open virtual appliance file deployments, the default `root` password is `dolby`. We recommend that you change the default password; a colleague may have already done so for your server. For RPM installations, Dolby software never sets your `root` password; consult the other system administrators in your organization to learn the password.

### Procedure

1. Log in as `root`, and locate the correct time zone file under /usr/share/zoneinfo.
2. Save a copy of the old symbolic link at /etc/localtime, and then update the link to reflect your time zone.

```
cp /etc/localtime /root/old.timezone
rm /etc/localtime
ln -s /usr/share/zoneinfo/my_zone /etc/localtime
```

3. Restart the Dolby Conferencing Console server:

```
service dcc restart
```

4. If you have a multiple-server installation, repeat these steps on each server.

# 5 Basic system usage

This chapter provides information on some basic tasks and a brief description of interactions between devices and the system.



## 5.1 Screen elements and their meanings

This section shows and describes the basic user-interface elements.

This table explains the Dolby Conferencing Console user interface.

| Button | Name | Description |
|---|---|---|
|  | Device edit | Edit device details. |
|  | Device information | Display device information. |
|  | Device list | Display list of devices in a pool. |
|  | Home | Return to home screen. |
|  | Logs | View system logs or device logs. |
|  | Search | Search for string across all pools and devices. |
|  | Settings | Display setting for selected device or pool. |
|  | Status | Display server and reference information and device pool call usage. |
|  | System settings | View/edit system settings. |
|  | Upload | Upload a file or files. |
|  | Users | Display information about users and controls for adding and editing users. |
|  | Add | Add a new pool or device. |
|  | Cancel | Cancel process. |
|  | Confirm | Confirm an action. |
|  | Download | Download information or certificate. |

| Button | Name | Description |
|---|---|---|
|  | Edit | Edit profile or other settings. |
|  | File | Access to a certificate or other file. |
|  | Help | View context-sensitive help. |
|  | Move | Move devices between pools. |
|  | Next | Next step of a task. |
|  | Push configuration | Push configuration from the Dolby Conferencing Console software to devices. |
|  | Reboot | Reboot a device or pool of devices. |
|  | Remove | Remove a device or pool of devices. |
|  | Trash | Delete. |

# 5.2 Search

To avoid clicking through pages to find the information, use the search feature to find the information that you need about your conference devices.

Search behaves the same way on every page. Predictive results display while you are typing. Type criteria associated with specific devices, device pools, or profiles, such as:

- Device display name
- Serial number
- Media access control (MAC) address
- IP address
- Firmware version number
- Profile name
- Device pool name
- CA certificate

The search results box is divided into six sections:

- Certificates
- Device pools
- Dolby Conference Phones
- Dolby Voice Rooms
- Firmwares
- Profiles

You click on the entries listed under the section name, not the section name itself.

# 5.3 Logging in and logging out

Use the Dolby Conferencing Console web interface to log in.

### Prerequisites

Before you can log in, you must have the IP address or host name of the Dolby Conferencing Console server. You can use the **`ifconfig`** command to obtain the IP address.

### Procedure

1. From an Internet browser, enter the IP address or host name of the Dolby Conferencing Console server.

   **Note:** If you have configured secure access, use an https:// URL to access the server.

2. Log in with the default user name and password (`admin`, `admin`) or your assigned user name and password.

   **Note:** User names and passwords are case sensitive. We recommend that you change the default password as soon as possible for security reasons.

3. Click **Log out**.

### What to do next

Non-LDAP users can retrieve passwords on their own with the **Forgot Password** link. However, this link displays only after the user enters an incorrect password.

### Related information

Resetting lost passwords for non-LDAP users on page 82

# 5.4 Editing system settings

Many Dolby Conferencing Console settings are accessible from the Dolby Conferencing Console web interface.

### About this task

You can edit certain settings that affect all users and devices, such as LDAP, and SMTP settings.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.

2. On the left side, click the other settings button.

   Submenus for LDAP and SMTP settings display.

3. From the menu, choose the type of setting that you would like to edit.
   The chosen screen displays.

### What to do next

After you set up the system, consider how your devices will be organized and set up device pools.

## 5.5 Provisioned parameters and locked devices

Users cannot change provisioned parameters. Performing a Dolby Voice device configuration by using the Dolby Conferencing Console software triggers a lock on the configured device. This prevents the device from being modified from its user interface.

When unlocked, the device itself does allow for local changes of more parameters than are available from the Dolby Conferencing Console software, including the device static IP address and provisioning server connection information. These parameters cannot be changed from the Dolby Conferencing Console software, because performing those changes will cause the device to lose connectivity with the Dolby Conferencing Console software.

# 6 Managing devices

The Dolby Conferencing Console software streamlines many of your management tasks with its simple user interface. With it, you can view status information for your entire system, manage devices, and manage pools of devices by using profiles.



## 6.1 Setting up devices

After you install the Dolby Conferencing Console software and deploy it on your network, the next step is to complete some initial setup tasks so that you can start using the Dolby Conferencing Console software to manage Dolby Voice devices.

Typically, initial setup includes performing these tasks:

1. Device pool management on page 56
2. Updating device firmware on page 78
3. Adding profiles on page 61
4. Uploading certificates for use with devices on page 58
5. Adding a device on page 65

## 6.2 Device pool management

You can group devices together for the purpose of sharing profile attributes in a single pool, called a device pool. You can also create device pools to separate out devices that require different attributes.

When you install the Dolby Conferencing Console software, it creates a default device pool. The default device pool cannot be deleted or renamed.

You can provision a connected device to a device pool or reassign it to another device pool.

Each device pool can have a single, specific device firmware version for each hardware type.

A device pool can contain numerous CA certificates.

You cannot delete a device pool if it contains any devices. Before deleting, you must first move all devices to another pool or delete them.

**Note:** Any change in a trusted CA certificate that is already associated with a device results in an automatic device reboot.

### 6.2.1 Adding device pools

Add new device pools to group devices in ways that make them easy to manage.

**Procedure**

1. From the Dolby Conferencing Console web interface, on the home screen, click the add button adjacent to **Device Pools**.
   
   The **Create New Device Pool** screen displays.
2. Enter a unique device pool name (for example, `DP1_Sydney`).

   **Note:** The device pool name cannot have the same name as an existing device pool.
3. (Optional) Enter a description for the device pool (for example, `Sydney Office Area 1 device pool`).
4. (Optional) Enter the device pool location (for example, `Sydney, Australia`).
5. (Optional) Enter the IT administrator name (for example, `jdoe`).
6. (Optional) Enter an email address (for example, `jdoe@yourcompany.com`).
7. (Optional) Enter a phone number (for example, `+61 02 5555 1111`).
8. (Optional) If you need to restrict access to the device pool, enable the restriction:
   a) Enter a device access ID and password.
   b) Verify the password by entering it again.
9. (Optional) Enter an email address if you want to be sent emails when there are device status changes in this pool.
   The SMTP server must be configured in **System Settings > SMTP Settings** before emails can be sent. You can send a test email once the SMTP server has been configured.
10. Click the confirm button to save your changes.

**Results**

The home screen redisplays with the new device pool at the bottom of the list.

## 6.2.2 Editing device pools

You can edit your device pools as a group.

**Procedure**

1. From the Dolby Conferencing Console web interface, on the home screen, select a device pool to edit.
   The device pool list displays.
2. On the left side, click the settings button.
   
3. From the settings menu, click **Edit pool settings**.
   The **Device pool settings** screen displays.
4. Make the desired changes.
5. To save your changes, click the confirm button.

## 6.2.3 Deleting device pools

Any empty device pool (except for the default pool) can be deleted.

### Prerequisites

Before you delete a device pool, you must either delete or move all devices from the pool.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool from the list.
2. On the left side, click the settings button.
   
3. From the settings menu, select **Edit pool settings**.
   The **Device pool settings** screen displays.
4. Click the trash button to delete.

### Results

The home screen displays the updated list.

## 6.2.4 Enabling device access restriction

Enabling device access restriction requires you to enter an ID and password in order to obtain provisioning information for any device in this pool. We highly recommend that you enable device access restriction to prevent unauthorized users from having unrestricted access to your device pool configurations, including passwords and instances.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool from the list.
2. On the left side, click the settings button.
   
3. From the settings menu, select **Edit pool settings**.
   The **Device pool settings** screen displays.
4. To enable **Device access restriction**, toggle the **ON/OFF** button..

   The **ON/OFF** button not only enables and disables **Device access restriction**, it also displays the state in which it's in.
5. Enter the **Device access ID**.
6. Enter the **Device access password**.
7. Click the check mark icon to save your changes.

## 6.2.5 Uploading certificates for use with devices

The Dolby Conferencing Console software allows you to upload certificates for later use, as needed.

### Prerequisites

**Note:** The certificates that you upload must be in Privacy-enhanced Electronic Mail (PEM) or Distinguished Encoding Rules (DER) format with the .pem, .crt, or .cer file-name extension.

**Procedure**

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.

2. On the left side, click the upload button.

3. From the **System upload** screen, perform one of these steps:
   - Drag and drop the certificate file to the system upload screen.
   - Click the select file button to browse the computer to find the CA certificate, and then click the upload icon to upload the file to the Dolby Conferencing Console server.


   If the file format is invalid or not recognized, this error message displays:

   `The file <filename> has an invalid file extension.`

## 6.2.6 Trusting certificates

You can add certificates to use for specific devices within the pool, or to use for the entire pool.

**Procedure**

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool from the list.
   The device list displays.
2. Select the device or devices for which you want to add certificates. You can also select all the devices under the device pool.
3. On the left side, click the settings button.

4. From the settings menu, select **Certificates**.
   The **System certificate store** screen displays.
5. Perform one of these steps:
   - Select only the certificates in the list that you want to trust.
   - Check **Select all**.

   This message displays:

   `You are about to change the CA certificate settings for this device pool. Do you wish to continue?`
6. Click the confirm button.
   An update confirmation displays.
7. To download the system certificate store to all devices in the device pool, click the confirm button in the pop-up window.

A change in the trusted CA certificate results in a device reboot.

## 6.2.7 Adding inventory information to device pools

Add inventory information to device pools so that you can then search devices based on city, state, country, department, or company. You can also add custom inventory information based on the needs or your organization.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool from the list.
   The device list displays.
2. On the left side, click the settings button.
   
3. From the settings menu, select **Inventory**.
4. Enter your information, and click the confirm button.

### What to do next

You can override inventory settings at the device level, if needed. For example, if there is a specific device that requires different inventory information, open the configuration page for that device, and then click the **Inventory** tab. From there, add or edit inventory information, and it will apply only to that one device.

## 6.2.8 Searching inventory

You can search devices based on pools, hardware type, device status, alarm state, call state, city, state, country, department, company, or custom inventory information.

### About this task

This task explains how to search inventory from the Dolby Conferencing Console web interface. However, you can also search inventory with Web API.

### Procedure

1. From the Dolby Conferencing Console web interface, on any screen, click the search button in the upper-right corner.
   
   The search field displays.
2. Below the search field, click the **Inventory Search** link.

   The **Inventory Search** page displays.
3. Use the drop-down lists and check boxes on the left side of the screen to further refine the results of your search.

### What to do next

Export the results of your inventory search, if desired.

### 6.2.9 Exporting information from an inventory search

You can export the results of an inventory search to a .csv file.

**About this task**

The report includes the same information that you see onscreen:

- Name
- Serial number
- Mac address
- IP address
- VLAN ID
- Software version number
- Alarm status
- Call state
- Uptime (in seconds)
- Pool name
- Hardware type

**Procedure**

From the **Inventory Search** page, click **Export CSV**.

## 6.3 Device profile management

Profiles provide you with a convenient way to group configuration parameters and apply them to groups of devices.

When you create a profile, it can be shared by multiple pools. Profiles can exist in the system even when it is no longer used by any pool. If a profile is removed from all pools but not explicitly deleted from the system, it appears in the list of available profiles each time you begin the procedure for assigning a profile to a device pool. To completely remove a profile from the system, you can delete it by clicking on the delete button in the **All profiles** page.

### 6.3.1 Adding profiles

Use the web interface to create new profiles and specify whether they are shared. You can create a profile within an existing pool, or you can create a stand-alone profile and assign it to a pool later.

**Prerequisites**

Before creating a new profile for a pool, make sure either that you have created a suitable pool for the profile, or that it makes sense to create the profile within the default pool. Also make sure that your firmware version is 2.1.x or later.

**About this task**

Some information on configuration parameters is provided in context-sensitive help and can be viewed by hovering the mouse. For more detailed information, see the *Dolby Conference Phone Administrator's Guide*.

These steps explain how to add a profile to an existing pool. To create a new profile outside the existing pools, begin from the **System: All profiles** page and skip to step 3.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the pool where you want to create the new profile.
   A screen displays the pool with a listing of all its devices.
2. From the **Settings** menu, select **Profiles**.
   The **Current profiles** screen displays.
3. Create a new profile by clicking the add button.
   The **Create new profile** screen displays.
4. (Optional) If you are creating a profile outside an existing pool, the newest firmware gets selected automatically. You can choose an older version from the **Firmware version** list box.

   If you are creating a profile in an existing pool, the new profile uses the same firmware as the pool.
5. Enter a profile name and continue editing as needed, until you have the desired configuration:
   - Drag any desired configuration parameters defined on the left side to the entry area on the right.
   - Delete any added parameter by clicking the cancel button.
6. To save your changes, click the confirm button.

   If you want to update all devices in pools using this profile, click the confirm button in the update-confirmation pop-up. Otherwise, click the cancel button and perform the update at a later time.

### Results

If you created the profile in an existing pool, the profile list screen displays all profiles in the indicated device pool. If you created the profile from the **System: All profiles** page, the **Update profile** page for the new profile displays.

## 6.3.2 Editing profiles

Use the web interface to edit an existing profile.

### About this task

For more detailed information about configuration parameters, see the *Dolby Conference Phone Administrator's Guide*.

These steps explain how to edit a profile in an existing pool. To edit a profile outside the existing pools, begin from the **System: All profiles** page and skip to step 3.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool with the profile you want to edit.
   A screen displays the device pool with a listing of all its devices.
2. On the left side, click the settings button.
   
3. From the settings menu, select **Profiles**.

The **Current profiles** screen displays.

4. Select the profile you wish to edit from the list.
   The list of parameters for the profile appears on the right side of the screen.
5. Click the modify selected profile button.
   
   The **Update profile** screen displays.
6. Edit as needed, until you have the desired configuration:
   - Drag any desired configuration parameters defined on the left side to the entry area on the right.
   - Delete any added parameter by clicking the remove button.
7. To save your changes, click the confirm button.
   If you want to update all devices in pools using this profile, click the confirm button in the update-confirmation pop-up. Otherwise, click the cancel button and perform the update at a later time. To resolve profile conflicts, see Resolving profile conflicts on page 63.

**Results**

The **Current profiles** screen displays again.

**Related information**

Resolving profile conflicts on page 63

## 6.3.3 Resolving profile conflicts

If a configuration parameter exists in more than one profile assigned to a single pool, this is viewed as a conflict. Use the web interface to resolve profile conflicts.

**About this task**

If a configuration parameter exists in more than one profile, but those profiles are not all assigned to the same pool, this is not viewed as a conflict.

Any parameter setting that is used in more than one profile within a pool creates a profile conflict. Profile conflicts display in red. When you make changes to profiles, you may discover that you have created a profile conflict.

**Procedure**

1. From the home screen, select the device pool, then from the left sidebar, click **Settings** and select **Profiles**.
   The **Current profiles** screen displays, with any conflicts highlighted in red.
2. Resolve any existing conflicts:
   a) To get more information about the conflict, click the help button next to the configuration parameter.
   A pop-up displays with more information about the conflict (for example, which profile already has the parameter defined).
   b) Remove conflicting configuration parameters from one or more profiles.
   c) Save the changed profiles.

**Related information**

Editing profiles on page 62
Provisioning firmware on page 79

## 6.3.4 Removing a profile from a pool

Removing a profile from a pool does not remove the profile from the system,.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool from the list.
   The device list displays.
2. On the left side, click the settings button.
   
3. From the settings menu, select **Profiles**.
   The **Current profiles** screen displays.
4. From the list, highlight the profile that you want to delete.
5. Click the modify selected profile button.
   
6. Click the remove button.
   
   The message `The profile <name> is about to be removed from this device pool. Do you wish to proceed?` displays.
7. Click the confirm button.
   The profile notification screen displays.
8. Choose from these options:
   - If you want to update all devices in the device pool now, click the confirm button in the update-confirmation pop-up.
   - To update all devices at a later time, click the cancel button.

### Results

The profile list screen displays. All profiles in this device pool are shown.

## 6.3.5 Deleting profiles

Use the web interface to delete a profile that does not belong to any pools.

### Prerequisites

If you need to delete a profile from the Dolby Conferencing Console software, you must first remove it from all pools. Only then will you be able to delete the profile from the system.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.
   
2. On the left side, click the other settings button.
   
3. From the settings menu, select **Profiles**.

The **All profiles** screen displays a comprehensive list of profiles and the pools to which they are assigned.

4. From the list, select the desired profile.
   The message `A profile that is not assigned to any device pool can be deleted permanently from the server. Do you wish to proceed?` displays.
5. Click the confirm button.

**Results**

The profile no longer displays on the screen.

### 6.3.6 Viewing all profiles

You can use the web interface to view all profiles in the system.

**About this task**

Although you typically want to view profiles within the context of a pool, you can also view a list of all profiles in the system.

**Procedure**

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.
   
2. On the left side, click the other settings button.
   
3. From the settings menu, select **Profiles**.

**Results**

The **All profiles** screen displays a comprehensive list of profiles and the pools to which they are assigned.

## 6.4 Device management

You can add devices, edit device parameters, delete devices, and move devices to other pools.

### 6.4.1 Adding a device

It is possible to add a device by simply plugging it in (as long as the system is properly set up); however, you can also add devices explicitly in the Dolby Conferencing Console software.

**Procedure**

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool to which you want to add a device:
   - If the pool contains no devices, the **Initial configuration** screen displays and prompts you to add devices to the device pool.
   - If the pool does contain devices, the device list displays.
2. Click the add button.

The **Create new phone record** screen displays.

3. Choose the device hardware type from the popup menu.

   If a device hardware type is not chosen, an error message displays.

4. Enter the MAC address of the Dolby Conference Phone that you want to add.

   - If the value that you enter is not a valid MAC address, an error message displays. Try again.
   - If the media access control addressaddress you entered has already been configured for another device, the message `Re-enter a MAC address using one that is not already configured` displays. Try again

5. Click the arrow button to navigate to the next step.
   Once the device is added and is ready to configure, the **Phone configuration** screen displays.

6. To immediately proceed with configuration, continue with these steps. Otherwise, click the cancel button and perform the configurations from the profile page:

   a) Enter the device name that you want to use.

   **Note:** The display name is not automatically displayed when entered. It is not displayed until the device is actually connected to the Dolby Conferencing Console software, as the device list relies on the device reported value. If you create an entry without the device, the entry will contain only the hardware type and the MAC addres.

   b) If one of the selected parameters is in another profile in the device pool, the parameter displays in red. Resolve the conflict.

   c) To save your changes, click the confirm button, and to update, click the confirm button again. Otherwise, click the cancel button.

### Results

The device information page displays.

### Related information

Resolving profile conflicts on page 63

## 6.4.2 Editing device parameters

Device parameters allow you to set parameters and apply them to a specific device. You can edit device parameters by using the web interface.

### About this task

Once applied to a device, device parameters overwrite any profile settings. Typical device parameters are SIP registration credentials and device display name.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool that contains the devices for which you want to edit parameters.
   The device list displays.

2. Select the device you want to edit.

   Use the right-click menu if you want to open the **Device information** screen in a new tab or window.

The **Device information** screen displays.

3. In the left navigation bar, click the edit button.
   The **Device information** screen displays.
4. To view the contents of a configuration parameter category, click the associated add button.
5. Drag any desired parameters from the list of those available (in the left pane) to the right entry pane.
   Details of all added parameters immediately display.
6. To remove a configuration parameter from a profile, click the **X** next to the text entry box for that parameter.
   The parameters you have deleted are moved to the available-parameters pane.
7. To save your changes, click the confirm button.
8. To update the device immediately, click the confirm button. Otherwise, click the cancel button and update the device at a later time.

## 6.4.3 Deleting devices

You can delete devices from a device pool.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool from the list.
   The device list within the selected device pool displays.
2. Select the devices that you want to remove by checking the boxes on the left side of the screen.

   You can select all the devices by:

   - Checking the top check box.
   - Clicking the triangle and choosing **All devices**.
3. Click **Actions** > **Delete** .
4. Confirm that you want to delete this device.

### Results

The device list displays with the deleted device removed from the list.

## 6.4.4 Moving devices between pools

Working from the device list of a device pool, you can move multiple devices to another pool. Working from the device information page, you can move that particular device to another pool.

#### Moving multiple devices to another device pool

You can move several devices to a different device pool with one operation.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool from the list.
   The device list displays.
2. Select the devices that you want to move by checking the boxes on the left side of the screen.

You can select all the devices by:

- Checking the top check box.
- Clicking the triangle and choosing **All devices**.

3. Click **Actions** > **Move**.
4. From the dropdown list, select the device pool to which you want to move the devices.
5. Click the confirm button to save your changes.
6. If you want to immediately update all of the devices that you moved, click the confirm button in the update-confirmation pop-up. Otherwise, click the cancel button to update the devices later.

**Moving one device to another pool**

Use the device information page to move a device to a different pool.

Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, select the device pool from the list.

   The device list displays.

2. Click on a device.

   The device information page displays.

3. Below the screen shot of the phone display, click **Move**.

4. Make a selection from the **Select a device Pool** drop-down list box, and click the confirm button.
5. Click the confirm button in the **Push Configuration Changes** pop-up to move the device.

# 6.5 Contact directory management

You can provision a local contract directory of up to 1,000 names and numbers on the devices in a pool. You can upload directory files, edit contact directories, and assign directories to pools.

Each pool may have zero or more contact directories assigned, totaling up to 1,000 contacts. If the total number of contacts exceeds 1,000, the directory that the Dolby Conferencing Console server downloads to the devices in the pool gets truncated to the first 1,000 entries.

You can assign a contact directory to multiple pools. If a contact directory is not assigned to any pools, you can delete it.

To see a list of all directories on the **System: All directories** screen, from the **Dashboard** select **Settings** > **Settings** > **Directories**.

Phone numbers may be extension numbers in your PBX or external numbers.

Contact directory files are .json text files that contain one or more contact entries in this format:

```
{
    "entries": [{
        "firstName": "Ben",
        "lastName": "Kennedy",
        "number": "2222"
```

```
    },
    {
        "firstName": "Leslie",
        "lastName": "Stewart",
        "number": "2324"
    }]
}
```

The `firstName` and `lastName` fields may each contain up to 32 characters. The `number` field may contain up to 15 digits.

## 6.5.1 Creating a contact directory for the current pool

When you create a contact directory, you can assign it to the current pool or to multiple pools. Contact directories are initially empty.

### About this task

**Note:** You can also create a contact directory from the **System: All directories** screen.

### Procedure

1. Navigate to the page for a pool to which you want to assign the new contact directory.
2. Select **Settings** > **Directories**.
   The **All directories** screen appears.
3. Click **Add directory**.
   The **Create a new directory** screen appears.
4. Enter a **Name** and **Description** for the contact directory.
5. Optionally, select additional pools to which to assign the new directory.
6. Click **Save**.

### What to do next

Click **View Entries** to begin creating contacts or to upload a file that contains contacts.

## 6.5.2 Adding contacts to a directory

You can add individual contacts to an existing contact directory, or upload a file that contains multiple contacts and add them to a directory.

### Procedure

1. Select **Settings** > **Directories**.
   The **All directories** screen for the pool appears.
2. Click the directory to which you want to add contacts.
3. Click **View Entries**.
4. Perform one of these steps:
   - To upload a contacts file, click the select file button and browse to the file on your local computer.

- To create a single new contact, click add directory entry button and enter the **First Name**, **Last Name**, and **Number**.

**Results**

After you upload the file or enter the new contact, the updated directory is pushed to the devices in the current pool and the devices in any other pools that use this contact directory.

### 6.5.3 Assigning an existing contact directory to a pool

All contact directories on the system are available for assignment to any pool.

**Prerequisites**

Navigate to the screen for the pool to which you want to add the contact directory.

**Procedure**

1. Select **Settings** > **Directories**.
   The **All directories** screen appears.
2. Click **Add directory**.
   The **Create a new directory** screen appears.
3. Click **Assign from system directories**, and select one or more directories.
4. Click **Save**.

## 6.6 Monitoring device status

You can view and download a variety of status information about the Dolby Voice device from Dolby Conferencing Console, especially if the statistics feature is enabled on the device.

**Note:** While you are viewing a list of devices, you can click a device to see its **Device information** screen in the current browser tab, or use the right-click menu to open the **Device information** screen in a new tab. If you are investigating problems that affect multiple devices, opening a separate tab for each **Device information** screen can often be helpful.

**Related information**

Reviewing Dolby Conferencing Console user activity logs on page 81

### 6.6.1 Enabling call statistics

You can enable call audio statistics and view WebRTC logs through Dolby Conferencing Console.

**About this task**

If you want to be able to review call records in the future, you must first enable the call audio statistics feature. Call audio statistics can be enabled for a pool or a single device.

Call records are recorded only after call audio statistics is enabled. For example, if you enable call audio statistics, the system does not provide call records of past calls.

Call audio statistics and WebRTC logs can be enabled from Dolby Conferencing Console or from the phone web interface. By default, these are both disabled.

For video conference calls, if enabled the WebRTC logs are shown beneath the audio statistics when viewing the call record.

**Procedure**

1. To enable call audio statistics from the Dolby Conferencing Console:
   a) Click **Logging** > **Audio**, and then drag **Audio Logging Level** to the device configuration.
   b) Set `Logging.Audio.Mode` to `Statistics`.
2. To enable audio call statistics from the phone web interface:
   a) From the **Settings** tab, navigate to **Logging** > **Audio**.
   b) Set `Audio Logging Level` to `Statistics`.
3. To enable WebRTC statistics from the Dolby Conferencing Console:
   a) Click **Logging** > **WebRTC**, and then drag **Debug Trace** to the device configuration.
   b) Set `Logging.WebRTC.DebugTrace` to `On`.
4. To enable WebRTC statistics from the phone web interface:
   a) From the **Settings** tab, navigate to **Logging** > **WebRTC**.
   b) Set `Debug Trace` to `On`.

**Results**

Each time a new call is placed from a device, call audio statistics and WebRTC statistics will be available when viewing the call, if they are enabled and appropriate.

**Related information**

Viewing recent calls on page 71

## 6.6.2 Viewing recent calls

The recent calls list provides a high-level overview of all recent calls on a particular Dolby Conference Phone. It includes general information about calls such as call type, start time, duration, and number of participants.

**About this task**
The recent calls list is always available. However, if you want to view detailed diagnostic information about calls, then you must enable call statistics.

**Procedure**

From the Dolby Conferencing Console web interface, choose a device and then click the **Logs** button.

The recent calls list displays.

**Related information**

Enabling call statistics on page 70

## 6.6.3 Viewing call records

If audio statistics is enabled, information about calls are recorded in call detail records (CDRs). You can view or download these records that contain statistics about calls, including

information on jitter, packet loss, and audio level. Video conference calls can also have WebRTC statistics. These will be displayed below the audio stats.

**About this task**
Audio and WebRTC statistics for a particular call are available only if the audio statistics or WebRTC Debug Trace features were enabled on the phone before the call was made.

**Procedure**

1. From the Dolby Conferencing Console web interface, choose device and then click the logs button.

   The recent calls list displays.

2. Choose a call, and then click the more information button.

   The call statistics screen displays.

   If the audio statistics feature is enabled, this information displays. If not, no audio statistics are available.

   **jitter**
   Variations in the amount of time required for audio packets to flow from one point to another on the network, resulting in sound distruptions. Measure in milliseconds (ms).

   **packet loss**
   The percentage of lost packets.

   **audio level**

   The **In level** shows the input level coming from the microphone on the Dolby Conference Phone.

   The **Out level** shows the output level coming from the speaker on the phone.

   You can use this information to understand when a speaker in the room talked and where they were speaking from (for example, the far end of the room).

   If WebRTC statistics are available for the call, this information is also displayed.

3. From the drop-down list, choose from these types of statistics:

   - **To and from the phone**
   - **To the phone**
   - **From the phone**

4. Click the download button.

   A raw data file downloads. This is a .zip file that includes .json files.

   If WebRTC statistics are available, these will also be in the .zip file.

   If you submit a support request to Dolby for an audio problem, include this file in your support request, if possible.

## 6.6.4 Viewing event logs

If statistics is enabled, events on the Dolby Voice device are recorded. You can then view and download events logs from Dolby Conferencing Console.

**About this task**
The event log captures a wide range of events that happened on the phone. For example:

- When calls were placed
- When calls ended
- When a problem occurred
- When the device rebooted

**Procedure**

1. From the Dolby Conferencing Console web interface, navigate to a device.
2. Click the logs button.

   The recent calls list displays.
3. Click the **Event logs** tab.
   A list of event logs displays.
4. Click the download button.

**Results**
The event log downloads as a .txt file.

## 6.6.5 Viewing core dump logs

If statistics is enabled, core dumps on the Dolby Voice device are recorded. You can then view, but not download, core dump logs from Dolby Conferencing Console.

**About this task**
If the device unexpectedly reboots and generates a core dump, contact Dolby for support and analysis of the problem. You may need to specify when the core dump occurred, and you can get this information from the log.

**Procedure**

1. From the Dolby Conferencing Console web interface, choose device and then click the logs button.

   The recent calls list displays.
2. Click the **Core dumps** tab.

   A list of core dump logs displays.

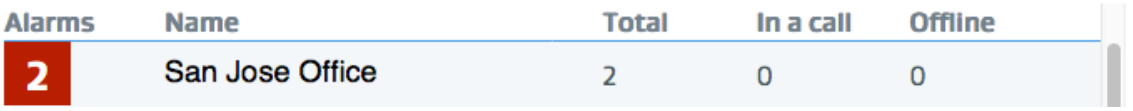
## 6.6.6 Responding to device alarms

From Dolby Conferencing Console, you can get a quick view of how many devices have issues. Look for red device alarms to help you know when there is a problem and to troubleshoot the problem.

**Procedure**

1. From the Dolby Conferencing Console web interface, navigate to the device pool with alarms.

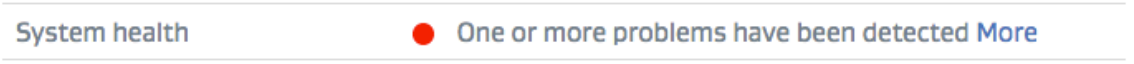
The alarms number represents the number of devices with alarms. For example, if **2** appears in red next to the name of a device pool, two devices in the device pool have alarms.




2. From the device pool, select a device with an alarm.

   The **Device information** screen displays.

   A red alarm displays next to **System Health** along with a basic description of the problem.



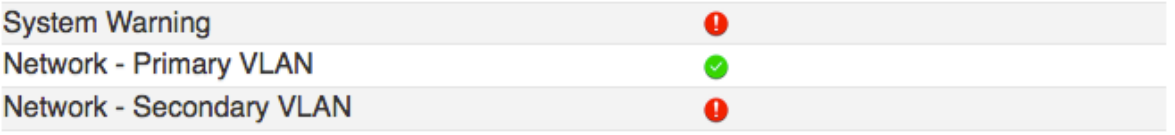

3. Click **More** to get more information about the problem and troubleshooting suggestions.
4. Review the categories below **System Health** for any other subalarms and additional information about problems.

**What to do next**

If you cannot find enough information about the problem from Dolby Conferencing Console, you can alternatively go to the device web interface.

For example, click the phone IP address and, when the device web interface displays, log in, if prompted. Then click the **Status** tab, expand the sections on the screen, and review them for red alarms.

For example, the alarms look like this:




# 6.7 Importing device configurations

You can import device configurations instead of adding devices one at a time manually.

**About this task**

For importing device configurations, a dowloadable template is provided that contains required and optional columns.

Required columns are MAC address and hardware type. Optional columns can be device configuration parameters, such as `Sip.Account.DisplayName`, `Sip.Credential.Name`, and so on.

For bulk uploads, you must import all of the devices into one pool. If you want to upload the devices to different pools, you have to perform a separate upload for each pool.

**Note:** Exported inventory files cannot be uploaded to Dolby Conferencing Console as device configuration files.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button  in the upper-right corner.
2. On the left side, click the upload button.
3. Perform one of these steps:
   - Drag your configuration file to the page.
   - Click the select file button  to select a file, and click **Upload**.

   Once the files are uploaded, you can view the summary of devices that will be imported into Dolby Conferencing Console.

   The file may be rejected if it has an incorrect file extension, duplicate column headers, or missing required columns. If this happens, you must make the appropriate corrections before reuploading the file.
4. Select a device pool from the drop-down list.

   You can choose only one. If needed, you can move certain devices to different pools after you import.
5. Review the information, and click **Next**.

# 7 System maintenance

System maintenance involves upgrading and downgrading the Dolby Conferencing Console software, updating device firmware, and database management.



## 7.1 Backing up the database

Periodically back up your database in case you encounter a problem and need to restore data. It is particularly important to back up the database as a precaution before you install an upgrade.

### About this task

Backing up your data is an important precaution. It protects you in case you encounter a problem with an upgrade. Data from newer versions is not guaranteed to be backward compatible with older versions. If you need to downgrade to an earlier version in the future, that is when you may need the backup to restore data.

### Procedure

1. From the Dolby Conferencing Console server, use the command line to log in as the root user.
2. Stop the Dolby Conferencing Console server by typing `service dcc stop`.
3. Back up your current Dolby Conferencing Console data by entering this command:

   ```
   su -m dcc -c "/usr/bin/dcc-backup /tmp/dcc-backup-07272018.dat"
   ```

   In this example, `dcc-backup-07272018.dat` represents a file name of your choosing. Choose a file name that makes sense based on your organization.
4. Copy the backup to a permanent folder:

   ```
   mv /tmp/dcc-backup-07272018.dat /backupfolder/dcc-backup-07272018.dat
   ```

## 7.2 Restoring the database

If you have a backup, you can restore your database to an earlier point. Only restore your database if necessary.

### About this task

Implementing a database restore is potentially dangerous, because it deletes and overwrites files. We suggest that you run the restore to prevent the possibility of damage from a malicious archive.

### Procedure

Log in as root, and enter this command:

```
su -m dcc -c "/usr/bin/dcc-restore --yes dcc-backup-filename.dat"
```

## 7.3 Upgrading the Dolby Conferencing Console software

If you already installed the Dolby Conferencing Console software, you may want to upgrade from an old version to a new version.

### Prerequisites

The Redis server is a new component in Dolby Conferencing Console version 1.2. If you are upgrading from version 1.1.x to version 1.2, you must first install a Redis server. This requirement applies to both open virtual appliance file and RPM installations. For instructions, see Installing and configuring a Redis server on page 30.

- For open virtual appliance file installations, install the Redis server on the virtual machine.
- For RPM installations, install the Redis server on a separate physical or virtual machine.

### Related information

Installation on page 27

### 7.3.1 Downloading the upgrade file

Before you can upgrade Dolby Conferencing Console, you need to download a new RPM package. If you cannot download the software from your provider, use this procedure to download the software from Dolby. We also recommend that you download the latest documentation.

### About this task

Dolby Conferencing Console software packages are available for download from your Dolby Voice device provider and Dolby. Check with your provider first. If your provider does not provide the packages for download, the RPM package, open virtual appliance file, and documentation are all available on the Dolby Voice device support page on dolby.com.

You need the upgrade file only if your original installation used the RPM package. If you original installation used the open virtual appliance file virtual machine, you can skip this procedure.

### Procedure

1. Go to the Dolby website.
2. Click the **Support** tab.
3. Scroll down to **Dolby Conferencing Console Software and Documents** and click **RPM package**.
4. Accept the End-User License Agreement, and follow any other onscreen instructions to download your software.

### What to do next

Download and review the *Release Notes*.

### 7.3.2 Installing the upgrade

Use the Dolby Conferencing Console command line to install the upgrade and restart the server.

**Prerequisites**

Before you upgrade the Dolby Conferencing Console software, make sure you complete all of the necessary prerequisite tasks first, such as backing up your data. See Backing up the database on page 76.

Download and review the *Release Notes* before you begin the upgrade. If the *Release Notes* provide different installation instructions than the steps below, follow the instructions in the *Release Notes* instead.

**Procedure**

1. From the Dolby Conferencing Console server, at the command line, log in as the root user.
2. Enter `yum upgrade` *`dcc-package-name`* `.rpm` to upgrade the server.
3. At the end of the upgrade, enter `service dcc start` to restart the server.
4. From the Dolby Conferencing Console user interface, confirm that the upgrade is complete.

## 7.4 Updating device firmware

The Dolby Conferencing Console software 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 individual devices and to device pools. During an initial deployment, you will typically upload the latest firmware release to the Dolby Conferencing Console software and then provision that firmware on the devices.

Before you update device firmware, we recommend that you:

- Review the *Release notes* associated with the firmware to learn about any new or changed features.
- Review system settings to see if there is a need for any new or changed configuration parameters.
- Verify that all profiles are still valid.
- Review existing certificates, and create and/or upload any new ones that will be needed as you perform the updates.

### 7.4.1 Uploading device firmware

Use the Dolby Conferencing Console web page to upload firmware to the Dolby Conferencing Console server.

**Procedure**

1. From the **System information** screen, click the settings button.
2. From the **Settings** menu, select **Firmware**.
3. Click the add firmware button.
4. Click the upload button, and perform one of these steps:

- Drag and drop the device firmware file (in .zip format) to the system upload screen.
- Click the select file button to browse the computer to find the device firmware file, and click the upload icon to upload the file to the Dolby Conferencing Console server.

The supported firmware types are Dolby Conference Phone VCP9000 and Dolby Voice Room VPU9000.

If the file format is invalid and not recognized, the error message `The file <filename> has an invalid file extension` displays. Confirm the error, and repeat step 2. The device firmware import displays.

5. To save your changes, click the confirm button.

## 7.4.2 Provisioning firmware

You can update firmware for all devices within a device pool at once.

### Procedure

1. From the **Settings** menu, select **Firmware**.
   Two dropdown lists, one for the phone firmware and the other for the hub firmware displays. If firmware is currently selected, the current firmware screen displays showing when the firmware was built, package size, and signature.
2. From one of the drop-down lists, select a new firmware release.
   If there are any firmware/configuration parameter conflicts in the device pool, the parameters in conflict display in red in the pool profiles list. See Resolving profile conflicts on page 63.
3. To save the updates, click the confirm button in the confirmation pop-up. Otherwise, click the cancel button to provision the updates to the devices at a later time.

### Results

The device list displays again. An animated firmware-update progress bar displays for each updating device until the update is complete.

### Related information

Resolving profile conflicts on page 63

# 7.5 Managing Dolby Conferencing Console users

The default user, created when you install the Dolby Conferencing Console software, is a system administrator with superuser access. You can add any number of additional users, with system administrator or lesser permissions.

Before you create users, make sure you understand what roles you can assign and how they impact what tasks those users can perform.

You can assign these roles to users:

| Role | Permissions |
|---|---|
| System administrator | Full control |
| Device administrator | Can change device configurations, but cannot make changes related to server setup |

| Role | Permissions |
|---|---|
| User | Can view status information and change password only |

## 7.5.1 Adding and editing user accounts

Each user has an assigned role (system administrator, device administrator, or user), which determines privileges.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.

2. On the left side, click the users button.

3. Perform one of these steps:
   - To add a user, click the add button.
   - To edit a user, select a user and then click on the edit button.
4. Enter information about the user into these fields, or update existing information:
   - **User ID**
   - **Use LDAP for authentication**
   - **User password**
   - **Confirm user password**
   - **Authentication settings**

     Note: **Authentication settings** is visible only when editing a user.
   - **Name**
   - **Description**
   - **Location**
   - **Department**
   - **Email**
   - **Phone**
   - **User role**

   **Note:** If you use LDAP for authentication, the user is required to enter their corporate password, so the **User password** field becomes unavailable. Make sure that you enter the login ID correctly. It must match the user's corporate user name.
5. Click the confirm button.

### Related information

Configuring LDAP for user authentication on page 82

## 7.5.2 Reviewing Dolby Conferencing Console user activity logs

The system records logs of Dolby Conferencing Console user activity that can be used for security and audit purposes. Only system administrators can view and download user activity logs.

### About this task

These logs can be accessed from two locations: one provides information about all users, and the other provides information about only a specific user.

Logs can be downloaded as a comma-separated values (.csv) file and include information such as time, user, and the type of event. You can use them to monitor how frequently Dolby Conferencing Consoles are used and by whom, or to help you troubleshoot problems, when needed.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.

2. To view information about all users, on the left side, click the logs button.

3. To view information about specific users, perform these steps:
   a) On the left side, click the users button.

   b) Select a user, and notice that additional buttons display on the right side.
   c) Click the logs button.
   The log displays.
4. If desired, download the log from either page by using the download button in the upper-right corner.


### Related information

Monitoring device status on page 70

## 7.5.3 Changing passwords

You can change your password from the Dolby Conferencing Console web interface.

### Procedure

1. On the home screen (in the upper-right corner), click your user name.
2. Click **Authentication settings**, and then enter your current password.
3. Enter a new password, and then enter it a second time.
4. Click the confirm button to save your changes.

## 7.5.4 Configuring SMTP to reset passwords

You can configure SMTP so that non-LDAP users can reset forgotten passwords.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.

2. On the left side, click the other settings button.

3. From the settings menu, select **SMTP**.
4. Enter information about your SMTP server into these fields:
   - **Sender**
   - **Server**
   - **Port**
   - **User name**
   - **User password**
5. (Optional) Select your encryption preference.
   - **Use none**
   - **Use SSL**
   - **Use STARTSSL**

   The port number is updated based on the selected encryption type.
6. (Optional) Enter an email address if you want to test the new settings .

## 7.5.5 Resetting lost passwords for non-LDAP users

Non-LDAP users can reset forgotten passwords with the **Forgot Password** link.

### Prerequisites

SMTP must be enabled.

### About this task

**Forgot Password** is supported only for non-LDAP users.

### Procedure

1. From an Internet browser, enter the IP address for the Dolby Conferencing Console server.
2. Enter your user name and password. Click **Log in**.
   If the password is incorrect, the **Forgot Password** link displays.
3. Click **Forgot Password**.
4. Enter your email address, and then click **Reset my password**.

### Results

You will receive an email containing a link for resetting your password.

## 7.5.6 Configuring LDAP for user authentication

Configure LDAP if you want users to be able to log in with their corporate credentials.

### Prerequisites

You must be a system administrator to complete this task.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.

2. On the left side, click the other settings button.

3. Click **LDAP**.
4. Enter information about your LDAP server into these fields:
   - **Server**
   - **Port**
   - **Base DN**
   - **Bind user name**
   - **Bind user password**
   - **User Filter**
5. (Optional) Select **Use Secure Socket Layer (SSL)**.
6. (Optional) Select **Use STARTTLS**.

### What to do next

After you complete this task, check the settings for each user account and make sure that **Use LDAP for authentication** is selected.

### Related information

Adding and editing user accounts on page 80

# 7.6 Using SNMP

The Dolby Conferencing Console software uses an Simple Network Management Protocol (SNMP) agent program to manage certain functions. When enabled, it can respond to queries, and the Dolby Conferencing Console software can send email notifications if there is a change in the status of a device.

## 7.6.1 Downloading the SNMP MIB file

Before you can enable SNMP, you need to download the SNMP management information base (MIB) file from the Dolby Conferencing Console software.

### Procedure

1. From the Dolby Conferencing Console web interface, on the home screen, click the settings button in the upper-right corner.

2. Click **References**.
3. Next to **SNMP MIB file**, click the word **link**.

## 7.6.2 Enabling SNMP on open virtual appliance-based installations

Use this procedure to enable SNMP on open virtual appliance file-based installations.

### Procedure

1. For security reasons, we recommend that you update community strings in /etc/snmp/snmpd.conf.
2. On the server that hosts your Dolby Conferencing Console software, log in as the root user.
3. Enter this command to make the `snmpd_t` domain permissive:

   ```
   semanage permissive -a snmpd_t
   ```

   The command may take a few minutes to run.
4. Enter this command to start the `snmpd` service.

   ```
   service snmpd start
   ```

5. Enter this command so that the **`snmpd`** service turns back on after every reboot.

   ```
   chkconfig snmpd on
   ```

6. If you want the Dolby Conferencing Console software to send out SNMP traps, add this command to /etc/snmp/snmpd.conf:

   ```
   informsink www.xxx.yyy.zzz TRAPCOMMUNITY PORT
   ```

   Replace *`www.xxx.yyy.zzz`* with the IP address or host name of `NMS`. Replace *`TRAPCOMMUNITY`* with the community string of `NMS`. Replace *`PORT`* with the **`snmptrapd`** port number. Detailed explanations can be found inside the file, as well as at http://net-snmp.sourceforge.net/docs/man/snmpd.conf.html.
7. As the root user, enter this command to restart the Dolby Conferencing Console server:

   ```
   service dcc restart
   ```

## 7.6.3 Enabling SNMP on RPM-based installations

You can enable SNMP on RPM-based installations.

### Procedure

1. On the server that hosts your Dolby Conferencing Console software, log in as the root user.
2. Install the SNMP agent packages and the **`SELinux`** policy management tool.
   Enter these commands, in the order shown, to install `net-snmp`:

   ```
   yum install -y net-snmp
   yum install -y net-snmp-utils
   ```

Enter this command to install the **SELinux** policy management tool:

```
yum install -y policycoreutils-python
```

3. Enter this command to make the snmpd_t domain permissive:

   ```
   semanage permissive -a snmpd_t
   ```

   The command may take a few minutes to run.

4. Edit the PostgreSQL client authentication configuration file at /var/lib/pgsql/data/pg_hba.conf. Add these lines to the beginning of the file if they do not exist already.

   ```
   local    all    dcc        md5
   host    all    dcc    127.0.0.1/32    md5
   host    all    dcc    ::1/128        md5
   ```

   If the Postgres installation is on Amazon, update the pg_hba.conf file to the following:

   ```
   host    all    all    127.0.0.1/32    trust
   ```

5. Restart the PostgreSQL database service.

   Enter these commands, in the order shown, to restart the database service:

   ```
   service postgresql reload
   service postgresql restart
   ```

6. Append these lines to the **snmpd** configuration file at /etc/snmp/snmpd.conf.

   ```
   view systemview included .1.3.6.1.4.1.6729
   pass_persist .1.3.6.1.4.1.6729.2.3.2.1 /usr/bin/dcc-snmp-agent pass_persist
   ```

7. For security reasons, we recommend that you update community strings in /etc/snmp/snmpd.conf.

8. If you want the Dolby Conferencing Console software to send out SNMP traps, add this command to /etc/snmp/snmpd.conf:

   ```
   informsink www.xxx.yyy.zzz TRAPCOMMUNITY PORT
   ```

   Replace *www.xxx.yyy.zzz* with the IP address or host name of NMS. Replace *TRAPCOMMUNITY* with the community string of NMS. Replace *PORT* with the **snmptrapd** port number. Detailed

explanations can be found inside the file, as well as at http://net-snmp.sourceforge.net/docs/man/snmpd.conf.html.

9. As the root user, enter this command to restart the Dolby Conferencing Console server:

```
service dcc restart
```

10. Enter this command to start the snmpd service.

```
service snmpd start
```

11. Enter this command so that the **snmpd** service turns back on after every reboot.

```
chkconfig snmpd on
```

12. Makes sure that the SNMP port (by default, User Datagram Protocol (UDP) port 161) is open on the Dolby Conferencing Console firewall. Enter this command to open the UDP port on the input chain:

```
iptables -I INPUT -p udp --dport 161 -j ACCEPT
service iptables save
service iptables status
```

For RHEL7:

1. Edit the /etc/firewalld/services/snmp.xml file.
2. Add these lines:

```
<?xml version="1.0" encoding="utf-8"?>
<service>
<short>SNMP</short>
<description>SNMP protocol</description>
<port protocol="udp" port="161"/>
</service>
```

3. Reload the firewall:

```
firewall-cmd --reload
```

4. Add the service to your public zone:

```
firewall-cmd --zone=public --add-service snmp --permanent
```

5. Reload the firewall again:

```
firewall-cmd --reload
```

## 7.6.4 Confirming that SNMP is enabled

Use the **snmpwalk** command to confirm that SNMP is enabled.

### Procedure

Enter these commands:

Replace the `public` string with the read-only community string of the SNMP server. Replace `10.203.22.33` with the IP address of your Dolby Conferencing Console server.

```
snmpwalk -v 2c -c public -m +DOLBY-CONFERENCING-CONSOLE-MIB -Os 10.203.22.33 .
1.3.6.1.4.1.6729.2.3.2.1
```

## 7.7 Using Webmin

Webmin is a web-based interface for system administration.

Webmin is included in the Open Virtual Appliance (OVA) installation. It is not part of the RPM Package Manager installation. To install Webmin on existing Dolby Conferencing Console servers, see http://www.webmin.com/rpm.html.

**Note:** We recommend changing your root password for security purposes.

**Note:** For RHEL7, you may have to install the perl-Digest-MD5 package, using the command `yum install perl-Digest-MD5` as a Webmin dependency.

Webmin is disabled by default. You can enable Webmin by running the following command as a root user:

```
service webmin start
```

**Note:** Webmin does not automatically restart when the system is restarted.

After you have enabled Webmin, it can be accessed using the following URL:

```
https://<DCC-server-IP:10000>
```

# 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.

**AWS**
Amazon Web Services. The Amazon cloud computing services platform.

**CentOS**
Community Enterprise Operating System.

**device access service**
A server or node on a network that manages device traffic for the Dolby Conferencing Console.

**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.

**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.

**MAC**
Multiply-accumulate. In digital signal processing, the multiply-accumulate operation is a common step that computes the product of two numbers and adds that product to an accumulator.

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

**MIB**
Management information base. A type of communications network management database.

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

**OVA file**
A single Open Virtualization Format (OVF) file packaged together with all of its supporting files. Also known as open virtual applications.

**OVF**
Open Virtualization Format. File format for the packaging and distribution of software to be run in a virtual machine.

**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.

**RPM**
RPM Package Manager. A system for managing Linux software installation packages.

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

**SMTP**
Simple Mail Transfer Protocol. An Internet standard for sending and receiving emails.

**SNMP**
Simple Network Management Protocol. A protocol for managing IP network devices

**SSH**
Secure Shell protocol. An encrypted network protocol for secure data communication, remote command-line login, 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.

**STARTTLS**
An extension to plain text communication protocols (such as Simple Mail Transfer Protocol [SMTP] and Lightweight Directory Access Procotol [LDAP] services) that changes a plain text connection to an encrypted (Transport Layer Security [TLS] or Secure Socket Layer [SSL]) connection instead of using a separate port for encrypted communication.

**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.

**UI**

User interface.