Administration Guide for Cisco Digital Media Suite 5.4.x Appliances

September 17, 2012

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

Administration Guide for Cisco Digital Media Suite 5.4.x Appliances

CONTENTS

CHAPTER 1

Introduction

Revised: September 17, 2012

Cisco Digital Media Suite is a product family that consists of Cisco Digital Media Manager (DMM) appliances, Cisco Digital Media Player (DMP) endpoints, associated software components, and hardware peripherals.

To set up and configure a DMM appliance, you must access some basic settings and controls through DMM and 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 back up or restore configurations.

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

Supported Appliances

This document describes how to set up and administer Cisco Digital Media Manager 5.4.x on a UCS C210 server (Cisco part number **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 *Release Notes for Cisco Digital Media Suite 5.4.x* on Cisco.com.
- To obtain documentation that you require for other Cisco DMS components, see *Guide to Documentation for Cisco Digital Media Suite* on Cisco.com.

Prepare to Set Up an Appliance

Complete these steps before you set up and configure an appliance.

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 5.4.x* on Cisco.com.

Step 3 Ensure that authorized users of your Cisco DMM appliance can send and receive packets through TCP ports 8080 and 8443.

Step 4 Ensure that a DNS entry has been created and published for your DMM appliance.

Step 5 Stop. You have completed this procedure.

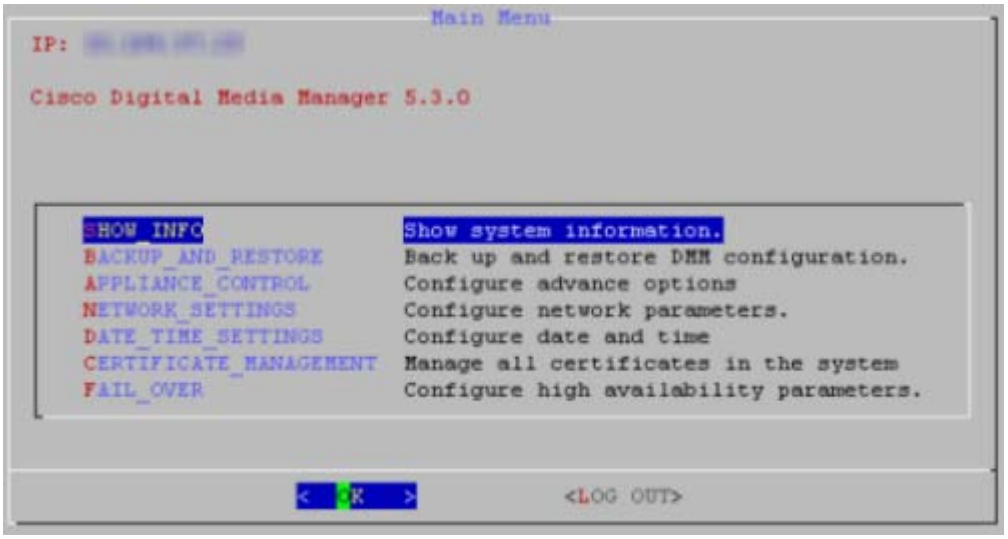
Access AAI

You can access AAI in two ways.

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

To start 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 and version appear above the menu.



Navigate in 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: September 17, 2012

This chapter explains how you can use AAI to administer a DMM appliance. It includes these sections.

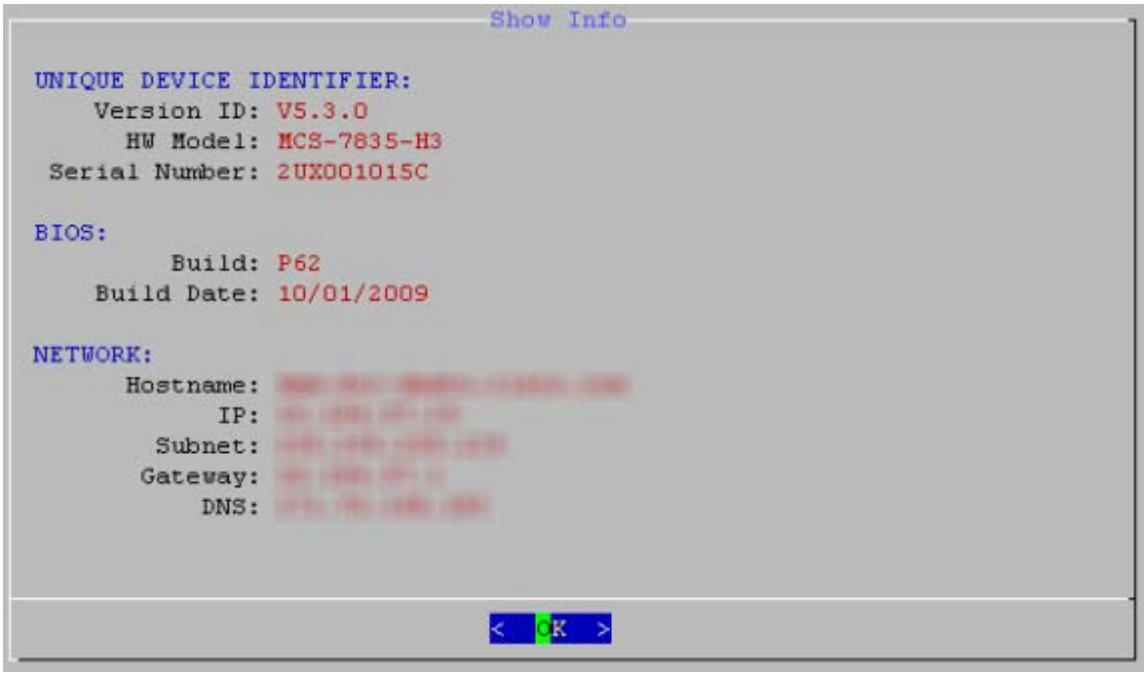
View Appliance System Information

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**.



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

Step 3 Stop. You have completed this procedure.

Manage System Log Information

This section contains these topics.

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.

Step 5 Stop. You have completed this procedure.

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.

Step 6 Stop. You have completed this procedure.

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 4-6.

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.

Step 9 Stop. You have completed this procedure.

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 states that all tomcat logs will be lost.

Step 5 Choose **Yes**.

It may take longer than 1 minute to complete the process. When the process is complete, you are returned to the main menu.

Step 6 Stop. You have completed this procedure.

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.

Step 4 Stop. You have completed this procedure.

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.

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 Stop. You have completed this procedure.

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 corresponding upgrade guide for your software release. Upgrade documentation contains 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:

a. Choose **CD_UPDATE** and press **Enter**.

b. Insert the CD-ROM and press **Enter**.

c. Follow the instructions on the screen.

Step 4 To update using a remote disc image (.iso file):

a. Choose **REMOTE_UPDATE** and press **Enter**.

b. 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**.

c. Follow the instructions on the screen.

Step 5 Stop. You have completed this procedure.

Restart the Appliance

You can reboot the appliance from AAI. 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.

Step 4 Stop. You have completed this procedure.

Restart the Web Services

You can restart the Tomcat web 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_WEB_SERVICES** and press **Enter** twice.

Step 4 Stop. You have completed this procedure.

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.

Step 4 Stop. You have completed this procedure.

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.

Step 3 Stop. You have completed this procedure.

CHAPTER 3

Back Up and Restore Appliance Configurations

Revised: September 17, 2012

This chapter explains how you can use AAI to back up a DMM appliance or restore from a previous backup. It includes these sections.

Guidelines and Limitations

- Media stored externally is not backed up.
- Back up and restore your entire system—DMM and your external hosting locations—at the same time to ensure that the restored data matches across all 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 5.4 software.
- Scheduled backup information is not retained in the backup file. When you restore your data you must reschedule any recurring backups.

Back Up Your Appliance

You can back up the appliance to a USB drive or to a remote rsync, SFTP, or FTP server. You have the option to back up the configuration only or back 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 these topics.

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 4-6.

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.

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.

a. Press **Tab** to highlight each field.

b. 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.

Step 15 Stop. You have completed this procedure.

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 3-6.

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 4-6.

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.

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.

Step 13 Stop. You have completed this procedure.

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 must clear the recurring backup configuration before you can schedule a one-time backup. See Cancel a Current or Scheduled Backup, page 3-6.

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.

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.

Step 10 Stop. You have completed this procedure.

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 these topics.

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 4-6.

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.

Step 10 Stop. You have completed this procedure.

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.

Step 10 Stop. You have completed this procedure.

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.

Step 5 Stop. You have completed this procedure.

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.

Step 4 Stop. You have completed this procedure.

CHAPTER 4

Change Appliance Network Settings

Revised: September 17, 2012

This chapter explains how you can use AAI to change the network settings or troubleshoot connectivity issues for a DMM appliance.

Note **We recommend that you do not change the static IP address that you assign to your DMM appliance.**

This chapter includes these sections.

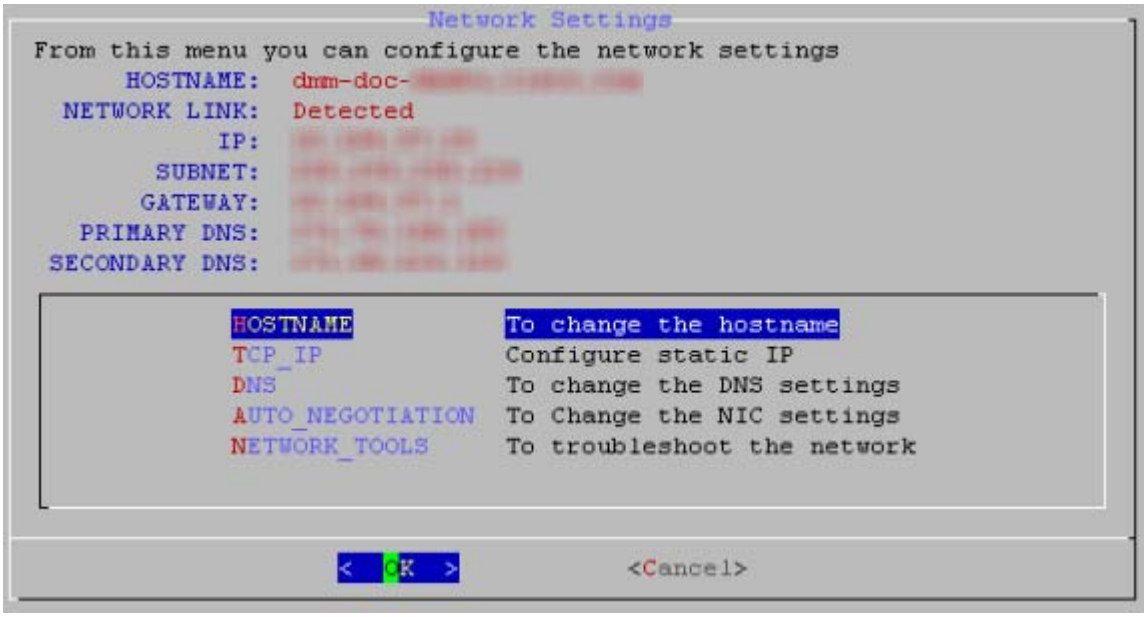
View Network Settings

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.



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

Step 3 Stop. You have completed this procedure.

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.

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. A message states when it is finished.

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

Step 6 Stop. You have completed this procedure.

Change the TCP/IP Settings

You can use AAI to change the IP address of your DMM appliance.

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.

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.

Step 7 Stop. You have completed this procedure.

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.

Step 7 Stop. You have completed this procedure.

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.

Step 4 Stop. You have completed this procedure.

Troubleshoot Network Issues

This section contains these topics.

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.

Step 5 Stop. You have completed this procedure.

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.

Step 5 Stop. You have completed this procedure.

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.

Step 6 Stop. You have completed this procedure.

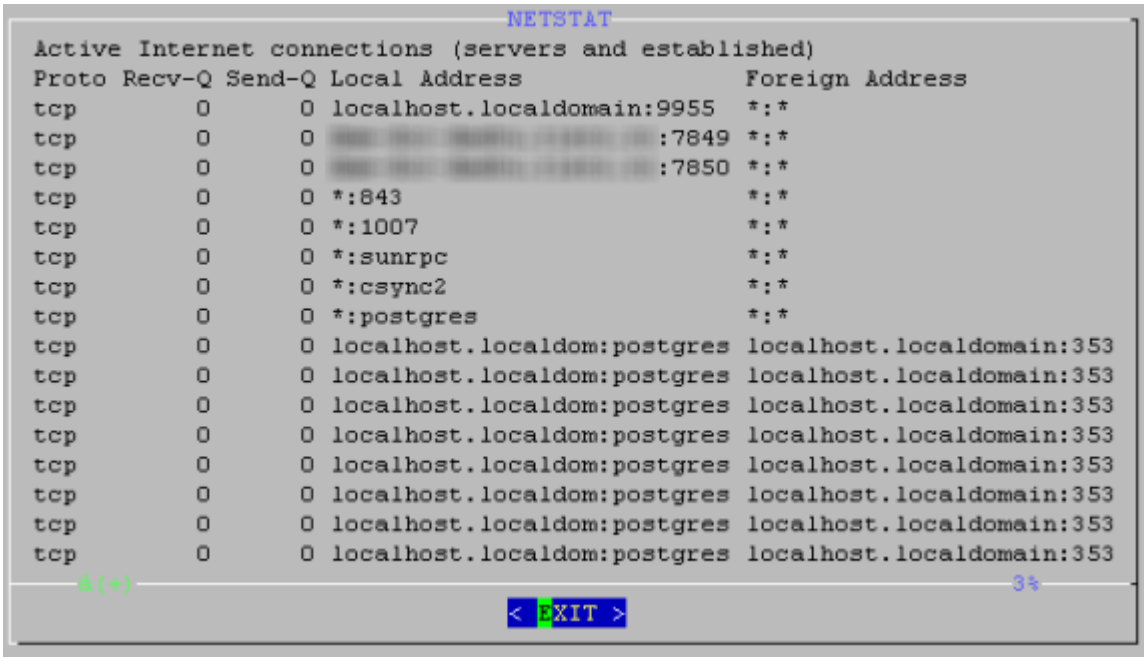
Use netstat to View Active Network Connections

Procedure

Step 1 Choose **NETWORK_SETTINGS** and press **Enter**.

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

Step 3 Choose **NETSTAT** and press **Enter**.



Step 4 Use the **UP/DOWN** arrows to scroll through the results.

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

Step 6 Stop. You have completed this procedure.

Use dig to Retrieve DNS Server Information

Domain information groper (dig) is a utility that queries DNS servers for their 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.

Step 6 Stop. You have completed this procedure.

Use nslookup to Retrieve DNS Server Information

nslookup is a utility that queries DNS servers for information about 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.

Step 6 Stop. You have completed this procedure.

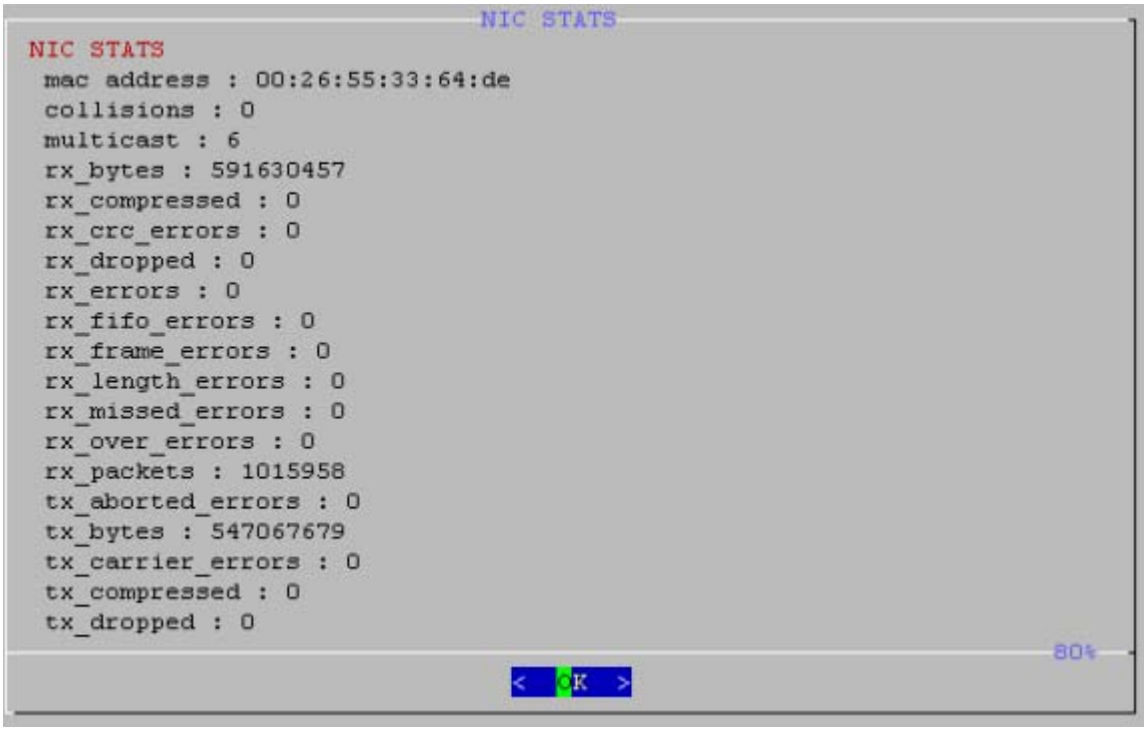
View Network Interface Traffic Statistics

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**.



Step 4 Use the **UP/DOWN** arrows to scroll through the results.

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

Step 6 Stop. You have completed this procedure.

CHAPTER 5

Configure System Time

Revised: September 17, 2012

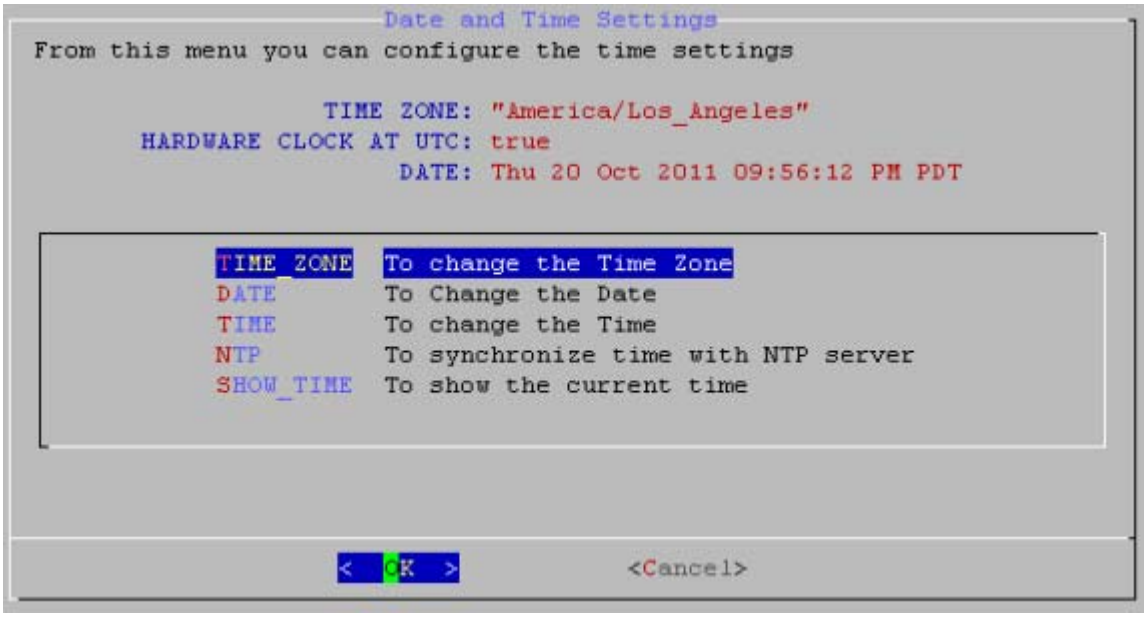
This chapter explains how to use AAI to configure the system time on a DMM appliance. This chapter includes these sections.

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.



Note The time does not update on this screen. To see the actual time, see Display the Current Time, page 5-7.

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

Step 3 Stop. You have completed this procedure.

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.

Step 6 Stop. You have completed this procedure.

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.

Step 8 Stop. You have completed this procedure.

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.

Step 8 Stop. You have completed this procedure.

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 5-4.

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.

Step 7 Stop. You have completed this procedure.

Use NTP to Provide System Time

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

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 5-7.

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 5-5.

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

Step 4 Stop. You have completed this procedure.

Specify NTP Servers

You can add up to three 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.

a. Use the **Up/Down** arrows to highlight the server field.

b. 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.

Step 7 Stop. You have completed this procedure.

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".

Step 6 Stop. You have completed this procedure.

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".

Step 6 Stop. You have completed this procedure.

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.

Step 6 Stop. You have completed this procedure.

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.

Step 5 Stop. You have completed this procedure.

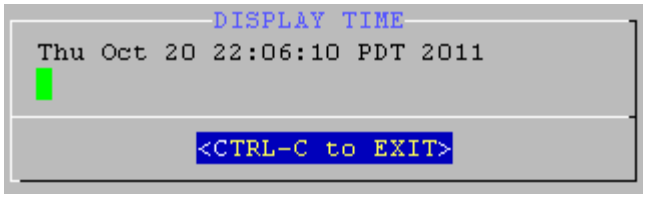
Display the Current Time

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.



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

Step 4 Stop. You have completed this procedure.

CHAPTER 6

Recover Passwords

Revised: September 17, 2012

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

Procedure

Step 1 Log in to AAI as **pwadmin**.

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 Stop. You have completed this procedure.

Change the PWADMIN Account Password

Procedure

Step 1 Log in to AAI as **pwadmin**.

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.

Step 6 Stop. You have completed this procedure.

Reset the Superuser Account Password

You cannot change the superuser account password from 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 in to AAI as **pwadmin**.

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.

Step 5 Stop. You have completed this procedure.

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: September 17, 2012

You can manage the digital certificates for a DMM appliance from its 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 import a certificate that includes an extra carriage return (**CSCth53389**).
- You can 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 DMM 5.4.x, go to Administration > Alerts > Notification Rules > Certificate is about to expire (**CSCth18904**).
- We support both the P7B and PEM certificate format.

Activation

We add and improve features often. This chapter describes options and features that do not necessarily exist in all 5.4.x releases. You must upgrade older software as needed before such enhancements can be available to you.

Concepts

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.

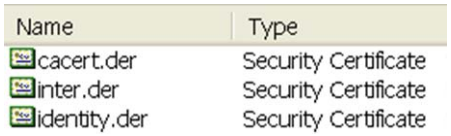
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwaDEXMBUGA1UEAxMOZHN5cy5jaXNjby5jb20xDzANBgNVBAsTBmp5Z2podjEO
MAwGA1UEChMFaGd1eWcxDzANBgNVBAcTBnV5dHlnajEOMAwGA1UECBMFbWhoanYxCzAJBgNVBAYT
AlVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlz+sEkBbIoXTiE13O28FX558enM0
6tVdnNlWmySbtKulYJ+xvHlsdzbCLOPYJhOvr1JJIxaNjf2dT1fdQp4Qd1U/lk5+v9Nmqtlr9Fxl
bUkxkCaYr6H4RYrmqi0+YpLyUgMXqoQ+vFRDdKUGHD5lxQK9dggXvdJQNgylGawXkqG8WepC3XwK
Zyl9CS2S4CbnLs6yHcz86/VE1X4+DqnS3yvfko+Yyg/yUe151Hcwp97C0KtFrZnQcnIDYU4rEaV+
nqKWc52cQ0kuoJjJlzNSlVUGLGA+yPf+fz+0K5liqA6HnE22yA7SWlskcR668JCR9tjqyWnIC+yu
Cd13HUfSpwIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAAVj0f6B6lmtVEvCaUxKAI7DDgFjBJhv
BRJMZA+3BVD6OOX8T2J8druEb18bloEX989f81124KceO8Y037/a4RPdxhXM3eeVYTMnz4QcbI6G
MU58jdHgRM1pxmYweixNTmzFTLc3uhp8JHWk286pHOMNHX2OR+cL+Cbj/mYRnmf4hg4LD0oCTS9f
pVEDgmiOpZ/go9OfAZ4nu1SwnqCaNpV+k/hM2RnlAqtaQDR89B4K18IF6odnjc9TL0kXUrsK79BD
Qp1bZQS+MElgnEqHpFjzvaopwXnZSv4CFHi6IwN2HPALY24Bo3XGW85j71HYPbwoVnZtcqdN56X6
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 either of our supported formats: PEM or P7B.



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

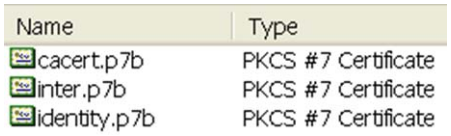
An exported KEYSTORE.DAT file from your Cisco *Show and Share* appliance (or, beginning with Cisco DMS 5.2.3, your DMM appliance) contains a backup copy of its digital certificates.

P

Return to Top

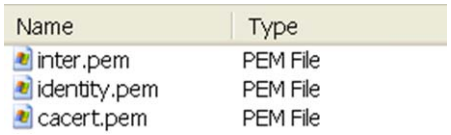
P7B

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.**



PEM

privacy enhanced email. An implementation of base64-encoded ASCII in X-509, used to protect identity certificates and CA certificates.



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

Encoding

We do not support DER encoding. Instead, you can use either of our supported formats: PEM or P7B.

Related Topics

- Verify If Your Certificate Format is PEM, page 7-8

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.

Concatenation

Caution **Do not combine multiple identity certificates together in one file that you will import to Cisco DMS.** Import will fail for merged 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 7-5*
- **Workflow B**—*Your Certificates Expire or You Do Not Have Any Certificates, page 7-5*
- **Workflow C**—*Back Up and Restore Certificates, page 7-5*

Workflow A

Obtain and Install Provider-signed Certificates

This sequence represents the typical workflow to use digital certificates from a trusted certification authority.

1. Generate and Submit Certificate Signing Requests (CSR), page 7-6
2. Import (Install) Provider-signed Certificates, page 7-9
3. View a Certificate Chain to Verify its Certificates, page 7-14
4. Export a Keystore to Back It Up, page 7-15

Workflow B

Your Certificates Expire or You Do Not Have Any Certificates

This sequence represents the typical workflow to use self-signed digital certificates.

1. Generate Self-signed Certificates, page 7-12
2. View a Certificate Chain to Verify its Certificates, page 7-14

Workflow C

Back Up and Restore Certificates

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 7-15
2. Import a Keystore to Restore It from a Backup, page 7-16
3. View a Certificate Chain to Verify its Certificates, page 7-14

Procedures

Generate and Submit Certificate Signing Requests (CSR)

Workflow Context

This topic is part of Workflow A.

Before You Begin

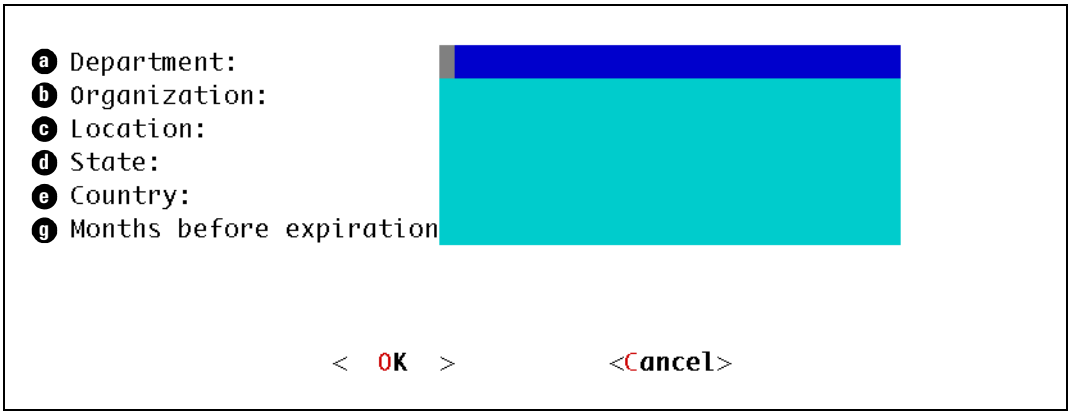
- Contact a certification authority to learn about its process to receive a request. Many CAs will expect to receive your request through their FTP or SFTP server. Although you can use any CA, these four are among the best known.
  - *VeriSign*—www.verisign.com
  - *GoDaddy*—www.godaddy.com
  - *Comodo*—www.comodo.com
  - *Network Solutions*—www.networksolutions.com
- Log in to AAI as **admin**.

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 7-16 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 or P7B encoding. Do not use DER.

- **Does the CA isolate each identity certificate?**

  We require that each imported identity certificate has its own, standalone file.

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

When 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 If Your Certificate Format is PEM" section on page 7-8.
- **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 7-9.

Verify If Your Certificate Format is PEM

You can use an ordinary text editor, such as Notepad on Windows or TextEdit on Mac, to confirm quickly if your certificates use PEM encoding.

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 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 7-9.

Import (Install) Provider-signed Certificates

Caution **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 to AAI as **admin**.
- 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.

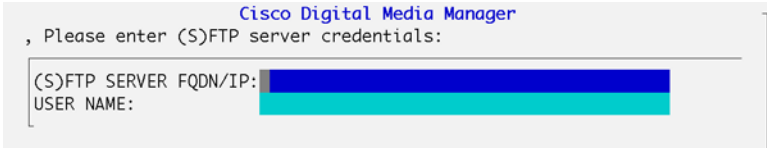
Step 3 Enter information about the FTP or SFTP server where you store your digital certificates.

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.

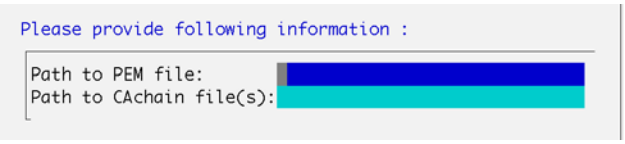
a. Use the first field to specify the path to one or more PEM files. If you will specify more than one file, comma-separate the filenames.

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

- **OPTIONAL**—*Would you like to verify any of your digital certificates?* Go to the "View Identity Certificates" section on page 7-13.

Related Topics

- Generate and Submit Certificate Signing Requests (CSR), page 7-6

Generate Self-signed Certificates

Workflow Context

This topic is part of Workflow B.

Before You Begin

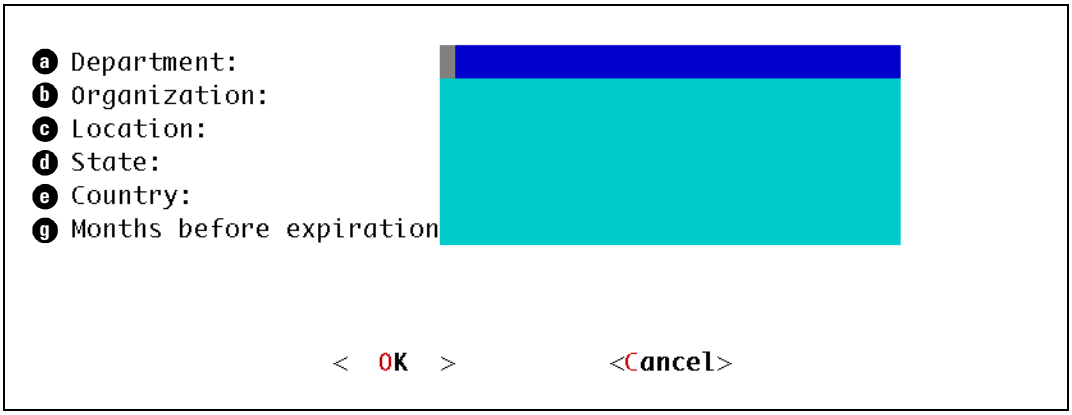
- Log in to AAI as **admin**.

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. 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 7-16 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

- **OPTIONAL**—*Would you like to verify any of your digital certificates?* Go to the "View Identity Certificates" section on page 7-13.

View Identity Certificates

Workflow Context

This topic is not part of any workflow.

Before You Begin

- Log in to AAI as **admin**.
- 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 7-15.

Related Topics

- Generate and Submit Certificate Signing Requests (CSR), page 7-6
- Import (Install) Provider-signed Certificates, page 7-9
- Generate Self-signed Certificates, page 7-12

View a Certificate Chain to Verify its Certificates

Workflow Context

This topic is part of Workflow A, Workflow B, and Workflow C.

Before You Begin

- Log in to AAI as **admin**.
- 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 7-15.

Related Topics

- Generate and Submit Certificate Signing Requests (CSR), page 7-6
- Import (Install) Provider-signed Certificates, page 7-9
- Generate Self-signed Certificates, page 7-12

Export a Keystore to Back It Up

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

Workflow Context

This topic is part of Workflow A and Workflow C.

Before You Begin

- Log in to AAI as **admin**.
- 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 7-16.

Related Topics

- Generate and Submit Certificate Signing Requests (CSR), page 7-6
- Import (Install) Provider-signed Certificates, page 7-9
- Generate Self-signed Certificates, page 7-12

Import a Keystore to Restore It from a Backup

Workflow Context

This topic is part of Workflow C.

Before You Begin

- Log in to AAI as **admin**.
- 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

- **OPTIONAL**—*Would you like to verify any of your digital certificates?* Go to the "View Identity Certificates" section on page 7-13.

Related Topics

- Export a Keystore to Back It Up, page 7-15

Reference

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
A	
AF	Afghanistan, Islamic State of
AX	Åland Islands *see also* Finland
AL	Albania
DZ	Algeria, Democratic Popular Republic of
AS	American Samoa, Territory of *see also* Guam, Territory of; Northern Mariana Islands, Commonwealth of the; Puerto Rico, Commonwealth of; Samoa, Independent State of; United States of America, Federal Union of the; and Virgin Islands, U.S. Territory of the
For *Andaman*, see India	
AD	Andorra, Principality of
AO	Angola
AI	Anguilla
AQ	Antarctica
AG	Antigua and Barbuda
For *Aosta Valley*, see Italy	
AR	Argentina
AM	Armenia
AW	Aruba
For *Ascension*, see Saint Helena, Ascension and Tristan da Cunha	
AC	Ascension Island *see also* Saint Helena, Ascension and Tristan da Cunha
For *Assam*, see India	
AU	Australia **Note All subdomains that previously used OZ as their country code top-level domain were transitioned to OZ.AU.**
AT	Austria
AZ	Azerbaijan

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

Code	Country or Region
B	
BS	Bahamas, Commonwealth of
BH	Bahrain, Emirate of
For *Bali*, see Indonesia	
BD	Bangladesh
For *Bangui*, see Central African Republic	
BB	Barbados
For *Barbuda*, see Antigua and Barbuda	
BY	Belarus
BE	Belgium, Kingdom of
BZ	Belize
For *Bengal*, see Bangladesh and India	
BJ	Benin
BM	Bermuda
BT	Bhutan, Kingdom of
For *Bodoland Territory*, see India	
BO	Bolivia
For *Bolzano-Bozen (Alto Adige-South Tyrol)*, see Austria; Germany, Federal Republic of; Hungary; and Italy	
For *Borneo*, see Indonesia	
BA	Bosnia and Herzegovina
BW	Botswana
For *Bougainville*, see Papua New Guinea, Independent State of	
BV	Bouvet Island, Territory of **Note Although the BV country code exists in *ISO-3166-1 alpha-2*, and exists as a country code top-level domain in DNS, it does not contain any subdomains.**
BR	Brazil, Federative Republic of
For *Britain*, see Ireland and United Kingdom of Great Britain and Northern Ireland	
IO	British Indian Ocean Territory
BN	Brunei Darussalam, Sultanate of
For *Brussels*, see Belgium, Kingdom of	
For *Buenos Aires*, see Argentina	
BG	Bulgaria
BF	Burkina Faso
For *Burma*, see Myanmar	
BI	Burundi

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

Code	Country or Region
C	
For *Caicos Islands*, see Turks and Caicos Islands, Territory of	
KH	Cambodia, Kingdom of
CM	Cameroon
CA	Canada
CV	Cape Verde
KY	Cayman Islands
CF	Central African Republic
For *Ceuta*, see Spain	
For *Ceylon*, see Sri Lanka	
TD	Chad
For *Chakma Autonomous District*, see India	
For *Channel Islands*, see Guernsey, Bailiwick of and Jersey, Bailiwick of	
For *Chiapas*, see Mexico	
CL	Chile
CN	China, People's Republic of *see also* Hong Kong; Macau, Special Administrative Region of; and Taiwan, Republic of China
CX	Christmas Island, Territory of
CC	Cocos (Keeling) Islands
CO	Colombia
KM	Comoros
CG	Congo *see also* Congo, the Democratic Republic of the
CD	Congo, the Democratic Republic of the *see also* Congo
CK	Cook Islands
For *Corsica, Territorial Collectivity of*, see France, Metropolitan	
CR	Costa Rica
CI	Cote d'Ivoire
HR	Croatia
CU	Cuba
CY	Cyprus
For *Czechoslovalia*, see Czech Republic	
CZ	Czech Republic *see also* Slovakia

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

Code	Country or Region
D	
	For *Darjeeling Gorkha Hills*, see India
DK	Denmark, Kingdom of *see also* Faroe Islands and Greenland
DJ	Djibouti
DM	Dominica, Commonwealth of *see also* Dominican Republic
DO	Dominican Republic *see also* Dominica, Commonwealth of
E	
	For *East Bengal*, see Bangladesh and Pakistan, Islamic Republic of
	For *East Indies*, see Indonesia; Malaysia, Kingdom of; Philippines; and Solomon Islands
	For *East Timor*, see Timor-Leste
EC	Ecuador
EG	Egypt, Arab Republic of
SV	El Salvador
GQ	Equatorial Guinea
	For *Ghana*, see Ghana
	For *Guiana*, see French Guiana, Overseas Department of
	For *Guinea*, see Guinea
	For *Guyana*, see Guyana, Cooperative Republic of
ER	Eritrea
EE	Estonia
ET	Ethiopia, Federal Democratic Republic of
EU	European Union
F	
FK	Falkland Islands (Malvinas Islas), Colony of
FO	Faroe Islands
FJ	Fiji
FI	Finland *see also* Åland Islands
FR	France
FX	France, Metropolitan

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

Code	Country or Region
GF	French Guiana, Overseas Department of
	For *Equatorial Guinea*, see Equatorial Guinea
	For *Ghana*, see Ghana
	For *Guinea*, see Guinea
	For *Guyana*, see Guyana, Cooperative Republic of
PF	French Polynesia, Overseas Territory of
TF	French Southern Territories
	For *Friuli-Venezia Giula*, see Croatia; Italy; and Slovenia
G	
GA	Gabon
GM	Gambia
	For *Garo Hills Autonomous District*, see India
GE	Georgia *see also* South Georgia and the South Sandwich Islands
DE	Germany, Federal Republic of
GH	Ghana
	For *Equatorial Guinea*, see Equatorial Guinea
	For *Guiana*, see French Guiana, Overseas Department of
	For *Guinea*, see Guinea
	For *Guyana*, see Guyana, Cooperative Republic of
GI	Gibraltar
	For *Gilbert Islands*, see Kiribati
	For *Great Britain*, see United Kingdom of Great Britain and Northern Ireland
GR	Greece
GL	Greenland *see also* Denmark, Kingdom of and Faroe Islands
GD	Grenada *see also* Saint Vincent and the Grenadines
	For *Grenadines*, see Saint Vincent and the Grenadines
GP	Guadeloupe and Dependencies, Overseas Department of
GU	Guam, Territory of *see also* American Samoa, Territory of; Northern Mariana Islands, Commonwealth of the; Puerto Rico, Commonwealth of; United States of America, Federal Union of the; and Virgin Islands, U.S. Territory of the
	For *Guangxi Zhung Autonomous Region*, see China, People's Republic of
GT	Guatemala

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

Code	Country or Region
GG	Guernsey, Bailiwick of *see also* Jersey, Bailiwick of
For *Guiana*, see French Guiana, Overseas Department of	
GN	Guinea *see also* Guinea-Bissau
GW	Guinea-Bissau *see also* Guinea
GY	Guyana, Cooperative Republic of
For *Equatorial Guinea*, see Equatorial Guinea For *Ghana*, see Ghana For *Guiana*, see French Guiana, Overseas Department of For *Guinea*, see Guinea	
H	
HT	Haiti
HM	Heard and McDonald Islands, Territory of
For *Herzegovina*, see Bosnia and Herzegovina	
VA	Holy See, State of Vatican City *see also* Italy
HN	Honduras
HK	Hong Kong *see also* China, People's Republic of; Macau, Special Administrative Region of; and Taiwan, Republic of China
HU	Hungary
I	
IS	Iceland
IN	India
ID	Indonesia
For *Inner Mongolia Autonomous Region*, see China, People's Republic of	
IR	Iran, Islamic Republic of
IQ	Iraq
For *Iraqi Kurdistan*, see Iraq	
IE	Ireland
IM	Isle of Man, Territory of
IL	Israel, State of *see also* Palestine, Occupied Territory of

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

Code	Country or Region
IT	Italy *see also* Holy See, State of Vatican City
For *Ivory Coast*, see Cote d'Ivoire	
J	
For *Jaintia Hills Autonomous District*, see India	
JM	Jamaica
For *Jammu*, see India	
For *Jan Mayen*, see Svalbard and Jan Mayen Islands, Territory of	
JP	Japan, Imperial State of
For *Java*, see Indonesia	
For *Jeju-do*, see Korea, Republic of	
JE	Jersey, Bailiwick of *see also* Guernsey, Bailiwick of
For *Jewish Autonomous Oblast*, see Russia, Federation of	
JO	Jordan, Hashemite Kingdom of
K	
For *Kampuchea*, see Cambodia, Kingdom of	
For *Karbi Anglong Autonomous Council*, see India	
For *Kashmir*, see China, People's Republic of; India; and Pakistan, Islamic Republic of	
KZ	Kazakhstan
For *Keeling Islands*, see Cocos (Keeling) Islands	
KE	Kenya
For *Khasi Hills Autonomous District*, see India	
KI	Kiribati *see also* Marshall Islands; Micronesia, Federated States of; and Nauru
KP	Korea, Democratic People's Republic of *see also* Korea, Republic of
KR	Korea, Republic of *see also* Korea, Democratic People's Republic of
For *Kosovo*, see Serbia	
For *Kurdistan*, see Armenia; Iran, Islamic Republic of; Iraq; Syria, Arab Republic of; and Turkey	
KW	Kuwait, Emirate of
KG	Kyrgyzstan
L	

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

Code	Country or Region
	For *Ladakh Autonomous Hill Development*, see India
	For *Lai Autonomous District*, see India
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 *Luzon*, see Philippines
M	
MO	Macau, Special Administrative Region of *see also* China, People's Republic of; Hong Kong; and Taiwan, Republic of China
MK	Macedonia, the former Yugoslav Republic of
MG	Madagascar
	For *Madeira*, see Portugal
MW	Malawi
	For *Malay Archipelago*, see Malaysia, Kingdom of and Philippines
	For *Malay Peninsula*, see Malaysia, Kingdom of; Myanmar; Philippines; Singapore; and Thailand, Kingdom of
MY	Malaysia, Kingdom of *see also* Singapore
MV	Maldives
ML	Mali
MT	Malta
	For *Malvinas*, see Falkland Islands (Malvinas Islas), Colony of
	For *Mara Autonomous District*, see India
MH	Marshall Islands *see also* Kiribati and Micronesia, Federated States of
	For *Mariana Islands*, see Northern Mariana Islands, Commonwealth of the
MQ	Martinique, Overseas Department of the
MR	Mauritania, Islamic Republic of *see also* Mauritius

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

Code	Country or Region
MU	Mauritius *see also* Mauritania, Islamic Republic of
YT	Mayotte, Territorial Collectivity of
For *McDonald Islands*, see Heard and McDonald Islands, Territory of	
For *Meghalaya*, see India	
For *Melilla*, see Spain	
MX	Mexico
FM	Micronesia, Federated States of *see also* Kiribati; Marshall Islands; and Northern Mariana Islands, Commonwealth of the
For *Mindanao*, see Philippines	
For *Miquelon*, see Saint Pierre and Miquelon, Overseas Territorial Collectivity of	
For *Mizoram*, see India	
For *Moldavia*, see Moldova, Republic of	
MD	Moldova, Republic of
MC	Monaco, Principality of
MN	Mongolia
ME	Montenegro
MS	Montserrat, Territory of
MA	Morocco, Kingdom of
For *Mount Athos*, see Greece	
MZ	Mozambique
MM	Myanmar
N	
NA	Namibia *see also* South Africa
NR	Nauru *see also* Kiribati; Marshall Islands; and Micronesia, Federated States of
NP	Nepal, Kingdom of
NL	Netherlands, Kingdom of the *see also* Netherlands Antilles
AN	Netherlands Antilles *see also* Netherlands, Kingdom of the
For *Nevis*, see Saint Kitts and Nevis	
NC	New Caledonia and Dependencies, Overseas Territory of
For *New Guinea*, see Papua New Guinea, Independent State of	

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

Code	Country or Region
	For *New Hebrides*, see Vanuatu
NZ	New Zealand *see also* Cook Islands; Niue; and Tokelau
NI	Nicaragua
	For *Nicobar Islands*, see India
NE	Niger *see also* Nigeria, Federal Republic of
NG	Nigeria, Federal Republic of *see also* Niger
	For *Ningxia Hui Autonomous Region*, see China, People's Republic of
NU	Niue *see also* Cook Islands; New Zealand; and Tokelau
NF	Norfolk Island, Territory of
	For *North Cachar Hills Autonomous District*, see India
	For *North Korea*, see Korea, Democratic People's Republic of
	For *North Sentinel Island*, see India
MP	Northern Mariana Islands, Commonwealth of the *see also* American Samoa, Territory of, Guam, Territory of, Puerto Rico, Commonwealth of, United States of America, Federal Union of the, and Virgin Islands, U.S. Territory of the
NO	Norway, Kingdom of
O	
OM	Oman, Sultanate of
P	
PK	Pakistan, Islamic Republic of
PW	Palau
PS	Palestine, Occupied Territory of *see also* Israel, State of
PA	Panama, Unified Republic of
PG	Papua New Guinea, Independent State of
PC	Paracel Islands, Territory of
PY	Paraguay
	For *Peninsular Malaysia*, see Malaysia, Kingdom of
PE	Peru
PH	Philippines
PN	Pitcairn

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

Code	Country or Region
PL	Poland
	For *Polynesia*, see French Polynesia, Overseas Territory of
PT	Portugal
TP	*Portuguese Timor* (being phased out)
	For *Principe*, see Sao Tome and Principe
PR	Puerto Rico, Commonwealth of *see also* American Samoa, Territory of, Guam, Territory of, Northern Mariana Islands, Commonwealth of the, United States of America, Federal Union of the, and Virgin Islands, U.S. Territory of the
Q	
QA	Qatar, Emirate of
R	
RE	Reunion, Overseas Department of the
	For *Rhodesia*, see Zambia and Zimbabwe
	For *Rodrigues*, see Mauritius
RO	Romania
RU	Russia, Federation of
RW	Rwanda
S	
	For *Sahara*, see Western Sahara
BL	Saint Barthelemy **Note** Although the BL country code exists in *ISO-3166-1 alpha-2*, 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 *see also* Ascension Island
KN	Saint Kitts and Nevis
LC	Saint Lucia
MF	Saint Martin **Note** Although the MF country code exists in *ISO-3166-1 alpha-2*, 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 *see also* Grenada
WS	Samoa, Independent State of *see also* American Samoa, Territory of

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

Code	Country or Region
SM	San Marino
For *Sandwich Islands*, see South Georgia and the South Sandwich Islands	
ST	Sao Tome and Principe
For *Sardinia*, see Italy	
SA	Saudi Arabia, Kingdom of
For *Scotland*, see United Kingdom of Great Britain and Northern Ireland	
SN	Senegal
RS	Serbia
SC	Seychelles
For *Siam*, see Thailand, Kingdom of	
For *Sicily*, see Italy	
SL	Sierra Leone
SG	Singapore *see also* Malaysia, Kingdom of
SK	Slovakia *see also* Czech Republic
SI	Slovenia *see also* Macedonia, the former Yugoslav Republic of
SB	Solomon Islands
SO	Somalia
ZA	South Africa *see also* Namibia
GS	South Georgia and the South Sandwich Islands
For *South Korea*, see Korea, Republic of	
For *South Sandwich Islands*, see South Georgia and the South Sandwich Islands	
For *South Yemen*, see Yemen	
For *Southern Sudan*, see Sudan	
SU	Soviet Union (being phased out)
ES	Spain
LK	Sri Lanka
SD	Sudan
For *Sulawesi*, see Indonesia	
For *Sumatra*, see Indonesia	
SR	Suriname

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

Code	Country or Region
SJ	Svalbard and Jan Mayen Islands, Territory of **Note** **Although the SJ country code exists in *ISO-3166-1 alpha-2*, 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
T	
TW	Taiwan, Republic of China *see also* China, People's Republic of, Hong Kong, and Macau, Special Administrative Region of
TJ	Tajikistan
For *Tanganyika*, see Tanzania, United Republic of	
TZ	Tanzania, United Republic of
For *Tashkent*, see Uzbekistan	
TH	Thailand, Kingdom of
For *Tibet Autonomous Region*, see China, People's Republic of	
TL	Timor-Leste
For *Tobago*, see Trinidad and Tobago	
TG	Togo
TK	Tokelau *see also* Cook Islands; New Zealand; and Niue
TO	Tonga, Kingdom of
For *Trento (Trentino)*, see Austria; Germany, Federal Republic of; Hungary; and Italy	
TT	Trinidad and Tobago
For *Tripura Tribal Areas Autonomous District*, see India	
For *Tristan da Cunha*, see Saint Helena, Ascension and Tristan da Cunha	
TN	Tunisia
TR	Turkey
TM	Turkmenistan
TC	Turks and Caicos Islands, Territory of
TV	Tuvalu
U	
UG	Uganda
UA	Ukraine

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

Code	Country or Region
AE	United Arab Emirates
GB	United Kingdom of Great Britain and Northern Ireland
UK	**Note** **Although the GB region code exists in *ISO-3166-1 alpha-2*, 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 *ISO 3166-1 alpha-2*.
US	United States of America, Federal Union of the *see also* American Samoa, Territory of, Guam, Territory of, Northern Mariana Islands, Commonwealth of the, Puerto Rico, Commonwealth of, and Virgin Islands, U.S. Territory of the
UM	United States Minor Outlying Islands **Note** **Although the UM country code top-level domain was deactivated, it is still available with restrictions.**
UY	Uruguay
UZ	Uzbekistan
V	
VU	Vanuatu
For *Vatican*, see Holy See, State of Vatican City	
VE	Venezuela, Bolivarian Republic of
VN	Viet Nam, Socialist Republic of
VG	Virgin Islands, British Territory of the
VI	Virgin Islands, U.S. Territory of the *see also* American Samoa, Territory of, Guam, Territory of, Northern Mariana Islands, Commonwealth of the, Puerto Rico, Commonwealth of, and United States of America, Federal Union of the
For *Visayas*, see Philippines	
For *Vojvodina*, see Serbia	
For *Volta*, see Burkina Faso	
W	
For *Wales*, see United Kingdom of Great Britain and Northern Ireland	
WF	Wallis and Futuna Islands, Overseas Territory of
For *West Bengal*, see Bangladesh and India	
EH	Western Sahara **Note** **Although the EH country code exists in *ISO-3166-1 alpha-2*, it does not exist as a country code top-level domain in DNS.**
X	
For *Xinjiang Uyghur Autonomous Region*, see China, People's Republic of	

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

Code	Country or Region
Y	
YE	Yemen
YU	Yugoslavia, Federation of **Note** **Most, if not all, sites that used the YU country code top-level domain have been reassigned to Serbia or Montenegro.**
	For *Yugoslav Republic*, see Bosnia and Herzegovina; Croatia; Macedonia, the former Yugoslav Republic of; Montenegro; Serbia; Slovenia; and Yugoslavia, Federation of
Z	
	For *Zaire*, see Congo, the Democratic Republic of the
ZM	Zambia
	For *Zanzibar*, see Tanzania, United Republic of
	For *Zelaya*, see Nicaragua
ZW	Zimbabwe

FAQs and Troubleshooting

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

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: September 17, 2012,

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 *Failover Configuration Guide for Cisco Digital Media Suite 5.4.x*:

http://cisco.com/en/US/docs/video/digital_media_systems/5_x/5_4/dms/failover_guide/dmsfailover.html

CHAPTER 9

Set Up and Configure a DMM Appliance

Revised: November 4, 2011

This chapter includes the following sections:

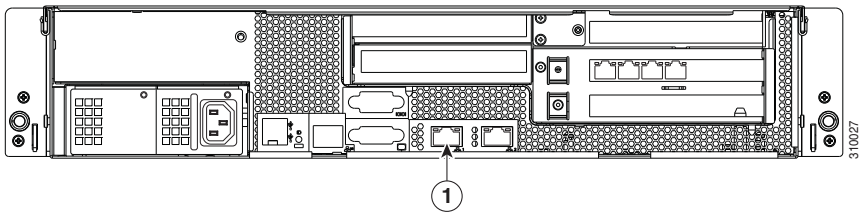
Set Up and Configure a DMM Appliance

Use the checklist in this section to set up a DMM 5.4 appliance and configure its software:

Before You Begin

- Obtain the IP address and subnet mask to assign to your DMM appliance.
- Obtain the IP addresses of the default network gateway, the primary DNS server, and the secondary DNS server.
- 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 appliance. For information about obtaining license keys, see the Licenses chapter of *User Guide for Cisco Digital Media Manager 5.4.x* on Cisco.com.
- Verify that at least one computer on your network is configured for access to other networked devices through TCP ports 8080 and 8443.
- Enable popup windows in your browser if they are disabled. You can complete the checklist only when popup windows are enabled.

Procedure

✓	Task	Steps
❑	**1.** Set up the server.	**a.** Unpack the equipment from its container and verify that all components are present. **b.** Plug in the redundant power cords. **c.** Connect an Ethernet cable to you network and to the appliance. (The number 1 in this illustration indicates which physical interface on a DMM appliance should connect to your network.)  **d.** Connect a monitor to the VGA output on the back of the appliance. **e.** Connect a standard PS2 keyboard to the purple PS2 port on the back of the appliance. **f.** Power On the appliance. **g.** Press **Enter** at the "Start of First Boot" message.
❑	**2.** Specify the fully qualified, DNS-resolvable hostname for your DMM appliance.	For example, you might enter `server.example.com`. **Note** **This field requires an FQDN.** Do not enter an IP address. Then, choose **OK**.
❑	**3.** Supply the required network information.	**a.** As prompted, enter: • The server IP address • The subnet mask • The default gateway IP address or DNS-resolvable hostname • The primary DNS server IP address or DNS-resolvable hostname • The secondary DNS server IP address or DNS-resolvable hostname **b.** Then, choose **OK**.
❑	**4.** Confirm that you entered the correct network settings.	*Are the settings correct?* **a.** Choose **Yes** or **No**. Then, if you chose No, go back and correct any errors.

✓	Task	Steps
❑	**5.** Configure settings for the appliance network interface card (NIC).	*Should the NIC auto-negotiate the fastest possible transmission mode when it is connected to another device?* • Choose **Yes** or **No**. Then, if you chose No: **a.** Choose the NIC speed and choose **OK**. **b.** Select the duplex method and choose **OK**. **c.** Choose **Yes**.
❑	**6.** Set the time zone settings.	**a.** Use the **Up/Down** arrow keys to navigate through the Time Zone list. **b.** Stop when the correct time zone is displayed. Then, choose **OK**. *Are the settings correct?* **c.** Choose **Yes** or **No**. Then, if you chose No, go back and correct any errors.
❑	**7.** Set the current month, year, and day.	**a.** Use the **Tab** key and the **Up/Down** arrow keys to navigate and change the selected values. **b.** When you are done, choose **OK**. *Are the settings correct?* **c.** Choose **Yes** or **No**. Then, if you chose No, go back and correct any errors.
❑	**8.** Set the current hour, minute, and second.	Use the 24 hour time format (24 hours that increment from 0100 to 2400). **a.** Use the **Tab** key and the **Up/Down** arrow keys to navigate and change the selected values. **b.** When you are done, choose **OK**. *Are the settings correct?* **c.** Choose **Yes** or **No**. Then, if you chose No, go back and correct any errors.
❑	**9.** Set the administrator password for *Appliance Administration Interface* (AAI), a command console for your DMM server.	**a.** Enter a password for the *admin* account. Then, choose **OK**. **b.** Re-enter the password. Then, choose **OK** twice. **Note** **This is the default account to use AAI.** These are not the credentials to open DMM in your browser. **Tip** **Your password must contain at least six characters.** However, we recommend that you use at least eight characters, including numbers and a mixture of uppercase and lowercase letters from the Latin-1 character set.

✓	Task	Steps
❑	**10.** Set the recovery password.	**a.** Enter a password for the *pwadmin* account. Then, choose **OK**. **b.** Re-enter the password. Then, choose **OK** twice. **Note** **DO NOT LOSE THE *pwadmin* PASSWORD.** You cannot recover it if you do. This account is used to recover the admin and superuser account passwords and to run diagnostic tools when troubleshooting with Cisco technical support engineers. The appliance reboots.
❑	**11.** Log in to Cisco DMM.	**Tip** **Use the server FQDN that you configured in Step 2.** **a.** Go to https://<*DMM_FQDN*>:8443/. **b.** Log in with these credentials: • Username: **superuser** • Password: **admin** (This password is valid only once. You change it immediately.) **c.** Click **Accept** to agree to the the End User License Agreement.
❑	**12.** Configure the superuser account.	**a.** Specify which carefully monitored email address should receive all DMM system notification messages and all “contact your administrator” messages from DMM users who cannot log in. **b.** Enter and confirm your NEW password for the superuser account. **c.** Click **Save**. The license installation page opens.
❑	**13.** Install the license keys to activate your purchased Cisco DMS features.	**a.** Click **Browse**. **b.** Find and choose the license file where you saved it. **c.** Click **Open**. **d.** Click **Install License**. The features and modules that you purchased are now enabled.

Setup and software configuration are now complete.