



## **Administration Guide for Cisco Digital Media Suite 5.3.x Appliances**

November 4, 2011

### **Americas Headquarters**

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

*Administration Guide for Cisco Digital Media Suite 5.3.x Appliances*  
© 2002–2014 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface**   vii

- Purpose   vii
- Audience   vii
- Document Conventions   vii
- Related Documentation   viii
- Obtaining Documentation and Submitting a Service Request   viii

---

## **CHAPTER 1**

### **Introduction**   1-1

- Supported Appliances   1-1
- Requirements to Set Up an Appliance   1-2
- Prepare to Set Up an Appliance   1-2
- Accessing the AAI   1-3
- Navigating the AAI   1-3

---

## **CHAPTER 2**

### **Configure Basic Appliance Settings and Control Appliance Services**   2-1

- View Appliance System Information   2-2
- Manage System Log Information   2-2
  - Change the Logging Level   2-3
  - Save a Copy of the System Log to a USB Drive   2-3
  - Transfer a Copy of the System Log to a Remote Server   2-4
  - Clear the Logs   2-4
- Configure the Java Cache   2-5
- Change the Appliance Administrator Password   2-6
- Update Appliance Software   2-7
- Restart the Appliance   2-7
- Restart the Web Services   2-7
- Restart the Database Services   2-8
- Restart the Streaming Server   2-8
- Shut Down the Appliance   2-9

**CHAPTER 3**

**Back Up and Restore Appliance Configurations 3-1**

- Guidelines and Limitations 3-1
- Back Up Your Appliance 3-2
  - Schedule Recurring Backups to a Remote Server 3-2
  - Perform a One-time Backup to a Remote Server 3-3
  - Perform a One-time Backup to a USB Drive 3-5
- Restore Your Appliance from a Backup 3-6
  - Restore from a Remote Server 3-6
  - Restore from a USB Drive 3-7
- Cancel a Current or Scheduled Backup 3-8
- View the Backup Log 3-9

**CHAPTER 4**

**Change Appliance Network Settings 4-1**

- View Network Settings 4-2
- Change the Appliance Hostname 4-3
- Change the TCP/IP Settings 4-4
- Change the DNS Settings 4-5
- Disable Auto Negotiation on the Network Interface Card 4-5
- Enable Auto Negotiation on the Network Interface Card 4-6
- Troubleshoot Network Issues 4-6
  - Start or Stop the Network Interface Card 4-6
  - Restart the Network Interface Card 4-7
  - Use ping to Troubleshoot Connectivity 4-7
  - Use netstat to View Active Network Connections 4-8
  - Use dig to Retrieve DNS Server Information 4-9
  - Use nslookup to Retrieve DNS Server Information 4-9
  - View Network Interface Traffic Statistics 4-10

**CHAPTER 5**

**Configure System Time 5-1**

- View Date and Time Settings 5-2
- Change the Time Zone 5-3
- Change the Date 5-3
- Set the System Time Manually 5-4
- Use NTP to Correct the System Clock 5-4
- Use NTP to Provide System Time 5-5
  - View NTP Settings 5-5
  - Specify NTP Servers 5-6

Start the NTP Service	5-6
Stop the NTP Service	5-6
Restart the NTP Service	5-7
Check the NTP Service Status	5-7
Display the Current Time	5-8

**CHAPTER 6****Recover Passwords 6-1**

Change the Admin Account Password	6-1
Change the PWADMIN Account Password	6-2
Reset the Superuser Account Password	6-2
Get Testroot Access	6-2

**CHAPTER 7****Manage Digital Certificates 7-1**

Concepts	7-2
Glossary	7-2
Restrictions	7-4
Expiration	7-5
Encoding	7-5
Carriage Returns	7-5
Subject CN Elements	7-5
Concatenation	7-6
Workflows for Certificate Management	7-6
Obtain and Install Provider-signed Certificates	7-6
Your Certificates Expire or You Do Not Have Any Certificates	7-6
Back Up and Restore Certificates	7-6
Procedures	7-7
Generate and Submit Certificate Signing Requests (CSR)	7-7
Verify That Your Certificate Format is PEM, as Needed	7-10
Import (Install) Provider-signed Certificates	7-11
Generate Self-signed Certificates	7-13
View Identity Certificates	7-15
View a Certificate Chain to Verify its Certificates	7-16
Export a Keystore to Back It Up	7-17
Import a Keystore to Restore It from a Backup	7-18
Reference	7-19
Internet Assigned Names Agency (IANA) Country Codes	7-19
FAQs and Troubleshooting	7-34
FAQs	7-34
Troubleshooting	7-34

---

**CHAPTER 8**

**Failover 8-1**

---

**CHAPTER 9**

**Set Up and Configure a DMM Appliance 9-1**

Set Up a DMM Appliance 9-1

Configure a DMM Appliance 9-2

---

**CHAPTER 10**

**Set Up and Configure a Cisco Show and Share Appliance 10-1**

Set Up a Show and Share Appliance 10-1

Configure a Show and Share Appliance 10-2

---

**CHAPTER 11**

**Pair the Cisco DMS Appliances 11-1**

Avoid Pairing Failures 11-1

Pair Your Appliances 11-2



# Preface

---

**Revised: November 4, 2011**

This chapter includes the following sections:

- [Purpose, page vii](#)
- [Audience, page vii](#)
- [Document Conventions, page vii](#)
- [Related Documentation, page viii](#)
- [Obtaining Documentation and Submitting a Service Request, page viii](#)

## Purpose

This guide describes how to set up, configure, and administer your Cisco DMM and Cisco Show and Share appliances. It also tells you how to use the Appliance Administration Interface (AAI), a text user interface that helps you to administer a DMS appliance.

## Audience

The intended audience for this guide is systems or network administrators who install, configure, or troubleshoot Cisco DMS appliance hardware.

## Document Conventions

This guide uses these text formatting conventions:

Item	Convention
Commands and keywords	<b>boldface</b> font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	screen font
Information you enter	<b>boldface screen</b> font
Variables you enter	<i>italic screen</i> font

Item	Convention
Menu items and button names	<b>boldface</b> font
Selecting a menu item in paragraphs	<b>Option &gt; Network Preferences</b>
Selecting a menu item in tables	Option > Network Preferences

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Tip**

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

## Related Documentation

For a list of all Cisco DMS product documentation, see the *Guide to Documentation for the Cisco Digital Media Suite* at the following URL:

[http://www.cisco.com/en/US/docs/video/digital\\_media\\_systems/5\\_x/5\\_0/dms/roadmap/dms50map.html](http://www.cisco.com/en/US/docs/video/digital_media_systems/5_x/5_0/dms/roadmap/dms50map.html)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.





# CHAPTER 1

## Introduction

---

**Revised: November 4, 2011**

Cisco Digital Media Suite is a product family that consists of Cisco Digital Media Manager (DMM) appliances, Cisco Show and Share appliances, Cisco Digital Media Player (DMP) endpoints, Cisco Digital Media Encoder (DME) devices, and all associated software components.

To set up and configure the Cisco DMM and Cisco Show and Share appliances, you need to access some basic settings and controls that are not a part of the Cisco DMS software. You access these settings and controls through the Cisco DMM and Cisco Show and Share Appliance Administrative Interface (AAI).

Using AAI, you can configure the appliance network, time, logging, certificate, and failover settings. You can also start and stop specific services, reboot or shut down the appliance, and backup or restore configurations.

This chapter explains how to access and use the AAI interface. It includes the following sections:

- [Supported Appliances, page 1-1](#)
- [Requirements to Set Up an Appliance, page 1-2](#)
- [Prepare to Set Up an Appliance, page 1-2](#)

## Supported Appliances

This document describes how to set up and administer the following Cisco Digital Media System (DMS) 5.2.x appliances:

- Cisco Show and Share appliances:
  - Cisco Show and Share 5.3.x on MCS 7835-H3
  - Cisco Show and Share 5.3.x on WAVE-574
  - Cisco Show and Share 5.3.x on UCS C210 (SNS-SVR-C210EN-K9)
  - Cisco Show and Share 5.3.x and Cisco Show and Share Reports 5.2.2 on UCS C200 (SNS-SVR-C200WG-K9)
- Cisco Digital Media Manager appliances:
  - Cisco Digital Media Manager 5.3.x on MCS 7835-H3
  - Cisco Digital Media Manager 5.3.x on UCS C210 (DMM-SVR-C210-K9)

# Requirements to Set Up an Appliance

- To understand the client system requirements to use Cisco DMS products or to learn about known issues and late-breaking information, see the [Release Notes for Cisco Digital Media Suite 5.3.x](#) on Cisco.com.
- To obtain documentation that you require for other Cisco DMS components, see the [Guide to Documentation for Cisco Digital Media Suite](#) on Cisco.com.

## Prepare to Set Up an Appliance

Before you set up and configure an appliance, complete the following steps:

### Procedure

---

- Step 1** Decide which networked computer you will use to administer the appliance remotely.
  - Step 2** On that computer, install and set up the necessary client software according to the client system requirements in [Release Notes for Cisco Digital Media Suite 5.3.x](#) on Cisco.com.
  - Step 3** Ensure that TCP port 22 is not blocked between the Show and Share appliance and the DMM appliance.
  - Step 4** Ensure that authorized users of your Cisco DMM appliance can send and receive packets through TCP port 8080.
  - Step 5** Ensure that authorized users of your Show and Share appliance can send and receive packets through TCP port 80 (Show and Share) and port 8080 (Show and Share Reports).
  - Step 6** Ensure that a DNS entry has been created and published for the Show and Share and DMM appliances.
-

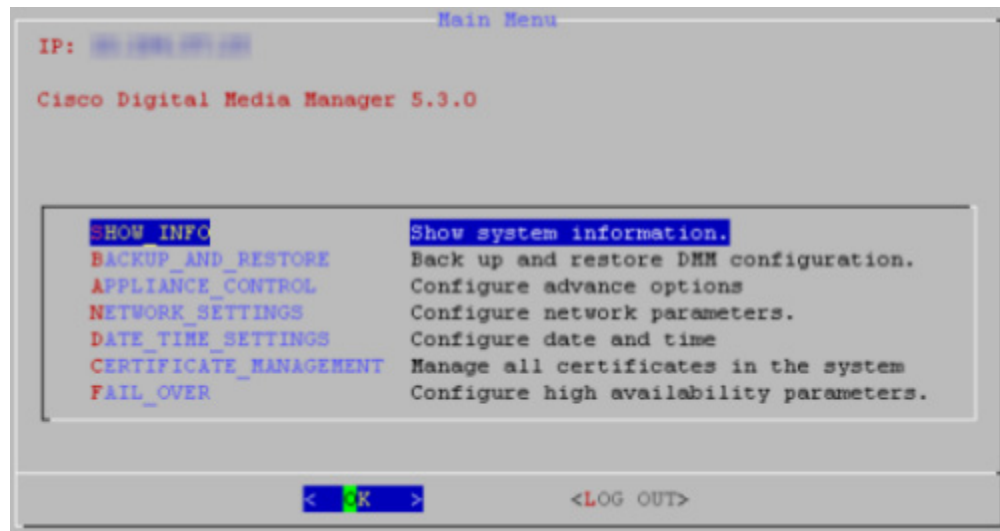
## Accessing the AAI

You can access the AAI in one of the following ways:

- Keyboard and monitor attached to the appliance.
- SSH terminal session to the appliance.

To start the AAI from the appliance login prompt, enter the username **admin** and password that you specified for the admin account when you first configured the appliance.

When you log in, the IP address, server type (Cisco Show and Share or Cisco DMM) and version appear above the menu.



## Navigating the AAI

To see options or change selections in AAI, do any of the following:

- To highlight an option, move between text input fields, or to navigate through the list of options, press the **Up/Down** arrow keys.
- To select or deselect a highlighted option, press **Space**.
- To highlight the buttons at the bottom of the screen, press **Tab**.
- To select the highlighted button, press **Enter**.





## CHAPTER 2

# Configure Basic Appliance Settings and Control Appliance Services

---

**Revised: November 4, 2011**

This chapter explains how you can use Appliance Administrative Interface (AAI) to administer a Cisco Show and Share or Cisco DMM appliance and includes the following sections:

- [View Appliance System Information, page 2-2](#)
- [Manage System Log Information, page 2-2](#)
- [Configure the Java Cache, page 2-5](#)
- [Change the Appliance Administrator Password, page 2-6](#)
- [Update Appliance Software, page 2-7](#)
- [Restart the Appliance, page 2-7](#)
- [Restart the Web Services, page 2-7](#)
- [Restart the Database Services, page 2-8](#)
- [Restart the Streaming Server, page 2-8](#)
- [Shut Down the Appliance, page 2-9](#)

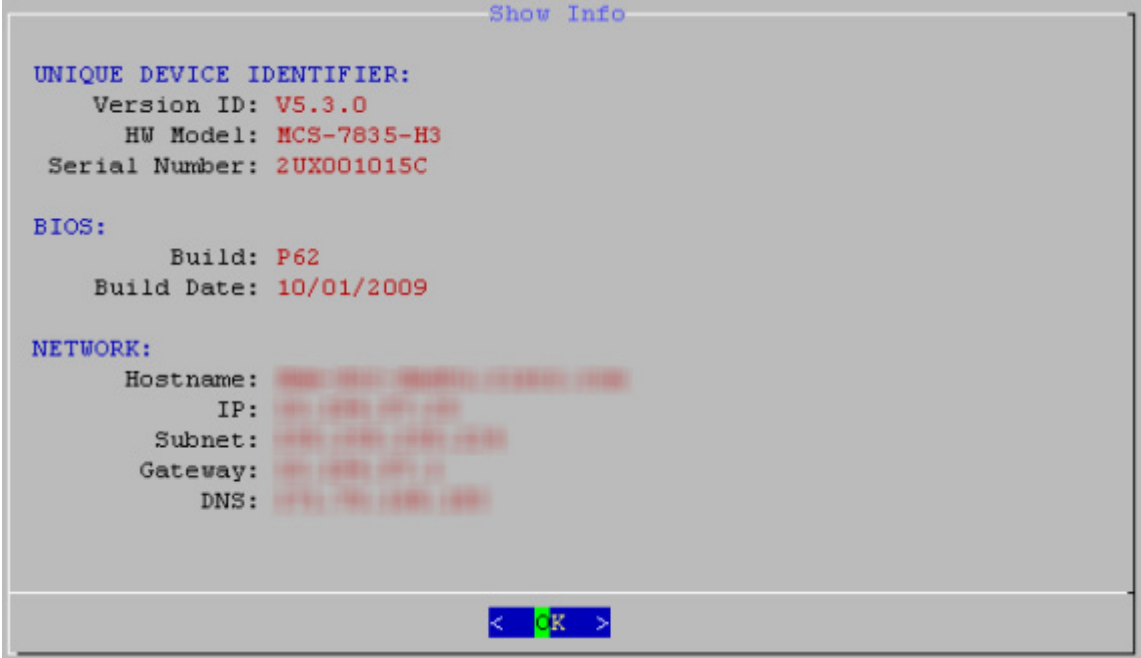
## View Appliance System Information

You can display the following system information for your Cisco DMS appliance:

- Device information: product ID, version ID, hardware model, and the appliance serial number.
- BIOS information: build and build date.
- Network information: hostname, IP address, subnet mask, default gateway, DNS server.

### Procedure

- Step 1** From the AAI Main Menu, choose **SHOW\_INFO** and then press **Enter**.



```

Show Info

UNIQUE DEVICE IDENTIFIER:
  Version ID: V5.3.0
  HW Model: MCS-7835-H3
  Serial Number: 2UX001015C

BIOS:
  Build: P62
  Build Date: 10/01/2009

NETWORK:
  Hostname:
  IP:
  Subnet:
  Gateway:
  DNS:

< OK >

```

- Step 2** Press **Enter** to return to the main menu.

## Manage System Log Information

This section contains the following topics:

- [Change the Logging Level, page 2-3](#)
- [Save a Copy of the System Log to a USB Drive, page 2-3](#)
- [Transfer a Copy of the System Log to a Remote Server, page 2-4](#)
- [Clear the Logs, page 2-4](#)

## Change the Logging Level

Changing the logging level temporarily stops the appliance web services. In failover configurations, this causes the appliance to fail over.

### Procedure

---

- Step 1** Choose **APPLIANCE\_CONTROL**, and then press **Enter**.
- Step 2** Choose **LOGGING\_OPTIONS**, and then press **Enter**.
- Step 3** Choose **CHANGE\_LOG\_LEVEL**, and then press **Enter**.
- Step 4** Choose one of the following logging levels, and then press **Enter**:
- **ERROR**—To receive messages of only the greatest severity.
  - **WARN**—To receive warning messages and error messages.
  - **INFO**—To receive informational, warning, and error messages.
  - **DEBUG**—To receive messages of every severity level.
- 

## Save a Copy of the System Log to a USB Drive

You can save a copy of the appliance log file to a USB drive that you attach directly to your appliance.

### Before You Begin

Obtain access to the appliance and plug in your USB device.

### Procedure

---

- Step 1** Choose **APPLIANCE\_CONTROL**, and then press **Enter**.
- Step 2** Choose **LOGGING\_OPTIONS**, and then press **Enter**.
- Step 3** Choose **GET\_SYSLOG** press **Enter**.
- Step 4** Choose **USB**, and then press **Enter**.
- A system message appears when the system log information is saved.
- Step 5** Press **Enter**.
- You are returned to the Main Menu.
-

## Transfer a Copy of the System Log to a Remote Server

You can transfer a copy of the appliance log file to an FTP or SFTP server.

### Before You Begin

- Verify you have permissions to write to the FTP or SFTP server.
- Verify your appliance can communicate with the FTP or SFTP server. See [Use ping to Troubleshoot Connectivity](#), page 4-7.

### Procedure

- 
- Step 1** Choose **APPLIANCE\_CONTROL**, and then press **Enter**.
- Step 2** Choose **LOGGING\_OPTIONS**, and then press **Enter**.
- Step 3** Choose **GET\_SYSLOG**, press **Enter**.
- Step 4** Choose one of the following, and then press **Enter**:
- **FTP**—To send the system log information to an FTP server.
  - **SFTP**—to send system log information to a secure FTP server.
- Step 5** Type the FTP or SFTP server address and press **Enter**.
- Step 6** Type the username that you use when you log into the FTP or SFTP server and press **Enter**.
- Step 7** Type the password that you use when you log into the FTP or SFTP server and press **Enter**.  
A system message appears when the transfer is complete.
- Step 8** Press **Enter**.  
You are returned to the Main Menu.
- 

## Clear the Logs

### Procedure

- 
- Step 1** Choose **APPLIANCE\_CONTROL**, and then press **Enter**.
- Step 2** Choose **LOGGING\_OPTIONS**, and then press **Enter**.
- Step 3** Choose **CLEAN\_LOGS**, and then press **Enter**.
- Step 4** Choose **CLEAN\_TOMCAT\_LOGS**, and then press **Enter**.  
A message appears, warning you that all tomcat logs will be lost.
- Step 5** Choose **Yes**.  
It may take more than a minute to complete the process. When the process is complete, you are returned to the main menu.
-



# Configure the Java Cache

The Java Cache option changes the Java cache policy for name lookup. The name lookup is used for Cisco Digital Media Encoders that are portable and that may change IP address when moved from location to location.

By default, the Java Cache timeout is set to 30 seconds. This should be sufficient for most usage. However, you can change the Java cache timeout value to cache name/IP address information forever (until the appliance is rebooted), for a specific amount of time, or never.

Changing this setting could have appliance security implications. You should not change this setting unless directed to by Cisco support personnel.

## Procedure

---

- Step 1** Choose **APPLIANCE\_CONTROL** and press **Enter**.
- Step 2** Choose **CHANGE\_JAVA\_CACHE** and press **Enter**.
- Step 3** Type a value, in seconds, for the cache timeout press **Enter**.
- A positive value indicates the number of seconds an address is cached for.
  - A negative values causes the address to be cached forever.
  - A value of 0 (zero) disables address caching.
-

# Change the Appliance Administrator Password

You can change the appliance administrator password. The appliance administrator user ID is “admin” (without the quotation marks). The password that you enter must contain at least 6 characters.

**Note**

If you change the administrator password on a Cisco Show and Share appliance, you must also change the password for any file types that are hosted locally on the appliance. See the [Administrator Guide for Cisco Show and Share 5.3.x](#) for information about setting the file hosting locations.

If you have forgotten the admin account password, you can change it using the pwadmin account that you created when you set up the appliance. See [Chapter 6, “Recover Passwords”](#).

**Procedure**

- 
- Step 1** Choose **APPLIANCE\_CONTROL** and press **Enter**.
  - Step 2** Choose **RESET\_PASSWORD** and press **Enter**.
  - Step 3** Enter the new password and press **Enter**.
  - Step 4** Enter the password again and press **Enter**.
  - Step 5** Press **Enter**.  
You are returned to the Main Menu.
  - Step 6** (Cisco Show and Share only) Log in as an administrator or as superuser to Cisco Show and Share and do the following:
    - a.** Choose **Show and Share** from global navigation.
    - b.** Choose **Administration**.
    - c.** Update the Publish locally... password or the password for any file type that is hosted on the Cisco Show and Share appliance.
-

# Update Appliance Software

You can upgrade from an upgrade disc or from an upgrade .iso image hosted on an FTP, SFTP, or HTTP server. You should always refer to the upgrade guide for the software you are upgrading to for specific instructions.

## Procedure

---

- Step 1** Choose **APPLIANCE\_CONTROL** and press **Enter**.
- Step 2** Choose **SOFTWARE\_UPDATE** and press **Enter**.
- Step 3** To update using a disc:
- Choose **CD\_UPDATE** and press **Enter**.
  - Insert the CD-ROM and press **Enter**.
  - Follow the instructions on the screen.
- Step 4** To update using a remote disc image (.iso file):
- Choose **REMOTE\_UPDATE** and press **Enter**.
  - Enter the following information:
    - For FTP/SFTP servers, enter the server name or IP address and a user account and press **Enter**. You will be prompted for a password. Enter the password and press **Enter**.
    - For HTTP server, enter the URL and press **Enter**.
  - Follow the instructions on the screen.
- 

# Restart the Appliance

You can reboot the appliance from the AAI interface. In failover configurations, this causes the appliance to fail over.

## Procedure

---

- Step 1** Choose **APPLIANCE\_CONTROL** and press **Enter**.
- Step 2** Choose **RESTART\_OPTIONS** and press **Enter**.
- Step 3** Choose **REBOOT** and press **Enter** twice.
- 

# Restart the Web Services

You can restart the Tomcat web services from the AAI interface without rebooting the appliance. In failover configurations, this causes the appliance to fail over.

**Procedure**

- 
- Step 1** Choose **APPLIANCE\_CONTROL** and press **Enter**.
  - Step 2** Choose **RESTART\_OPTIONS** and press **Enter**.
  - Step 3** Choose **RESTART\_WEB\_SERVICES** and press **Enter** twice.
- 

## Restart the Database Services

You can restart the database services from AAI without rebooting the appliance. In failover configurations, this causes the appliance to fail over.

**Procedure**

- 
- Step 1** Choose **APPLIANCE\_CONTROL** and press **Enter**.
  - Step 2** Choose **RESTART\_OPTIONS** and press **Enter**.
  - Step 3** Choose **RESTART\_DATABASE\_SERVER** and press **Enter** twice.
- 

## Restart the Streaming Server

This procedure applies to appliances running Cisco Show and Share software only. This option does not appear on appliances running Cisco DMM. In failover configurations, this causes the appliance to fail over.

**Procedure**

- 
- Step 1** Choose **APPLIANCE\_CONTROL** and press **Enter**.
  - Step 2** Choose **RESTART\_OPTIONS** and press **Enter**.
  - Step 3** Choose **RESTART\_STREAMING\_SERVER** and press **Enter** twice.
-

# Shut Down the Appliance

You can shut down an appliance. In failover configurations, this causes the appliance to fail over.

## Procedure

---

- Step 1** Choose **APPLIANCE\_CONTROL** and press **Enter**.
  - Step 2** Choose **SHUTDOWN** and press **Enter** twice.
-





## CHAPTER 3

# Back Up and Restore Appliance Configurations

---

**Revised: November 4, 2011**

This chapter explains how you can use Appliance Administrative Interface (AAI) to backup a Cisco DMS appliance or restore a previous backup. It includes the following sections:

- [Guidelines and Limitations, page 3-1](#)
- [Back Up Your Appliance, page 3-2](#)
- [Restore Your Appliance from a Backup, page 3-6](#)
- [Cancel a Current or Scheduled Backup, page 3-8](#)
- [View the Backup Log, page 3-9](#)

## Guidelines and Limitations

- Media stored on external hosting locations is not backed up. If you delete a video from Cisco Show and Share, it is removed from the external hosting location. If you restore a backup taken before the video was deleted, you will see the video listed in Cisco Show and Share but will receive a file not found error if you try to play the video because the video had previously been removed from the external hosting location.
- Backup and restore your entire system—Cisco Show and Share, Cisco DMM, and your external hosting locations—at the same time to ensure that the restored data matches across all three components.
- When restoring a backup to a replacement appliance, you must install the license on the appliance before restoring the data.
- You cannot restore a backup taken on one version of the software to another version of the software. Backups must be restored on an appliance running the same version of software as when the backup was taken. For example, you cannot restore a backup taken on an appliance running Cisco DMS 5.2 software to an appliance running Cisco DMS 5.3 software.
- Scheduled backup information is not retained in the backup file. When you restore your data you will need to reschedule any recurring backups.

# Back Up Your Appliance

You can backup the appliance to a USB drive or to a remote rsync, SFTP, or FTP server. You have the option of backing up the configuration only or backing up the configuration and any locally stored media. Media stored on external servers is not backed up.

The backup creates two files on the target device, one with a time stamp in the name and one without. When you perform a restore, the most recent backup (the file without the time stamp in the name) is used. To restore an earlier backup, copy the earlier backup file and rename the copy to the same name as the backup file that does not contain the timestamp.

This section contains the following topics:

- [Schedule Recurring Backups to a Remote Server, page 3-2](#)
- [Perform a One-time Backup to a Remote Server, page 3-3](#)
- [Perform a One-time Backup to a USB Drive, page 3-5](#)

## Schedule Recurring Backups to a Remote Server

### Before You Begin

- Verify you have permissions to write to the rsync, FTP, or SFTP server.
- Verify your appliance can communicate with the rsync, FTP, or SFTP server. See [Use ping to Troubleshoot Connectivity, page 4-7](#).

### Procedure

- 
- Step 1** Choose **BACKUP\_AND\_RESTORE** and press **Enter**.
- Step 2** Choose **BACKUP** and press **Enter**.
- Step 3** Choose one of the following options and press **Enter**.
- **CONFIGURATION**—Only configuration files are backed up. Media files stored on the server are not backed up.
  - **CONTENT+CONFIG**—Locally-stored media and configuration files are backed up (you cannot backup media files stored on a Cisco DMM appliance running 5.2.2 or earlier).
- Step 4** Choose **REMOTE** and press **Enter**.
- Step 5** Choose one of the following remote server types and press **Enter**:
- **RSYNC** (recommended)
  - **SFTP**
  - **FTP**
- Step 6** Enter the server IP address and press the **Down** arrow.
- Step 7** Enter the username for an account on the remote server, press **Tab** to highlight the OK button, and then press **Enter**.
- Step 8** Type the password for the account on the remote server and press **Enter**.

The appliance tests the connectivity to the remote server. If you entered the server IP address and credentials correctly, you can proceed to schedule the backup. If not, you will have to start this procedure over from the beginning.



- Step 9** Press **Enter**.
- Step 10** Press **Space** to select Recurring backup, and then press **Enter**.
- Step 11** Use the **Up/Down** arrows to highlight the frequency in which you want the backup to occur. Press **Space** to select the highlighted frequency, and then press **Enter**.
- Step 12** Set the time for the recurring backup to occur. Use 00:00:00 for midnight.
- Press **Tab** to highlight each field.
  - Use the **Up/Down** arrows to change the value.
- Step 13** Press **Enter**.
- A success message appears.
- Step 14** Press **Enter**.
- The appliance Backup/Restore screen appears. The information for the scheduled backup appears at the top of the screen.
- 

## Perform a One-time Backup to a Remote Server

You can perform a one-time backup to a remote server.



### Note

You cannot perform a one-time backup if you already have a recurring backup scheduled. You need to clear the recurring backup configuration before you can schedule a one-time backup. See [Cancel a Current or Scheduled Backup, page 3-8](#).

---

### Before You Begin

- Verify you have permissions to write to the rsync, FTP, or SFTP server.
- Verify your appliance can communicate with the rsync, FTP, or SFTP server. See [Use ping to Troubleshoot Connectivity, page 4-7](#).

### Procedure

---

- Step 1** Choose **BACKUP\_AND\_RESTORE** and press **Enter**.
- Step 2** Choose **BACKUP** and press **Enter**.
- Step 3** Choose one of the following options and press **Enter**:
- CONFIGURATION**—Only configuration files are backed up. Media files stored on the server are not backed up.
  - CONTENT+CONFIG**—Locally-stored media and configuration files are backed up.



### Note

You cannot backup media files stored on a Cisco DMM appliance running 5.2.2 or earlier.

---

- Step 4** Choose **REMOTE** and press **Enter**.
- Step 5** Choose one of the following remote server types and press **Enter**:
- RSYNC** (recommended)

- SFTP
- FTP

**Step 6** Enter the server IP address and press the **Down** arrow.

**Step 7** Enter the username for an account on the remote server, press **Tab** to highlight the OK button, and then press **Enter**.

**Step 8** Type the password for the account on the remote server and press **Enter**.

The appliance tests the connectivity to the remote server. If you entered the server IP address and credentials correctly, you can proceed to schedule the backup. If not, you will have to start this procedure over from the beginning.

**Step 9** Press **Enter**.

**Step 10** Press the **Down** arrow to highlight **Backup once (now)**, press **Space** to select that option, and then press **Enter**.

**Step 11** Press **Enter** to start the backup.

**Step 12** Press **Enter** to return to the appliance Backup/Restore screen.

The appliance Backup/Restore screen appears.

---

## Perform a One-time Backup to a USB Drive



**Note** You cannot perform a one-time backup if you already have a recurring backup scheduled. You need to clear the recurring backup configuration before you can schedule a one-time backup. See [Cancel a Current or Scheduled Backup](#), page 3-8.

---

### Procedure

- 
- Step 1** Plug the USB drive into the appliance USB port.
- Step 2** Choose **BACKUP\_AND\_RESTORE** and press **Enter**.
- Step 3** Choose **BACKUP** and press **Enter**.
- Step 4** Choose one of the following options and press **Enter**:
- **CONFIGURATION**—Only configuration files are backed up. Media files stored on the server are not backed up.
  - **CONTENT+CONFIG**—Locally-stored media and configuration files are backed up.



**Note** You cannot backup media files stored on a Cisco DMM server running 5.2.2 or earlier.

- 
- Step 5** Choose **LOCAL** and press **Enter**.
- Step 6** Press **Enter** to return to the appliance Backup/Restore menu.
- Step 7** When the backup is complete, choose **EJECT\_USB** and press **Enter**.
- Step 8** Remove the USB drive.
- Step 9** Press **Enter**.
- You are returned to the Main Menu.
-

# Restore Your Appliance from a Backup

AAI automatically restores the latest backup. To restore an earlier backup, copy the earlier backup file and rename the copy to the same name as the backup file that does not contain the timestamp.

In failover configurations, performing a restore causes the appliance to fail over. This is expected behavior and does not cause any problems with the restored data.

This section contains the following topics:

- [Restore from a Remote Server, page 3-6](#)
- [Restore from a USB Drive, page 3-7](#)

## Restore from a Remote Server

### Before You Begin

- Verify you have permissions to read from the rsync, FTP, or SFTP server.
- Verify your appliance can communicate with the rsync, FTP, or SFTP server. See [Use ping to Troubleshoot Connectivity, page 4-7](#).

### Procedure

- 
- Step 1** Choose **BACKUP\_AND\_RESTORE** and press **Enter**.
- Step 2** Choose **RESTORE** and press **Enter**.
- Step 3** Choose one of the following options and press **Enter**:
- **CONFIGURATION**—Restore configuration files only. Media files are not restored.
  - **CONTENT+CONFIG**—Restore media and configuration files.
- Step 4** Choose **REMOTE** and press **Enter**.
- Step 5** Choose one of the following remote server types and press **Enter**:
- **RSYNC** (recommended)
  - **SFTP**
  - **FTP**
- Step 6** Enter the server IP address and press the **Down** arrow.
- Step 7** Enter the username for an account on the remote server, press **Tab** to highlight the OK button, and then press **Enter**.
- Step 8** Type the password for the account on the remote server and press **Enter**.  
The restore begins.
- Step 9** Press **Enter** to return to the appliance Backup/Restore screen.  
The appliance Backup/Restore screen appears. The **BACKUP/RESTORE STATUS** shows **RUNNING** while the restore is in progress.



### Warning

**After the restore procedure has successfully completed, you need to ensure the desired Fully Qualified Domain Name (FQDN) of the DMM is properly configured both on the Application Administration Interface and also in the web-browser UI. On the Application Administration**

Interface, access **NETWORK\_SETTINGS**, select **HOSTNAME**, then enter the desired **FQDN** for this server. On the web-browser UI, log in to the Digital Media Manager as an administrator. Go to Digital Signs, select Settings from the top navigation bar, and select the Server Settings tab. In the Servlet Server Address field, enter the desired **FQDN** for this server.

---

## Restore from a USB Drive

### Procedure

---

- Step 1** Plug the USB drive into the appliance USB port.
- Step 2** Choose **BACKUP\_AND\_RESTORE** and press **Enter**.
- Step 3** Choose **RESTORE** and press **Enter**.
- Step 4** Choose one of the following options and press **Enter**:
- **CONFIGURATION**—Restore configuration files only. Media files are not restored.
  - **CONTENT+CONFIG**—Restore media and configuration files.
- Step 5** Choose **LOCAL** and press **Enter**.
- Step 6** Press **Enter** to return to the appliance Backup/Restore menu.
- Step 7** When the restore is complete, choose **EJECT\_USB** and press **Enter**.
- Step 8** Remove the USB drive.
- Step 9** Press **Enter**.
- You are returned to the Main Menu.



### Warning

After the restore procedure has successfully completed, you need to ensure the desired Fully Qualified Domain Name (FQDN) of the DMM is properly configured both on the Application Administration Interface and also in the web-browser UI. On the Application Administration Interface, access **NETWORK\_SETTINGS**, select **HOSTNAME**, then enter the desired **FQDN** for this server. On the web-browser UI, log in to the Digital Media Manager as an administrator. Go to Digital Signs, select Settings from the top navigation bar, and select the Server Settings tab. In the Servlet Server Address field, enter the desired **FQDN** for this server.

---

## Cancel a Current or Scheduled Backup

Stopping a backup stops the currently running backup and clears the scheduled backup, if any.

### Procedure

---

**Step 1** Choose **BACKUP\_AND\_RESTORE** and press **Enter**.

**Step 2** Choose **STOP\_BACKUP** and press **Enter**.

A confirmation screen appears.

**Step 3** Press **Enter** to confirm your choice.

**Step 4** Press **Enter**.

You are returned to the Main Menu.

---

# View the Backup Log

## Procedure

---

- Step 1** Choose **BACKUP\_AND\_RESTORE** and press **Enter**.
  - Step 2** Choose **SHOW\_BACKUP\_LOG** and press **Enter**.
  - Step 3** Press **Enter** to close the log and return to the appliance Backup/Restore screen.
-







## CHAPTER 4

# Change Appliance Network Settings

---

**Revised: November 4, 2011**

This chapter explains how you can use the Appliance Administrative Interface (AAI) to change the network settings or troubleshoot connectivity issues for a Cisco Show and Share or Cisco DMM appliance.



**Note**

- We recommend that you do not change the static IP address that you assign to your Cisco Show and Share and Cisco DMM appliances.
  - If your network uses a DNS server, you must reassociate the resolvable DNS hostname for your Show and Share appliance each time that you change its IP address.
- 

This chapter includes the following sections:

- [View Network Settings, page 4-2](#)
- [Change the Appliance Hostname, page 4-3](#)
- [Change the TCP/IP Settings, page 4-4](#)
- [Change the DNS Settings, page 4-5](#)
- [Disable Auto Negotiation on the Network Interface Card, page 4-5](#)
- [Enable Auto Negotiation on the Network Interface Card, page 4-6](#)
- [Troubleshoot Network Issues, page 4-6](#)

# View Network Settings

The Network Settings screen displays the hostname, network link status, IP address, subnet mask, default gateway, and primary and secondary DNS server.

## Procedure

**Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.

The Network Settings screen displays the network configuration of the appliance and options for changing the configuration.

```

                                Network Settings
From this menu you can configure the network settings
  HOSTNAME:  dmm-doc-
  NETWORK LINK:  Detected
      IP:
      SUBNET:
  GATEWAY:
  PRIMARY DNS:
  SECONDARY DNS:

  HOSTNAME      To change the hostname
  TCP_IP        Configure static IP
  DNS           To change the DNS settings
  AUTO_NEGOTIATION  To Change the NIC settings
  NETWORK_TOOLS  To troubleshoot the network

  < OK >           <Cancel>

```

**Step 2** Choose **Cancel** and press **Enter** to return to the Main Menu.

# Change the Appliance Hostname

You can change the appliance hostname from the AAI interface. In failover configurations, changing the appliance hostname causes the appliance to fail over.

Changing the hostname causes the appliance to regenerate a self-signed certificate. If you are using a certificate provided by a certificate authority, you will need to obtain a new certificate and install it on the appliance. See [Chapter 7, “Manage Digital Certificates”](#) for more information about obtaining and installing certificates.

If you are using both a Cisco Show and Share and a Cisco DMM appliance, you must re-pair the appliances after changing the hostname on either appliance.

If you change the hostname for a Cisco Show and Share appliance, you must change the hostname setting for any files that are hosted on the appliance.

## Procedure

---

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
  - Step 2** Choose **HOSTNAME** and press **Enter**.  
The current hostname appears on the Hostname Configuration screen.
  - Step 3** Enter a fully qualified domain name for the appliance, for example server.example.com. Press **Enter**.
  - Step 4** Press **Enter** to confirm the change.  
Changing the hostname can take over a minute to complete. When it is finished, a results message appears.
  - Step 5** Press **Enter** to return to the Network Settings screen.
  - Step 6** If you are using Cisco DMM and Cisco Show and Share appliances, go to [Chapter 11, “Pair the Cisco DMS Appliances”](#).
  - Step 7** If you change the hostname of a Cisco Show and Share appliance, you need to update the hostname for file types that are hosted on the local appliance. See the [User Guide for Cisco Show and Share Administration 5.3.x](#) for information about setting the file hosting locations.
-

# Change the TCP/IP Settings

You can use AAI to change the IP address of the appliance. If you change the IP address of a Cisco Show and Share appliance or of a Cisco DMM appliance that is paired with a Cisco Show and Share appliance, you will need to pair the appliances after performing this procedure.

Changing the IP address of your appliance causes the appliance to reboot. If you are connected to your appliance using SSH, you will lose your connection.

In failover configurations, changing the TCP/IP settings causes the appliance to fail over.

## Procedure

---

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
- Step 2** Choose **TCP\_IP** and then press **Enter**.
- Step 3** Use the Up/Down arrows to navigate between the fields and provide the following information:
- IP address and subnet mask of the appliance.
  - IP address of the default gateway for the appliance.
- Step 4** Press **Tab** to highlight the OK button. Press **Enter** to accept your changes.
- A message appears warning you that the appliance will reboot and will need to be paired again.
- Step 5** Press **Enter**.
- The Static IP Configuration confirmation screen appears.
- Step 6** Review your configuration. Press **Enter** to accept your configuration changes and reboot the appliance. Press **Tab** to highlight No and press **Enter** to change the settings again.
- If you accepted the configuration changes, the appliance reboots.
- 

## What to do Next

If the appliances was part of a paired Cisco DMM/Cisco Show and Share configuration, you must re-pair the appliances. See [Chapter 11, “Pair the Cisco DMS Appliances”](#).

# Change the DNS Settings

## Procedure

---

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
  - Step 2** Choose **DNS** and press **Enter**.
  - Step 3** Type the primary DNS server IP address in the PRIMARY DNS field.
  - Step 4** (Optional) Use the **Down** arrow to move to the SECONDARY DNS field. Type the secondary DNS server IP address, if there is one.
  - Step 5** Press **Tab** to highlight the Ok button, and then press **Enter**.  
The DNS Configuration confirmation screen appears.
  - Step 6** Press **Enter** to confirm the settings and return to the Network Settings screen.
- 

# Disable Auto Negotiation on the Network Interface Card

By default, the network interface card is set to auto-negotiate the speed and duplex settings for the network interface. You can turn off auto negotiation and manually configure these properties.

## Procedure

---

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
  - Step 2** Choose **AUTO\_NEGOTIATION** and press **Enter**.  
The Auto Negotiation Configuration screen appears. If auto negotiation is enabled, the system asks if you want to disable it.
  - Step 3** Press **Enter** to disable auto negotiation.  
The NIC Speed screen appears.
  - Step 4** Use the **Up/Down** arrows to highlight the desired NIC speed. Press the **Spacebar** to select the speed.
  - Step 5** Press **Enter**.  
The NIC Duplex screen appears.
  - Step 6** Use the **Up/Down** arrows to highlight the desired duplex setting. Press the **Spacebar** to select the setting.
  - Step 7** Press **Enter**.  
The Auto Negotiation Configuration screen displays your chosen settings.
  - Step 8** Press **Enter** to accept your changes and return to the Network Settings screen.
-

# Enable Auto Negotiation on the Network Interface Card

## Procedure

---

- Step 1** Choose `NETWORK_SETTINGS` and press **Enter**.
- Step 2** Choose `AUTO_NEGOTIATION` and press **Enter**.  
The Auto Negotiation Configuration screen appears. If auto negotiation is disabled, the system asks if you want to enable it.
- Step 3** Press **Enter** to enable auto negotiation and return to the Network Settings screen.
- 

## Troubleshoot Network Issues

This section contains the following topics:

- [Start or Stop the Network Interface Card, page 4-6](#)
- [Restart the Network Interface Card, page 4-7](#)
- [Use ping to Troubleshoot Connectivity, page 4-7](#)
- [Use netstat to View Active Network Connections, page 4-8](#)
- [Use dig to Retrieve DNS Server Information, page 4-9](#)
- [Use nslookup to Retrieve DNS Server Information, page 4-9](#)
- [View Network Interface Traffic Statistics, page 4-10](#)

## Start or Stop the Network Interface Card

You can stop and start the network interface card from the AAI interface. If you are using SSH to access the AAI interface, you will lose connectivity to the appliance. You need to start the network interface card from a terminal connected to the appliance. In failover configurations, this causes the appliance to fail over.

## Procedure

---

- Step 1** Choose `NETWORK_SETTINGS` and press **Enter**.
- Step 2** Choose `NETWORK_TOOLS` and press **Enter**.
- Step 3** Choose `START/STOP` and press **Enter**.
- Step 4** Choose **Yes** and press **Enter**.  
The NIC will start up or stop, depending upon its previous state.
-

## Restart the Network Interface Card

You can restart the network interface card (NIC) on the appliance through the AAI interface. If you are logged-in to the appliance through an SSH session, your connection will be dropped when you restart the NIC. You will need to log back in. In failover configurations, this causes the appliance to fail over.

### Procedure

---

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
  - Step 2** Choose **NETWORK\_TOOLS** and press **Enter**.
  - Step 3** Choose **RESTART** and press **Enter**.  
You are asked to confirm that you want to restart the NIC.
  - Step 4** Choose **Yes** and press **Enter**.  
If you are connected to the appliance through an SSH session, your session is dropped.
- 

## Use ping to Troubleshoot Connectivity

The AAI interface contains a front end to the ping utility. Use the ping utility to troubleshoot connectivity issues to other devices, for example to ensure the appliance can reach your FTP server for backup or system log.

### Procedure

---

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
  - Step 2** Choose **NETWORK\_TOOLS** and press **Enter**.
  - Step 3** Choose **PING** and press **Enter**.
  - Step 4** Type the IP address or hostname of the target device and press **Enter**.
  - Step 5** Press **Enter** to close the results screen.  
You are returned to the Network Settings screen.
-

## Use netstat to View Active Network Connections

### Procedure

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
- Step 2** Choose **NETWORK\_TOOLS** and press **Enter**.
- Step 3** Choose **NETSTAT** and press **Enter**.

```

NETSTAT
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost.localdomain:9955  *:*                     LISTEN
tcp        0      0 0.0.0.0:7849             *:*                     LISTEN
tcp        0      0 0.0.0.0:7850             *:*                     LISTEN
tcp        0      0 *:843                    *:*                     LISTEN
tcp        0      0 *:1007                    *:*                     LISTEN
tcp        0      0 *:sunrpc                  *:*                     LISTEN
tcp        0      0 *:csync2                   *:*                     LISTEN
tcp        0      0 *:postgres                 *:*                     LISTEN
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
tcp        0      0 localhost.localdom:postgres localhost.localdomain:353 ESTABLISHED
a(+)
< EXIT >
    
```

- Step 4** Use the **UP/DOWN** arrows to scroll through the results.
- Step 5** Press **Enter** to return to the Network Settings screen.



## Use dig to Retrieve DNS Server Information

Domain information proper (dig) is a utility for querying DNS servers for DNS records.

### Procedure

---

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
- Step 2** Choose **NETWORK\_TOOLS** and press **Enter**.
- Step 3** Choose **DIG** and press **Enter**.
- Step 4** Enter a hostname or IP address to query the DNS server with and press **Enter**.



**Tip** Enter **-h** and press **Enter** to see advanced information about using the dig utility.

---

The results screen appears with the DNS information for the IP address or hostname.

- Step 5** Press **Enter** to return to the Network Settings screen.
- 

## Use nslookup to Retrieve DNS Server Information

nslookup is a utility for querying DNS servers for DNS details for a particular host.

### Procedure

---

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
  - Step 2** Choose **NETWORK\_TOOLS** and press **Enter**.
  - Step 3** Choose **NSLOOKUP** and press **Enter**.
  - Step 4** Enter a hostname or IP address to query the DNS server with and press **Enter**.  
The results screen appears with the DNS information for the IP address or hostname.
  - Step 5** Press **Enter** to return to the Network Settings screen.
-

## View Network Interface Traffic Statistics

### Procedure

- Step 1** Choose **NETWORK\_SETTINGS** and press **Enter**.
- Step 2** Choose **NETWORK\_TOOLS** and press **Enter**.
- Step 3** Choose **NIC\_STATS** and press **Enter**.

```

NIC STATS
mac address : 00:26:55:33:64:de
collisions : 0
multicast : 6
rx_bytes : 591630457
rx_compressed : 0
rx_crc_errors : 0
rx_dropped : 0
rx_errors : 0
rx_fifo_errors : 0
rx_frame_errors : 0
rx_length_errors : 0
rx_missed_errors : 0
rx_over_errors : 0
rx_packets : 1015958
tx_aborted_errors : 0
tx_bytes : 547067679
tx_carrier_errors : 0
tx_compressed : 0
tx_dropped : 0
    
```

80%

< OK >

- Step 4** Use the **UP/DOWN** arrows to scroll through the results.
- Step 5** Press **Enter** to return to the Network Settings screen.



## CHAPTER 5

# Configure System Time

---

**Revised: November 4, 2011**

This chapter explains how to use the Appliance Administrative Interface (AAI) to configure the system time on a Cisco Show and Share or Cisco DMM appliance. This chapter includes the following sections:

- [View Date and Time Settings, page 5-2](#)
- [Change the Time Zone, page 5-3](#)
- [Change the Date, page 5-3](#)
- [Set the System Time Manually, page 5-4](#)
- [Use NTP to Correct the System Clock, page 5-4](#)
- [Use NTP to Provide System Time, page 5-5](#)
- [Display the Current Time, page 5-8](#)

# View Date and Time Settings

## Procedure

**Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.

The Date and Time Settings screen appears. The screen shows the currently configured time zone, whether the hardware clock is set to UTC or not, and the date and time the screen was accessed.

```

Date and Time Settings
From this menu you can configure the time settings

TIME_ZONE: "America/Los_Angeles"
HARDWARE CLOCK AT UTC: true
DATE: Thu 20 Oct 2011 09:56:12 PM PDT

TIME_ZONE To change the Time Zone
DATE      To Change the Date
TIME      To change the Time
NTP       To synchronize time with NTP server
SHOW_TIME To show the current time

< OK >          <Cancel>

```



**Note** The time does not update on this screen. To see the actual time, see [Display the Current Time](#), page 5-8.

**Step 2** Choose **Cancel** to return to the Main menu.

## Change the Time Zone

### Procedure

---

- Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.
- Step 2** Choose **TIME\_ZONE** and press **Enter**.
- Step 3** Use the **Up/Down** arrows to select the time zone. Press **Tab**.
- Step 4** Press **Space** to select or deselect **System clock uses UTC**.
- Step 5** Press **Tab** to highlight the OK button and press **Enter**.

It may take a minute for the changes to take effect. When the changes are complete, the Date and Time Settings screen appears.

---

## Change the Date

### Procedure

---

- Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.
  - Step 2** Choose **DATE** and press **Enter**.
  - Step 3** Press **Tab** until the month is highlighted. Use the **Up/Down** arrows to change the month.
  - Step 4** Press **Tab** to highlight the year. Use the **Up/Down** arrows to change the year.
  - Step 5** Press **Tab** to highlight the day. Use the **Up/Down** and **Left/Right** arrows to change the day.
  - Step 6** Press **Tab** to highlight the OK button. Press **Enter**.  
The Date and Time Settings confirmation screen appears.
  - Step 7** Press **Enter** to confirm the date and return to the Date and Time Settings screen.
-

# Set the System Time Manually

You can manually enter the system time.

**Note**

See [Use NTP to Correct the System Clock, page 5-4](#) for information about performing a one-time correction of the manually-entered system time against an NTP server.

**Procedure**

- 
- Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.
  - Step 2** Choose **TIME** and press **Enter**.
  - Step 3** Press **Tab** until the hour is highlighted. Use the **Up/Down** arrows to change the hour.
  - Step 4** Press **Tab** to highlight the minutes. Use the **Up/Down** arrows to change the minutes.
  - Step 5** Press **Tab** to highlight the seconds. Use the **Up/Down** arrows to change the seconds.
  - Step 6** Press **Tab** to highlight the OK button. Press **Enter**.  
The Time Configuration confirmation screen appears.
  - Step 7** Press **Enter** to confirm the settings and return to the Date and Time Settings screen.
- 

# Use NTP to Correct the System Clock

You can use NTP to perform a one-time correction of the system clock.

This procedure provides a one-time correction only; it does not enable NTP to keep the system clock synchronized with the NTP server. To enable NTP on the appliance, see [Use NTP to Provide System Time, page 5-5](#).

**Procedure**

- 
- Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.
  - Step 2** Choose **NTP** and press **Enter**.
  - Step 3** Choose **CLOCK\_CORRECTION** and press **Enter**.
  - Step 4** Enter the IP address or name of the NTP server you want to use to correct the system clock.
  - Step 5** Press **Enter**.  
A message displaying the status of the time correction appears.
  - Step 6** Press **Enter**.  
You are returned to the Network Time Protocol Configuration screen.
-

# Use NTP to Provide System Time

You must use NTP on the appliances if you are going to configure failover. This section contains the following topics:

- [View NTP Settings, page 5-5](#)
- [Specify NTP Servers, page 5-6](#)
- [Start the NTP Service, page 5-6](#)
- [Stop the NTP Service, page 5-6](#)
- [Restart the NTP Service, page 5-7](#)
- [Check the NTP Service Status, page 5-7](#)

## View NTP Settings

### Procedure

---

**Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.

**Step 2** Choose **NTP** and press **Enter**.

The Network Time Protocol Configuration screen appears. The configured NTP servers, the date and time that the screen was accessed, and the status of the NTP service is displayed at the top of the screen.



**Note** The date and time do not update on this screen; it only displays the date and time you accessed the screen. To view a live display of the system time, see [Display the Current Time, page 5-8](#).

---

If the STATUS field contains “Unable to talk to NTP daemon,” the NTP service is not started. See [Start the NTP Service, page 5-6](#) for information about starting the service. If you have not yet specified any NTP servers, see [Specify NTP Servers, page 5-6](#).

**Step 3** Choose **Cancel** and press enter to return to the Main Menu.

---

## Specify NTP Servers

You can add up to 3 NTP servers for the appliance to use to synchronize its clock.

### Procedure

---

- Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.
- Step 2** Choose **NTP** and press **Enter**.
- Step 3** Choose **ADD/CHANGE** and press **Enter**.
- Step 4** Enter up to three servers, starting with the NTP SERVER 1: field:
- Use the **Up/Down** arrows to highlight the server field.
  - Enter the server IP address or fully qualified domain name.
- Step 5** Press **Tab** to highlight the OK button, and then press **Enter**.
- The Network Time Protocol Client Configuration confirmation screen appears. You can review the servers that you specified.
- Step 6** Press **Enter** to confirm your settings and return to the Network Time Protocol Configuration screen.
- 

## Start the NTP Service

The NTP service polls the server every 64 seconds.

### Procedure

---

- Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.
- Step 2** Choose **NTP** and press **Enter**.
- Step 3** Choose **NTP\_SERVICE** and press **Enter**.
- Step 4** Choose **START/STOP** and press **Enter**.
- The Start NTP confirmation screen appears.
- Step 5** Press **Enter** to start the service.
- The Network Time Protocol Configuration screen appears. When the appliance is synchronized with the NTP server, the status on this screen is “synchronized to NTP server (*server\_ip\_address*)....” If the appliance has not yet synchronized with the NTP server, the status shows “unsynchronized”.
- 

## Stop the NTP Service

### Procedure

---

- Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.
- Step 2** Choose **NTP** and press **Enter**.



- Step 3** Choose `NTP_SERVICE` and press **Enter**.
- Step 4** Choose `START/STOP` and press **Enter**.  
The Stop NTP confirmation screen appears.
- Step 5** Press **Enter** to stop the service.  
The Network Time Protocol Configuration screen appears. When the NTP service is stopped, the Status on this screen is “Unable to talk to NTP daemon”.
- 

## Restart the NTP Service

Restarting the NTP service stops and restarts the service if it is already running; it does not start the service if it is stopped.

### Procedure

---

- Step 1** Choose `DATE_TIME_SETTINGS` and press **Enter**.
- Step 2** Choose `NTP` and press **Enter**.
- Step 3** Choose `NTP_SERVICE` and press **Enter**.
- Step 4** Choose `RESTART` and press **Enter**.  
The Restart NTP confirmation screen appears.
- Step 5** Press **Enter** to restart the service.  
The Network Time Protocol Configuration screen appears.
- 

## Check the NTP Service Status

### Procedure

---

- Step 1** Choose `DATE_TIME_SETTINGS` and press **Enter**.
- Step 2** Choose `NTP` and press **Enter**.
- Step 3** Choose `STATUS` and press **Enter**.  
The Network Time Protocol Client Status screen appears.
- Step 4** Press **Enter** to close the Network Time Protocol Client Status screen and return to the Network Time Protocol Configuration screen.
-

# Display the Current Time

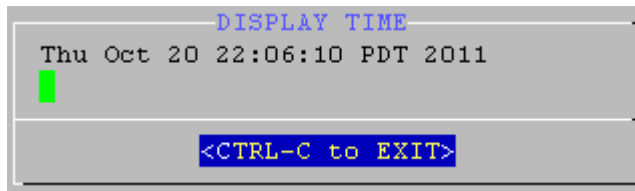
## Procedure

---

**Step 1** Choose **DATE\_TIME\_SETTINGS** and press **Enter**.

**Step 2** Choose **SHOW\_TIME** and press **Enter**.

The Display Time screen displays the current time on the appliance.



```
DISPLAY TIME
Thu Oct 20 22:06:10 PDT 2011
█
<CTRL-C to EXIT>
```

**Step 3** To return to the Date and Time Settings menu, press **Enter**.

---



## CHAPTER 6

# Recover Passwords

---

**Revised: November 4, 2011**

This chapter explains how to use the Appliance Administrative Interface (AAI) to recover forgotten passwords.

The procedures in this chapter require that you login with the pwadmin account that you set up when you initially configured the appliance.

- [Change the Admin Account Password, page 6-1](#)
- [Change the PWADMIN Account Password, page 6-2](#)
- [Reset the Superuser Account Password, page 6-2](#)

## Change the Admin Account Password

### Procedure

---

- Step 1** Log into the AAI using the pwadmin username and password.
  - Step 2** Choose **CHANGE\_ADMIN\_PASSWORD** and press **Enter**.
  - Step 3** Enter the new password and press **Enter**. The password must contain at least 6 characters.
  - Step 4** Enter the password again and press **Enter**.
  - Step 5** Press **Enter** to return to the Main Menu.
  - Step 6** (Cisco Show and Share only) Log in as an administrator or as superuser to Cisco Show and Share and do the following:
    - a. Choose **Show and Share** from global navigation.
    - b. Choose **Administration**.
    - c. Update the Publish locally... password or the password for any file type that is hosted on the Cisco Show and Share appliance.
-

## Change the PWADMIN Account Password

### Procedure

---

- Step 1** Log into the AAI using the pwadmin username and password.
  - Step 2** Choose **CHANGE\_PWADMIN\_PASSWORD** and press **Enter**.
  - Step 3** Enter the new password and press **Enter**. The password must contain at least 6 characters.
  - Step 4** Enter the password again and press **Enter**.
  - Step 5** Press **Enter** to return to the Main Menu.
- 

## Reset the Superuser Account Password

You cannot change the superuser account password from the AAI. However, you can reset it to Cisco123. You should immediately log into the Cisco DMM and change the superuser account password after performing a reset.

### Procedure

---

- Step 1** Log into the AAI using the pwadmin username and password.
  - Step 2** Choose **RESET\_SUPERUSER\_PASSWORD** and press **Enter**.
  - Step 3** Press **Enter** to reset the password.  
The password is changed to Cisco123.
  - Step 4** Press **Enter** to return to the Main Menu.
- 

## Get Testroot Access

Testroot access is used during troubleshooting sessions with Cisco support personnel. Do not use this option except under the guidance of Cisco support staff.



# CHAPTER 7

## Manage Digital Certificates

---

Revised: July 29, 2014

You can manage the digital certificates for a Cisco Show and Share and Cisco DMM appliances from the local instance of Appliance Administration Interface (AAI). Furthermore:

- You can import multiple CA chain certificates simultaneously:
  - Inside a single \*.ZIP archive (CSCth65646).
  - Inside a single certificate file (CSCti11768).

**However, we do not support these methods for the import of identity certificates. All identity certificates must remain separate during import.**

- You can now correctly import a certificate that includes an extra carriage return (CSCth53389).
- You can now configure a Cisco DMS appliance to notify you daily that an imported CA certificate or identity certificate will expire soon. Such notifications begin 10 days before the actual expiration date. To access this feature in the web-based user interface for DMS-Admin, go to Alerts > Notification Rules > Certificate is about to expire (CSCth18904).
- We now support the P7B certitude format in addition to the PEM certificate format.



### Note

- Subject Alternative Names (SANs) are supported in Cisco Show and Share and Cisco Digital Media Manager. To use a SAN name, you must generate a Certificate Signing Request (CSR) as described in the [Generate and Submit Certificate Signing Requests \(CSR\)](#) procedure. For the SAN option, when requesting the signing certificate from the certificate authority, the SAN name should be added at the same time and will be included in the certificate.



### Activation

**We add and improve features often. This chapter describes options and features that do not necessarily exist in all releases. You must upgrade older software as needed before such enhancements can be available to you.**

- [Concepts, page 7-2](#)
- [Procedures, page 7-7](#)
- [Reference, page 7-19](#)

# Concepts

- [Glossary, page 7-2](#)
- [Restrictions, page 7-4](#)
- [Workflows for Certificate Management, page 7-6](#)

## Glossary

**Timesaver**

---

Go to terms that start with... [ [A](#) | [C](#) | [D](#) | [K](#) | [P](#) | [S](#) | [X](#) ].

---

### A

**asymmetric key exchange**

Asymmetric or *public key* cryptography is based on the concept of a key pair. Each half of the pair (one key) can encrypt information so that only the other half (the other key) can decrypt it. One part of the key pair, the private key, is known only by the designated owner; the other part, the public key, is published widely but is still associated with the owner.

### C

[Return to Top](#)

### CA

*certification authority*. Authority in a network that issues and manages security credentials and public keys for message encryption and decryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

**CA signature**

Digital code that vouches for the authenticity of a digital certificate. The certification authority (CA) that issues a certificate also signs it.

- certificate chain** Hierarchical list of public-key certificates, each signed by the subsequent certificate, ending with a Root CA certificate.
- CSR** *certificate signing request*. A block of ciphertext that (1.) describes an entity to a CA and (2.) requests a digital identity certificate to authenticate the entity for SSL. The CSR includes encrypted information to identify the entity, such as its location, serial number, and public key. This example shows a CSR.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwADEXMBUGA1UEAxMOZHNS5cy5jaXNjby5jb20xZDZANBgNVBAsTBmp5Z2podjEOMAwGA1UEChMFaGdlZWV5dHlnajEOMAwGA1UECBMFbWhoanYxZzAJBgNVBAYT
AlVTMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlz+sEkBbIoXTiE13O28FX558enM0
6tVdnNlWmySbtKulYJ+XvH1sdzbCLOPYJhOvr1JJIxaNjfdT1fdQp4Qd1U/1k5+v9Nmqt1r9Fx1
bUkxkCaYr6H4RYrmqi0+YpLyUgMXqoQ+vFRDgKUGHD5lxQK9dggXvdJQNgylGawXkG8WepC3XwK
Zy19CS2S4CbnLs6yHcz86/VE1X4+DqnS3yvfkoyYg/yUe151Hcwp97C0KtFrZnQcnIDYU4rEaV+
nqKWc52cQ0kuoJjJlzNS1VUGLGA+yPf+fz+0K5liqA6HnE22yA7SWlskcR668JCR9tjqyWnIC+yu
Cd13HUfSpwIDAQABAAAwDQYJKoZIhvcNAQEFBQADggEBAAVj0f6B6lmtVEvCaUxKAI7DDgFjBJhv
BRJMZA+3BVD60OX8T2J8druEb18b1oEX989f81124Kce08Y037/a4RPdxhXM3eeVYTMnz4QcbI6G
MU58jdHgRM1pxmYweixNTmzFTLc3uhp8JHWk286pHOMNHX2OR+cL+Cbj/mYRnmf4hg4LD0oCTS9f
pVEDgmiOpZ/go9OfAZ4nu1SwnqCaNpV+k/hM2RnlAqtaQDR89B4K18IF6odnjc9TL0kXUrsK79BD
Qp1bZQS+ME1gmEqHpFjzvaopwXnZSv4CFHi6IwN2HPALY24Bo3XGW85j71HYPbwoVnZtcqdN56X6
HM0lto8=
-----END NEW CERTIFICATE REQUEST-----
```

## D [Return to Top](#)

- DER** A certificate encoding format that we **DO NOT SUPPORT** in any Cisco DMS release. Instead, you can use [PEM](#). Alternatively, starting with Cisco DMS 5.2.3, you can use [P7B](#).

Name	Type
 cacert.der	Security Certificate
 inter.der	Security Certificate
 identity.der	Security Certificate

- digital certificate** Digital representation of an entity (human or otherwise), as defined in International Organization for Standardization (ISO) standard X.509. A certificate is normally issued by a CA on behalf of an entity. Common fields within a certificate include distinguished names (DN) for the entity and CA, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority, so that a recipient can verify certificate legitimacy.




- DN** *distinguished name*. A set of attributes that help a CA to authenticate an entity for SSL.

## K [Return to Top](#)




- keystore** An exported KEYSTORE.DAT file from your Cisco *Show and Share* appliance (or, beginning with Cisco DMS 5.2.3, your DMM appliance) contains a backup copy of its digital certificates.

**P** [Return to Top](#)

**P7B** **NEW IN CISCO DMS 5.2.3**—An implementation of base64-encoded ASCII in X-509, used to protect identity certificates and CA certificates. **P7B certificates must NOT use binary (DER) encoding. Instead, use Base64 (ASCII) encoding.**

Name	Type
 cacert.p7b	PKCS #7 Certificate
 inter.p7b	PKCS #7 Certificate
 identity.p7b	PKCS #7 Certificate

**PEM** *privacy enhanced email*. An implementation of base64-encoded ASCII in X-509, used to protect identity certificates and CA certificates. **Cisco DMS 5.2.1 and 5.2.2 support PEM alone. They reject all other certificate encoding formats.**

Name	Type
 inter.pem	PEM File
 identity.pem	PEM File
 cacert.pem	PEM File

**private key** A cryptographic value to decrypt messages and digital signatures upon receipt by one authenticated entity from another. Each private key is unique and confidential to one entity. As one half of an asymmetric key pair, each private key is bound to its opposite half, a public key.

**public key** A cryptographic value to encrypt messages and digital signatures for delivery from one authenticated entity to another. Each public key is verifiably unique to one entity, which can reveal it widely without compromising the private key. As one half of an asymmetric key pair, each public key is bound to its opposite half, a private key.

**S** [Return to Top](#)

**self-signed** Acknowledgement from an entity that its own digital certificate was not issued by, and is not signed by, any trusted certification authority. Instead, the entity issued and affixed its own signature to its digital certificate. In common practice, a self-signed digital certificate is not considered valid, authentic, or trustworthy until proven so.

**signed** Endorsement from a trusted certification authority, affixed to another entity's digital certificate. In common practice, a signed digital certificate is considered valid, authentic, and trustworthy unless proven otherwise.

**X** [Return to Top](#)

**X-509** A standard for public key infrastructure. X.509 specifies, among other things, standard formats for public key certificates and a certification path validation algorithm.

## Restrictions

- [Expiration, page 7-5](#)



- [Encoding, page 7-5](#)
- [Carriage Returns, page 7-5](#)
- [Subject CN Elements, page 7-5](#)
- [Concatenation, page 7-6](#)

## Expiration



### Caution

- **Before Cisco DMS 5.2.3, we did not show any advance notice that an imported certificate was approaching its expiration date.** Because most certificates are valid for years at a time, this condition is not likely to disrupt anything in a production network. Even so, in Cisco DMS 5.2.3, we added a notification service that you can enable from DMS-Admin.
- **Show and Share appliances refuse web connections unless their certificates are current and valid.** When they are not, you must import a new certificate. You can obtain and install one from your CA or—temporarily—you can generate and use a self-signed certificate.

## Encoding



### Caution

**We support only PEM in Cisco DMS releases 5.2.1 and 5.2.2.** Certificate import to these releases fails when you use any other encoding format. Likewise for these same releases, import of PEM-compliant certificates fails when their wrapper is a ZIP archive or any binary format. (Cisco DMS 5.2.3 introduces support for P7B.)

### Related Topics

- [Verify That Your Certificate Format is PEM, as Needed, page 7-10](#)

## Carriage Returns



### Caution

**Avoid extra carriage returns in any certificate file that you import to Cisco DMS 5.2.1 or 5.2.2.** Certificate import to these releases fails whenever extra carriage returns are present. (Cisco DMS 5.2.3 forgives these carriage returns.)

## Subject CN Elements



### Caution

- **Do not use any wildcards (\*) in the common name (CN) element of a certificate's subject.** Certificate import fails when a wildcard is present. For example, we would reject a certificate with \*.example.com as its subject.
- **Do not import to Cisco DMS 5.2.1 or 5.2.2 any certificate whose subject omits the CN element.** Certificate import to these releases fails when the subject is missing its CN. At least one well known certification authority, Go Daddy, sometimes issues certificates without any CN in their subject. (Cisco DMS 5.2.3 forgives these subjects.)

## Concatenation



### Caution

**Do not combine multiple CA certificates together in one file that you will import to Cisco DMS 5.2.1 or 5.2.2.** Import to these releases will fail for merged CA certificates. Similar restrictions apply to identity certificates. (Although Cisco DMS 5.2.3 forgives merged CA certificates, it continues to prohibit any merging of identity certificates.)

## Workflows for Certificate Management

You are most likely to use AAI certificate management features in the context of a workflow.

- **Workflow A**—*Obtain and Install Provider-signed Certificates, page 7-6*
- **Workflow B**—*Your Certificates Expire or You Do Not Have Any Certificates, page 7-6*
- **Workflow C**—*Back Up and Restore Certificates, page 7-6*

### Workflow A

## Obtain and Install Provider-signed Certificates

**NEW IN CISCO DMS 5.2.1**—This sequence represents the typical workflow to use digital certificates from a trusted certification authority.

1. [Generate and Submit Certificate Signing Requests \(CSR\), page 7-7](#)
2. [Import \(Install\) Provider-signed Certificates, page 7-11](#)
3. [View a Certificate Chain to Verify its Certificates, page 7-16](#)
4. [Export a Keystore to Back It Up, page 7-17](#)

### Workflow B

## Your Certificates Expire or You Do Not Have Any Certificates

**NEW IN CISCO DMS 5.2.1**—This sequence represents the typical workflow to use self-signed digital certificates.

1. [Generate Self-signed Certificates, page 7-13](#)
2. [View a Certificate Chain to Verify its Certificates, page 7-16](#)

### Workflow C

## Back Up and Restore Certificates

**NEW IN CISCO DMS 5.2.1**—This sequence represents the typical workflow to back up your digital certificates and, later, restore them.

1. [Export a Keystore to Back It Up, page 7-17](#)
2. [Import a Keystore to Restore It from a Backup, page 7-18](#)
3. [View a Certificate Chain to Verify its Certificates, page 7-16](#)

# Procedures

- [Generate and Submit Certificate Signing Requests \(CSR\)](#), page 7-7
- [Verify That Your Certificate Format is PEM, as Needed](#), page 7-10
- [Import \(Install\) Provider-signed Certificates](#), page 7-11
- [Generate Self-signed Certificates](#), page 7-13
- [View Identity Certificates](#), page 7-15
- [View a Certificate Chain to Verify its Certificates](#), page 7-16
- [Export a Keystore to Back It Up](#), page 7-17
- [Import a Keystore to Restore It from a Backup](#), page 7-18

## Generate and Submit Certificate Signing Requests (CSR)

**Caution**

In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance. Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

**Workflow Context**

This topic is part of [Workflow A](#).

**Before You Begin**

- Contact a certification authority to learn about its process to receive a request. Many CAs will expect to receive your request through their FTP or SFTP server. Although you can use any CA, these four are among the best known.
  - *VeriSign*—[www.verisign.com](http://www.verisign.com)
  - *GoDaddy*—[www.godaddy.com](http://www.godaddy.com)
  - *Comodo*—[www.comodo.com](http://www.comodo.com)
  - *Network Solutions*—[www.networksolutions.com](http://www.networksolutions.com)
- Subject Alternative Names (SANs) are supported in Cisco Show and Share and Cisco Digital Media Manager. To use a SAN name, you must generate a Certificate Signing Request (CSR) as described in this procedure. For the SAN option, when requesting the signing certificate from the certificate authority, the SAN names should be added at the same time and will be included in the certificate.
- Log in as **admin** to the Appliance Administration Interface (AAI).

**Procedure**





**Step 1** Choose **CERTIFICATE\_MANAGEMENT > MANAGE\_SIGNED\_CERTS > GENERATE\_CSR**.

**Step 2** Enter values in the fields, as illustrated.



**Note** Do not use any of these characters.

, + = " \ ' ` < > # ;

- a. Use the Department field to enter the name for your organizational unit—such as *Finance Ministry*, *Taiwan Office*, *College of Engineering*, or *Publications Department*. Then, press the **Down** () key.
- b. Use the Organization field to enter the full legal name for your entire organization, as it is known to your national government or intergovernmental authority—such as *Cisco Systems*, *Cambridge University*, or *Médecins Sans Frontières*. Then, press the **Down** () key.
- c. Use the Location field to enter the full and officially designated place name of your city, town, township, village, hamlet, civil parish, or settlement—such as *Madrid* or *Tokyo*. Then, press the **Down** () key.
- d. Use the State field to enter the full name of your state, province, commonwealth, territory, republic, periphery, dependency, or protectorate—such as *Montserrat*, *California*, *Tamil Nadu*, *Chechnya*, *São Paulo*, or *Crete*. Then, press the **Down** () key.
- e. Use the Country field to enter the 2-character country code, as managed by the Internet Assigned Names Agency (IANA).
  - Even if this code **is not part** of your Internet domain name, it is a necessary attribute of your digital certificate.
  - Even if this code **is part** of your Internet domain name, you must not prefix it here with a period.



**Note** Your IANA country code might differ from all country name abbreviations that you know. The [“Internet Assigned Names Agency \(IANA\) Country Codes”](#) section on page 7-19 directs you to your country code.

- f. Press the **Down** () key.



**Note** The “Months Before Expiration” field is not useful in this procedure. You can safely ignore it.

**Step 3** Choose **OK**.

**Step 4** Use this checklist to prequalify a CA.

**Does the CA use PEM or P7B, as appropriate?**

We require certificates that use PEM encoding (exclusively in Cisco DMS 5.2.1 and 5.2.2) or P7B encoding (alternatively to PEM, beginning with Cisco DMS 5.2.3).

**Does the subject include a CN element in cases where it must do so?**

We require for Cisco DMS 5.2.1 and 5.2.2 that all certificate subjects include a CN element. Cisco DMS 5.2.3 eliminates this requirement.

**Does the CA isolate each certificate in cases where it must do so?**

We require in Cisco DMS 5.2.1 and 5.2.2 that each imported CA certificate and each imported identity certificate has its own, standalone file.

Although Cisco DMS 5.2.3 eliminates this restriction for CA certificates, it continues to enforce the restriction for identity certificates.

**Step 5** After you choose a CA, enter values that it provides to you, which identify its server specifically and you specifically. Then, choose **OK**.

**OR**

If your CA does not use an FTP or SFTP server to receive CSRs, enter values to identify a server that you control. Later, you can retrieve your encrypted CSR for delivery to your CA through its alternative process. For example, you might paste your CSR ciphertext into a form on the CA website.



---

**Note** **Your CA might ask you to specify what server platform—such as Apache or Microsoft Internet Application Server (IIS)—will use your new certificate.** You must choose Apache. Otherwise, your new certificate is not encoded correctly for Cisco DMS products to use it.

---

**Step 6** Stop. You have completed this procedure.

---

#### What to Do Next

- **OPTIONAL**—*Would you like to check whether your digital certificates use the correct format?* Go to the [“Verify That Your Certificate Format is PEM, as Needed”](#) section on page 7-10.
- **OPTIONAL**—*Would you like to install signed digital certificates that you received from a CA?* Go to the [“Import \(Install\) Provider-signed Certificates”](#) section on page 7-11.

## Verify That Your Certificate Format is PEM, as Needed

**Note**

We support only [PEM](#) in Cisco DMS 5.2.1 and 5.2.2. **These two releases do not support any other digital certificate encoding format, including PB7.** However, we began supporting P7B certificates as an alternative to PEM in Cisco DMS 5.2.3.

You can use an ordinary text editor, such as Notepad on Windows or TextEdit on Mac, to confirm quickly that your certificates use PEM encoding—as they must do for Cisco DMS 5.2.1 and 5.2.2.

**Procedure**

- 
- Step 1** Start your text editor.
- Step 2** Use its **Open** command to load your unaltered certificate file for viewing.
- Step 3** Examine the certificate.

- Does its first line say exactly `-----BEGIN CERTIFICATE-----` and nothing else?
- Does its last line say exactly `-----END CERTIFICATE-----` and nothing else?

When an unaltered certificate meets these requirements, it is encoded correctly for use with this release. You can import it.

**Note**

**Do not merely add the BEGIN and END statements to a certificate file that lacks them.** Their presence does not—by itself—change how a certificate is encoded.

- Step 4** Otherwise, do not import the certificate. We cannot use it with Cisco DMS 5.2.1 or 5.2.2. Contact your CA instead and request a replacement certificate that uses PEM encoding.
- Step 5** Stop. You have completed this procedure.
- 

**What to Do Next**

- **OPTIONAL**—*Would you like to install signed digital certificates that you received from a CA?* Go to the [“Import \(Install\) Provider-signed Certificates”](#) section on page 7-11.

## Import (Install) Provider-signed Certificates



### Caution

In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance. Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

When you import certificates, they overwrite all others.

### Workflow Context

This topic is part of [Workflow A](#).

### Before You Begin

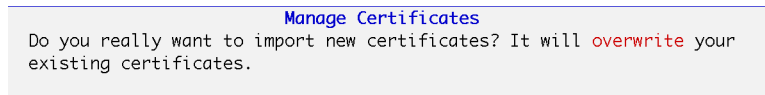
- Request and obtain a digital certificate from a trusted CA.
- Log in as **admin** to the Appliance Administration Interface (AAI).
- Consider certificate restrictions for:
  - [Expiration](#)
  - [Encoding](#)
  - [Carriage Returns](#)
  - [Subject CN Elements](#)
  - [Concatenation](#)


### Procedure

- Step 1** Choose **CERTIFICATE\_MANAGEMENT > MANAGE\_SIGNED\_CERTS > IMPORT\_CERTIFICATE**.



- Step 2** Choose **Yes** at the prompt to overwrite your active certificates with their replacements.



- Step 3** Enter information about the FTP or SFTP server where you store your digital certificates.
- a. Use the first field to enter a routable IP address or DNS-resolvable FQDN for the server.
  - b. Press the **Down** () key.

- c. Use the second field to enter a username that has sufficient permissions to read your certificates from the server.
- d. Choose **OK**.


- Step 4** Enter your password for the FTP or SFTP server, and then choose **OK**.

- Step 5** Enter absolute file paths, as prompted.

- a. Use the first field to specify the path to one or more PEM files. If you will specify more than one file, comma-separate the filenames.



**Note** Do not specify a ZIP archive that contains your PEM files. If you do, an error message will state that the certificate chain is damaged and at least one of your certificates is not formatted correctly.

- b. Press the **Down** () key.
- c. Use the second field to specify the path to one or more CAchain files.
- d. Choose **OK**.



**Note** An error message might state that AAI could not retrieve any CAchain files from the remote server. If so, several additional messages might load in sequence. In this case, you must choose OK after each message to dismiss it. For example, a sequence of messages might say:

- Failed to get file usage: from remote server.
- Failed to get file tokenize from remote server.
- Failed to get file [separator] from remote server.
- Failed to get file [string\_to\_tokneize] from remote server.
- 1 MISSING\_CA\_CERTIFICATE

If access failed after AAI exceeded that maximum number of retries, please check that the server is running and reachable, and that you entered both paths correctly.

- Step 6** Stop. You have completed this procedure.



**What to Do Next**

- **MANDATORY**—*The appliance identity has changed. You must now re-establish trust among your Cisco DMS appliances. Go to the “Pair Your Appliances” section on page 11-2.*
- **OPTIONAL**—*Would you like to verify any of your digital certificates? Go to the “View Identity Certificates” section on page 7-15.*

**Related Topics**

- [Generate and Submit Certificate Signing Requests \(CSR\), page 7-7](#)

## Generate Self-signed Certificates

**Caution**

In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance. Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

**Workflow Context**

This topic is part of [Workflow B](#).

**Before You Begin**

- Log in as **admin** to the Appliance Administration Interface (AAI).

**Procedure**

**Step 1** Choose **CERTIFICATE\_MANAGEMENT > MANAGE\_SELF\_SIGNED\_CERTS > GENERATE\_NEW\_CERT**.

**Step 2** Enter values in the fields, as illustrated.





**Note**

**Do not use any of these characters.**

, + = " ' ` \ < > # ;

**a** Department:  
**b** Organization:  
**c** Location:  
**d** State:  
**e** Country:  
**g** Months before expiration

< **OK** >      <Cancel>


- a. Use the Department field to enter the name for your organizational unit—such as *Finance Ministry*, *Taiwan Office*, *College of Engineering*, or *Publications Department*. Then, press the **Down** () key.
- b. Use the Organization field to enter the full legal name for your entire organization, as it is known to your national government or intergovernmental authority—such as *Cisco Systems*, *Cambridge University*, or *Médecins Sans Frontières*. Then, press the **Down** () key.
- c. Use the Location field to enter the full and officially designated place name of your city, town, township, village, hamlet, civil parish, or settlement—such as *Madrid* or *Tokyo*. Then, press the **Down** () key.
- d. Use the State field to enter the full name of your state, province, commonwealth, territory, republic, periphery, dependency, or protectorate—such as *Montserrat*, *California*, *Tamil Nadu*, *Chechnya*, *São Paulo*, or *Crete*. Then, press the **Down** () key.
- e. Use the Country field to enter the 2-character country code, as managed by the Internet Assigned Names Agency (IANA).
  - Even if this code **is not part** of your Internet domain name, it is a necessary attribute of your digital certificate.
  - Even if this code **is part** of your Internet domain name, you must not prefix it here with a period.




---

**Note** Your IANA country code might differ from all country name abbreviations that you know. The [“Internet Assigned Names Agency \(IANA\) Country Codes”](#) section on page 7-19 directs you to your country code.

---

- f. Press the **Down** () key.
- g. Use the Months Before Expiration field to count the months until your digital certificate should expire.
  - Briefer durations improve security at the cost of convenience.
  - Longer durations improve convenience at the cost of security.
  - Permitted values range from **1** to **999**.

**Step 3** Choose **OK**.

**Step 4** Stop. You have completed this procedure.

---

#### What to Do Next

- **MANDATORY**—*The appliance identity has changed. You must now re-establish trust among your Cisco DMS appliances. Go to the [“Pair Your Appliances”](#) section on page 11-2.*
- **OPTIONAL**—*Would you like to verify any of your digital certificates? Go to the [“View Identity Certificates”](#) section on page 7-15.*

# View Identity Certificates

**Caution**

In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance. Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

**Workflow Context**

This topic is not part of any workflow.

**Before You Begin**

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Obtain and install certificates.

**Procedure**

- 
- Step 1** Choose **CERTIFICATE\_MANAGEMENT > VIEW\_CERTIFICATE**.
- Step 2** Examine the certificate.
- Step 3** Choose **EXIT** when you are done.
- Step 4** Stop. You have completed this procedure.
- 

**What to Do Next**

- **OPTIONAL**—*Would you like to back up your digital certificates?* Go to the [“Export a Keystore to Back It Up”](#) section on page 7-17.

**Related Topics**

- [Generate and Submit Certificate Signing Requests \(CSR\)](#), page 7-7
- [Import \(Install\) Provider-signed Certificates](#), page 7-11
- [Generate Self-signed Certificates](#), page 7-13

## View a Certificate Chain to Verify its Certificates

**Caution**

In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance. Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

**Workflow Context**

This topic is part of [Workflow A](#), [Workflow B](#), and [Workflow C](#).

**Before You Begin**

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Obtain and install certificates.

**Procedure**

- 
- Step 1** Choose **CERTIFICATE\_MANAGEMENT > VIEW\_CERT\_CHAIN**.
- Step 2** Examine the certificate chain.
- Step 3** Choose **EXIT** when you are done.
- Step 4** Stop. You have completed this procedure.
- 

**What to Do Next**

- **OPTIONAL**—*Would you like to back up your digital certificates?* Go to the [“Export a Keystore to Back It Up”](#) section on page 7-17.

**Related Topics**

- [Generate and Submit Certificate Signing Requests \(CSR\)](#), page 7-7
- [Import \(Install\) Provider-signed Certificates](#), page 7-11
- [Generate Self-signed Certificates](#), page 7-13

## Export a Keystore to Back It Up

Your certificates are included whenever you back up your appliance from its local instance of AAI.

**Caution**

**In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance.** Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.


**Workflow Context**

This topic is part of [Workflow A](#) and [Workflow C](#).

**Before You Begin**

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Obtain and install certificates.
- Delete any old keystore \*.DAT file from your FTP or SFTP server before you export a new one.

**Procedure**

- 
- Step 1** Choose **CERTIFICATE\_MANAGEMENT > EXPORT\_KEYSTORE**.
- Step 2** Enter the passphrase from which your private key was derived.
- Step 3** Press **Enter**.
- Step 4** Use the first field to enter a routable IP address or DNS-resolvable FQDN for the FTP or SFTP server where you will transfer an exported copy of your digital certificates.
- Step 5** Press the **Down** () key.
- Step 6** Use the second field to enter a username that has read-write permissions on the server that you specified. Then, press **Enter**.
- Step 7** Enter the password that authenticates the username. Then, press **Enter**.
- Step 8** Enter the full pathname where to save your keystore file on the remote server. Then, press **Enter**.
- Step 9** Stop. You have completed this procedure.
- 

**What to Do Next**

- **OPTIONAL**—*Would you like to restore certificates from a backup?* Go to the [“Import a Keystore to Restore It from a Backup”](#) section on page 7-18.

**Related Topics**

- [Generate and Submit Certificate Signing Requests \(CSR\)](#), page 7-7
- [Import \(Install\) Provider-signed Certificates](#), page 7-11
- [Generate Self-signed Certificates](#), page 7-13

# Import a Keystore to Restore It from a Backup

**Caution**

In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance. Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

**Workflow Context**

This topic is part of [Workflow C](#).

**Before You Begin**

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Export a keystore.

**Procedure**

- 
- Step 1** Choose **CERTIFICATE\_MANAGEMENT > IMPORT\_KEYSTORE**.
- Step 2** Enter the passphrase from which your private key was derived.
- Step 3** Press **Enter**.
- Step 4** Use the first field to enter a routable IP address or DNS-resolvable FQDN for the FTP or SFTP server where you store your digital certificates.
- Step 5** Press the down key.
- Step 6** Use the second field to enter a username that has sufficient permissions to read your certificates from the server that you specified. Then, press **Enter**.
- Step 7** Enter the password that authenticates the username. Then, press **Enter**.
- Step 8** Enter the full pathname that points to your keystore file on the remote server. Then, press **Enter**.
- Step 9** Stop. You have completed this procedure.
- 

**What to Do Next**

- **MANDATORY**—*The appliance identity has changed. You must now re-establish trust among your Cisco DMS appliances. Go to the “Pair Your Appliances” section on page 11-2.*
- **OPTIONAL**—*Would you like to verify any of your digital certificates? Go to the “View Identity Certificates” section on page 7-15.*

**Related Topics**

- [Export a Keystore to Back It Up, page 7-17](#)

# Reference

- [Internet Assigned Names Agency \(IANA\) Country Codes, page 7-19](#)
- [FAQs and Troubleshooting, page 7-34](#)

## Internet Assigned Names Agency (IANA) Country Codes

Digital certificates use one standard set of codes to describe the international locations of entities whose identities are certified. IANA assigns these codes. IANA closely derives almost all of its codes from “A2” country and region codes, which the *ISO 3166-1 alpha-2* standard defines. However, the set of IANA-assigned codes is not perfectly identical to the set of A2 codes. In some cases, IANA has defined new country and region codes for its own purposes. Some of these, in turn, were then added to ISO 3166.

Furthermore, geopolitical changes over time cause governmental federations to develop and dissolve. Lands are conquered, colonized, reapportioned, renamed, and so on. Slow but continual changes like these can create confusion about which country and region code to use in a certificate signing request (CSR). And while there are precedents for deleting country codes from ISO 3166, removal there does not result in immediate removal also from the country code top-level domains (ccTLDs) that exist in DNS.

[Table 7-1](#) sorts countries and regions alphabetically by their names in English. Its cross-references redirect you in cases where geopolitical events, shared governance, or other factors might lead to confusion about which code to use.

**Table 7-1 IANA Country and Region Codes**

Code	Country or Region
<b>A</b>	
AF	Afghanistan, Islamic State of
AX	Åland Islands <i>see also</i> <a href="#">Finland</a>
AL	Albania
DZ	Algeria, Democratic Popular Republic of
AS	American Samoa, Territory of <i>see also</i> <a href="#">Guam, Territory of</a> ; <a href="#">Northern Mariana Islands, Commonwealth of the</a> ; <a href="#">Puerto Rico, Commonwealth of</a> ; <a href="#">Samoa, Independent State of</a> ; <a href="#">United States of America, Federal Union of the</a> ; and <a href="#">Virgin Islands, U.S. Territory of the</a>
	For <i>Andaman</i> , see <a href="#">India</a>
AD	Andorra, Principality of
AO	Angola
AI	Anguilla
AQ	Antarctica
AG	Antigua and Barbuda
	For <i>Aosta Valley</i> , see <a href="#">Italy</a>
AR	Argentina

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
AM	Armenia
AW	Aruba
	For <i>Ascension</i> , see <a href="#">Saint Helena, Ascension and Tristan da Cunha</a>
AC	Ascension Island <i>see also</i> <a href="#">Saint Helena, Ascension and Tristan da Cunha</a>
	For <i>Assam</i> , see <a href="#">India</a>
AU	Australia <b>Note</b> All subdomains that previously used OZ as their country code top-level domain were transitioned to OZ.AU.
AT	Austria
AZ	Azerbaijan
<b>B</b>	
BS	Bahamas, Commonwealth of
BH	Bahrain, Emirate of
	For <i>Bali</i> , see <a href="#">Indonesia</a>
BD	Bangladesh
	For <i>Bangui</i> , see <a href="#">Central African Republic</a>
BB	Barbados
	For <i>Barbuda</i> , see <a href="#">Antigua and Barbuda</a>
BY	Belarus
BE	Belgium, Kingdom of
BZ	Belize
	For <i>Bengal</i> , see <a href="#">Bangladesh</a> and <a href="#">India</a>
BJ	Benin
BM	Bermuda
BT	Bhutan, Kingdom of
	For <i>Bodoland Territory</i> , see <a href="#">India</a>
BO	Bolivia
	For <i>Bolzano-Bozen (Alto Adige-South Tyrol)</i> , see <a href="#">Austria</a> ; <a href="#">Germany, Federal Republic of</a> ; <a href="#">Hungary</a> ; and <a href="#">Italy</a>
	For <i>Borneo</i> , see <a href="#">Indonesia</a>
BA	Bosnia and Herzegovina
BW	Botswana
	For <i>Bougainville</i> , see <a href="#">Papua New Guinea, Independent State of</a>
BV	Bouvet Island, Territory of <b>Note</b> Although the BV country code exists in <i>ISO-3166-1 alpha-2</i> , and exists as a country code top-level domain in DNS, it does not contain any subdomains.



Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
BR	Brazil, Federative Republic of
	For <i>Britain</i> , see <a href="#">Ireland</a> and <a href="#">United Kingdom of Great Britain and Northern Ireland</a>
IO	British Indian Ocean Territory
BN	Brunei Darussalam, Sultanate of
	For <i>Brussels</i> , see <a href="#">Belgium, Kingdom of</a>
	For <i>Buenos Aires</i> , see <a href="#">Argentina</a>
BG	Bulgaria
BF	Burkina Faso
	For <i>Burma</i> , see <a href="#">Myanmar</a>
BI	Burundi
<b>C</b>	
	For <i>Caicos Islands</i> , see <a href="#">Turks and Caicos Islands, Territory of</a>
KH	Cambodia, Kingdom of
CM	Cameroon
CA	Canada
CV	Cape Verde
KY	Cayman Islands
CF	Central African Republic
	For <i>Ceuta</i> , see <a href="#">Spain</a>
	For <i>Ceylon</i> , see <a href="#">Sri Lanka</a>
TD	Chad
	For <i>Chakma Autonomous District</i> , see <a href="#">India</a>
	For <i>Channel Islands</i> , see <a href="#">Guernsey, Bailiwick of</a> and <a href="#">Jersey, Bailiwick of</a>
	For <i>Chiapas</i> , see <a href="#">Mexico</a>
CL	Chile
CN	China, People's Republic of <i>see also</i> <a href="#">Hong Kong; Macau, Special Administrative Region of</a> ; and <a href="#">Taiwan, Republic of China</a>
CX	Christmas Island, Territory of
CC	Cocos (Keeling) Islands
CO	Colombia
KM	Comoros
CG	Congo <i>see also</i> <a href="#">Congo, the Democratic Republic of the</a>
CD	Congo, the Democratic Republic of the <i>see also</i> <a href="#">Congo</a>

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
CK	Cook Islands
For <i>Corsica, Territorial Collectivity of</i> , see <a href="#">France, Metropolitan</a>	
CR	Costa Rica
CI	Cote d'Ivoire
HR	Croatia
CU	Cuba
CY	Cyprus
For <i>Czechoslovakia</i> , see <a href="#">Czech Republic</a>	
CZ	Czech Republic <i>see also</i> <a href="#">Slovakia</a>
<b>D</b>	
For <i>Darjeeling Gorkha Hills</i> , see <a href="#">India</a>	
DK	Denmark, Kingdom of <i>see also</i> <a href="#">Faroe Islands</a> and <a href="#">Greenland</a>
DJ	Djibouti
DM	Dominica, Commonwealth of <i>see also</i> <a href="#">Dominican Republic</a>
DO	Dominican Republic <i>see also</i> <a href="#">Dominica, Commonwealth of</a>
<b>E</b>	
For <i>East Bengal</i> , see <a href="#">Bangladesh</a> and <a href="#">Pakistan, Islamic Republic of</a>	
For <i>East Indies</i> , see <a href="#">Indonesia</a> ; <a href="#">Malaysia, Kingdom of</a> ; <a href="#">Philippines</a> ; and <a href="#">Solomon Islands</a>	
For <i>East Timor</i> , see <a href="#">Timor-Leste</a>	
EC	Ecuador
EG	Egypt, Arab Republic of
SV	El Salvador
GQ	Equatorial Guinea
For <i>Ghana</i> , see <a href="#">Ghana</a>	
For <i>Guiana</i> , see <a href="#">French Guiana, Overseas Department of</a>	
For <i>Guinea</i> , see <a href="#">Guinea</a>	
For <i>Guyana</i> , see <a href="#">Guyana, Cooperative Republic of</a>	
ER	Eritrea
EE	Estonia
ET	Ethiopia, Federal Democratic Republic of

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
EU	European Union
<b>F</b>	
FK	Falkland Islands (Malvinas Islas), Colony of
FO	Faroe Islands
FJ	Fiji
FI	Finland <i>see also</i> Åland Islands
FR	France
FX	France, Metropolitan
GF	French Guiana, Overseas Department of
	For <i>Equatorial Guinea</i> , see <a href="#">Equatorial Guinea</a>
	For <i>Ghana</i> , see <a href="#">Ghana</a>
	For <i>Guinea</i> , see <a href="#">Guinea</a>
	For <i>Guyana</i> , see <a href="#">Guyana, Cooperative Republic of</a>
PF	French Polynesia, Overseas Territory of
TF	French Southern Territories
	For <i>Friuli-Venezia Giulia</i> , see <a href="#">Croatia</a> ; <a href="#">Italy</a> ; and <a href="#">Slovenia</a>
<b>G</b>	
GA	Gabon
GM	Gambia
	For <i>Garo Hills Autonomous District</i> , see <a href="#">India</a>
GE	Georgia <i>see also</i> <a href="#">South Georgia and the South Sandwich Islands</a>
DE	Germany, Federal Republic of
GH	Ghana
	For <i>Equatorial Guinea</i> , see <a href="#">Equatorial Guinea</a>
	For <i>Guiana</i> , see <a href="#">French Guiana, Overseas Department of</a>
	For <i>Guinea</i> , see <a href="#">Guinea</a>
	For <i>Guyana</i> , see <a href="#">Guyana, Cooperative Republic of</a>
GI	Gibraltar
	For <i>Gilbert Islands</i> , see <a href="#">Kiribati</a>
	For <i>Great Britain</i> , see <a href="#">United Kingdom of Great Britain and Northern Ireland</a>
GR	Greece

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
GL	Greenland <i>see also</i> <a href="#">Denmark, Kingdom of</a> and <a href="#">Faroe Islands</a>
GD	Grenada <i>see also</i> <a href="#">Saint Vincent and the Grenadines</a>
For <i>Grenadines</i> , <i>see</i> <a href="#">Saint Vincent and the Grenadines</a>	
GP	Guadeloupe and Dependencies, Overseas Department of
GU	Guam, Territory of <i>see also</i> <a href="#">American Samoa, Territory of</a> ; <a href="#">Northern Mariana Islands, Commonwealth of the</a> ; <a href="#">Puerto Rico, Commonwealth of</a> ; <a href="#">United States of America, Federal Union of the</a> ; and <a href="#">Virgin Islands, U.S. Territory of the</a>
For <i>Guangxi Zhung Autonomous Region</i> , <i>see</i> <a href="#">China, People's Republic of</a>	
GT	Guatemala
GG	Guernsey, Bailiwick of <i>see also</i> <a href="#">Jersey, Bailiwick of</a>
For <i>Guiana</i> , <i>see</i> <a href="#">French Guiana, Overseas Department of</a>	
GN	Guinea <i>see also</i> <a href="#">Guinea-Bissau</a>
GW	Guinea-Bissau <i>see also</i> <a href="#">Guinea</a>
GY	Guyana, Cooperative Republic of
For <i>Equatorial Guinea</i> , <i>see</i> <a href="#">Equatorial Guinea</a>	
For <i>Ghana</i> , <i>see</i> <a href="#">Ghana</a>	
For <i>Guiana</i> , <i>see</i> <a href="#">French Guiana, Overseas Department of</a>	
For <i>Guinea</i> , <i>see</i> <a href="#">Guinea</a>	
<b>H</b>	
HT	Haiti
HM	Heard and McDonald Islands, Territory of
For <i>Herzegovina</i> , <i>see</i> <a href="#">Bosnia and Herzegovina</a>	
VA	Holy See, State of Vatican City <i>see also</i> <a href="#">Italy</a>
HN	Honduras
HK	Hong Kong <i>see also</i> <a href="#">China, People's Republic of</a> ; <a href="#">Macau, Special Administrative Region of</a> ; and <a href="#">Taiwan, Republic of China</a>
HU	Hungary

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
<b>I</b>	
IS	Iceland
IN	India
ID	Indonesia
For <i>Inner Mongolia Autonomous Region</i> , see <a href="#">China, People's Republic of</a>	
IR	Iran, Islamic Republic of
IQ	Iraq
For <i>Iraqi Kurdistan</i> , see <a href="#">Iraq</a>	
IE	Ireland
IM	Isle of Man, Territory of
IL	Israel, State of <i>see also</i> <a href="#">Palestine, Occupied Territory of</a>
IT	Italy <i>see also</i> <a href="#">Holy See, State of Vatican City</a>
For <i>Ivory Coast</i> , see <a href="#">Cote d'Ivoire</a>	
<b>J</b>	
For <i>Jaintia Hills Autonomous District</i> , see <a href="#">India</a>	
JM	Jamaica
For <i>Jammu</i> , see <a href="#">India</a>	
For <i>Jan Mayen</i> , see <a href="#">Svalbard and Jan Mayen Islands, Territory of</a>	
JP	Japan, Imperial State of
For <i>Java</i> , see <a href="#">Indonesia</a>	
For <i>Jeju-do</i> , see <a href="#">Korea, Republic of</a>	
JE	Jersey, Bailiwick of <i>see also</i> <a href="#">Guernsey, Bailiwick of</a>
For <i>Jewish Autonomous Oblast</i> , see <a href="#">Russia, Federation of</a>	
JO	Jordan, Hashemite Kingdom of
<b>K</b>	
For <i>Kampuchea</i> , see <a href="#">Cambodia, Kingdom of</a>	
For <i>Karbi Anglong Autonomous Council</i> , see <a href="#">India</a>	
For <i>Kashmir</i> , see <a href="#">China, People's Republic of</a> ; <a href="#">India</a> ; and <a href="#">Pakistan, Islamic Republic of</a>	
KZ	Kazakhstan
For <i>Keeling Islands</i> , see <a href="#">Cocos (Keeling) Islands</a>	
KE	Kenya

**Table 7-1 IANA Country and Region Codes (continued)**

Code	Country or Region
	For <i>Khasi Hills Autonomous District</i> , see <a href="#">India</a>
KI	Kiribati <i>see also</i> <a href="#">Marshall Islands</a> ; <a href="#">Micronesia, Federated States of</a> ; and <a href="#">Nauru</a>
KP	Korea, Democratic People's Republic of <i>see also</i> <a href="#">Korea, Republic of</a>
KR	Korea, Republic of <i>see also</i> <a href="#">Korea, Democratic People's Republic of</a>
	For <i>Kosovo</i> , see <a href="#">Serbia</a>
	For <i>Kurdistan</i> , see <a href="#">Armenia</a> ; <a href="#">Iran, Islamic Republic of</a> ; <a href="#">Iraq</a> ; <a href="#">Syria, Arab Republic of</a> ; and <a href="#">Turkey</a>
KW	Kuwait, Emirate of
KG	Kyrgyzstan
<b>L</b>	
	For <i>Ladakh Autonomous Hill Development</i> , see <a href="#">India</a>
	For <i>Lai Autonomous District</i> , see <a href="#">India</a>
LA	Lao People's Democratic Republic
LV	Latvia
LB	Lebanon
LS	Lesotho, Kingdom of
LR	Liberia
LY	Libyan Arab Jamahiriya, Socialist People's
LI	Liechtenstein, Principality of
LT	Lithuania
LU	Luxembourg, Grand Duchy of
	For <i>Luzon</i> , see <a href="#">Philippines</a>
<b>M</b>	
MO	Macau, Special Administrative Region of <i>see also</i> <a href="#">China, People's Republic of</a> ; <a href="#">Hong Kong</a> ; and <a href="#">Taiwan, Republic of China</a>
MK	Macedonia, the former Yugoslav Republic of
MG	Madagascar
	For <i>Madeira</i> , see <a href="#">Portugal</a>
MW	Malawi
	For <i>Malay Archipelago</i> , see <a href="#">Malaysia, Kingdom of</a> and <a href="#">Philippines</a>
	For <i>Malay Peninsula</i> , see <a href="#">Malaysia, Kingdom of</a> ; <a href="#">Myanmar</a> ; <a href="#">Philippines</a> ; <a href="#">Singapore</a> ; and <a href="#">Thailand, Kingdom of</a>

**Table 7-1 IANA Country and Region Codes (continued)**

<b>Code</b>	<b>Country or Region</b>
MY	Malaysia, Kingdom of <i>see also</i> <a href="#">Singapore</a>
MV	Maldives
ML	Mali
MT	Malta
	For <i>Malvinas</i> , see <a href="#">Falkland Islands (Malvinas Islas), Colony of</a>
	For <i>Mara Autonomous District</i> , see <a href="#">India</a>
MH	Marshall Islands <i>see also</i> <a href="#">Kiribati</a> and <a href="#">Micronesia, Federated States of</a>
	For <i>Mariana Islands</i> , see <a href="#">Northern Mariana Islands, Commonwealth of the</a>
MQ	Martinique, Overseas Department of the
MR	Mauritania, Islamic Republic of <i>see also</i> <a href="#">Mauritius</a>
MU	Mauritius <i>see also</i> <a href="#">Mauritania, Islamic Republic of</a>
YT	Mayotte, Territorial Collectivity of
	For <i>McDonald Islands</i> , see <a href="#">Heard and McDonald Islands, Territory of</a>
	For <i>Meghalaya</i> , see <a href="#">India</a>
	For <i>Melilla</i> , see <a href="#">Spain</a>
MX	Mexico
FM	Micronesia, Federated States of <i>see also</i> <a href="#">Kiribati</a> ; <a href="#">Marshall Islands</a> ; and <a href="#">Northern Mariana Islands, Commonwealth of the</a>
	For <i>Mindanao</i> , see <a href="#">Philippines</a>
	For <i>Miquelon</i> , see <a href="#">Saint Pierre and Miquelon, Overseas Territorial Collectivity of</a>
	For <i>Mizoram</i> , see <a href="#">India</a>
	For <i>Moldavia</i> , see <a href="#">Moldova, Republic of</a>
MD	Moldova, Republic of
MC	Monaco, Principality of
MN	Mongolia
ME	Montenegro
MS	Montserrat, Territory of
MA	Morocco, Kingdom of
	For <i>Mount Athos</i> , see <a href="#">Greece</a>
MZ	Mozambique
MM	Myanmar

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
<b>N</b>	
NA	Namibia <i>see also</i> <a href="#">South Africa</a>
NR	Nauru <i>see also</i> <a href="#">Kiribati</a> ; <a href="#">Marshall Islands</a> ; and <a href="#">Micronesia, Federated States of</a>
NP	Nepal, Kingdom of
NL	Netherlands, Kingdom of the <i>see also</i> <a href="#">Netherlands Antilles</a>
AN	Netherlands Antilles <i>see also</i> <a href="#">Netherlands, Kingdom of the</a>
	For <i>Nevis</i> , <i>see</i> <a href="#">Saint Kitts and Nevis</a>
NC	New Caledonia and Dependencies, Overseas Territory of
	For <i>New Guinea</i> , <i>see</i> <a href="#">Papua New Guinea, Independent State of</a>
	For <i>New Hebrides</i> , <i>see</i> <a href="#">Vanuatu</a>
NZ	New Zealand <i>see also</i> <a href="#">Cook Islands</a> ; <a href="#">Niue</a> ; and <a href="#">Tokelau</a>
NI	Nicaragua
	For <i>Nicobar Islands</i> , <i>see</i> <a href="#">India</a>
NE	Niger <i>see also</i> <a href="#">Nigeria, Federal Republic of</a>
NG	Nigeria, Federal Republic of <i>see also</i> <a href="#">Niger</a>
	For <i>Ningxia Hui Autonomous Region</i> , <i>see</i> <a href="#">China, People's Republic of</a>
NU	Niue <i>see also</i> <a href="#">Cook Islands</a> ; <a href="#">New Zealand</a> ; and <a href="#">Tokelau</a>
NF	Norfolk Island, Territory of
	For <i>North Cachar Hills Autonomous District</i> , <i>see</i> <a href="#">India</a>
	For <i>North Korea</i> , <i>see</i> <a href="#">Korea, Democratic People's Republic of</a>
	For <i>North Sentinel Island</i> , <i>see</i> <a href="#">India</a>
MP	Northern Mariana Islands, Commonwealth of the <i>see also</i> <a href="#">American Samoa, Territory of</a> , <a href="#">Guam, Territory of</a> , <a href="#">Puerto Rico, Commonwealth of</a> , <a href="#">United States of America, Federal Union of the</a> , and <a href="#">Virgin Islands, U.S. Territory of the</a>
NO	Norway, Kingdom of
<b>O</b>	
OM	Oman, Sultanate of



Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
<b>P</b>	
PK	Pakistan, Islamic Republic of
PW	Palau
PS	Palestine, Occupied Territory of <i>see also</i> <a href="#">Israel, State of</a>
PA	Panama, Unified Republic of
PG	Papua New Guinea, Independent State of
PC	Paracel Islands, Territory of
PY	Paraguay
For <i>Peninsular Malaysia</i> , see <a href="#">Malaysia, Kingdom of</a>	
PE	Peru
PH	Philippines
PN	Pitcairn
PL	Poland
For <i>Polynesia</i> , see <a href="#">French Polynesia, Overseas Territory of</a>	
PT	Portugal
TP	<i>Portuguese Timor</i> (being phased out)
For <i>Principe</i> , see <a href="#">Sao Tome and Principe</a>	
PR	Puerto Rico, Commonwealth of  <i>see also</i> <a href="#">American Samoa, Territory of</a> , <a href="#">Guam, Territory of</a> , <a href="#">Northern Mariana Islands, Commonwealth of the</a> , <a href="#">United States of America, Federal Union of the</a> , and <a href="#">Virgin Islands, U.S. Territory of the</a>
<b>Q</b>	
QA	Qatar, Emirate of
<b>R</b>	
RE	Reunion, Overseas Department of the  For <i>Rhodesia</i> , see <a href="#">Zambia</a> and <a href="#">Zimbabwe</a>  For <i>Rodrigues</i> , see <a href="#">Mauritius</a>
RO	Romania
RU	Russia, Federation of
RW	Rwanda

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
<b>S</b>	
For <i>Sahara</i> , see <a href="#">Western Sahara</a>	
BL	Saint Barthelemy <b>Note</b> Although the BL country code exists in <i>ISO-3166-1 alpha-2</i> , and exists as a country code top-level domain in DNS, it does not contain any subdomains.
SH	Saint Helena, Ascension and Tristan da Cunha <i>see also</i> <a href="#">Ascension Island</a>
KN	Saint Kitts and Nevis
LC	Saint Lucia
MF	Saint Martin <b>Note</b> Although the MF country code exists in <i>ISO-3166-1 alpha-2</i> , and exists as a country code top-level domain in DNS, it does not contain any subdomains.
PM	Saint Pierre and Miquelon, Overseas Territorial Collectivity of
VC	Saint Vincent and the Grenadines <i>see also</i> <a href="#">Grenada</a>
WS	Samoa, Independent State of <i>see also</i> <a href="#">American Samoa, Territory of</a>
SM	San Marino
For <i>Sandwich Islands</i> , see <a href="#">South Georgia and the South Sandwich Islands</a>	
ST	Sao Tome and Principe
For <i>Sardinia</i> , see <a href="#">Italy</a>	
SA	Saudi Arabia, Kingdom of
For <i>Scotland</i> , see <a href="#">United Kingdom of Great Britain and Northern Ireland</a>	
SN	Senegal
RS	Serbia
SC	Seychelles
For <i>Siam</i> , see <a href="#">Thailand, Kingdom of</a>	
For <i>Sicily</i> , see <a href="#">Italy</a>	
SL	Sierra Leone
SG	Singapore <i>see also</i> <a href="#">Malaysia, Kingdom of</a>
SK	Slovakia <i>see also</i> <a href="#">Czech Republic</a>
SI	Slovenia <i>see also</i> <a href="#">Macedonia, the former Yugoslav Republic of</a>
SB	Solomon Islands

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
SO	Somalia
ZA	South Africa <i>see also</i> <a href="#">Namibia</a>
GS	South Georgia and the South Sandwich Islands
	For <i>South Korea</i> , <i>see</i> <a href="#">Korea, Republic of</a>
	For <i>South Sandwich Islands</i> , <i>see</i> <a href="#">South Georgia and the South Sandwich Islands</a>
	For <i>South Yemen</i> , <i>see</i> <a href="#">Yemen</a>
	For <i>Southern Sudan</i> , <i>see</i> <a href="#">Sudan</a>
SU	Soviet Union (being phased out)
ES	Spain
LK	Sri Lanka
SD	Sudan
	For <i>Sulawesi</i> , <i>see</i> <a href="#">Indonesia</a>
	For <i>Sumatra</i> , <i>see</i> <a href="#">Indonesia</a>
SR	Suriname
SJ	Svalbard and Jan Mayen Islands, Territory of <b>Note</b> Although the SJ country code exists in <i>ISO-3166-1 alpha-2</i> , and exists as a country code top-level domain in DNS, it does not contain any subdomains.
SZ	Swaziland
SE	Sweden, Kingdom of
CH	Switzerland
SY	Syria, Arab Republic of
<b>T</b>	
TW	Taiwan, Republic of China <i>see also</i> <a href="#">China, People's Republic of</a> , <a href="#">Hong Kong</a> , and <a href="#">Macau, Special Administrative Region of</a>
TJ	Tajikistan
	For <i>Tanganyika</i> , <i>see</i> <a href="#">Tanzania, United Republic of</a>
TZ	Tanzania, United Republic of
	For <i>Tashkent</i> , <i>see</i> <a href="#">Uzbekistan</a>
TH	Thailand, Kingdom of
	For <i>Tibet Autonomous Region</i> , <i>see</i> <a href="#">China, People's Republic of</a>
TL	Timor-Leste
	For <i>Tobago</i> , <i>see</i> <a href="#">Trinidad and Tobago</a>
TG	Togo

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
TK	Tokelau <i>see also</i> <a href="#">Cook Islands</a> ; <a href="#">New Zealand</a> ; and <a href="#">Niue</a>
TO	Tonga, Kingdom of  <i>For Trento (Trentino)</i> , <i>see</i> <a href="#">Austria</a> ; <a href="#">Germany, Federal Republic of</a> ; <a href="#">Hungary</a> ; and <a href="#">Italy</a>
TT	Trinidad and Tobago  <i>For Tripura Tribal Areas Autonomous District</i> , <i>see</i> <a href="#">India</a>  <i>For Tristan da Cunha</i> , <i>see</i> <a href="#">Saint Helena, Ascension and Tristan da Cunha</a>
TN	Tunisia
TR	Turkey
TM	Turkmenistan
TC	Turks and Caicos Islands, Territory of
TV	Tuvalu
<b>U</b>	
UG	Uganda
UA	Ukraine
AE	United Arab Emirates
GB	United Kingdom of Great Britain and Northern Ireland
UK	<b>Note</b> Although the GB region code exists in <i>ISO-3166-1 alpha-2</i> , and exists as a country code top-level domain (ccTLD) in DNS, it contains only one subdomain. Other United Kingdom sites use UK as their ccTLD. Nonetheless, IANA defined the UK region code, which does not exist in <i>ISO 3166-1 alpha-2</i> .
US	United States of America, Federal Union of the  <i>see also</i> <a href="#">American Samoa, Territory of</a> , <a href="#">Guam, Territory of</a> , <a href="#">Northern Mariana Islands, Commonwealth of the</a> , <a href="#">Puerto Rico, Commonwealth of</a> , and <a href="#">Virgin Islands, U.S. Territory of the</a>
UM	United States Minor Outlying Islands  <b>Note</b> Although the UM country code top-level domain was deactivated, it is still available with restrictions.
UY	Uruguay
UZ	Uzbekistan
<b>V</b>	
VU	Vanuatu  <i>For Vatican</i> , <i>see</i> <a href="#">Holy See, State of Vatican City</a>
VE	Venezuela, Bolivarian Republic of
VN	Viet Nam, Socialist Republic of
VG	Virgin Islands, British Territory of the

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
VI	Virgin Islands, U.S. Territory of the <i>see also</i> <a href="#">American Samoa, Territory of</a> , <a href="#">Guam, Territory of</a> , <a href="#">Northern Mariana Islands, Commonwealth of the</a> , <a href="#">Puerto Rico, Commonwealth of</a> , and <a href="#">United States of America, Federal Union of the</a>
	For <i>Visayas</i> , see <a href="#">Philippines</a>
	For <i>Vojvodina</i> , see <a href="#">Serbia</a>
	For <i>Volta</i> , see <a href="#">Burkina Faso</a>
<b>W</b>	
	For <i>Wales</i> , see <a href="#">United Kingdom of Great Britain and Northern Ireland</a>
WF	Wallis and Futuna Islands, Overseas Territory of
	For <i>West Bengal</i> , see <a href="#">Bangladesh</a> and <a href="#">India</a>
EH	Western Sahara <b>Note</b> Although the EH country code exists in <i>ISO-3166-1 alpha-2</i> , it does not exist as a country code top-level domain in DNS.
<b>X</b>	
	For <i>Xinjiang Uyghur Autonomous Region</i> , see <a href="#">China, People's Republic of</a>
<b>Y</b>	
YE	Yemen
YU	Yugoslavia, Federation of <b>Note</b> Most, if not all, sites that used the YU country code top-level domain have been reassigned to <a href="#">Serbia</a> or <a href="#">Montenegro</a> .
	For <i>Yugoslav Republic</i> , see <a href="#">Bosnia and Herzegovina</a> ; <a href="#">Croatia</a> ; <a href="#">Macedonia, the former Yugoslav Republic of</a> ; <a href="#">Montenegro</a> ; <a href="#">Serbia</a> ; <a href="#">Slovenia</a> ; and <a href="#">Yugoslavia, Federation of</a>
<b>Z</b>	
	For <i>Zaire</i> , see <a href="#">Congo, the Democratic Republic of the</a>
ZM	Zambia
	For <i>Zanzibar</i> , see <a href="#">Tanzania, United Republic of</a>
	For <i>Zelaya</i> , see <a href="#">Nicaragua</a>
ZW	Zimbabwe

## FAQs and Troubleshooting

- [FAQs, page 7-34](#)
- [Troubleshooting, page 7-34](#)

### FAQs

- Q.** What's the difference between a provider-signed certificate and a self-signed certificate?
- A.** Please compare and contrast these definitions from the “Glossary” section on page 7-2.
- [signed](#)
  - [self-signed](#)

### Troubleshooting

- [Error Messages, page 7-34](#)

### Error Messages

Error messages guide you if problems affect your digital certificates. These messages describe a problem and suggest possible ways to solve it.

**Error Message** `Cannot process CA certificate.`

**Explanation** `<exception message>`

**Recommended Action** Cause unknown. We cannot recommend any workaround.

**Error Message** `Cannot unpack <archive file path>.`

**Explanation** The archive is corrupted or its source was not valid.

**Recommended Action** Cause unknown. We cannot recommend any workaround.

**Error Message** `Certificate import failed.`

**Explanation** An internal error occurred.

**Recommended Action** Please contact Cisco technical support.

**Error Message** `Certificate import failed.`

**Explanation** At least one parameter is not valid.

**Recommended Action** Cause unknown. We cannot recommend any workaround.

**Error Message** Certificate is not readable or does not exist.

**Explanation** <absolute file path>

**Recommended Action** Cause unknown. We cannot recommend any workaround.

**Error Message** Certificate not yet valid.

**Explanation** It takes effect in the future, on <date in YYYY-MM-DD format>.

**Recommended Action** Please check that it is correct.

**Error Message** Certificate rejected.

**Explanation** It does not match the newest certificate signing request (CSR) for <FQDN>.

**Recommended Action** Please generate a new certificate signing request (CSR), and then contact your certification authority (CA).

**Error Message** Certificate rejected.

**Explanation** It has expired and is no longer valid.

**Recommended Action** Please generate a new certificate signing request (CSR), and then contact your certification authority (CA).

**Error Message** Certificate rejected.

**Explanation** Its subject does not match <FQDN>.

**Recommended Action** Please confirm that you imported the correct identity certificate. Alternatively, please generate a new certificate signing request (CSR), and then contact your certification authority (CA).

**Error Message** Internal Error.

**Explanation** Cannot build certificate chain.

**Recommended Action** Confirm that no CA certificates are missing.

**Error Message** The certificate chain is broken.

**Explanation** An identity certificate is missing for <FQDN>.

**Recommended Action** Please edit the certificate chain to include all digital certificates that your certification authority (CA) has issued to you.

**Error Message** Warning! Browsers will reject this certificate.

**Explanation** It is self-signed.

**Recommended Action** We recommend that you use certificates from a valid certification authority (CA).





## CHAPTER 8

# Failover

---

**Revised: November 4, 2011,**

The failover area in the AAI enable you to revert a failover configuration to a standalone configuration, recover from a situation known as “split-brain mode”, or check the failover status.

These topics are covered in detail in the *Failover Configuration Guide for Cisco Digital Media Suite 5.3.x*:

[http://www.cisco.com/en/US/docs/video/digital\\_media\\_systems/5\\_x/5\\_3/dms/failover\\_guide/dmsfailover.html](http://www.cisco.com/en/US/docs/video/digital_media_systems/5_x/5_3/dms/failover_guide/dmsfailover.html)





## CHAPTER 9

# Set Up and Configure a DMM Appliance

---

**Revised: November 4, 2011**

This chapter includes the following sections:

- [Set Up a DMM Appliance, page 9-1](#)
- [Configure a DMM Appliance, page 9-2](#)

## Set Up a DMM Appliance

### Before You Begin

- Ensure that a DNS entry has been created and published for the DMM appliance.
- Ensure that you have obtained the license keys to unlock the software features on your DMM and Show and Share appliances. For information about obtaining license keys, see the [Licenses](#) chapter of the *User Guide for Cisco Digital Media Manager* on Cisco.com.
- Verify that at least one computer on your network is configured for access to other networked devices through TCP ports 80 and 8080.
- Enable popup windows in your browser if they are disabled. You can complete the checklist only if popup windows are enabled.
- Determine if your network uses dynamic (DHCP) or static IP addresses. If your network uses static IP addresses, obtain the following information:
  - Learn what IP address to assign to the DMM appliance.
  - Learn what subnet mask (netmask) to use.
  - Learn what IP addresses are assigned to the default network gateway, the primary DNS server, and the secondary DNS server.

### Procedure

---

- Step 1** Unpack the equipment from its container and verify that all components are present.
- Step 2** Plug in the redundant power cables on the back of the appliance.
- Step 3** Connect a live Ethernet cable to Port 1 on the back of the appliance.
- Step 4** Connect a monitor to the VGA output on the back of the appliance.
- Step 5** Connect a standard PS2 keyboard to the purple PS2 port in the back of the appliance.

- Step 6** Power on the appliance.  
The “Start of First Boot” message displays.

## Configure a DMM Appliance

Use the following checklist to set up a DMM appliance and configure its software:

✓	Task
<input type="checkbox"/>	<p>1. Set up the appliance hardware:</p> <ol style="list-style-type: none"> <li>Unpack the equipment from its container and verify that all components are present.</li> <li>Plug in the redundant power cables on the back of the appliance.</li> <li>Connect a live Ethernet cable to Port 1 on the back of the appliance.</li> <li>Connect a monitor to the VGA output on the back of the appliance.</li> <li>Connect a standard PS2 keyboard to the purple PS2 port in the back of the appliance.</li> <li>Power on the appliance.</li> </ol> <p>The “Start of First Boot” message displays.</p>
<input type="checkbox"/>	<p>2. At the “Start of First Boot” message, press <b>Enter</b>.</p>
<input type="checkbox"/>	<p>3. Specify the fully qualified, DNS-resolvable hostname for the Cisco DMM appliance, for example <code>server.example.com</code>. <b>Do not enter an IP address</b>. Choose <b>OK</b>.</p>
<input type="checkbox"/>	<p>4. Enter the following network information and then choose <b>OK</b>:</p> <ul style="list-style-type: none"> <li>The server IP address</li> <li>The subnet mask</li> <li>The default gateway IP address or DNS-resolvable hostname</li> <li>The primary DNS server IP address or DNS-resolvable hostname</li> <li>The secondary DNS server IP address or DNS-resolvable hostname</li> </ul>
<input type="checkbox"/>	<p>5. Confirm that you entered the correct network settings. If the settings are correct, choose <b>Yes</b>. If they are wrong, choose <b>No</b> to go back and correct them.</p>
<input type="checkbox"/>	<p>6. Configure settings for the appliance network interface card (NIC) by completing one of the following steps:</p> <ul style="list-style-type: none"> <li>If the NIC for your appliance should auto-negotiate the fastest possible transmission mode when it is connected to another device, choose <b>Yes</b>.</li> <li>If the NIC should not auto-negotiate, choose <b>No</b>, choose the NIC speed, choose <b>OK</b>, select the duplex method, choose <b>OK</b>, and then choose <b>Yes</b>.</li> </ul>
<input type="checkbox"/>	<p>7. Set the time zone settings, as follows:</p> <ol style="list-style-type: none"> <li>Use the <b>Up/Down</b> arrow keys to navigate through the Time Zone list.</li> <li>Stop when the correct time zone is displayed, and then choose <b>OK</b>.</li> </ol> <p>If the settings are correct, choose <b>Yes</b>. If they are wrong, choose <b>No</b> to go back and correct them.</p>

✓	Task
<input type="checkbox"/>	<p>8. Set the current month, year, and day, as follows:</p> <ol style="list-style-type: none"> <li>Use the <b>Tab</b> key and the <b>Up/Down</b> arrow keys to navigate and change the selected values.</li> <li>When you are done, choose <b>OK</b>.</li> </ol> <p>If the settings are correct, choose <b>Yes</b>. If they are wrong, choose <b>No</b> to go back and correct them.</p>
<input type="checkbox"/>	<p>9. Set the current hour, minute, and second. Use the 24 hour time format (24 hours that increment from 0100 to 2400).</p> <ol style="list-style-type: none"> <li>Use the <b>Tab</b> key and the <b>Up/Down</b> arrow keys to navigate and change the selected values.</li> <li>When you are done, choose <b>OK</b>.</li> </ol> <p>If the settings are correct, choose <b>Yes</b>. If they are wrong, choose <b>No</b> to go back and correct them.</p>
<input type="checkbox"/>	<p>10. Enter a password for the <i>admin</i> account, and choose <b>OK</b>. Re-enter the password and choose <b>OK</b> twice.</p> <p>This is the default account to use when you administer the appliance. The password that you enter must contain at least six characters.</p> <p><b>Tip</b> We recommend that you use a strong password. A strong password has at least eight characters and contains numbers, uppercase and lowercase letters, and symbols.</p>
<input type="checkbox"/>	<p>11. Enter a password for the <i>pwdadmin</i> account, and choose <b>OK</b>. Re-enter the password and choose <b>OK</b> twice.</p> <p><b>DO NOT LOSE THE PASSWORD FOR THIS ACCOUNT.</b> You cannot recover it if you do. This account is used to recover the admin and superuser account passwords and to access diagnostic tools when troubleshooting with Cisco support personnel.</p> <p>After a moment, the appliance reboots, and a login prompt appears.</p>
<input type="checkbox"/>	<p>12. Load the administrative interface for Cisco DMM in a web browser (<a href="http://&lt;DMM_server_name&gt;:8080/">http://&lt;DMM_server_name&gt;:8080/</a>). Use the Cisco DMM appliance fully qualified domain name that you configured in Step 3 for the server name.</p>
<input type="checkbox"/>	<p>13. Log into Cisco DMM by entering the following default username and password.</p> <ul style="list-style-type: none"> <li>Username: superuser</li> <li>Password: admin</li> </ul>
<input type="checkbox"/>	<p>14. Click <b>Accept</b> to agree to the terms of the End User License Agreement and then enter the following information for the superuser account:</p> <ul style="list-style-type: none"> <li>Email Address—Enter the e-mail address for the superuser account for system notifications.</li> <li>Password and Re-enter password—Enter and confirm a new password for the superuser account.</li> </ul> <p>Click <b>Save</b>. The license installation page displays.</p>
<input type="checkbox"/>	<p>15. Install the license keys to activate the DMM modules that you purchased, as follows.</p> <ol style="list-style-type: none"> <li>Click <b>Browse</b>, find and select the license file where you saved it, and then click <b>Open</b>.</li> <li>Click <b>Install License</b>. The DMM software features and modules that you purchased are now enabled.</li> </ol>

Setup and software configuration are now complete.





## CHAPTER 10

# Set Up and Configure a Cisco Show and Share Appliance

---

**Revised: November 4, 2011**

This chapter includes the following sections:

- [Set Up a Show and Share Appliance, page 10-1](#)
- [Configure a Show and Share Appliance, page 10-2](#)

## Set Up a Show and Share Appliance

### Before You Begin

- Ensure that a DNS entry has been created and published for the Show and Share appliance.
- Enable popup windows in your browser.
- Determine if your network uses dynamic (DHCP) or static IP addresses. If your network uses static IP addresses, obtain the following information:
  - Learn what IP address and subnet mask to assign to the Show and Share appliance.
  - Learn what IP addresses are assigned to the default network gateway, the primary DNS server, and the secondary DNS server.
- Configure your Cisco DMM Server.

### Procedure

---

- Step 1** Unpack the equipment from its container and verify that all components are present.
  - Step 2** Plug in the redundant power cables on the back of the appliance.
  - Step 3** Connect a live Ethernet cable to Port 1 on the back of the appliance.
  - Step 4** Connect a monitor to the VGA output on the back of the appliance.
  - Step 5** Connect a standard PS2 keyboard to the purple PS2 port in the back of the appliance.
  - Step 6** Power on the appliance.  
The “Start of First Boot” message displays.
-

# Configure a Show and Share Appliance

Use the following checklist to set up a Show and Share appliance and configure its software:

Your Show and Share installation will be complete after you complete the required steps to obtain a license and activate the Show and Share features.

✓	Task
☐	<p>1. Set up the appliance hardware:</p> <ol style="list-style-type: none"> <li>Unpack the equipment from its container and verify that all components are present.</li> <li>Plug in the redundant power cables on the back of the appliance.</li> <li>Connect a live Ethernet cable to Port 1 on the back of the appliance.</li> <li>Connect a monitor to the VGA output on the back of the appliance.</li> <li>Connect a standard PS2 keyboard to the purple PS2 port in the back of the appliance.</li> <li>Power on the appliance.</li> </ol> <p>The “Start of First Boot” message displays.</p>
☐	<p>2. At the “Start of First Boot” message, press <b>Enter</b>.</p>
☐	<p>3. Specify the fully qualified, DNS-resolvable hostname for the Cisco Show and Share appliance, for example: <code>server.example.com</code>. <b>Do not enter an IP address</b>. Choose <b>OK</b>.</p>
☐	<p>4. Enter the following network information and choose <b>OK</b>:</p> <ul style="list-style-type: none"> <li>The server IP address</li> <li>The subnet mask.</li> <li>The default gateway IP address or DNS-resolvable hostname</li> <li>The primary DNS server IP address or DNS-resolvable hostname</li> <li>The secondary DNS server IP address or DNS-resolvable hostname</li> </ul>
☐	<p>5. Confirm that you entered the correct network settings. If the settings are correct, choose <b>Yes</b>. If they are wrong, choose <b>No</b> to go back and correct them.</p>
☐	<p>6. Configure settings for the appliance network interface card (NIC) by completing one of the following steps:</p> <ul style="list-style-type: none"> <li>If the NIC for your appliance should auto-negotiate the fastest possible transmission mode when it is connected to another device, choose <b>Yes</b>.</li> <li>If the NIC should not auto-negotiate, choose <b>No</b>, select the NIC speed, choose <b>OK</b>, select the duplex method, choose <b>OK</b>, and then choose <b>Yes</b>.</li> </ul>
☐	<p>7. Set the time zone settings, as follows:</p> <ol style="list-style-type: none"> <li>Use the <b>Up/Down</b> arrow keys to navigate through the Time Zone list.</li> <li>Stop when the correct time zone is displayed, and then choose <b>OK</b>.</li> </ol> <p>If the settings are correct, choose <b>Yes</b>. If they are wrong, choose <b>No</b> to go back and correct them.</p>



✓	Task
<input type="checkbox"/>	<p>8. Set the current month, year, and day, as follows:</p> <ol style="list-style-type: none"> <li>Use the <b>Tab</b> key and the <b>Up/Down</b> arrow keys to navigate and change the selected values.</li> <li>When you are done, choose <b>OK</b>.</li> </ol> <p>If the settings are correct, choose <b>Yes</b>. If they are wrong, choose <b>No</b> to go back and correct them.</p>
<input type="checkbox"/>	<p>9. Set the current hour, minute, and second. Use 24-hour time format (24 hours that increment from 0100 to 2400).</p> <ol style="list-style-type: none"> <li>Use the <b>Tab</b> key and the <b>Up/Down</b> arrow keys to navigate and change the selected values.</li> <li>When you are done, choose <b>OK</b>.</li> </ol> <p>If the settings are correct, choose <b>Yes</b>. If they are wrong, choose <b>No</b> to go back and correct them.</p>
<input type="checkbox"/>	<p>10. Enter a password for the <i>admin</i> account, and choose <b>OK</b>. Re-enter the password and choose <b>OK</b> twice.</p> <p>This is the default account to use when you administer the appliance. The password that you enter must contain at least six characters.</p> <p><b>Tip</b> We recommend that you use a strong password. A strong password has at least eight characters and contains numbers, uppercase and lowercase letters, and symbols.</p>
<input type="checkbox"/>	<p>11. Enter a password for the <i>pwadmin</i> account, and choose <b>OK</b>. Re-enter the password and choose <b>OK</b> twice.</p> <p><b>DO NOT LOSE THE PASSWORD FOR THIS ACCOUNT.</b> You cannot recover it if you do. This account is used to recover the admin and superuser account passwords and to access diagnostic tools when troubleshooting with Cisco support personnel.</p> <p>After a moment, the appliance reboots, and a login prompt appears.</p>





## CHAPTER 11

# Pair the Cisco DMS Appliances

---

**Revised: November 4, 2011**

This chapter explains how you can use Appliance Administrative Interface (AAI) to pair a Cisco Show and Share appliance with a Cisco Digital Media Manager (DMM) appliance. You must pair your Cisco DMM appliance and your Cisco Show and Share appliance after initial configuration, after performing a software recovery on one or both appliances, or after changing the hostname of one or both appliances.

This chapter contains the following sections:

- [Avoid Pairing Failures, page 11-1](#)
- [Pair Your Appliances, page 11-2](#)

## Avoid Pairing Failures

To avoid pairing failures:

- Pairing fails when you complete these steps in the wrong order. You must use AAI on your Cisco Show and Share appliance **before** you use AAI on your Cisco DMM appliance. **Do not reverse this order or try to use AAI simultaneously on both appliances.**
- Do not use the **POP** option on the pairing menu. Doing so may cause Cisco Show and Share to fail. If you accidentally choose the POP option, you will need to re-pair the Cisco Show and Share and DMM appliances.

# Pair Your Appliances

## Procedure

---

- Step 1** From the appliance that runs Cisco Show and Share:
- Log in as **admin** to the Appliance Administration Interface (AAI).
  - Choose **APPLIANCE\_CONTROL > PAIR APPLIANCE**.
  - Choose **DMM**.



### Warning

---

**Do not choose any other option than DMM.**

---

- Enter the fully-qualified domain name (FQDN) for your Cisco DMM appliance.  
This is the DNS name. **Do not enter an IP address.**
- Press **Enter**.  
Your Cisco Show and Share appliance receives and successfully imports a digital certificate from your Cisco DMM appliance.

- Step 2** From the appliance that runs Cisco Digital Media Manager:

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Choose **APPLIANCE\_CONTROL > PAIR APPLIANCE**.
- Choose **SHOW\_AND\_SHARE**.



### Warning

---

**Do not choose any other option than SHOW\_AND\_SHARE.**

---

- Enter the fully-qualified domain name (FQDN) for your Cisco Show and Share appliance.  
This is the DNS name. **Do not enter an IP address.**
  - Press **Enter**.  
Your Cisco DMM appliance receives and successfully imports a digital certificate from your Cisco Show and Share appliance.
-